TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
SİBER GÜVENLİK BAŞKANLIĞI

BİLGİ ve İLETİŞİM GÜVENLİĞİ REHBERİ

MART 2026

BELGE ADI: Bilgi ve İletişim Güvenliği Rehberi

SÜRÜM NO: 1.1

SÜRÜM TARİHİ: 01.03.2026

GİZLİLİK DERECESİ: Tasnif Dışı

Değişiklik No	Değişiklik Tarihi	Değişiklik Nedeni
1.0	Temmuz 2020	İlk Yayın
1.1	Mart 2026	Mülga olan Dijital Dönüşüm Ofisi'nin yetkilerinin Siber Güvenlik Başkanlığı'na devredilmesi nedeniyle doküman üzerinde tasarımsal ve kurumsal değişiklikler yapılmıştır.

https://www.siberguvenlik.gov.tr

Bilgi ve İletişim Güvenliği Rehberi hakkındaki

görüş ve öneriler aşağıda yer alan elektronik posta adresine iletilebilir.

Elektronik Posta: bgrehber@siberguvenlik.gov.tr

Bilgi ve İletişim Güvenliği Rehberi, Creative Commons Atıf 4.0
Uluslararası lisansı ile lisanslanmıştır.

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
SİBER GÜVENLİK BAŞKANLIĞI

BİLGİ ve İLETİŞİM GÜVENLİĞİ REHBERİ

MART 2026

İÇİNDEKİLER

ŞEKİLLER

TABLOLAR

KISALTMALAR

Kısaltma	Açıklama
API	Application Programming Interface / Uygulama Programlama Arayüzü
ASLR	Address Space Layout Randomization / Adres Alanı Düzeni Rastgele Seçimi
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BT	Bilgi Teknolojisi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart / İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Test
COMSEC	Communication Security / Haberleşme Güvenliği
CORS	Cross-Origin Resource Sharing / Kökler Arası Kaynak Paylaşımı
CSRF	Cross-Site Request Forgery / Siteler Arası İstek Sahteciliği
DEP	Data Execution Prevention / Veri Yürütme Engellemesi
DHCP	Dynamic Host Configuration Protocol / Dinamik Bilgisayar Yapılandırma Protokolü
DKIM	Domain Keys Identified Mail / Alan Adı Anahtarıyla Tanımlanmış E-Posta
DMZ	Demilitarized Zone / Sivil Bölge
DNS	Domain Name System / Alan Adı Sistemi
DoS	Denial of Service / Hizmet Engelleme
DDoS	Distributed Denial of Service / Dağıtık Hizmet Engelleme
EAP	Extensible Authentication Protocol / Genişletilebilir Kimlik Doğrulama Protokolü
EBYS	Elektronik Belge Yönetim Sistemi
EKS	Endüstriyel Kontrol Sistemi
EPDK	Enerji Piyasası Düzenleme Kurumu
FTP	File Transfer Protocol / Dosya Transfer Protokolü
G2B	Government to Business / Devletten Kuruma
G2G	Government to Government / Devletten Devlete
GPS	Global Positioning System / Küresel Konumlama Sistemi
HDD	Hard Disk Drive / Sabit Disk Sürücüsü
HIDS	Host Intrusion Detection System / Bilgisayar Tabanlı Saldırı Tespit Sistemi
HIPS	Host Intrusion Prevention System / Bilgisayar Tabanlı Saldırı Önleme Sistemi
HMI	Human Machine Interface / Makine ile İnsan Arasında Bilgi Aktarımı Sağlayan Arayüz
HSTS	HTTP Strict Transport Security / HTTP Sıkı Aktarım Güvenliği
HSM	Hardware Security Module / Donanımsal Güvenlik Modülü
HTML	Hypertext Markup Language / Standart Metin İşaretleme Dili
HTTP	Hypertext Transfer Protocol / Bağlantılı Metin Aktarım Protokolü
HTTPS	Hypertext Transfer Protocol Secure / Güvenli Bağlantılı Metin Aktarım Protokolü
IEC	International Electrotechnical Commission / Uluslararası Elektroteknik Komisyonu
IED	Intelligent Electronic Device / Akıllı Elektronik Cihaz
IMAPs	Internet Message Access Protocol Secure / Güvenli İnternet Mesaj Erişim Protokolü
IoT	Internet of Things / Nesnelerin İnterneti
IP	Internet Protocol / İnternet Protokolü
IPS	Intrusion Prevention System / Saldırı Önleme Sistemi
IPSec	IP Security / İnternet Protokolü Güvenliği
ISO	International Organization for Standardization / Uluslararası Standartlar Örgütü
LAN	Local Area Network / Yerel Ağ Bağlantısı
LDAP	Lightweight Directory Access Protocol / Hafif Dizin Erişim Protokolü
LUN	Logical Unit Number / Mantıksal Birim Numarası
MAC	Media Access Control Address / Ortam Erişim Kontrol Adresi
MMS	Manufacturing Message Specification / Üretim Mesaj Spesifikasyonu

Kısaltma	Açıklama
NAC	Network Access Control / Ağ Erişim Kontrolü
NES	Nitelikli Elektronik Sertifika
NFC	Near Field Communication / Yakın Alan İletişimi
NTP	Network Time Protocol / Ağ Zaman Protokolü
OCSP	Online Certificate Status Protocol / Çevrimiçi Sertifika Durum Protokolü
OT	Operasyonel Teknolojiler
PCMCIA	Personal Computer Memory Card International Association / Kişisel Bilgisayar Bellek Kartı Uluslararası Birliği
PLC	Programmable Logic Controller / Programlanabilir Mantıksal Denetleyici
PoC	Proof of Concept / Demo ve Kavram İspatı
POP3	Post Office Protocol / Posta İleti Protokolü
PRNG	Pseudo Random Numerator Generator / Varsayımsal Rastsal Sayı Üreteci
SAM	Sorumluluk Atama Matrisi
REST	Representational State Transfer / Temsili Durum Transferi
RTU	Remote Terminal Unit / Uzak Terminal Ünitesi
SAN	Storage Area Network / Depolama Alanı Ağı
SCADA	Supervisory Control And Data Acquisition / Merkezi Kontrol ve Veri Toplama
SCAP	Security Content Automation Protocol / Güvenlik İçeriği Otomasyon Protokolü
SFTP	Secure File Transfer Protocol / Güvenli Dosya Transfer Protokolü
SGB	Siber Güvenlik Başkanlığı
SMB	Server Message Block / Sunucu İleti Bloğu
SMS	Short Message Service / Kısa Mesaj Hizmeti
SMTP	Simple Mail Transfer Protocol / Basit Posta Aktarım Protokolü
SMTPS	Secure Simple Mail Transfer Protocol / Güvenli Basit Posta Aktarım Protokolü
SOME	Siber Olaylara Müdahale Ekibi
SPF	Sender Policy Framework / Gönderen Politika Çerçevesi
SPK	Sermaye Piyasası Kurulu
SQL	Structured Query Language / Yapısal Sorgulama Dili
SSD	Solid State Disk / Katı Hal Sürücüsü
SSH	Secure Shell / Güvenli Kabuk
SSL	Secure Sockets Layer / Güvenli Soket Katmanı
TCP	Transmission Control Protocol / Gönderi Kontrol Protokolü
TEE	Trusted Execution Environment / Güvenilir İşletim Ortamı
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions / Elektromanyetik İletimlerin Yayılımından Korunan Telekomünikasyon Elektronik Malzemesi
TLS	Transport Layer Security / Taşıma Katmanı Güvenliği
TRNG	True Random Number Generator / Gerçek Rassal Sayı Üreteci
TRSM	Tamper Resistant Security Module / Kurcalamaya Dayanıklı Güvenlik Modülü
TS	Türk Standardı
UDP	User Datagram Protocol / Kullanıcı Veri Bloğu Protokolü
UPS	Uninterruptible Power Supply / Kesintisiz Güç Kaynağı
URL	Uniform Resource Locator / Tek Düzen Kaynak Konum Belirleyicisi
USB	Universal Serial Bus / Evrensel Seri Veri Yolu
VLAN	Virtual Local Area Network / Sanal Yerel Alan Ağı
VPN	Virtual Private Network / Sanal Özel Ağ
WAF	Web Application Firewall / Uygulama Güvenlik Duvarı
WebDAV	Web Distributed Authoring and Versioning / Web Dağıtımlı Yayın ve Sürümleme
WiFi	Wireless Fidelity / Kablosuz Bağlantı Alanı
XML	Extensible Markup Language / Genişletilebilir İşaretleme Dili
XSS	Cross Site Scripting / Siteler Arası Betik Çalıştırma

TANIMLAR

Tanım	Açıklama
Delfi Metodu	Bir karar alma durumuna ilişkin uzman görüşlerinin sistematik ve etkileşimli bir şekilde ele alınmasını sağlayan bir yöntem
Denetim Kaydı	Bir bilgi varlığına kimin eriştiğini veya erişmeye çalıştığını ve erişim sağlayan kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtlar
Genelge	06.07.2019 Tarihli ve 30823 Sayılı Resmi Gazete'de yayımlanan 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi
Gizlilik Dereceli Bilgi/Veri	Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke menfaatleri bakımından sakıncalı görülen ve haiz olduğu önem derecelerine göre "ÇOK GİZLİ", "GİZLİ", "ÖZEL" veya "HİZMETE ÖZEL" şeklinde sınıflandırılan bilgi/veri
İlgili Kişi	6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan kişisel verisi işlenen gerçek kişi
İz Kaydı	Operasyonel bir işlemin başlangıcından bitişine kadar adım adım takip edilmesini sağlayacak kayıtlar
Kritik Bilgi/Veri	• Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, içeriğinin yetkisiz personel veya kişiler tarafından görülmesinin kuruma çok ciddi maddi veya manevi zarar vereceği her türlü bilgi/veri, • Kritiklik derecesi 3 olarak hesaplanan varlıkların işlediği veriler, • 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile tanımlanan özel nitelikli kişisel veriler
Kurum	Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmeler
Kurumsal SOME Kurulum ve Yönetim Rehberi	Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanmış en güncel "Kurumsal SOME Kurulum ve Yönetim Rehberi" dokümanı
Rehber	Bilgi ve İletişim Güvenliği Rehberi
Varlık	Elektronik ve/veya fiziksel ortamlarda yer alan; iletişim yoluyla aktarılabilen bilgiyi içeren; kurumun iş süreçleri açısından değer taşıyan tüm bilgi ve bilgi işleme olanakları, bilgiyi kullanan ve taşıyan personel ile bilgiyi barındıran fiziksel mekânlar
Varlık Grubu	Varlıkların içerdiği verinin kritikliği göz önünde bulundurularak, aynı grup altında değerlendirilmek üzere sınıflandırılan varlıklar bütünü
Varlık Grubu Ana Başlığı	Her varlık grubunun özelliği dikkate alınarak yapılan sınıflandırma
Kritik Altyapı	İşlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar
Kritik Altyapı Sektörleri	Ulusal Siber Güvenlik Stratejisinde belirlenen kritik altyapı sektörleri

GİRİŞ

1. BÖLÜM

1. GİRİŞ

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında genel olarak alması gereken tedbirleri belirlemek için 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Yayımlanan Genelge doğrultusunda Bilgi ve İletişim Güvenliği Rehberi hazırlanmıştır.

Genelge kapsamında yer alan maddelerin Rehberde yer alan tedbirlerle eşleştirilmesini gösteren tablo EK-A'da sunulmuştur.

1.1. Amaç ve Kapsam

Rehberin temel amacı; bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır.

Rehber, bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmeleri kapsamaktadır.

Rehberin uygulanması sonucu elde edilmesi beklenenler somutlaştırılarak 12 hedef tanımlanmıştır. Şekil 1'de gösterilen hedefler aşağıda listelenmiştir:

1. Yerli ve milli ürün kullanımının teşvik edilmesi
2. Rehberi uygulayacak kurum ve kuruluşlarda yapılacak mükerrer çalışmaların ve yatırımların önüne geçilmesi
3. Güvenlik tedbirlerinin üç seviyeli olacak şekilde derecelendirilmesi ve varlık gruplarına güvenlik dereceleri ile uyumlu asgari güvenlik tedbirlerinin uygulanması
4. Rehberin güvenlik tedbirleri ile ilgili detayların izlenebilirliğinin sağlanacak şekilde yapılandırılması
5. Güvenlik tedbirlerinin ürün ve teknoloji bağımsız olarak uygulanabilir olması
6. Güvenlik tedbirlerinin uygulanıp uygulanmadığının denetlenebilmesi
7. Güvenlik tedbirlerinin birbirinden bağımsız şekilde uygulanabilirliğini sağlayacak şekilde gruplandırılması ve rehberin modülerliğinin sağlanması
8. Tedbirlerin teknik olarak tüm kurum ve kuruluşlar tarafından uygulanabilir olması
9. İhtiyaçlar, gelişen ve değişen şartlar dikkate alınarak rehberin sürdürülebilirliğinin sağlanması
10. Rehberin format ve içeriğinin özgün olması
11. Rehberin hem güvenlik tedbirlerini uygulayacak personele hem de bu tedbirlerin uygulanıp uygulanmadığını kontrol edecek denetçilere hitap etmesi
12. Rehber içeriğinin bilgi güvenliği çerçevesinde oluşturulmuş mevzuat ve rehberler ile ulusal/uluslararası standartlara uyumlu olması

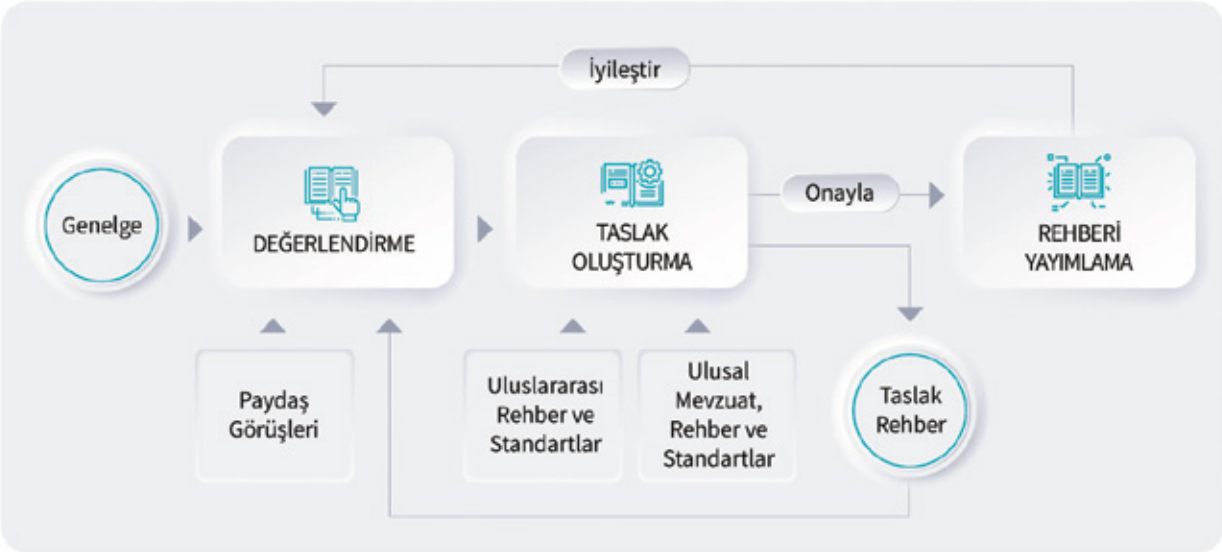
Şekil 1. Bilgi ve İletişim Güvenliği Rehberinin Hedefleri

1.2. Rehberin İçeriği ve Güncelleme Süreci

Rehberin içeriği; amaç ve hedefler doğrultusunda, ulusal/uluslararası standartlar ve rehberler, iyi uygulama örnekleri ile güncel mevzuat göz önünde bulundurularak oluşturulmuştur. EK-B'de rehber içeriğinin uluslararası standartlar ve yayımlı kılavuzlar ile eşleştirilmesini gösteren tablo yer almaktadır. Rehberin içeriği aşağıda listelenen dört ana bölümden oluşmaktadır:

- **Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci:** Rehberde yer alan tedbirlerin uygulanabilmesini sağlamak amacı ile rehber uygulama süreci tanımlanmıştır. Rehber uygulama süreci, bilgi güvenliği yönetim süreçlerine alternatif olarak uygulanacak bir süreç olarak hazırlanmamış olup mevcut bilgi güvenliği yönetim süreçlerine teknik olarak katkı sağlayacak tedbirleri ve faaliyetleri içermektedir. Kurumlar rehber uygulama süreci ile tanımlanan faaliyetleri, mevcut bilgi güvenliği yönetim süreçleri kapsamında ve uyarlama yaparak yürütmelidir.
- **Varlık Gruplarına Yönelik Güvenlik Tedbirleri:** Tanımlanan her bir varlık grubuna dâhil olduğu ana başlığa göre uygulanacak olan asgari güvenlik tedbirleri belirlenmiş ve detaylandırılmıştır.
- **Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri:** Varlık grupları özelinde tanımlanan güvenlik tedbirlerine ek olarak, uygulama ve teknoloji alanlarına özel güvenlik tedbirleri tanımlanmış ve detaylandırılmıştır. Her bir varlık grubu için ilgili uygulama ve teknoloji alanları belirlenmeli ve belirlenen alanlar için tanımlanan güvenlik tedbirleri de ilgili varlık gruplarına uygulanmalıdır.
- **Sıkılaştırma Tedbirleri:** İşletim sistemi, veri tabanı ve sunucular için sıkılaştırma tedbirlerini içermektedir.

Rehber, yaşayan bir doküman olacak şekilde; ihtiyaçlar, gelişen teknoloji ve değişen şartlar göz önünde bulundurularak sürekli güncellenecektir. Rehberin güncellenmesi için Şekil 2'de tanımlanan sürecin işletilmesi planlanmaktadır. Rehberin eski sürümlerine ve güncel sürümüne https://www.siberguvenlik.gov.tr adresinden erişilebilir olması sağlanacaktır.



Şekil 2. Rehber Güncelleme Süreci

1.3. Rehber Uyum Planı

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmeler tarafından, Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci'nin ve tanımlanan güvenlik tedbirlerinin uyum planı çerçevesinde ele alınması gerekmektedir. Uyum planı kapsamında yapılacak çalışmalar ve zaman planlamaları Şekil 3'te yer almaktadır. Uygulama yol haritası, uyum planında tanımlanan zaman dilimleri çerçevesinde oluşturulmalıdır.

Şekil 3. Rehber Uyum Planı

Kurumlar rehber uygulama sürecini, yürüttükleri bilgi güvenliği yönetim süreçlerine entegre etmeli ve bilgi güvenliği risk yönetimi faaliyetleri kapsamında rehberde tanımlanan tedbirleri uygulamalıdır. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci kapsamında gerçekleştirilmesi gereken çalışmalar ile Bilgi Güvenliği Yönetim Sistemi ana maddeleri arasındaki ilişki Şekil 4'te yer almaktadır.

Şekil 4. Rehber ve Bilgi Güvenliği Yönetim Sistemi İlişkisi

Rehberin 2. Bölümünde rehber uygulama süreci açıklanmıştır. Bu süreç kapsamında kullanılacak anket EK-C.1 olarak sunulmuştur. Bölüm 3'te varlık gruplarına yönelik tedbirlere, Bölüm 4'te de uygulama ve teknoloji alanına yönelik tedbirlere yer verilmiştir. Bölüm 3, 4 ve 5'te yer alan güvenlik tedbirleri açıklanırken tedbirler gruplandırılmış ve tedbir alt başlıkları oluşturulmuştur.

Tedbir ana başlıkları; amacı, önemi ve uygulama adımları ile açıklanmış olup, tedbir alt başlıkları ise aşağıdaki başlıklarda detaylandırılmıştır:

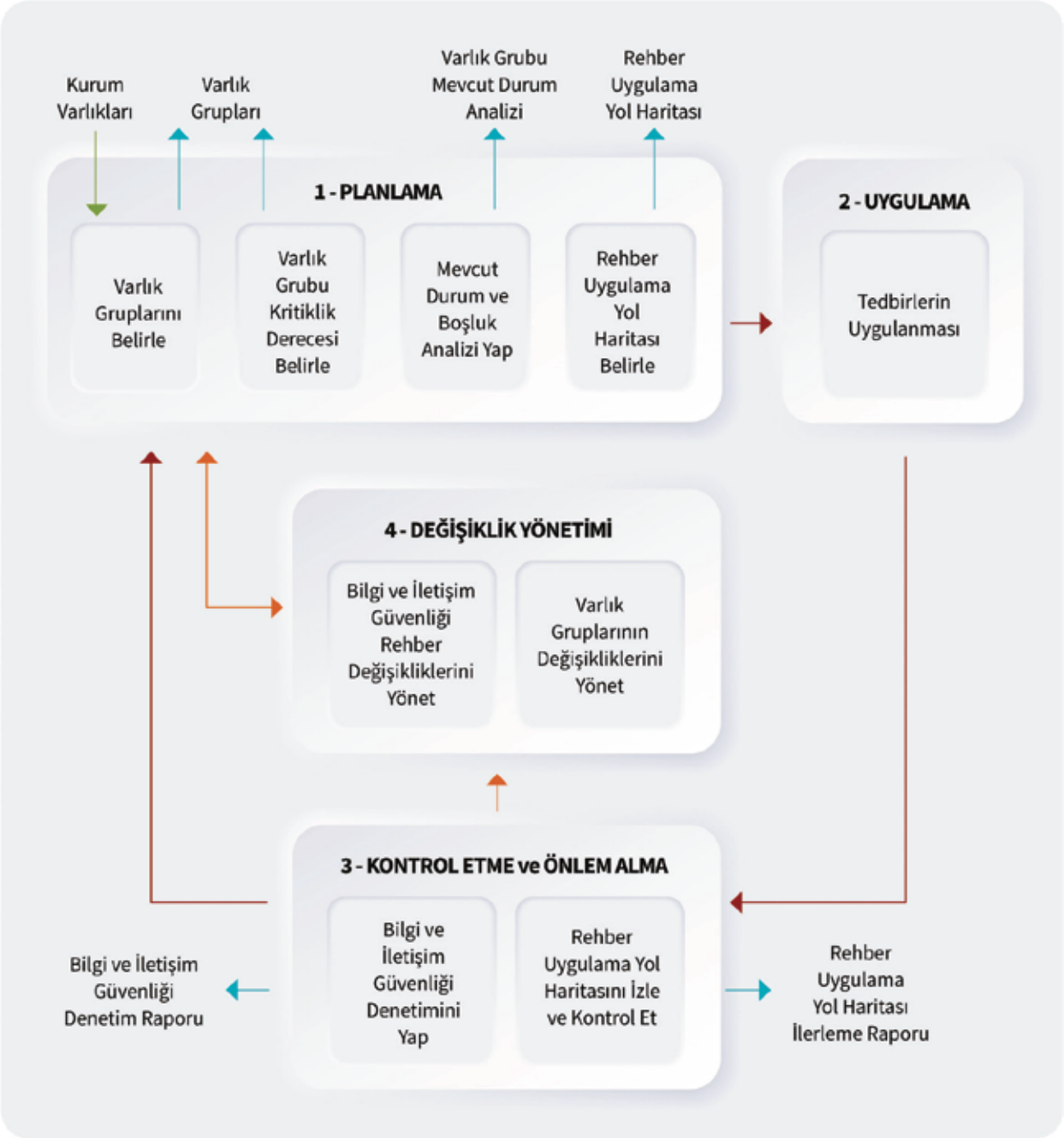
- **Tedbirler:** Alınması gereken tedbirleri seviyelendirerek listeler.
- **Denetim Maddeleri:** Grupta yer alan güvenlik tedbirlerinin uygulanıp uygulanmadığının kontrolü için kullanılabilecek denetim yöntemlerini ve soru örneklerini içerir. Tedbir maddeleri özelinde tanımlanan denetim yöntem önerileri; mülakat, gözden geçirme, güvenlik denetimi, sızma testi ve kaynak kod analizi yöntemlerini içermektedir. Denetim yöntemlerine ilişkin açıklamalar aşağıda yer almaktadır.
    - Mülakat: Denetim yapılan birim kapsamında söz konusu çalışmaların nasıl gerçekleştirildiği bilgisinin ilgili kurum personeli ile yüz yüze görüşülerek edinilmesidir. Gerekli görülmesi durumunda dokümantasyon inceleme çalışması ile desteklenmektedir.
    - Gözden Geçirme: Denetim yapılan birim kapsamında söz konusu çalışmalara yönelik güvenlik gereksinimleri göz önünde bulundurularak detaylı ve sistematik olarak yapılan incelemedir.
    - Güvenlik Denetimi: Bilgi teknolojileri ve güvenlik sistemlerine ait kuralların, sıkılaştırma ve yapılandırma çalışmalarının teknik olarak denetlenmesidir. Gerekli görülmesi durumunda otomatik araç kullanımı ile desteklenmektedir.
    - Sızma Testi: Bilgi teknolojileri ve güvenlik sistemleri kapsamında güvenlik açıklarının tespit edilmesini sağlayan, yetkin kişiler tarafından ve yasalara uygun olarak gerçekleştirilen güvenlik testleridir.
    - Kaynak Kod Analizi: Güvenli yazılım geliştirme konusunda uzman kişiler tarafından kaynak kodların incelenmesi ve güvenlik açıklarının tespit edilmesini sağlayan denetim çalışmasıdır. Gerekli görülmesi durumunda otomatik araç kullanımı ile desteklenmektedir.

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ

2. BÖLÜM

2. BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ

Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci Şekil 5'te tanımlanmıştır. Süreç; planlama, uygulama, kontrol etme ve önlem alma ile değişiklik yönetimi alt süreçlerinden oluşmaktadır.



Şekil 5. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci

Planlama kapsamında özet olarak; kurum varlıklarının gruplandırılması, gruplama sonucu elde edilen varlık gruplarının kritiklik derecelendirmesinin yapılması, bu varlık grubuna uygulanması gereken güvenlik tedbirlerinin mevcut durumunun analizi ve boşluk analizinin yapılarak yol haritasının hazırlanması faaliyetleri yürütülür. Yol haritasına uygun olarak yürütülecek çalışmalar uygulama alt sürecinde gerçekleştirilir. Rehber kapsamında yürütülen çalışmaların izlenmesi ve kontrolü faaliyetleri, kontrol etme ve önlem alma süreci kapsamında gerçekleştirilir. Kontrol etme ve önlem alma fazında ayrıca, rehberde yer alan tedbirlerin uygulanma durumunu tespit edebilmek için iç ve dış denetim faaliyetleri yürütülür. Rehberdeki güncellemelere uyum için yapılacak değişikliklerin belirlenmesi, kurum varlık gruplarında gerçekleşecek değişikliklerin (varlık grubu içeriğinin değişmesi, yeni varlık

gruplarının tanımlanması, varlık grubu kritiklik derecesinin değişmesi vb.) rehberde tanımlanan tedbirlerle uyumunun sağlanması çalışmaları değişiklik yönetimi kapsamında ele alınır.

Sonraki alt başlıklarda Şekil 5'te tanımlanan fazlar ve bu süreçler kapsamında yürütülecek faaliyetler açıklanmaktadır. Tablo 1'de SAM rollerine ilişkin kısaltmaların açıklamaları yer almaktadır. Alt süreçler kapsamında gerçekleştirilecek faaliyetler ve her bir faaliyet için örnek roller özelinde tanımlanmış sorumluluklar Tablo 2'deki SAM tablosu ile belirtilmektedir.

Tablo 1. SAM Rolleri Açıklamaları

Kısaltma	Açıklaması
S	Sorumlu: Görevi gerçekleştiren personel
O	Onaylayan: Görevi durdurabilen, devam ettirebilen, son kararı verebilen ve hesap veren personel
D	Danışılan: Görev yapılmadan önce bilgisine başvurulması gereken personel
B	Bilgilendirilen: Görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel

Tablo 2'de roller; iç paydaş ve dış paydaş olmak üzere iki kategori altında ele alınmakta olup, ilgili personelin üstlendiği veya o kişiye atanan görev olarak ifade edilmektedir. Alt süreçler doğrultusunda gerçekleştirilecek çalışmalar ise faaliyet olarak tanımlanmakta olup, her bir rolün faaliyetler özelinde tanımlanan sorumluluk ve yetki alanları yer almaktadır.

Tablo 2. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci için Sorumluluk Atama Matrisi

No.	FAALİYET ADI	ROL ADI												
		İÇ PAYDAŞLAR								DIŞ PAYDAŞLAR				
		Kurumun En Üst Düzey Yöneticisi	Bilgi Güvenliği Yöneticisi	Bilgi Sistemleri Yöneticisi	İç Denetçi	İlgili Birim Yöneticileri	İlgili Birim Uzman Personeli	Kurumsal SOME Yöneticisi	Varlık Grubu Koordinatörü	Dış Denetim Personeli	SGB	Bağlı/İlgili/İlişkili Üst Kurum	İlgili Düzenleyici ve Denetleyici Kurum	Teknik Danışman
1	Varlık Gruplarını Belirle	O	S	S	B	S	S	B	D					D
2	Varlık Grubu Kritiklik Derecesi Belirle	O	S	S		S	S	B	D					D
3	Mevcut Durum ve Boşluk Analizi Yap	O	S	S	B	S	S	S	D					D
4	Rehber Uygulama Yol Haritası Belirle	O	S	S		B	S	S	D					D
5	Rehber Uygulama Yol Haritasını Hayata Geçir	O	S	S		S	S	S	B					
6	Bilgi ve İletişim Güvenliği Denetimi Yap	O	B	B	S	B		B	D	S	S,B	B	B	
7	Rehber Uygulama Yol Haritasını İzle ve Kontrol Et	O	S	S		S	S	S	B					D
8	Bilgi ve İletişim Güvenliği Rehber Değişikliklerini Yönet	O	S	S	B	S	S	B	D					D
9	Varlık Gruplarının Değişikliklerini Yönet	O	S	S	B	S	S	B	D					D

Tablo 2'de adı geçen rollerin açıklamaları aşağıda verilmiştir:

Kurumun En Üst Düzey Yöneticisi: Kurum hiyerarşisinde bilgi güvenliğinin sağlanmasından ve yönetiminden sorumlu en üst mevkide yer alan kişi.

Bilgi Güvenliği Yöneticisi: Kurumda bilgi güvenliğinin sağlanmasından ve yönetiminden sorumlu personel.

Bilgi Sistemleri Yöneticisi: Kurumda bilgi sistemlerinin yönetiminden sorumlu personel/birim yöneticisi.

İç Denetçi: Kurumda iç denetimi gerçekleştiren personel.

İlgili Birim Yöneticileri: Kurumda, Rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim yöneticileri.

İlgili Birim Uzman Personeli: Rehber uygulama sürecinde yer alan aşamaları gerçekleştirme hususunda sorumluluk alacak birim personeli.

Kurumsal SOME Yöneticisi: Kurumda bulunan siber olaylara müdahale ekibinin yöneticisi.

Varlık Grubu Koordinatörü: Rehber uygulama sürecinde yer alan aşamalarda bilgi birikimine danışılan ve bu aşamaları koordine eden personel.

Dış Denetim Personeli: Rehber uygulama sürecinin ve güvenlik tedbirlerinin kurumda uygulanıp uygulanmadığını denetleyen üçüncü taraf denetçiler.

SGB: Cumhurbaşkanlığı Siber Güvenlik Başkanlığı

Bağlı/İlgili/İlişkili Üst Kurum: Kurumun bağlı/ilgili/ilişkili olduğu üst kurum (Ör. Bakanlıklar).

İlgili Düzenleyici ve Denetleyici Kurum: BDDK, EPDK, SPK ve BTK gibi düzenleyici/denetleyici kurumlar.

Teknik Danışman: Rehber uygulama sürecinde bilgi birikimine danışılan üçüncü taraf personel.

2.1. Planlama

2.1.1. Varlık Gruplarının Belirlenmesi

Rehber kapsamında yürütülen çalışmalarda varlıkların belirlenen başlıklar altında toplanarak gruplandırılması ve bu gruplar dikkate alınarak tedbirlerin uygulanması gerekmektedir. Rehber; elektronik ortamda yer alan bilgi/verinin depolandığı, aktarıldığı, işlendiği bilgi işleme olanakları, bilgi işleme olanaklarını kullanan personel ile bilgi işleme olanaklarını barındıran fiziksel ortamlara ilişkin varlıkları kapsamaktadır.

Rehberde tanımlanan varlık grubu ana başlıkları aşağıda listelenmiştir:

- Ağ ve Sistemler
- Uygulamalar
- Taşınabilir Cihaz ve Ortamlar
- Nesnelerin İnterneti (IoT) Cihazları
- Fiziksel Mekânlar
- Personel

Rehberde tanımlanan varlık grubu başlıkları, kurumların tanımlayacakları varlık grupları ve bilgi güvenliği kapsamında yönetilen varlıklar arasındaki ilişki Şekil 6'da tanımlanmıştır.

Şekil 6. Varlıklar, Varlık Grupları ve Varlık Ana Başlıkları

Hâlihazırda, kurumlar tarafından bilgi güvenliği yönetim süreci kapsamında tüm varlıklar belirlenmekte ve bu varlıklar için alınması gereken güvenlik önlemleri uygulanmaktadır. Varlık grupları belirlenirken aşağıdaki hususların dikkate alınması önerilmektedir:

- Tüm kurumsal varlıkların hangi varlık grubu ana başlığı altında yer alacağının belirlenmesi
- Tüm kurumsal varlıkların mümkün olduğunca tek bir varlık grubunda yer almasının sağlanması (Birden fazla varlık grubu tarafından adreslenmesi gereken kurumsal varlıklar, kritiklik derecesi en yüksek olan varlık grubu üzerinden değerlendirilmeli ve dâhil edildiği tüm varlık grupları ile ilgili tedbir maddeleri kurumsal varlık için ele alınmalıdır.)
- Varlık gruplarının tanımlanması için kullanılacak alt kırılımların kurumsal ihtiyaçlar doğrultusunda belirlenmesi (kurum hizmet alanları, kurum organizasyon yapısı, teknolojiler, uluslararası iyi örnekler, BT altyapıları vb.)
- Aynı güvenlik izolasyonunda yer alan varlıkların mümkün olduğunca aynı varlık grubuna dâhil edilmesi
- Farklı güvenlik seviyesine sahip olması gereken varlıkların farklı varlık gruplarında olacak şekilde gruplandırılması
- Aynı seviyede güvenlik tedbirlerinin uygulanacağı düşünülen varlık gruplarının birleştirilerek varlık grubu sayısının azaltılması
- Her bir varlık grubu ana başlığı altında yer alan varlık gruplarının sayılarının yönetilebilecek sayıda olması

Tanımlanan her bir varlık grubu için ilişkili uygulama ve teknoloji alanına yönelik güvenlik tedbiri ana başlıkları seçilir. Uygulama ve teknoloji alanı ana başlıkları altındaki tedbirler için ilgili varlık grubuna atanan kritiklik derecesi göz önünde bulundurulur. Aşağıda örnek bir kurumda varlık grubu belirleme çalışmaları sonucu elde edilebilecek varlık grubu listesi yer almaktadır:

- Ağ ve Sistem varlık grubu ana başlığı
  - Merkez bina açık ağ ve BT sistemi (1 adet)
  - Felaket kurtarma merkezi ağ ve BT sistemi (1 adet)
  - Kapalı ağ ve BT sistemi (1 adet)
  - Test ağ ve BT sistemi (1 adet)
  - OT sistemi (1 adet)
  - A tipi taşra ağ ve BT sistemi (5 adet)
  - B tipi taşra ağ ve BT sistemi (8 adet)

- Uygulama varlık grubu ana başlığı
  - E-devlet üzerinden erişilebilen G2G uygulama (5 adet)
  - Kritik veri işleyen G2B uygulama (15 adet)
  - Kritik veri işleyen kurum içi uygulama (20 adet)
  - Kritik veri işlemeyen kurum içi uygulama (60 adet)

- Taşınabilir Cihaz ve Ortam varlık grubu ana başlığı
  - İdari yöneticilerin kullandığı tablet ve cep telefonları (40 adet)
  - Sistem yöneticilerin kullandığı dizüstü bilgisayarlar (20 adet)
  - Yazılım geliştiricilerin kullandığı dizüstü bilgisayarlar (30 adet)
  - Personelin kullandığı taşınabilir ortamlar (USB cihazı) (400 adet)

- Nesnelerin İnterneti (IoT) Cihazları varlık grubu ana başlığı
  - Sistem odası kameraları (10 adet)
  - Ortam sensör cihazları (nem, gaz, sıcaklık) (30 adet)

- Fiziksel Mekânlar varlık grubu ana başlığı
  - Merkez bina veri merkezi (1 adet)
  - Felaket kurtarma merkezi (1 adet)
  - A tipi taşra veri merkezi (5 adet)
  - B tipi taşra veri merkezi (8 adet)
  - İdari yönetici odası (2 adet)
  - Sistem yöneticisi odası (3 adet)
  - Personel odası (100 adet)

- Personel varlık grubu ana başlığı
  - Üst yönetici (5 personel)
  - Birim yöneticisi ve daire başkanı (40 personel)
  - Sistem yöneticisi (20 personel)
  - Yazılım geliştirici (40 personel)
  - Son kullanıcı (1500 personel)
  - Altyüklenici personeli (10 personel)

2.1.2. Varlık Grubu Kritiklik Derecesinin Belirlenmesi

Varlık gruplarının belirlenmesinin ardından bu varlık gruplarının hangi kritiklik derecesine sahip olduğu belirlenmelidir. Her bir varlık grubunun kritiklik derecesi, işlenen verinin gizlilik, bütünlük ve erişilebilirlik açısından kritikliği ile oluşabilecek güvenlik ihlallerinin etki alanları dikkate alınarak belirlenecektir. Bu kapsamda kullanılacak boyutlar Şekil 7'de tanımlanmıştır.

Şekil 7. Kritiklik Derecesi Belirlemek için Kullanılan Boyutlar

Kritiklik derecesi belirleme boyutları aşağıda özetlenmiştir:

- İşlenen veri ile ilgili boyutlar
    - **Gizlilik**: Bilginin yetkisiz kişilerin erişimine karşı korunması
    - **Bütünlük**: Bilginin tam ve doğru olma durumunun korunması
    - **Erişilebilirlik**: Bilginin yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması
- Etki alanı ile ilgili boyutlar
    - **Bağımlı Varlıklar**: Varlık grubuna bağımlı olan diğer varlıklar üzerindeki etkisi
    - **Etkilenen Kişi Sayısı**: Bilgi güvenliği ihlal olayı meydana geldiğinde etkilenebilecek kişi sayısı
    - **Kurumsal Sonuçlar**: Bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılacak kurumsal durum

- **Sektörel Etki**: Varlık grubunun hizmet verdiği sektöre etkisi
- **Toplumsal Sonuçlar**: Bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılacak toplumsal durum

Bu boyutlar dikkate alınarak bir anket formu oluşturulmuş ve EK-C.1'de sunulmuştur. Her bir varlık grubu için bu anket formu doldurularak ilgili varlık grubunun kritiklik derecesi belirlenmelidir. "Varlık Grubu Kritiklik Derecelendirme Anketi" olarak tanımlanan anket her bir varlık grubu özelinde rehber uyumluluk denetimi kapsamında kontrol edilecektir. İlgili varlık grubu için uygulanması gereken tedbir maddeleri, varlık grubu için belirlenmiş olan kritiklik derecesi göz önünde bulundurularak belirlenir.

Varlık grubu kritiklik derecesi belirleme aşamasında aşağıdaki adımlar takip edilir:

- Her bir varlık grubu için EK-C.1'de yer alan anket formu ilgili paydaşların katılımı ile doldurulur. Anket çalışması kapsamında varlıkların sahipleri, sistem yöneticileri, geliştiriciler, kullanıcı temsilcileri, yöneticileri ve kurumun sahip olduğu en yetkin personel katılım sağlamalıdır. Anket doldurma çalışmalarında Delfi metodunun kullanılması önerilmektedir. Anket çalışması aşağıda yer alan Delfi metodu uygulama adımları izlenerek gerçekleştirilmelidir.
    1. Anketin uygulanacağı uzman kişiler belirlenir.
    2. Anket uzman kişiler tarafından doldurulur.
    3. Anket sonuçları değerlendirilir.
    4. Tüm katılımcılar bir fikir üzerinde ortak karar verene kadar anket uygulanmaya devam edilir ve 2. adıma dönülür.
    5. Tüm anket sonuçlarına göre uzlaşılan karar uygulanır.
- Her varlık grubu için doldurulan anket sorularının cevapları için anket formunda yer alan puanlar toplanarak anket puanı hesaplanır. Tablo 3 kullanılarak anket puanına karşılık gelen kritiklik derecesi belirlenir. Belirlenen derece, varlık grubunun kritiklik derecesi olarak kullanılır.

Tablo 3. Anket Puanına Karşılık Gelen Kritiklik Derecesi

Anket Puanı	Varlık Grubu Kritiklik Derecesi
Anket puanı 18'den küçük ise	Derece 1
Anket puanı 18 (dâhil) ile 28 arasında ise	Derece 2
Anket puanı 28 ve daha yüksek ise	Derece 3

- Varlık grubu içinde yer alan tüm varlıklara aynı güvenlik tedbirlerinin uygulanacağı dikkate alınarak anket sonuçları tekrar değerlendirilir. Gerekli görülmesi durumunda varlık grupları güncellenerek anket çalışmaları tekrarlanır.
- Kritiklik derecesi tanımlanan her bir varlık grubu için kritiklik dereceleri ile uygulama ve teknoloji alanlarına yönelik güvenlik tedbirlerinin uygulanma durumlarının kayıt altına alındığı EK-C.2'de yer alan form doldurulur.

Aşağıdaki maddelerde kritiklik derecesinin belirlenmesi ile ilgili çeşitli örnekler verilmektedir.

- Tablo 4'te örnek iki varlık grubu için uygulanan anketler sonucunda elde edilen puanlar ve toplam anket puanları verilmiştir. Tablo 3 kullanılarak varlık grubu 1'in kritiklik derecesinin "Derece 2" ve varlık grubu 2'nin kritiklik derecesinin "Derece 3" olduğu belirlenir.

Tablo 4. Varlık Grubu Kritiklik Derecesinin Belirlenmesi

Anket Sorusu	Varlık Grubu 1 İçin Puan	Varlık Grubu 2 İçin Puan
1. Soru	3	5
2. Soru	3	5
3. Soru	3	5
4. Soru	2	4
5. Soru	3	5
6. Soru	3	3
7. Soru	3	5
8. Soru	2	6
	22 (Anket Puanı)	**38 (Anket Puanı)**

- Tablo 5'te örnek bir kuruma ait varlık gruplarının anket çalışmaları sonucunda elde edilen kritiklik derecelerine ve varlık grubu ana başlıklarına göre dağılımı gösterilmektedir.

Tablo 5. Alt Varlık Gruplarının Kritiklik Derecesinin Belirlenmesi

Varlık Grubu Ana Başlıkları	Varlık Grubu Sayıları			
	Derece 1	Derece 2	Derece 3	Toplam
Ağ ve Sistemler	2	1	4	7
Uygulamalar	-	2	2	4
Taşınabilir Cihaz ve Ortamlar	1	-	3	4
Nesnelerin İnterneti (IoT) Cihazları	-	2	-	2
Fiziksel Mekânlar	2	3	3	8
Personel	-	3	3	6

- Tablo 6'da varlık grubu 1, varlık grubu 2'ye ait varlık grupları ile uygulama ve teknoloji alanlarına ve sıkılaştırma tedbirlerine yönelik uygulanması gereken tedbir ana başlıkları ve tedbir maddeleri için ilgili seviyeler yer almaktadır.

Tablo 6. Varlık Gruplarına Yönelik Tedbir Uygulanabilirlik Örnek Çalışması

Varlık Grubu Ana Başlığı	**Varlık Grubu No**	**Varlık Grubu Adı**	**Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)						**Sıkılaştırma Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)			**Kritiklik Derecesi (Derece 1/ Derece 2/ Derece 3)**
			Kişisel Verilerin Güvenliği	**Anlık Mesajlaşma Güvenliği**	**Bulut Bilişim Güvenliği**	**Kripto Uygulamaları Güvenliği**	**Kritik Altyapılar Güvenliği**	**Yeni Geliştirmeler ve Tedarik**	**İşletim Sistemi Sıkılaştırma Tedbirleri**	**Veri Tabanı Sıkılaştırma Tedbirleri**	**Sunucu Sıkılaştırma Tedbirleri**	
Uygulamalar	1	Kritik Verileri İşlemeyen Kurum İçi Uygulama	U	U	U	U	UD	U	U	UD	U	Derece 2
	2	Kritik Verileri İşleyen Kurum İçi Uygulama	U	U	UD	U	UD	U	U	UD	U	Derece 3

2.1.3. Mevcut Durum ve Boşluk Analizi

Varlık gruplarının kritiklik dereceleri dikkate alınarak Bölüm 3, 4 ve 5'te yer alan güvenlik tedbirlerinin hangilerinin uygulanması gerektiğinin belirlenmesi ve belirlenen güvenlik tedbirlerine göre mevcut durumun tespiti için detaylı çalışma yapılmalıdır. Rehberde tanımlanan güvenlik tedbirleri aşağıda yer alan üç ana başlık altında sınıflandırılmıştır.

Varlık gruplarına yönelik güvenlik tedbirleri ana başlıkları:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirleri ana başlıkları:

- Kişisel Verilerin Güvenliği
- Anlık Mesajlaşma Güvenliği
- Bulut Bilişim Güvenliği
- Kripto Uygulamaları Güvenliği
- Kritik Altyapılar Güvenliği
- Yeni Geliştirmeler ve Tedarik

Sıkılaştırma faaliyetlerine yönelik güvenlik tedbirleri ana başlıkları:

- İşletim Sistemi Sıkılaştırma Tedbirleri
- Veri Tabanı Sıkılaştırma Tedbirleri
- Sunucu Sıkılaştırma Tedbirleri

Bölüm 3, 4 ve 5 ana başlıklarının altında yer alan her bir güvenlik tedbiri temel, orta ve ileri seviye olarak derecelendirilmiştir. Varlık grubuna uygulanacak tedbirler aşağıdaki sınıflandırmaya göre belirlenir.

- **1. Seviye Tedbirler:** Kritiklik derecesi 1 olan varlık gruplarında yer alan tüm varlıklara temel seviye güvenlik tedbirleri uygulanır.
- **2. Seviye Tedbirler:** Kritiklik derecesi 2 olan varlık gruplarında yer alan tüm varlıklara temel seviye güvenlik tedbirlerine ek olarak orta seviye güvenlik tedbirleri uygulanır.
- **3. Seviye Tedbirler:** Kritiklik derecesi 3 olan varlık gruplarında yer alan tüm varlıklara temel ve orta seviye güvenlik tedbirlerine ek olarak ileri seviye güvenlik tedbirleri uygulanır.

Her bir varlık grubu kapsamında mevcut durum tespiti için analiz çalışmaları gerçekleştirilir. Bu kapsamda aşağıdaki adımlar takip edilir:

- Her bir varlık grubu için öncelikle Bölüm 3'ten ilgili güvenlik tedbirleri ana başlığı (Ağ ve Sistem Güvenliği, Uygulama ve Veri Güvenliği, Personel Güvenliği vb.) seçilir. Seçilen başlıkta yer alan tedbirlerden varlık grubunun kritiklik derecesine uygun olan tedbirler belirlenir.
- Her varlık grubunda yer alan varlıklar dikkate alınarak Bölüm 4 ve 5'te yer alan güvenlik tedbiri ana başlıkları (Bulut Bilişim Güvenliği, Kişisel Verilerin Güvenliği, İşletim Sistemi Sıkılaştırma, Veri Tabanı Sıkılaştırma vb.) seçilir. Seçilen başlıklarda yer alan tedbirlerden, varlık grubunun kritiklik derecesine uygun olan tedbirler belirlenir.
- Varlık grupları için belirlenen tüm tedbirler ile ilgili mevcut durum analiz edilir ve varlık grubu mevcut durum analiz raporu hazırlanır. Mevcut durum analizi çalışmaları kapsamında teknik çalışma, toplantı, otomatik araç ile durum tespiti, dokümantasyon inceleme vb. faaliyetler gerçekleştirilebilir. Varlık grubuna bir tedbirin uygulanıp uygulanmadığı tespit edilirken öncelikle aşağıdaki sınıflandırmaya göre uygulama durumuna karar verilir ve mevcut durum ile ilgili açıklayıcı bilgi yazılır.
    - Tedbir varlık grubunda yer alan tüm varlıklara uygulanmakta ise "tamamen"
    - Tedbir varlık grubunda yer alan varlıkların çoğuna uygulanmakta fakat bazı varlıklara kısmen uygulanmakta veya henüz uygulanmamakta ise "çoğunlukla"
    - Tedbir varlık grubunda yer alan bir kısım varlığa uygulanmakta veya tedbir kısmen uygulanmakta ise "kısmen"
    - Tedbir hiç uygulanmamakta ise "hiç"
    - Tedbirin teknik olarak uygulanma ihtimali bulunmuyorsa "uygulanamaz"
- Her bir varlık grubu için yapılan değerlendirmeler EK-C.3'te yer alan form ile kayıt altına alınır.
- Varlık grupları için hazırlanan mevcut durum analizi raporlarından faydalanılarak varlık grubunun kritiklik derecesi ile uyumlu tedbirler seçilir. Seçilen tedbirlerden uygulanmayan veya kısmen uygulananlar listelenerek boşluk analizi çalışması gerçekleştirilir.

Örnek olarak, bir kurumda "kurum iç uygulamaları" olarak tanımlanan bir varlık grubunun kritiklik derecesinin "Derece 2" olduğu görülmüştür. Bu varlık grubu için mevcut durum analizi çalışması için aşağıdaki adımlar gerçekleştirilir:

- Bu varlık grubu Uygulama Varlık Grubu Ana Başlığı altında olduğu için Bölüm 3'ten "Uygulama ve Veri Güvenliği" başlığı seçilir. Bu başlık altında yer alan tüm tedbirlerden 1. ve 2. seviye tedbirler listelenir.
- Bu varlık grubunda yer alan uygulamalar kişisel veri işlediği ve bulut servisleri kullandığı düşünüldüğünde Bölüm 4'ten "Kişisel Verilerin Güvenliği" ve "Bulut Bilişim Güvenliği" başlıkları seçilir. Seçilen bu başlıklar altında yer alan tedbirlerden 1. ve 2. seviye tedbirler listelenir.

- Bu varlık grubunda yer alan uygulamaların; işletim sistemi, veri tabanı ve web sunucusu kullandığı düşünüldüğünde Bölüm 5'ten "İşletim Sistemi Sıkılaştırma Tedbirleri", "Veri Tabanı Sıkılaştırma Tedbirleri" ve "Sunucu Sıkılaştırma Tedbirleri" başlığı seçilerek, bu başlıklar altında yer alan tedbirlerden 1. ve 2. seviye tedbirler listelenir.
- Önceki adımlarda belirlenen tedbirlerin tümü için mevcut durumuna karar verilir. Bu kapsamda her bir tedbirin varlık grubunda yer alan tüm varlıklara uygulanıp uygulanmadığı tespit edilerek raporlanır. Çalışma sonucunda varlık grubu mevcut durum analizi raporu hazırlanır.
- Varlık grupları için hazırlanan mevcut durum analiz raporlarından faydalanılarak boşluk analizi gerçekleştirilir. 1. ve 2. seviye tedbirleri içeren ilgili uygulama adımlarından gerçekleştirilmeyenler veya kısmen gerçekleştirilenler listelenerek raporlanır.

2.1.4. Rehber Uygulama Yol Haritasının Hazırlanması

Boşluk analizi sonucunda tespit edilen eksikliklerin giderilmesi için gereken faaliyetler belirlendikten sonra planlama yapılır. Planlamalar kapsamında ilgili tüm yasal, düzenleyici ve sözleşmeden doğan gereksinimler dikkate alınır.

Rehber uygulama yol haritası kapsamında yapılacak çalışmalar belirlenir. Çalışmalar, aşağıdaki gruplarla sınırlı olmamakla birlikte şu şekilde gruplandırılabilir:

- Yetkinlik kazanımı ve eğitimler
- Ürün tedariki
- Hizmet alımı
- Danışmanlık
- Geliştirme / yeniden geliştirme
- Tasarlama / yeniden tasarlama
- Sıkılaştırma
- Sürüm güncelleme
- Dokümantasyon
- Kurumsal süreç iyileştirme

Yapılacak çalışmalar belirlendikten sonra her çalışma için 2-3 aylık dönemler halinde hedefler belirlenir ve gerekli kaynak tahsisi (personel, bütçe, fiziksel ortam vb.) için planlama yapılır. Uygulama yol haritası kapsamında yapılan planlamalar EK-C.4'te yer alan form ile kayıt altına alınır.

Kurum, boşluk analizi sonucunda uygulanması gereken ilave tedbirler kapsamındaki herhangi bir gereksinimi; üst yönetim tarafından onaylanmış teknik kısıtlamalar ve iş gereksinimlerinden dolayı rehberde tanımlandığı şekli ile karşılayamaması durumunda telafi edici kontroller uygulayabilir. Telafi edici kontroller, yerine uygulandıkları tedbir maddeleri ile aynı amaç ve etkiye sahip olmaları durumunda kullanılabilir olarak kabul edilecektir. Uygulanmasına karar verilen her bir telafi edici kontrol EK-C.5'te yer alan form ile kayıt altına alınmalıdır.

Bilgi güvenliğinde en zayıf halkanın insan faktörü olduğu göz önünde bulundurulduğunda, hem güvenlik tedbirlerinin uygulanmasında hem de uygulanan güvenlik tedbirlerinin denetlenmesinde görev alacak kurum personelinin belirli bir yetkinliğe sahip olması önem arz etmektedir. Bu çerçevede, bilgi güvenliği ile ilgili eğitimler kaynaklar dâhilinde planlanmalı ve personelin gelişimi hakkında ışık tutacak ölçüm mekanizmaları hayata geçirilmelidir. Eğitimlerin sadece teorik bilgi vermekten ziyade, personelin ilgili alanda pratik becerisini arttıracak uygulamaları içermesi önemlidir. Bu kapsamda planlanacak eğitimlerde, laboratuvar ortamının bulunması ve bu ortamda katılımcıların öğrendikleri bilgiyi beceriye dönüştürmesi sağlanmalıdır.

Rehberin uygulanması için yürütülecek çalışmalara dâhil olacak personele yetkinlik kazandırmak amacıyla rehberde bulunan uygulama adımları ve denetim tablolarının nasıl ele alınacağıyla ilgili olarak çeşitli uygulama çalıştaylarının düzenlenmesi veya bu kapsamda gerçekleştirilecek çalışmalara katılım sağlanması gerekmektedir.

Bu kapsamda gerçekleştirilen tüm çalışmalar rehber uygulama yol haritası olarak dokümante edilecektir.

2.2. Uygulama

Rehber uygulama yol haritası, dönemsel olarak belirlenen hedefler dikkate alınarak planlanan şekilde kurum personeli tarafından hayata geçirilecektir. Bu kapsamda yol haritasında belirlenen tedarik, hizmet alımı, yeniden tasarım vb. tüm çalışmaların gerekli kaynak ihtiyaçlarının tahsis faaliyetleri önceliklendirilmelidir.

2.2.1. Bilgi ve İletişim Güvenliği Temel Prensipleri

Yol haritasının planlanması ve uygulanması aşamalarında gerçekleştirilecek tüm çalışmalarda Şekil 8'de yer alan temel prensipler dikkate alınmalıdır.

Şekil 8. Temel Prensipler

- **Yetkin Personel:** Yol haritasını uygulayacak ve denetim faaliyetlerini yürütecek personel bilgi güvenliği, siber güvenlik veya kişisel verilerin korunması konularında temel eğitimleri almış olmalıdır.
- **Güvenlik Temelli Tasarım (Security by Design):** Güvenlik tasarım aşamasında dikkate alınmalı ve tasarım aşamasında güvenlik tasarımı yapılmalıdır.
- **Mahremiyet Temelli Tasarım (Privacy by Design):** Kişisel veri güvenliği tasarım aşamasında dikkate alınmalı ve tasarım aşamasında güvenlik tasarımı yapılmalıdır.
- **Derinlemesine Savunma (Defence in Depth):** Varlıkların güvenliği ihtiyaçlar dikkate alınarak birden fazla savunma katmanı ile sağlanmalıdır.
- **Saldırı Yüzeyinin Azaltılması:** Saldırıya maruz kalınabilecek alanların en aza indirilmesi sağlanmalıdır.
- **Asgari Yetki Tanımlama:** Bir işin gerçekleştirilmesi için yeterli ve en az yetkiyle çalıştırılması sağlanmalıdır.
- **En Zayıf Halkanın Tespiti:** Yapılan çalışmalarda ve tasarımlarda en zayıf halkanın tespit edilerek güçlendirilmesi için planlama yapılmalıdır.
- **Güvenlik Hedeflerinin İş Hedefleriyle Uyumu:** Güvenlik hedefleriyle iş hedeflerinin birbirleriyle uyumu sağlanmalıdır.
- **Yerli ve Milli Ürünlerin Tercih Edilmesi:** İhtiyaç duyulan güvenlik gereksinimlerinin karşılanması durumunda yerli ve milli ürünler tercih edilmelidir.
- **Mükerrer Çalışma ve Yatırımların Önlenmesi:** Mükerrer çalışma ve yatırımların önüne geçilecek şekilde çalışmalar yürütülmelidir.
- **Bilmesi Gereken Prensibi:** Herhangi bir konu veya işi, görev ve sorumlulukları gereği; öğrenme, inceleme, gereğini yerine getirme ve koruma sorumluluğu bulunanlar yetkileri düzeyinde bilgi sahibi olmalıdır.

2.3. Kontrol Etme ve Önlem Alma

2.3.1. Rehber Uygulama Yol Haritasının İzlenmesi ve Kontrol Edilmesi

Rehber uygulama yol haritası çalışmalarının ilerleme durumlarının takibi ve hazırlanan plandan sapmaların tespit edilerek gerekli önlemlerin alınması ile ilgili faaliyetlerin yürütülmesi gerekmektedir. Ayrıca uygulama yol haritası çalışmaları yürütülürken karşılaşılacak sorun ve risklerin yönetimi de gerçekleştirilmelidir.

Dönem sonlarında uygulama yol haritasında yürütülen çalışmalar, planlanan hedeflerden sapmalar, sorun ve riskler, alınan önlemler hakkında bilgileri içeren yol haritası ilerleme raporları hazırlanmalıdır.

2.3.2. Bilgi ve İletişim Güvenliği Denetimi

Rehberin uygulamasına ilişkin denetimler, gerekli mekanizmalar oluşturularak, yılda en az bir kez olmak üzere iç denetim yolu ile gerçekleştirilir. Denetim faaliyetleri Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınarak yürütülür.

2.4. Değişiklik Yönetimi

2.4.1. Rehber Değişikliklerinin Yönetilmesi

Bilgi ve İletişim Güvenliği Rehberi; ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı tarafından rehberde yapılacak değişiklikler sürekli izlenerek kurum tarafından mevcut rehber uygulama yol haritası güncellenir veya yeni bir yol haritası hazırlanması için çalışmalar yürütülür.

2.4.2. Varlık Gruplarının Değişikliklerinin Yönetilmesi

Kurumun varlık grupları ile uygulama ve teknoloji alanlarında oluşabilecek değişiklikler aşağıdakilerle sınırlı olmamakla birlikte sürekli izlenmelidir.

- Yeni varlık gruplarının oluşturulması
- Varlık gruplarında yer alan varlıkların değişmesi
- Mevcut varlık grupları yerine farklı varlık gruplarının tanımlanması
- Varlık gruplarının kritiklik derecelerinin değişmesi
- Varlık gruplarına uygulanacak uygulama ve teknoloji alanlarının değişmesi
- Varlık gruplarını etkileyen mevzuat, standart veya ikincil düzenlemelerin değişmesi

Kurumsal ihtiyaçlar ve gelişmeler dikkate alınarak varlık grupları ile uygulama ve teknoloji ya da sıkılaştırma tedbirleri kapsamında gerçekleşecek bir değişiklik tespit edildiğinde tekrar planlama yapılarak yeni yol haritasının oluşturulması veya mevcut yol haritasının güncellenmesi gerekmektedir.

VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

3. BÖLÜM

3. VARLIK GRUPLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

Varlık grubuna yönelik güvenlik tedbirleri, varlık grubu ana başlık gruplarına uygun olarak başlıklara ayrılarak tanımlanmıştır. Rehberde tanımlanan varlık grubu ana başlıkları ve varlık gruplarında yer alabilecek örnek varlıklar aşağıda listelenmiştir:

- Ağ ve Sistemler: Kurumsal ağ, sunucu, donanım, güvenlik cihazı, kimlik yönetim ve doğrulama sistemi, veri sızıntısı önleme sistemi vb. varlıkların oluşturduğu mantıksal / fiziksel gruplar
- Uygulamalar: Kurumsal olarak geliştirilen veya tedarik edilen yazılımların oluşturduğu mantıksal gruplar
- Taşınabilir Cihaz ve Ortamlar: Kurumsal olarak kullanılan taşınabilir dizüstü bilgisayar, tablet, telefon vb. cihazlar ile taşınabilir ortam (CD, USB disk vb.) grupları
- Nesnelerin İnterneti (IoT) Cihazları: Kurumsal ortamlarda kullanılan sensör, kamera vb. cihaz grupları
- Personel: Kurum bünyesinde görev yapan personel / uzman grupları
- Fiziksel Mekânlar: Bilgi güvenliği kapsamında yönetilen kurumsal sunucu odası, felaket kurtarma merkezi, personel odası vb. fiziksel mekânların grupları

3.1. Ağ ve Sistem Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, ağ ve sistem güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Ağ ve Sistem Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Donanım Varlıklarının Envanter Yönetimi
- Yazılım Varlıklarının Envanter Yönetimi
- Tehdit ve Zafiyet Yönetimi
- E-Posta Sunucusu ve İstemcisi Güvenliği
- Zararlı Yazılımlardan Korunma
- Ağ Güvenliği
- Veri Sızıntısı Önleme
- İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi
- Sanallaştırma Güvenliği
- Siber Güvenlik Olay Yönetimi
- Sızma Testleri ve Güvenlik Denetimleri
- Kimlik Doğrulama ve Erişim Yönetimi
- Felaket Kurtarma ve İş Sürekliliği Yönetimi
- Uzaktan Çalışma

3.1.1. Donanım Varlıklarının Envanter Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.1.1	1	Donanım Envanterinin Yönetimi	Veri saklama, işleme ve iletme yeteneği olan tüm donanımların güncel bir envanteri tutulmalı, yalnızca yetkilendirilmiş personelin varlık envanterine erişimi mümkün kılınmalıdır.
3.1.1.2	1	Donanım Envanter İçeriğinin Yönetimi	Donanım envanteri en az; her bir donanımın ağ adresini, donanım adresini, makine adını, seri numarasını, markasını, modelini, destek alınan tedarikçi sözleşme bilgilerini (bakım süresi, kapsamı vb.), donanımın sorumlusunu, sorumlu kişinin birimini ve donanımın kurum tarafından onaylı olup olmadığı bilgisini içermelidir. Donanım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.
3.1.1.3	1	Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi	Yeni tedarik edilen ya da ağa yeni bağlanacak donanımların, donanım varlık envanterine kaydı yapılmadan kurum ağına bağlanmamasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır.
3.1.1.4	2	Aktif Keşif Araçlarının Kullanılması	Kurum ağına bağlı cihazları tanımlamak ve donanım varlık envanterindeki değişiklikleri takip etmek için aktif keşif araçları kullanılmalıdır.
3.1.1.5	2	DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti	Kurumun donanım envanterini güncel tutmak için tüm DHCP sunucularında ya da IP adres yönetim araçlarında kayıt mekanizmasının kullanımı sağlanmalıdır.
3.1.1.6	2	Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri	Kullanım ömrünü tamamlayan cihazların veri depolama üniteleri (HDD, SSD, USB, disk, harici bellek vb.) güvenli bir şekilde imha edilmelidir. Kurum içinde tekrar kullanılması durumunda ise veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra kullanıma alınmalıdır.
3.1.1.7	2	Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması	Sadece onaylı donanımların kurum ağına bağlanabilmesi için, 802.1x standardı veya NAC çözümleri kullanılarak kurum ağına bağlanan cihazlara kimlik denetimi yapılmalıdır.
3.1.1.8	3	Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması	Destekleyen cihazlarda, kurumun güvenli ağlarına bağlanan donanım varlıklarının kimlik denetimi için istemci sertifikaları kullanılmalıdır. Sertifika, yetkilendirilmiş personel tarafından güvenli alanda oluşturulmalıdır. Sertifikanın anahtar uzunluğu, tipi (NES/NES olmayan) ve oluşturulma yöntemi bilgi güvenliği gereksinimleri doğrultusunda seçilmelidir. Oluşturulan sertifika güvenli alanda saklanmalı ve sertifika yaşam döngüsünün takibi yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.1.9	3	Sabit Disk Güvenliği	Kurum tarafından satın alınan kullanıcı bilgisayarlarına ait sabit diskler, veri kurtarmaya imkân sağlamayacak şekilde güvenli silme işlemine tabi tutulduktan sonra sistemlere dâhil edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.1.1	Donanım Envanterinin Yönetimi	Mülakat, Gözden Geçirme	Kurum bünyesinde detaylı ve güncel bir donanım envanteri tutulmakta mıdır? Envanter yönetim süreci tanımlanmış mıdır? Donanım envanterine hangi personelin erişim yetkisi bulunmaktadır?
3.1.1.2	Donanım Envanter İçeriğinin Yönetimi	Mülakat, Gözden Geçirme	Donanım envanterinde; her bir donanım için ağ adresi, donanım adresi, makine adı, seri numarası, marka, model, donanımın sorumlusu ve donanımın kurum tarafından onaylı olup olmadığı bilgisi tutulmakta mıdır? Donanım envanterinde yer alan varlıklara ait hangi bilgiler detaylandırılmaktadır? Donanım envanter içeriğinde yapılan değişiklikler kayıt altına alınmakta mıdır?
3.1.1.3	Donanım Envanterine Kaydedilmemiş Donanımların Yönetimi	Mülakat, Güvenlik Denetimi	Donanım varlık envanterine kaydedilmemiş olan donanımlar kurum ağına nasıl bağlanmaktadır? Donanım envanterinde yer almayan donanımların yönetimi ile ilgili politika/prosedür bulunmakta mıdır? İlgili politika/prosedürler uygulanmakta mıdır?
3.1.1.4	Aktif Keşif Araçlarının Kullanılması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kurumda, ağa bağlanılan cihazları tanımak ve donanım envanterindeki değişiklikleri takip etmek amacıyla aktif keşif araçları kullanılmakta mıdır? Aktif keşif araçları ile keşif işlemi en son ne zaman yapılmıştır? Keşif sonuçları nasıl analiz edilmektedir? Keşif sonuçları nasıl saklanmaktadır?
3.1.1.5	DHCP Kayıt Mekanizması ile Yeni Donanımların Tespiti	Mülakat, Güvenlik Denetimi	Kuruma ait DHCP sunucularında kayıt tutulmakta mıdır? Tespit edilen yeni donanımlar, donanım envanterine kontrollü olarak eklenmekte midir? Varsa IP adres yönetimi aracında ilgili kayıt tutulmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.1.6	Kullanım Ömrünü Tamamlayan Cihazların Veri Depolama Üniteleri	Mülakat, Gözden Geçirme	Kullanım ömrünü tamamlayan cihazların imha edilmesine veya tekrar kullanılmasına yönelik bir politika/prosedür tanımlanmış mıdır? İlgili politika/prosedür uygulanmakta mıdır? Cihazların veri depolama ünitelerini güvenli silmek amacıyla hangi yöntemler kullanılmaktadır? Kullanım ömrünü tamamlayan cihazların veri depolama ünitelerini imha etmek için hangi yöntemler kullanılmaktadır?
3.1.1.7	Kurum Ağı Bağlantı Noktalarında Kimlik Denetimi Yapılması	Mülakat, Sızma Testi	Port seviyesinde erişim kontrolü yapılmakta mıdır? Kurum ağına bağlanan cihazlar için 802.1x veya NAC çözümleri kullanılarak kimlik denetimi yapılmakta mıdır?
3.1.1.8	Donanım Varlıklarının Kimlik Denetimi için İstemci Sertifikalarının Kullanılması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kuruma ait güvenli ağlara bağlanan hangi donanımlar için istemci sertifikası ile kimlik doğrulaması yapılmaktadır? Sertifika, yetkilendirilmiş personel tarafından güvenli bir alanda oluşturulmakta mıdır? Sertifikanın anahtar uzunluğu, tipi (NES/NES olmayan) ve oluşturulma yöntemi seçilirken bilgi güvenliği gereksinimleri dikkate alınmakta mıdır? Oluşturulan sertifika güvenli alanda saklanmakta mıdır? Sertifika yaşam döngüsünün takibi yapılmakta mıdır?
3.1.1.9	Sabit Disk Güvenliği	Mülakat, Gözden Geçirme	Kurum tarafından temin edilen ve kullanıcı bilgisayarlarında kullanılması planlanan sabit diskleri sisteme dâhil etmek amacıyla bir süreç tanımlanmış ve uygulanmakta mıdır? Temin edilen sabit diskler, sisteme dâhil edilmeden önce hangi güvenli silme işlemlerine tabi tutulmaktadır?

3.1.2. Yazılım Varlıklarının Envanter Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.2.1	1	Yazılım Envanterinin Yönetimi	Kurumda kullanılan tüm yazılımların (işletim sistemleri, donanım yazılımları, üçüncü parti yazılımlar, uygulama yazılımları vb.) güncel bir listesi tutulmalı ve listeye yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.2.2	1	Yazılım Envanter İçeriğinin Yönetimi	Yazılım envanter yönetim araçlarında, kurum tarafından yetkilendirilen işletim sistemleri dâhil olmak üzere en az; yazılımların adı, sürümü, yayımcısı, destek alınan tedarikçi sözleşme bilgileri (bakım süresi, kapsamı vb.), lisans bilgileri ve edinim tarihi bilgileri, yazılımın yüklendiği donanımlar kayıt altına alınmalı ve izlenebilir olmalıdır. Yazılım envanter içeriğinde yapılan değişiklikler kayıt altına alınmalıdır.
3.1.2.3	1	Yazılımın Üreticisi Tarafından Desteklenmesi	Kurumun onaylı yazılım envanterine yalnızca üreticisi tarafından desteklenen yazılımlar dâhil edilmelidir. Yazılım envanterinde kayıtlı olan yazılımlar için güncelleme desteği devamlılığı sağlanmalıdır. Üreticisi tarafından sunulan destek hizmeti sona ermiş ancak iş gereksinimleri sebebi ile kullanılması gereken yazılımlar, yazılım envanterinde "üretici tarafından desteklenmeyen" olarak etiketlenmelidir.
3.1.2.4	1	Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi	Kurum tarafından onaylanmayan yazılımların kullanılmasına yönelik politika ve prosedürler oluşturulmalı ve uygulanmalıdır.
3.1.2.5	2	Yazılım Envanteri Yönetim Araçlarının Kullanımı	Kurum sistemlerindeki tüm yazılımlar için envanter yönetim araçları kullanılmalıdır. Söz konusu envanter yönetim araçları, yazılımların mevcut durumları ile ilgili raporlama yeteneğine sahip olmalıdır.
3.1.2.6	3	Yazılım ve Donanım Envanterinin Entegre Edilmesi	Yazılım ve donanım envanteri birbirleri ile entegre edilmelidir. Entegre edilen envanter merkezi olarak yönetilmelidir.
3.1.2.7	3	Beyaz Liste Yönetimi	Kurum uygulama beyaz liste yönetimi yazılımı kullanmalıdır. Uygulama tarafından en az aşağıda yer alan kısıtlamalar devreye alınmalıdır. Yalnızca onaylı yazılım kütüphanelerinin (* .dll, * .ocx, * .so vb.) yüklenmesi Yalnızca onaylı ve dijital olarak imzalanmış betik dosyalarının (* .ps1, * .py, makrolar vb.) çalıştırılması.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.2.1	Yazılım Envanterinin Yönetimi	Mülakat, Gözden Geçirme	Kurum bünyesinde detaylı ve güncel bir yazılım envanteri tutulmakta mıdır? Envanter yönetim süreci tanımlanmış mıdır? Yazılım envanterine hangi personelin erişim yetkisi bulunmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.2.2	Yazılım Envanter İçeriğinin Yönetimi	Mülakat, Gözden Geçirme	Yazılım envanterinde yazılımlara ait isim, versiyon, lisans bilgileri ve edinim tarihi gibi bilgiler tutulmakta mıdır? Yazılım envanterinde, yazılımların yüklü olduğu donanım veya sanallaştırma ortamının kaydı tutulmakta mıdır? Yazılım envanter içeriğinde yapılan değişiklikler kayıt altına alınmakta mıdır?
3.1.2.3	Yazılımın Üreticisi Tarafından Desteklenmesi	Mülakat, Gözden Geçirme	Kurumda kullanılan yazılımların üretici tarafından desteklendiği takip edilmekte midir? Desteklenmeyen yazılımlar envanterde yer almakta mıdır? Desteklenmeyen yazılımlar envanterde nasıl etiketlenmektedir?
3.1.2.4	Yazılım Envanterine Kaydedilmemiş Yazılımların Yönetimi	Mülakat, Gözden Geçirme	Kurum tarafından onaylanmayan yazılımların kullanımı ile ilgili süreç ve sistem bulunmakta mıdır?
3.1.2.5	Yazılım Envanteri Yönetim Araçlarının Kullanımı	Mülakat, Gözden Geçirme	Kurumda kullanılan yazılımların envanterini otomatik olarak oluşturmak için hangi yazılım envanter araçları kullanılmaktadır? Kullanılan yazılım envanteri yönetim aracı hangi özelliklere sahiptir?
3.1.2.6	Yazılım ve Donanım Envanterinin Entegre Edilmesi	Mülakat, Gözden Geçirme	Yazılım envanter sistemi ve donanım envanter sistemi entegre midir?
3.1.2.7	Beyaz Liste Yönetimi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama beyaz liste yönetimi için yazılım kullanılmakta mıdır? Beyaz liste yazılımı, *.dll, *.ocx gibi sadece onaylı kütüphanelerin yüklenmesine ya da *.ps1, *.py gibi sadece onaylı betiklerin çalışmasına olanak sağlamakta mıdır?

3.1.3. Tehdit ve Zafiyet Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.3.1	1	Yazılım Güncelleme Araçlarının Kullanımı	Tüm sistemlerdeki yazılımların, mevcut iş gereksinimlerini karşılayacak ve yazılım üreticisi tarafından sağlanan en kararlı ve güncel güvenlik sürümleri ile çalıştırılmakta olduğu otomatik yazılım güncelleme araçları kullanılarak kontrol edilmelidir. Otomatik yazılım güncelleme araçlarının kullanılamadığı durumlarda uzman personel tarafından manuel olarak gerekli kontroller periyodik olarak yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.3.2	1	Zararlı Yazılımların Engellenmesi	Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için politikalar/prosedürler tanımlanmalı ve işletilmelidir. Personelin beyaz listede bulunan uygulamalar haricinde uygulama kurmasının engellenmesine yönelik politika/prosedür oluşturulmalıdır. Politika/prosedürün uygulanmasını temin etmek üzere gerekli teknolojik altyapılar ve uyarı mekanizmaları aktif edilmelidir.
3.1.3.3	1	Zafiyet/Yama Yönetimi	Kurumsal uygulamaların, kurum ağının ve sistem bileşenlerinin güvenlik açıklarının zamanında tespit edilmesi için uygulanacak politikalar ve süreçler tanımlanmalıdır. Zafiyet ve yama yönetimine ilişkin değişiklikler, tanımlanmış değişiklik yönetimi süreci üzerinden kontrollü olarak gerçekleştirilmelidir.
3.1.3.4	1	Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/Uygulamaların Yalıtılması	Yüksek ve üzeri seviyede zafiyet barındıran sunucu ve uygulamalar, diğer sistemlerden fiziksel ya da mantıksal olarak izole edilmelidir. İzolasyon yapılamadığı durumlarda söz konusu sunucu ve uygulamalarda katmanlı güvenlik prensibine uygun şekilde güvenliğin artırılması sağlanmalıdır.
3.1.3.5	1	Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan programlar haricinde program kurmalarının engellenmesi için son kullanıcı hesaplarının yerel yönetici yetkileri kaldırılmalıdır. Bk. Tedbir No: 5.1.3.4
3.1.3.6	1	Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	Tespit edilen güvenlik açıklarının giderilmesi için hazırlanan aksiyon planına yönelik önceliklendirme risk analizi tabanlı yapılmalıdır.
3.1.3.7	1	Güvenlik Sıkılaştırmalarının Yapılması	Kurumsal uygulamalar (web, DNS, e-posta, FTP vb. ile diğer uygulamalar) ve kurum ağındaki bileşenler, işletim sisteminin ve paket yazılımların kurulumuyla gelen varsayılan güvenlik ayarlarıyla kullanılmamalıdır. Kullanıma alınmadan önce bilgi güvenliği gereksinimleri dikkate alınarak gerekli güvenlik sıkılaştırmaları yapılmalıdır. Bk. Bölüm 5
3.1.3.8	2	İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	Güvenlik güncellemeleri başta olmak üzere işletim sistemlerine yönelik güncellemelerin ve yamaların üreticisi tarafından bildirilen en kararlı, güncel ve güvenilir sürüm dikkate alınarak yapıldığı, otomatik yazılım güncelleme araçları ile kontrol edilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.3.9	2	Zafiyet Tarama Araçlarının Kullanımı	Kurum ağında yer alan tüm sistemler (test sistemleri de dâhil olmak üzere) güvenlik içeriği otomasyon protokolü (SCAP) uyumlu güvenlik zafiyeti tarama aracı kullanılarak periyodik olarak taranmalıdır. Güvenlik taramaları için oluşturulan hesaplar farklı bir amaç için kullanılmamalı, en az yetki ve bilmesi gereken prensibi doğrultusunda yetkilendirme yapılarak ilgili erişim kayıtları tutulmalıdır. Güvenlik taramaları için oluşturulan hesaplar düzenli olarak kontrol edilmeli ve izlenmelidir. Zafiyet tarama araçları, güvenlik açıklarına yönelik yapılan doğrulama faaliyetleri öncesi ve sonrası durumu içerecek şekilde raporlama yapmalıdır. Üretilen raporların güvenliği sağlanmalı ve raporlara sadece yetkili personel erişim sağlamalıdır.
3.1.3.10	2	Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması	Aktif bağlantı portları, servisler ve protokoller donanım ve yazılım varlık envanterinde yer alan varlıklar ile eşleştirilmelidir. Kurum sistemlerinin tümünü kapsayacak şekilde port, servis ve protokol taramaları gerçekleştirilmeli, açık ve kullanımına ihtiyaç olmayan portların tespit edilmesi durumunda alarm üreten mekanizmalar devreye alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.3.1	Yazılım Güncelleme Araçlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda kullanılan yazılımların güvenlik güncellemeleri zamanında yapılmakta mıdır? Bu güncellemelerin devreye alınıp alınmadığı, yazılım güncelleme araçları vasıtasıyla otomatik olarak kontrol edilmekte midir? Yazılım güncelleme araçlarının kullanılmadığı durumlarda güncellemelere yönelik kontroller nasıl yapılmaktadır?
3.1.3.2	Zararlı Yazılımların Engellenmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Zararlı yazılımların engellenmesi ve beyaz liste denetim yöntemi için nasıl bir süreç işletilmektedir? Beyaz liste nasıl oluşturulmuştur? Kullanıcıların yazılım yükleme yetkisi var mıdır? Kurum bilgi sistemleri altyapısında zararlı yazılımları engellemek için hangi mekanizma/yöntemler kullanılmaktadır? Kurum bilgi sistemleri altyapı bileşenlerinde hangi sıkılaştırma önlemleri devreye alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.3.3	Zafiyet/Yama Yönetimi	Mülakat, Gözden Geçirme	Zafiyet ve yama yönetimine ilişkin politikalar/süreçler tanımlanmış mıdır? İlgili politika/süreçler işletilmekte midir? Zafiyet ve yama yönetimine ilişkin değişiklikler nasıl ele alınmaktadır?
3.1.3.4	Yüksek ve Üzeri Seviyede Zafiyet İçeren Sunucu/Uygulamaların Yalıtılması	Mülakat, Güvenlik Denetimi	Yüksek ve üzeri seviyede zafiyet içeren sunucu ve uygulamalar diğer sistemlerden fiziksel ve/veya mantıksal olarak izole edilmekte midir? Yüksek ve üzeri seviyede zafiyet içeren sunucu ve uygulamaların diğer sistemlerden fiziksel ve/veya mantıksal olarak izole edilememesi durumunda hangi önlemler alınmaktadır?
3.1.3.5	Son Kullanıcıların Yetkisiz Program Ekleme/Kaldırma İşlemlerinin Engellenmesi	Mülakat, Güvenlik Denetimi	Program ekleme, kaldırma ve konfigürasyon işlemleri nasıl yapılmaktadır? Yerel yönetici hakkına sahip olan hesaplar nasıl yönetilmektedir?
3.1.3.6	Güvenlik Açıkları için Risk Analizi Tabanlı Önceliklendirme	Mülakat, Gözden Geçirme	Tespit edilen güvenlik açıklarının giderilmesi ile ilgili aksiyon planlamaları kapsamında önceliklendirme nasıl yapılmaktadır?
3.1.3.7	Güvenlik Sıkılaştırmalarının Yapılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Güvenli olarak kabul edilmeyen ve/veya varsayılan konfigürasyon ile çalışan kurumsal uygulama var mıdır? Kurumsal uygulamaları ve kurum ağındaki diğer bileşenleri devreye alma sürecinde nasıl bir sıkılaştırma süreci izlenmektedir?
3.1.3.8	İşletim Sistemi Yama Yönetimi Araçlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda kullanılan işletim sistemlerinin kritik güvenlik güncellemeleri/yamaları zamanında yapılmakta mıdır? Bu güncellemeler/yamalar yazılım güncelleme araçları vasıtasıyla otomatik olarak takip edilmekte midir?
3.1.3.9	Zafiyet Tarama Araçlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurumdaki sistemler düzenli olarak zafiyet taramalarından geçirilmekte midir? Güvenlik taramaları için oluşturulan hesaplar taramalar dışında başka faaliyetler için kullanılmakta mıdır? Bu hesapların yetkileri sadece belirli IP adreslerinden gerekli makinelere bağlanabilecek şekilde kısıtlanmış mıdır? Bu hesaplar düzenli olarak kontrol edilmekte midir? Geçmişte tespit edilen zafiyetlerin giderilip giderilmediği sonraki taramalarda kontrol edilmekte midir? Zafiyet tarama raporları nasıl muhafaza edilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.3.10	Aktif Portların, Servislerin ve Protokollerin Varlık Envanterinde Tutulması	Mülakat, Güvenlik Denetimi, Sızma Testi	Aktif bağlantı portları, servisleri ve protokolleri varlık envanterindeki donanım ve yazılım varlıklarıyla eşleştirilmekte midir? Kuruma ait sistemlerde kullanımına ihtiyaç olmayan ve onaylanmamış servislerin, port ve protokollerin çalışıp çalışmadığı kontrol edilmekte midir? Kullanımına ihtiyaç olmayan portların tespiti için düzenli tarama yapılmakta mıdır?

3.1.4. E-Posta Sunucusu ve İstemcisi Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.4.1	1	Tekrar Yayınlama (Relay) İşleminin Engellenmesi	Tekrar yayınlama (relay) işlemine, belirlenen IP adresleri dışında izin verilmemeli ve e-posta hizmet protokollerinden kullanılmayanlar kapatılmalıdır.
3.1.4.2	1	SMTP Kimlik Doğrulaması Kullanımı	E-posta gönderiminde kullanıcı adı ve parola kullanılarak kimlik doğrulaması yapılmalıdır.
3.1.4.3	1	Kurum Tarafından Onaylanan İnternet Tarayıcıları ve E-Posta İstemcilerinin Kullanımı	Kurum tarafından onaylanmış, üretici tarafından desteği devam eden kararlı ve güncel sürüme sahip internet tarayıcıları ile e-posta istemcileri kullanılmalıdır.
3.1.4.4	1	E-posta İçeriğindeki Zararlı Bağlantılara (URL) Erişimin Engellenmesi	E-posta içeriğindeki zararlı bağlantılara erişim engellenmelidir.
3.1.4.5	1	İstenmeyen E-posta (Spam) Koruması	Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste yöntemleri uygulanmalıdır.
3.1.4.6	1	Servis Dışı Bırakma Saldırıları (DoS) Koruması	E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırılarına karşı SMTP sunucusunda bağlantı sayısı sınırlama vb. yöntemler ile koruma sağlanmalıdır.
3.1.4.7	1	E-posta İçerik Kontrollerinin Yapılması	Gelen/giden tüm e-posta hesaplarına ait içerikler, istenmeyen e-postalar ve e-posta ile yayılabilecek zararlı yazılımlara karşı güvenliği sağlamak amacıyla SMTP Gateway vb. sistemler kullanılarak kontrol edilmelidir.
3.1.4.8	1	Sahte ya da Değiştirilmiş E-Postaların Engellenmesi	Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için SPF, DKIM vb. teknoloji ve standartlar kullanılmalıdır.
3.1.4.9	1	Risk İçeren İzinsiz ve/veya Çalıştırılabilir Dosya Türlerinin Engellenmesi	Kurum politikaları ile belirlenmiş olan risk içeren izinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta veya e-posta ekleri engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.4.10	1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması	Bk. Tedbir No: 3.1.5.1
3.1.4.11	1	Güvenlik Sıkılaştırmalarının Yapılması	E-posta sunucuları, varsayılan ayarlarıyla kullanılmamalı ve kullanıma alınmadan önce tüm sunucuların güvenlik sıkılaştırmaları yapılmalıdır. Bk. Bölüm 5
3.1.4.12	1	E-Posta İletişim Güvenliğinin Sağlanması	İstemci ve e-posta sunucuları arasındaki iletişimde bilinen zafiyet içermeyen güvenilir SSL/TLS sürümleri ile birlikte güvenli e-posta iletişim protokolleri (SMTPs, POP3s, IMAPs, HTTPs vb.) kullanılmalıdır. Bk. Tedbir No: 3.2.9.1
3.1.4.13	1	E-Posta Sunucu Mimarisi	E-posta sunucuları internetten gelebilecek her türlü saldırıları önlemek üzere katmanlı güvenlik tasarımı prensiplerine göre yapılandırılmalıdır.
3.1.4.14	1	Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri	Üçüncü taraflardan temin edilen e-posta hizmetlerinin güvenliği garanti altına alınmalıdır. Bk. Bölüm 4.3
3.1.4.15	2	Onaylı İnternet Tarayıcısı ve E-Posta İstemcisi Eklentilerinin Kullanımı	Sadece kurum tarafından onaylı internet tarayıcısı ve e-posta istemcisi eklentileri kullanılmalıdır.
3.1.4.16	2	E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama	E-posta istemcilerinde sadece kurum tarafından izin verilen betik kodları çalıştırılmalıdır.
3.1.4.17	2	E-Posta Alışverişlerinin Şifreli ve İmzalı Yapılması	Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmalıdır. E-posta alışverişleri şifreli ve imzalı olarak yapıldığı durumda kullanılan sertifikalar kuruma özel olarak üretilmelidir.
3.1.4.18	2	E-Posta Sunucularına Uzaktan Erişim	E-posta sunucularına uzaktan yapılacak erişimlerde çok faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır.
3.1.4.19	3	E-Posta Eklerinin Kum Havuzlarında Çalıştırılması	Kuruma dışarıdan gelen e-posta ekleri çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs, anti-malware taramaları vb.) geçirilmelidir. Bu aşamadan sonra hala kategorilendirilmemiş e-posta ekleri kum havuzunda çalıştırılmalıdır. Kum havuzu çözümlerinde dosyalar yurt içinde yerleşik olan sunucularda taranmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.4.1	Tekrar Yayınlama (Relay) İşleminin Engellenmesi	Mülakat, Güvenlik Denetimi	E-posta tekrar yayınlama (relay) işlemine belirli IP adresleri dışında izin verilmekte midir? İzin verilen IP adreslerinden oluşan liste düzenli olarak kontrol edilmekte ve güncellenmekte midir? E-posta hizmet protokollerinden kullanılmayanlar kapatılmakta mıdır?
3.1.4.2	SMTP Kimlik Doğrulaması Kullanımı	Mülakat, Güvenlik Denetimi	E-posta gönderiminde kimlik doğrulaması yapılmakta mıdır?
3.1.4.3	Kurum Tarafından Onaylanan İnternet Tarayıcıları ve E-Posta İstemcilerinin Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda kullanılan internet tarayıcıları ve e-posta istemcileri üretici tarafından desteklenmekte midir? Üretici tarafından desteği devam eden internet tarayıcıları ve e-posta istemcileri harici yazılımların kullanılması gerektiği durumlar nasıl yönetilmektedir?
3.1.4.4	E-Posta İçeriğindeki Zararlı Bağlantılara (URL) Erişimin Engellenmesi	Güvenlik Denetimi	Zararlı bağlantılara erişimi engellemek için hangi önlemler alınmaktadır?
3.1.4.5	İstenmeyen E-Posta (Spam) Koruması	Güvenlik Denetimi	Spam e-postaları engellemek üzere DNS tabanlı filtreleme ve kara liste kullanılmakta mıdır?
3.1.4.6	Servis Dışı Bırakma Saldırıları (DoS) Koruması	Güvenlik Denetimi	E-posta bombardımanı ve bağlantı temelli servis dışı bırakma saldırıları nasıl engellenmektedir?
3.1.4.7	E-Posta İçerik Kontrollerinin Yapılması	Güvenlik Denetimi	Gelen/giden tüm e-posta içerikleri nasıl kontrol edilmektedir?
3.1.4.8	Sahte ya da Değiştirilmiş E-Postaların Engellenmesi	Mülakat, Güvenlik Denetimi	Sahte ya da bütünlüğü bozulmuş e-postaların geçerli etki alanlarına sızma ihtimalini azaltmak için hangi kontroller uygulanmaktadır?
3.1.4.9	Risk İçeren İzinsiz ve/veya Çalıştırılabilir Dosya Türlerinin Engellenmesi	Mülakat, Güvenlik Denetimi	İzinsiz ve/veya çalıştırılabilir dosya türleri içeren e-posta eklerine yönelik hangi kontroller uygulanmaktadır?
3.1.4.10	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.5.1
3.1.4.11	Güvenlik Sıkılaştırmalarının Yapılması	Mülakat, Sızma Testi	E-posta sunucularına yönelik hangi güvenlik sıkılaştırma çalışmaları yapılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.4.12	E-Posta İletişim Güvenliğinin Sağlanması	Güvenlik Denetimi, Sızma Testi	İstemci ve e-posta sunucuları arasındaki iletişimde hangi protokoller kullanılmaktadır?
3.1.4.13	E-Posta Sunucu Mimarisi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	E-posta sunucu yapılandırmaları kapsamında katmanlı güvenlik tasarımı prensipleri dikkate alınmakta mıdır?
3.1.4.14	Üçüncü Taraflardan Temin Edilen E-Posta Hizmetleri	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Üçüncü taraflardan temin edilen e-posta hizmetlerinin güvenliği kapsamında hangi kontroller uygulanmaktadır?
3.1.4.15	Onaylı İnternet Tarayıcısı ve E-Posta İstemcisi Eklentilerinin Kullanımı	Mülakat, Güvenlik Denetimi	Kurum tarafından onaylanmamış internet tarayıcısı ve/veya e-posta istemcisi eklentilerinin kullanılmasını engellemeye yönelik hangi kontroller uygulanmaktadır?
3.1.4.16	E-Posta İstemcilerinde Betik Kodlarının Kullanımını Sınırlama	Mülakat, Güvenlik Denetimi	E-posta istemcilerinde betik kodlarının çalıştırılması sınırlandırılmakta mıdır?
3.1.4.17	E-posta Alışverişlerinin Şifreli ve İmzalı Yapılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Kurum politikalarına göre gizlilik dereceli bilgi/veri içeren e-posta alışverişleri şifreli ve imzalı olarak yapılmakta mıdır? Şifreli ve imzalı e-posta alışverişleri için kullanılan sertifikalar kuruma özel olarak üretilmekte midir?
3.1.4.18	E-Posta Sunucularına Uzaktan Erişim	Mülakat, Güvenlik Denetimi	E-posta sunucularına uzaktan yapılacak erişimler için hangi kontroller uygulanmaktadır?
3.1.4.19	E-Posta Eklerinin Kum Havuzlarında Çalıştırılması	Mülakat, Güvenlik Denetimi	Kuruma dışarıdan gelen e-posta eklerine yönelik hangi güvenlik analizleri yapılmaktadır? İlgili dosyalar nasıl ve nerede taranmaktadır?

3.1.5. Zararlı Yazılımlardan Korunma

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.5.1	1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi	İstemci ve sunucu sistemlerinin tamamında zararlı yazılımdan korunma uygulamaları kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmelidir.
3.1.5.2	1	Taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi	Kurumdaki tüm bilgisayarlar, taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.5.3	1	Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	Kurumdaki tüm bilgisayarlar, taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmalıdır.
3.1.5.4	1	Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması	Zararlı yazılımlardan korunma uygulaması üretici veya ilgili kurum tarafından önerilen şekilde yapılandırılmalı ve güncel tutulmalıdır.
3.1.5.5	1	İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi	Bk. Tedbir No: 5.1.1.12
3.1.5.6	2	Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması	Tüm zararlı yazılım tespitleri, merkezi yönetim ve kayıt sunucularına iletilmelidir.
3.1.5.7	3	DNS Sorgularının Kayıtlarının Tutulması	Zararlı IP adreslerine erişimin denetlenmesi için DNS sorguları kayıt altına alınmalıdır.
3.1.5.8	3	Komut Satırı Kayıtlarının Tutulması	Kurumda, kullanıcı tarafından PowerShell ve Bash gibi komut satırı kullanılarak yapılan işlemler denetlenmeli ve merkezi olarak kayıt altına alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.5.1	Zararlı Yazılımdan Korunma Uygulamalarının Kullanılması ve Merkezi Olarak Yönetilmesi	Mülakat, Güvenlik Denetimi	Kurum bünyesinde hangi zararlı yazılımdan korunma uygulamaları kullanılmaktadır? Zararlı yazılımdan korunma uygulamalarına ait politikalar merkezi olarak yönetilmekte midir?
3.1.5.2	Taşınabilir Disklerin Zararlı Yazılım Taramalarından Geçirilmesi	Mülakat, Güvenlik Denetimi	Kurumdaki tüm bilgisayarlar taşınabilir diskleri otomatik olarak zararlı yazılım taramasından geçirecek şekilde yapılandırılmakta mıdır?
3.1.5.3	Cihazların Otomatik Kod Çalıştırmasına İzin Vermemesi	Mülakat, Güvenlik Denetimi	Kurumdaki tüm bilgisayarlar taşınabilir ortamlarda otomatik kod çalıştırılmasına izin vermeyecek şekilde yapılandırılmakta mıdır?
3.1.5.4	Zararlı Yazılımdan Korunma Uygulamalarının Yapılandırılması ve Güncel Tutulması	Mülakat, Güvenlik Denetimi	Kurumda kullanılan zararlı yazılımdan korunma uygulamaları, üreticisi veya ilgili kurum tarafından önerilen şekilde yapılandırılmış mıdır? Yazılımın imza veri tabanı düzenli aralıklarla güncellenmekte midir?
3.1.5.5	İşletim Sistemlerinin Güvenlik Mekanizmalarının Etkinleştirilmesi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 5.1.1.12

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.5.6	Zararlı Yazılımdan Korunma Uygulamalarına Ait Kayıtların Merkezi Olarak Tutulması	Mülakat, Güvenlik Denetimi	Kurumda tespit edilen zararlı yazılım bilgileri merkezi yönetim ve kayıt sunucularına iletilmekte midir?
3.1.5.7	DNS Sorgularının Kayıtlarının Tutulması	Gözden Geçirme	Kurumda DNS sorguları kayıt edilmekte midir?
3.1.5.8	Komut Satırı Kayıtlarının Tutulması	Gözden Geçirme	Kurumda, PowerShell ve Bash gibi komut satırından yapılan şüpheli işlemler denetlenmekte midir? Bu işlemler merkezi olarak kayıt altına alınmakta mıdır?

3.1.6. Ağ Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.1	1	Ağ Topolojisi	Kurum ağlarına ait topolojiler güvenli bir şekilde tutulmalı ve güncelliği kontrol edilmelidir.
3.1.6.2	1	Ağ Cihazlarının Güvenli Konfigürasyonu	Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmalıdır. Varsayılan parola ve kullanıcı adları değiştirilmelidir. Ağ altyapısındaki cihazlar ağ üzerinden yönetilebilir olmalıdır. Yönetimsel erişimlerde komut satırına, konsol erişimine parola ile giriş sağlanmalıdır. Güvenli protokoller ile yönetimsel işlemler gerçekleştirilmelidir.
3.1.6.3	1	Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	Tüm ağ cihazlarında güvenlikle ilgili güncellemelerin üretici tarafından yayımlanan kararlı ve güncel sürümü kullanılmalıdır.
3.1.6.4	1	Kara Liste veya Beyaz Liste Kullanımı	Kara liste veya beyaz liste kullanılarak varlıkların ağ erişimleri sınırlandırılmalıdır.
3.1.6.5	1	İzin Verilmeyen Trafiğin Engellenmesi	Kurum ağ sınırlarından sadece izin verilen kaynaklardan izin verilen hedeflere, izin verilen port ve protokoller ile trafiğin akışı sağlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.6	1	Ağların İzole Edilmesi	Kablolu ve kablosuz ağlar, bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmalıdır. Yalnızca yetkili sistemlerin, belirli sorumluluklarını yerine getirmek amacıyla gerekli diğer sistemlerle iletişim kurabilmelerini sağlamak için oluşturulan LAN/VLAN'lar arasında erişim denetimi yapılmalıdır. İstemcilerin yer aldığı ağlar ile sunucu/uygulamaların yer aldığı ağlar ayrılmalıdır. Sunucu ağında istemci yer almamalıdır. Yönetimsel işlemler için ayrı yönetim ağları kullanılmalıdır.
3.1.6.7	1	DoS/DDoS Koruması	Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarına karşı servis dışı kalmasını önlemek, iş sürekliliğini sağlamak amacıyla en az aşağıdaki önlemler alınmalıdır. • Güvenlik ürünleri üzerinde DoS/DDoS saldırılarına özel konfigürasyonların yapılması • DDoS engelleme sistemlerinin sınırları ve yeteneklerinin düzenli aralıklarla test edilmesi ve sürekli iyileştirilmesi/güncellenmesi • DDoS koruma için bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınması, tedarik şartname ve sözleşmelerinde bu hususların belirtilmesi
3.1.6.8	1	İnternet Ortamından Kurum İçi Kaynaklara Erişim	İnternet ortamından kurum içi kaynaklara kontrol dışı erişim engellenmelidir. İnternet ortamından kurum içi kaynaklara erişim gerekli ise VPN teknolojileri kullanılmalıdır. Uzaktan erişimlerin kurum politika ve prosedürlerine uygun olarak, kısıtlı süre ve yetkilerle yapılması sağlanmalıdır.
3.1.6.9	1	Kablosuz Erişim Noktalarının Envanterinin Tutulması	Kurum ağına bağlı yetkili kablosuz erişim noktalarının envanteri tutulmalı ve güncelliği sağlanmalıdır.
3.1.6.10	1	Misafir Ağı Yönetimi	Kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilmiş bir misafir ağı oluşturulmalıdır. Misafirlerin, misafir ağına bağlanmaları öncesinde kimlik bilgilerini doğrulayan mekanizmalar devreye alınmalı ve misafirler tarafından misafir ağı üzerinden yapılan tüm erişimler kayıt altına alınmalıdır. Misafir cihazlarının yalnızca misafir ağına erişimleri mümkün kılınmalıdır.
3.1.6.11	1	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Tüm sunucu ve istemcilerde yerel güvenlik duvarı yapılandırılmalıdır. Bu yapılandırma en az yetki prensibi göz önüne alınarak yapılmalıdır. Yapılandırma varsayılan reddetme (default deny) kuralını içermelidir. Tüm açık portlara ilişkin güvenlik duvarı kuralları yazılmalıdır.
3.1.6.12	1	IP Telefon Kullanımı	IP telefon kullanılması durumunda ilgili sistem, altyapı sağlayıcısı veya kurum tarafından güvenlik duvarları ile korunmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.13	1	IP Telefon Sistemlerine Ait İz Kayıtlarının Tutulması	IP telefon sistemlerinin iz kayıtları tutulmalıdır. İlgili kayıtlar düzenli aralıklarla bir sunucuda yedeklenmelidir. Bk. Tedbir No: 3.1.8.1
3.1.6.14	1	IP Telefon Kullanımında Parola Politikası	IP telefon sisteminde kullanılacak parolalar güçlü olmalı ve periyodik olarak güncellenmelidir. Bk. Tedbir No: 3.2.1.8
3.1.6.15	2	Ağ Erişim Denetimleri	Bk. Tedbir No: 3.1.1.7
3.1.6.16	2	Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi	Kurum ağ cihazlarına ait güvenlik yapılandırmaları; ağ trafiğini düzenleyen kurallara ait tanımlar, kullanılma amacı ve kuralı tanımlayan kişi bilgisi yer alacak şekilde dokümante edilmeli ve güncelliği sağlanmalıdır.
3.1.6.17	2	Ağ Paketlerinin Kaydedilmesi	Kurum tarafından gerekli görülen durumlarda, belirlenen kaynak(lar) ve hedef(ler) arasındaki tüm ağ trafiğinin izlenebilmesi için (pcap vb. formatlarda tüm ağ paketlerinin alınabilmesi) kayıt mekanizmaları oluşturulmalıdır. İhtiyaç duyulması durumunda (güvenlik ihlali, şüpheli ağ trafiği vb.) bu mekanizmalar kullanılarak kurum tarafından belirlenen zaman aralığında ilgili trafik kaydı incelenebilmelidir.
3.1.6.18	2	Ağ Sınır Cihazlarında Kayıt Tutulması	Ağ sınır cihazlarındaki bağlantı trafiği, kullanıcı işlemleri gibi bilgiler kayıt altına alınmalıdır.
3.1.6.19	2	Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	Saldırıları tespit etmek ve engellemek için ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmalıdır.
3.1.6.20	2	Uygulama Katmanında Filtreleme Yapılması	İnternetten gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek için uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmelidir.
3.1.6.21	2	Ağ Tabanlı URL Filtreleri Kullanımı	Kurumdaki sistemlerin, kurum tarafından onaylanmayan ve mevzuat gereği erişimi yasak olan web sitelerine bağlanmasını engelleyen ağ tabanlı URL filtreleri uygulanmalıdır.
3.1.6.22	2	URL Kategori Hizmeti Kullanımı	URL sınıflandırma servisleri kullanılmalıdır. Bu servislerin kullandığı listeler güncel tutulmalıdır. Kategorilendirilmemiş siteler varsayılan olarak engellenmelidir.
3.1.6.23	2	URL'lerin Kayıt Altına Alınması	Potansiyel olarak zararlı etkinlikleri tanımlamak ve saldırıya uğramış sistemlerin belirlenmesine yardımcı olmak için sistemlerden gelen tüm isteklere ait URL'ler kaydedilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.24	2	Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti	Kurum ağına bağlı yetkisiz kablosuz erişim noktalarının tespit edilmesini ve alarm üretilmesini sağlayan ağ tabanlı keşif araçları kullanılmalıdır.
3.1.6.25	2	İstemcilerin Kablosuz Ağ Erişimlerinin Sınırlandırılması	İstemciler, iş gereksinimleri doğrultusunda yalnızca yetkilendirilmiş kablosuz ağlara erişim sağlamalıdır.
3.1.6.26	2	Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi	Eşler arası (Peer to Peer) kablosuz ağ erişimine olanak sağlayan yöntemler (ad hoc yöntemi vb.) engellenmelidir.
3.1.6.27	2	Kablosuz Çevre Birimleri Aracılığı ile Yapılan Erişimin Engellenmesi	Cihazların, kablosuz çevre birimleri aracılığı ile yapacakları yetkisiz erişimler (bluetooth, NFC vb.) engellenmelidir.
3.1.6.28	2	Uygulama Seviyesi Saldırıların Engellenmesi	Kurum ağının uygulama seviyesi saldırılara karşı korunması için gerekli yapılar (WAF, IPS, DDoS vb.) uygun şekilde konumlandırılmalı, test edilmeli ve sürekli iyileştirilmelidir. Bu amaçla bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınmalı, tedarik şartname ve sözleşmelerinde bu hususlar belirtilmelidir.
3.1.6.29	2	IP Telefon Erişim Kontrol Listeleri	IP telefon sistemlerinde erişim kontrol listeleri kullanılmalı ve kimlik sahteciliği saldırılarına karşı önlem alınmalıdır.
3.1.6.30	3	Ağ Cihazlarının Yapılandırma Yönetimi	Ağ cihazı mevcut yapılandırmaları, onaylanmış ve olması gereken güvenlik yapılandırma içerikleri ile karşılaştırılmalı ve herhangi bir uyumsuzluk tespit edildiğinde alarm üreten mekanizmalar devreye alınmalıdır.
3.1.6.31	3	Ağ Cihazlarının Yönetimi	Ağ cihazlarının yönetimi, çok faktörlü kimlik doğrulama mekanizmaları kullanılarak şifreli ağ trafiği üzerinden yapılmalıdır. Ağ yönetimi için gerekli işlemler, bu amaç için tahsis edilen ve internet erişimi olmayan makineler üzerinden yapılmalıdır.
3.1.6.32	3	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Kuruma uzaktan bağlanacak cihazların; zararlı yazılımdan korunma, işletim sistemi ve uygulama güncelliği vb. hususlar kapsamında kurum politikalarına uygunluğu güvenli uzaktan bağlantı sağlayan sistemler üzerinden (VPN vb.) kontrol edilmelidir. Kurum politikasına uymayan cihazlara bağlantı izni verilmemelidir.
3.1.6.33	3	Kripto Ağ Cihazlarının Kullanımı	Kritik ağ ortamları arasındaki iletişim için kripto ağ cihazları kullanılmalıdır.
3.1.6.34	3	Kablosuz İletişim Güvenliği	Kritik veri kablosuz ağ üzerinde taşınırken çok faktörlü kimlik doğrulaması gerektiren kimlik doğrulama protokollerinin (EAP/TLS vb.) bilinen zafiyet içermeyen güvenilir sürümleri kullanılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.6.35	3	Kablosuz Çevre Birimleri Kullanımının Engellenmesi	Kritik veri işleyen, internete herhangi bir erişimi bulunmayan kapalı ağlarda kablosuz fare ve klavye gibi çevre birimlerinin kullanılması engellenmelidir.
3.1.6.36	3	Veri Transferi	Düzenli veri aktarımı ihtiyacı bulunan kritik seviyeli ağlarda veri diyotu, hava boşluğu şeklinde çalışan güvenli aktarım yöntemleri üzerinden tek yönlü veri aktarımı yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.1	Ağ Topolojisi	Gözden Geçirme	Kurum ağlarına ait topolojiler tutulmakta mıdır? Kurum ağlarının fiziksel ve mantıksal topolojileri dokümante edilmekte midir? Mevcut donanım ve yazılım envanteri ile ağ topolojileri eşleşmekte midir?
3.1.6.2	Ağ Cihazlarının Güvenli Konfigürasyonu	Mülakat, Güvenlik Denetimi, Sızma Testi	Ağ cihazları endüstri standartları, en iyi uygulamalar ve üretici tavsiyelerine uygun olarak yapılandırılmakta mıdır? Varsayılan parola ve kullanıcı adları kullanılmakta mıdır? Ağ altyapısındaki cihazların tamamı ağ üzerinden yönetilebilmekte midir? Komut satırı ve konsol erişimi nasıl sağlanmaktadır? Cihazların yönetimi nasıl yapılmaktadır? Cihazlara nasıl erişim sağlanmaktadır?
3.1.6.3	Ağ Cihazlarında Güvenlik Güncellemelerinin Yapılması	Mülakat, Güvenlik Denetimi	Ağ cihazları üzerinde üretici tarafından yayımlanmış kararlı ve güncel sürümlerin kullanıldığına dair kontroller nasıl yapılmaktadır?
3.1.6.4	Kara Liste veya Beyaz Liste Kullanımı	Mülakat, Güvenlik Denetimi	IP/MAC adresleri ve/veya TCP/UDP portları için beyaz liste/kara liste yapısı kullanılmakta mıdır?
3.1.6.5	İzin Verilmeyen Trafiğin Engellenmesi	Mülakat, Güvenlik Denetimi	Kurum ağ sınırlarından akan trafiğin erişim denetimi nasıl sağlanmaktadır?
3.1.6.6	Ağların İzole Edilmesi	Mülakat, Güvenlik Denetimi	Kurum ağları, bilgi güvenliği gereksinimleri doğrultusunda katmanlara ayrılmakta mıdır? Kurum ağlarına yönelik erişim denetimi nasıl yapılmaktadır? Sunucuların bulunduğu ağlar ile istemcilerin bulunduğu ağlar birbirinden ayrılmakta mıdır? Yönetimsel işlemler için ayrı yönetim ağları kullanılmakta mıdır?
3.1.6.7	DoS/DDoS Koruması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarını engellemek amacıyla hangi önlemler alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.8	İnternet Ortamından Kurum İçi Kaynaklara Erişim	Mülakat, Güvenlik Denetimi	İnternet ortamından kurum içi kaynaklara erişilmekte midir? İnternet ortamından kurum içi kaynaklara erişim için VPN teknolojileri kullanılmakta mıdır?
3.1.6.9	Kablosuz Erişim Noktalarının Envanterinin Tutulması	Mülakat, Gözden Geçirme	Kurum ağına bağlı yetkili kablosuz erişim noktalarının envanteri tutulmakta mıdır? Envanter içeriğinde hangi bilgiler yer almaktadır?
3.1.6.10	Misafir Ağı Yönetimi	Mülakat, Güvenlik Denetimi	Kurum ağı ile fiziksel ve/veya mantıksal olarak izole edilmiş bir misafir ağı oluşturulmuş mudur? Misafirlerin, misafir ağına bağlanmaları öncesinde kimlik bilgilerini doğrulayan mekanizmalar devreye alınmış mıdır?
3.1.6.11	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Mülakat, Güvenlik Denetimi	Kurum sunucu ve istemcilerinde güvenlik duvarı kullanılmakta mıdır? İzin verilenler dışındaki tüm bağlantılar varsayılan olarak reddedilmekte midir?
3.1.6.12	IP Telefon Kullanımı	Mülakat, Güvenlik Denetimi	Sistem güvenlik duvarlarıyla korunmakta mıdır? Erişim kısıtlaması yapılmış mıdır?
3.1.6.13	IP Telefon Sistemlerine Ait İz Kayıtlarının Tutulması	Mülakat, Güvenlik Denetimi	IP telefon sistemlerine ait iz kayıtları tutulmakta mıdır? İlgili kayıtlar düzenli aralıklarla yedeklenmekte midir? Alınan iz kayıtları hangi bilgileri içermektedir?
3.1.6.14	IP Telefon Kullanımında Parola Politikası	Mülakat, Güvenlik Denetimi	IP telefon sisteminde kullanılacak parolalar için nasıl bir politika tanımlanmıştır? Parolalar periyodik olarak yenilenmekte midir?
3.1.6.15	Ağ Erişim Denetimleri	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.1.7
3.1.6.16	Ağ Cihazlarına Ait Yapılandırmaların Dokümante Edilmesi	Mülakat	Kurum ağ cihazlarına ait güvenlik yapılandırmaları hangi bilgileri içerecek şekilde dokümante edilmektedir? Kurum ağ cihazlarına ait yapılandırmalar için güncellik kontrolü nasıl yapılmaktadır?
3.1.6.17	Ağ Paketlerinin Kaydedilmesi	Mülakat	Kurum tarafından gerekli görülen durumlarda, belirlenen kaynak(lar) ve hedef(ler) arasındaki ağ trafiğinin izlenebilmesi için kayıt mekanizmaları oluşturulmuş mudur?
3.1.6.18	Ağ Sınır Cihazlarında Kayıt Tutulması	Mülakat	Kurum bünyesinde yer alan ağ sınır cihazlarına ait hangi bilgiler kayıt altına alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.19	Ağ Tabanlı Saldırı Tespit/Engelleme Sistemi Kullanımı	Mülakat, Güvenlik Denetimi	Ağ tabanlı saldırı tespit ve engelleme sistemleri kullanılmakta mıdır?
3.1.6.20	Uygulama Katmanında Filtreleme Yapılması	Mülakat, Güvenlik Denetimi	İnternetten gelen veya internete giden tüm ağ trafiği, yetkisiz bağlantıları engellemek amacıyla uygulama katmanında filtreleme ve kimlik doğrulaması yapılarak iletilmekte midir?
3.1.6.21	Ağ Tabanlı URL Filtreleri Kullanımı	Mülakat, Sızma Testi	Kurumda tüm sistemler için ağ tabanlı URL filtreleme yapılmakta mıdır?
3.1.6.22	URL Kategori Hizmeti Kullanımı	Mülakat, Sızma Testi	Kurumda URL sınıflandırma servisi kullanılmakta mıdır? Bu servislerden alınan listeler periyodik olarak güncellenmekte midir? Kategorilendirilmemiş siteler varsayılan olarak engellenmekte midir?
3.1.6.23	URL'lerin Kayıt Altına Alınması	Mülakat, Güvenlik Denetimi	Kurumdaki sistemlerden gelen tüm isteklere ait URL'ler kayıt altına alınmakta mıdır?
3.1.6.24	Kurum Ağına Bağlı Kablosuz Erişim Noktalarının Tespiti	Mülakat, Güvenlik Denetimi	Kurum ağına bağlı yetkisiz kablosuz erişim noktalarını tespit etmek için hangi kontroller uygulanmaktadır?
3.1.6.25	İstemcilerin Kablosuz Ağ Erişimlerinin Sınırlandırılması	Mülakat, Güvenlik Denetimi	İstemcilerin yetkisiz kablosuz ağ noktalarına erişimi nasıl kontrol edilmektedir?
3.1.6.26	Eşler Arası Kablosuz Ağ Erişiminin Engellenmesi	Mülakat, Güvenlik Denetimi	Eşler arası (Peer to Peer) kablosuz ağ erişimi nasıl engellenmektedir?
3.1.6.27	Kablosuz Çevre Birimleri Aracılığı ile Yapılan Erişimin Engellenmesi	Mülakat, Güvenlik Denetimi	Cihazların, kablosuz çevre birimleri aracılığı ile yapacakları yetkisiz erişimler nasıl engellenmektedir?
3.1.6.28	Uygulama Seviyesi Saldırıların Engellenmesi	Mülakat, Güvenlik Denetimi	Kurum uygulamalarının uygulama seviyesi saldırılara karşı korunması için hangi önlemler alınmaktadır? Alınan önlemler kapsamında bir servis sağlayıcıdan destek alınmakta ise, ilgili tedarik şartname ve sözleşmelerinde bilgi güvenliğine yönelik hangi hususlar ele alınmaktadır?
3.1.6.29	IP Telefon Erişim Kontrol Listeleri	Mülakat, Güvenlik Denetimi	IP telefon sistemlerinde kimlik sahteciliği saldırılarına karşı hangi önlemler alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.6.30	Ağ Cihazlarının Yapılandırma Yönetimi	Mülakat, Güvenlik Denetimi	Ağ cihazlarına yönelik yapılandırma işlemleri nasıl takip edilmektedir? Ağ cihazları mevcut yapılandırmaları periyodik olarak kontrol edilmekte midir? Ağ cihazı mevcut yapılandırmalarının, onaylanmış ve olması gereken güvenlik yapılandırma içerikleri ile değişkenlik göstermesi durumunda alarm üreten mekanizmalar devreye alınmakta mıdır?
3.1.6.31	Ağ Cihazlarının Yönetimi	Mülakat, Güvenlik Denetimi	Ağ cihazlarının yönetimi kapsamında çok faktörlü kimlik doğrulama mekanizmaları kullanılmakta mıdır? Ağ cihazlarının yönetiminde güvenli iletişim protokolleri kullanılmakta mıdır? Ağ cihazlarını yönetmek için kullandığınız internete erişimi bulunmayan ayrı bir bilgisayar mevcut mudur? Bu bilgisayarlar ağ yönetimi dışında farklı amaçlar için de kullanılmakta mıdır?
3.1.6.32	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Mülakat, Güvenlik Denetimi	Kuruma uzaktan bağlanacak cihazların uymaları gereken güvenlik politikaları tanımlanmakta mıdır? Kuruma uzaktan bağlanacak cihazların kurum politikalarına uygunluğu cihaz bağlanmadan önce kontrol edilmekte midir? Kurum politikalarına uymayan cihazlara bağlantı izni verilmekte midir?
3.1.6.33	Kripto Ağ Cihazlarının Kullanımı	Mülakat, Güvenlik Denetimi	Kritik ağ ortamları arasındaki iletişim için kripto ağ cihazları kullanılmakta mıdır?
3.1.6.34	Kablosuz İletişim Güvenliği	Mülakat, Güvenlik Denetimi	Kritik veri kablosuz ağ üzerinde taşınırken hangi kimlik doğrulama protokolleri kullanılmaktadır?
3.1.6.35	Kablosuz Çevre Birimleri Kullanımının Engellenmesi	Mülakat, Güvenlik Denetimi	Kritik veri işleyen kapalı ağlarda, kablosuz fare ve klavye gibi çevre birimlerinin kullanılması engellenmekte midir?
3.1.6.36	Veri Transferi	Mülakat, Güvenlik Denetimi, Sızma Testi	Kritik seviyeli ağlarda veri aktarımı hangi yöntemler ile gerçekleştirilmektedir?

3.1.7. Veri Sızıntısı Önleme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.7.1	1	Veri Sınıflandırma Politikasının Oluşturulması	Kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar oluşturulmalıdır.
3.1.7.2	1	Servis Sağlayıcıdan Alınan Hizmetlerde Veri Güvenliği Hususları	Bulut servisleri kullanımı durumunda veri erişimi, muhafazası, kullanımı kapsamındaki güvenlik hususları servis şartname ve sözleşmelerinde belirtilmelidir.
3.1.7.3	1	Kritik Verinin Envanteri Yönetimi	Kurum bünyesinde veya dışında, kurumun teknoloji sistemleri tarafından depolanan, işlenen veya iletilen tüm kritik verinin envanteri tutulmalıdır.
3.1.7.4	1	Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması	Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler ağdan çıkarılmalıdır. Bu sistemler ihtiyaç duyulmadığı durumlarda ağ bağlantısı kesilmiş olarak tutulmalıdır.
3.1.7.5	1	Bulut Servislerinin Kullanımı	Bulut depolama ve bulut e-posta servisi kullanımında Bölüm 4.3'te ifade edilen hususlar uygulanmalıdır. Bk. Bölüm 4.3
3.1.7.6	1	Taşınabilir Ortam Yönetimi	İş ihtiyaçları gereği taşınabilir ortamların kullanılması gerektiği durumlarda, yalnızca kurum tarafından yetkilendirilmiş ve kurum envanterine kayıt edilmiş taşınabilir ortamların kullanılmasına izin verecek şekilde gerekli önlemler alınmalıdır. Bk. Tedbir Başlık No: 3.3.3
3.1.7.7	1	Ağda Kritik Veri Taşınması	Ağda kritik verinin taşınmasında güvenli protokoller kullanılmalı (VPN teknolojileri, SSL/TLS vb.) ve kritik veri şifreli olarak taşınmalıdır.
3.1.7.8	2	Ağ İçerisinde Veri Sızıntısı Önleme	Ağ içerisinde veri akışını kontrol etmek, izlemek ve izinsiz ağ trafiğini takip etmek amacıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmalıdır.
3.1.7.9	3	Durağan Veri Güvenliğinin Sağlanması	Durağan veri ortamlarında yer alan kritik veri, şifrelenerek muhafaza edilmelidir. Depolanan kritik veri kimlik doğrulama mekanizması gerektiren ikincil bir araç kullanarak şifrelenmelidir. Kritik veriyi görüntülemek veya kritik veride değişiklik yapmak için gerçekleştirilen tüm işlemler kayıt altına alınmalıdır.
3.1.7.10	3	Taşınabilir Ortam Engelleme	Kritik sistemler taşınabilir depolama birimlerini desteklemeyecek şekilde yapılandırılmalıdır. Taşınabilir depolama birimleri takıldığında uyarı üretecek mekanizmalar aktif edilmelidir. Bu uyarılar izlenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.7.1	Veri Sınıflandırma Politikasının Oluşturulması	Mülakat, Gözden Geçirme	Kurum verilerinin sistematik olarak kategorilere ayrılması ve sınıflandırılması için politikalar mevcut mudur?
3.1.7.2	Servis Sağlayıcıdan Alınan Hizmetlerde Veri Güvenliği Hususları	Mülakat, Gözden Geçirme	Servis sağlayıcının veri erişim, muhafaza ve kullanımındaki hizmet koşulları ve veri güvenliği hususları sözleşme ve tedarik şartnamelerinde nasıl ele alınmıştır?
3.1.7.3	Kritik Verinin Envanteri Yönetimi	Mülakat, Gözden Geçirme	Kuruma ait kritik verinin envanteri tutulmakta mıdır? Güncelliği nasıl kontrol altına alınmaktadır?
3.1.7.4	Düzenli Olarak Erişilmeyen Kritik Verinin ve Sistemlerin Kaldırılması	Mülakat, Güvenlik Denetimi	Kurum tarafından düzenli olarak erişilmeyen kritik veri veya sistemler kullanılmadıkları durumda ağa bağlı tutulmakta mıdır? Bu veri veya sistemler ihtiyaç duyulana kadar izole bir ağda tutulmakta mıdır?
3.1.7.5	Bulut Servislerinin Kullanımı	Mülakat, Güvenlik Denetimi	Bk. Bölüm 4.3
3.1.7.6	Taşınabilir Ortam Yönetimi	Mülakat, Güvenlik Denetimi	Kurum bünyesinde sadece kurum tarafından yetkilendirilmiş taşınabilir ortamların kullanımı nasıl kontrol altına alınmaktadır? Kurum tarafından yetkilendirilmiş taşınabilir ortamların envanteri tutulmakta mıdır?
3.1.7.7	Ağda Kritik Veri Taşınması	Mülakat, Güvenlik Denetimi	Ağda kritik veri nasıl taşınmaktadır?
3.1.7.8	Ağ İçerisinde Veri Sızıntısı Önleme	Mülakat, Güvenlik Denetimi	Ağ içerisinde veri akışını kontrol etmek ve izlemek maksadıyla ağ tabanlı veri sızıntısı önleme sistemi kullanılmakta mıdır? Kritik verinin güvenlik politikalarına uyumsuz şekilde taşındığının tespiti halinde nasıl bir aksiyon alınmaktadır?
3.1.7.9	Durağan Veri Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Durağan veri ortamlarında yer alan kritik veri nasıl muhafaza edilmektedir? Kritik veriyi görüntülemek ve bu veri üzerinde değişiklik yapmak için gerçekleştirilen işlemlere ait kayıtlar tutulmakta mıdır?
3.1.7.10	Taşınabilir Ortam Engelleme	Mülakat, Güvenlik Denetimi	Kritik sistemler taşınabilir ortamları desteklemeyecek şekilde yapılandırılmakta mıdır? Kritik sistemler kapsamında taşınabilir ortamların engellenmesine yönelik uyarı mekanizmaları devreye alınmakta mıdır?

3.1.8. İz ve Denetim Kayıtlarının Tutulması ve İzlenmesi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.8.1	1	İz ve Denetim Kayıtlarının Tutulması	Tüm sistemlerde ve ağ cihazlarında kayıt mekanizması etkin olmalıdır. Kayıtlar, bilgi güvenliği gereksinimleri ve ilgili mevzuat gereği kabul edilebilir süre boyunca cihaz üzerinde veya harici sistemlerde tutulmalı, yetkisiz erişime ve değişime karşı korunmalıdır. Kayıtlar, muhafazaları için tanımlanan kabul edilebilir sürenin sona ermesi ile birlikte güvenli bir şekilde yok edilmelidir.
3.1.8.2	1	Denetim Kayıtlarının Yönetimi	Sistem yöneticisi, operatörler ve kullanıcıların faaliyetleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.
3.1.8.3	1	Zaman Sunucusu Kullanımı	Kayıtlarda zaman damgalarının tutarlı olması için ağa bağlı tüm sistemlerin (sunucular, iş istasyonları, güvenlik ürünleri, ağ aygıtları vb.) düzenli olarak zaman bilgisinin alındığı; yedekli yapıda ve senkronize zaman sunucusu kullanılmalıdır. Bk. Tedbir No: 5.1.1.11
3.1.8.4	1	Detaylı Kayıt Tutulması	Sistem iz kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmalı ve bütünlüğü zaman damgası ile korunmalıdır.
3.1.8.5	1	Kayıtlar için Yeterli Depolama Alanı Tahsisi	Kayıt tutan sistemlerde yeterli depolama alanı tahsis edilmelidir. Depolama alanı doluluk oranı düzenli olarak kontrol edilmelidir.
3.1.8.6	2	Merkezi Kayıt Yönetimi	Analiz ve inceleme amacıyla kayıtlar merkezi bir kayıt yönetim sisteminde toplanmalı ve düzenli olarak yetkili personel tarafından gözden geçirilmelidir. Kayıt tutma veya gönderme işlemi sırasında hata oluştuğunda uyarı mekanizmaları aktif edilmeli ve izlenmelidir.
3.1.8.7	2	Kayıt Analizi Araçları Kullanımı	Siber olayların korelasyon kuralları doğrultusunda tespiti ve detaylı analizi için siber tehdit ve olay yönetim sistemleri veya kayıt analizi araçları kullanılmalıdır.
3.1.8.8	2	Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	Aksiyon alınabilecek olayların daha iyi tanımlanabilmesi ve gereksiz olayların elenebilmesi amacıyla siber tehdit ve olay yönetim sistemlerinin yapılandırması düzenli olarak gözden geçirilmelidir. Kayıtlar düzenli olarak izlenmelidir. Bk. Tedbir Başlık No: 3.1.10

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.8.1	İz ve Denetim Kayıtlarının Tutulması	Mülakat, Güvenlik Denetimi	Kurumun sistem ve ağ cihazlarının yüzde kaçında kayıt tutulmaktadır? Kayıtlar nasıl saklanmaktadır? Kayıtlar için saklama süreleri tanımlanmış mıdır? Saklama süresi sona eren kayıtlar güvenli şekilde imha edilmekte midir? Saklama süreleri ilgili varlığın tabi olduğu yasal mevzuata uygun mudur?
3.1.8.2	Denetim Kayıtlarının Yönetimi	Mülakat, Gözden Geçirme	Sistem yöneticisi, operatörler ve kullanıcıların faaliyetlerine yönelik denetim kayıtları tutulmakta mıdır? Tutulan kayıtlar düzenli olarak gözden geçirilmekte midir? Denetim kayıtları üzerinde değişiklik yapılması engellenmekte midir?
3.1.8.3	Zaman Sunucusu Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda senkronize ve yedekli zaman sunucusu kullanılmakta mıdır?
3.1.8.4	Detaylı Kayıt Tutulması	Mülakat, Güvenlik Denetimi	Kayıtlar en az; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmakta mıdır? Tutulan kayıtların bütünlüğü nasıl sağlanmaktadır?
3.1.8.5	Kayıtlar için Yeterli Depolama Alanı Tahsisi	Mülakat, Güvenlik Denetimi	Kayıtlar için yeterli depolama alanı sağlanmakta mıdır? Depolama alanı doluluk oranı düzenli olarak takip edilmekte midir?
3.1.8.6	Merkezi Kayıt Yönetimi	Mülakat, Güvenlik Denetimi	Kayıtlar merkezi bir kayıt yönetim sistemi üzerinde toplanmakta mıdır? Kayıtlar yetkili personel tarafından düzenli olarak gözden geçirilmekte midir? Kayıt tutma ve gönderme işlemi sırasında oluşan hataları takip etmek amacıyla uyarı mekanizması kullanılmakta mıdır?
3.1.8.7	Kayıt Analizi Araçları Kullanımı	Mülakat, Güvenlik Denetimi	Kurumda hangi siber tehdit ve olay yönetim sistemleri veya kayıt analiz araçları kullanılmaktadır?
3.1.8.8	Siber Tehdit ve Olay Yönetim Sistemlerinin Düzenli Yapılandırılması	Mülakat, Güvenlik Denetimi	Siber tehdit ve olay yönetim sistemlerine ait yapılandırmalar hangi aralıklarla gözden geçirilmektedir?

3.1.9. Sanallaştırma Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.9.1	1	Güncel Sürümlerin Kullanılması	Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmalıdır. Bu ürünlerin güvenliği ile ilgili duyurular takip edilmelidir.
3.1.9.2	1	Kapasite Planlaması	Gelecekteki ihtiyaçlar, yasal yükümlülükler ve olası güvenlik riskleri göz önünde bulundurularak sistem kaynaklarının planlaması yapılmalı ve kaynaklar sürekli izlenmelidir. Kapasite artırımı için kurumsal eşik değerleri tanımlanmalıdır.
3.1.9.3	1	Sanal Makinelerin Yönetilmesi	Sanallaştırma ortamında kullanılmayan sanal makineler kapatılmalı, ağdan izole edilmeli ve sanal makine görev ömrünü tamamlayınca üzerinde yer alan veriler güvenli silme yöntemleri ile imha edilmelidir.
3.1.9.4	1	İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	Kullanılmakta olan işletim sistemleri, iş gereksinimlerini karşılamak için ihtiyaç duyulan bağlantı noktaları, protokoller ve servisleri sağlayacak şekilde sıkılaştırılmalıdır. Zararlı yazılımdan korunma uygulamaları kullanılmalı, dosya bütünlüğünü izleyecek ve kayıt tutacak mekanizmalar devreye alınmalıdır. Bk. Bölüm 5.1
3.1.9.5	1	Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması	Sanallaştırma hizmetinin üçüncü taraflar aracılığıyla sunulması durumunda, sanallaştırma ortamının güvenliği garanti altına alınmalıdır. Bk. Tedbir No: 3.5.3.3 Bk. Bölüm 4.3
3.1.9.6	2	İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi	Tüm sanal makine imajlarının bütünlüğünü denetleyecek ve izleyecek mekanizmalar devreye alınmalıdır.
3.1.9.7	2	Sanal Ağ Güvenliği	Ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmalıdır. Bu yapılandırmalar düzenli olarak gözden geçirilmeli; izin verilen tüm servisler, protokoller, portlar dokümante edilmeli ve kullanım gerekçesi gösterilmelidir. Bk. Tedbir No: 3.1.6.6
3.1.9.8	2	Operasyon ve Test Ortamlarının İzolasyonu	Operasyon ve test ortamları güvenlik duvarları, alan/bölge bazlı kimlik doğrulama vb. yöntemler kullanılarak birbirinden ayrılmalı ve bu ortamların yöneticileri için görevler ayrılığı prensibi uygulanmalıdır.
3.1.9.9	2	Sanallaştırma Yönetim Ortamına Erişim	Sanallaştırma sistemleri yönetim arayüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.9.10	2	Sanallaştırma Ortamı Sertifika Yönetimi	Sanallaştırma ortamında kendinden imzalı sertifikalar yerine kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmalıdır.
3.1.9.11	2	Sanal Makineler Arası Trafiğin Kontrol Edilmesi	Sanal makineler arasındaki trafik güvenlik kontrollerinden geçirilmeli, olası zararlı trafiğin ağdaki diğer sanal ve fiziksel makinelere ulaşmaması için gerekli önlemler alınmalıdır.
3.1.9.12	2	Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	Sanallaştırma ortamları ile birlikte kullanılacak veya kurum bünyesinde müstakil olarak kullanılacak depolama ortamları ile iletişimin güvenliğinin sağlanmasında aşağıdaki hususlar dikkate alınmalıdır. • Ağ dosya paylaşım servisleri, ayrılmış depolama ağlarında veya yönlendirilemeyen ağlarda hizmet vermelidir. • Ağ dosya paylaşım servislerinde, eğer destekleniyorsa trafik şifreli olmalı, uygun kimlik doğrulama protokolleri kullanılarak erişim denetimi yapılmalı ve kayıtlar tutulmalıdır.
3.1.9.13	2	Fiziksel Kaynakların İzole Edilmesi	Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.9.1	Güncel Sürümlerin Kullanılması	Mülakat, Güvenlik Denetimi	Sanallaştırma ürünlerinin üretici tarafından desteği devam eden ve kararlı sürümleri kullanılmakta mıdır? Bu ürünlere yönelik sürüm değişiklikleri nasıl takip edilmektedir?
3.1.9.2	Kapasite Planlaması	Mülakat, Gözden Geçirme	Kaynaklara yönelik kapasite planlaması hangi kriterler göz önüne alınarak yapılmaktadır? Kapasite planları ne kadar sürede bir gözden geçirilmektedir?
3.1.9.3	Sanal Makinelerin Yönetilmesi	Mülakat, Güvenlik Denetimi	Sanallaştırma ortamında sanal makinelerin yaşam döngüsü nasıl yönetilmektedir? Kullanılmayan sanal makineler kapatılmakta mıdır? Sanal makine görev ömrünü tamamlayınca üzerindeki veriler ile ilgili nasıl aksiyon alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.9.4	İşletim Sistemi Sıkılaştırmalarının ve Güvenlik Kontrollerinin Yapılması	Mülakat, Güvenlik Denetimi	İşletim sistemleri için güvenlik sıkılaştırmaları hangi sıklıkta kontrol edilmektedir? Zararlı yazılımdan korunma uygulamaları kullanılmakta mıdır? İşletim sistemleri dosya bütünlüğü kontrolü yapmakta mıdır? İşletim sistemleri seviyesinde gerçekleşen olayların kayıtları tutulmakta mıdır?
3.1.9.5	Tedarik Edilen Sanallaştırma Hizmeti Ortam Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Servis sağlayıcıdan hizmet koşulları ile ilgili taahhüt alınmış mıdır? Sözleşmelerde ve tedarik şartnamelerinde sanallaştırma güvenliği hususları nasıl ele alınmaktadır?
3.1.9.6	İmaj Bütünlüğünün Denetlenmesi ve İzlenmesi	Mülakat, Güvenlik Denetimi	Kurumda sanal makine imajlarının bütünlüğü kontrol edilmekte midir?
3.1.9.7	Sanal Ağ Güvenliği	Mülakat, Güvenlik Denetimi	Kurumda kullanılan servisler, protokoller ve port numaraları dokümante edilmekte midir? Dokümante edilen bilgiler hangi hususları içermektedir? Bu yapılandırmalar düzenli olarak gözden geçirilmekte midir?
3.1.9.8	Operasyon ve Test Ortamlarının İzolasyonu	Mülakat, Güvenlik Denetimi	Operasyon ve test ortamları birbirlerinden izole edilmiş midir? Bu ortamların yönetimleri görevlerin ayrılığı prensibi göz önünde bulundurularak yapılmakta mıdır?
3.1.9.9	Sanallaştırma Yönetim Ortamına Erişim	Mülakat, Sızma Testi	Sanallaştırma sistemlerinin yönetimi kapsamında hangi erişim kontrolleri uygulanmaktadır?
3.1.9.10	Sanallaştırma Ortamı Sertifika Yönetimi	Mülakat, Güvenlik Denetimi	Sanallaştırma ortamında kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmakta mıdır?
3.1.9.11	Sanal Makineler Arası Trafiğin Kontrol Edilmesi	Mülakat, Güvenlik Denetimi	Sanal makineler arasındaki trafik kontrol edilmekte midir?
3.1.9.12	Depolama Ortamları ile İletişim Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Depolama ortamları kullanılmakta mıdır? Sanallaştırma ortamı ile depolama ortamları iletişim güvenliği nasıl sağlanmaktadır? Ağ dosya paylaşım servisleri hangi ağlarda konumlandırılmıştır? Ağ dosya paylaşım trafiği kritik veri içermekte midir? Ağ üzerindeki trafik şifrelenmekte midir? Erişim kayıtları tutulmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.9.13	Fiziksel Kaynakların İzole Edilmesi	Mülakat, Güvenlik Denetimi	Farklı güvenlik seviyesinde yer alan ağlarda kullanılan sanal sistemlere ait kaynaklar fiziksel olarak izole edilmekte midir?

3.1.10. Siber Güvenlik Olay Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.10.1	1	Siber Olaylara Müdahale Planlarının Hazırlanması	Siber olaylara müdahale planları; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde dokümante edilmelidir. Kurumsal SOME Kurulum ve Yönetim Rehberi'ne uygun olarak çalışmalar yürütülmelidir.
3.1.10.2	1	Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi	Siber olayların yönetimi aşamalarında görev alacak personelin rol ve sorumlulukları tanımlanmalı, olay müdahale için gerekli teknik alt yapı personele sağlanmalı ve belirlenen personel ilgili taraflara bildirilmelidir. Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olmalıdır.
3.1.10.3	1	İletişim Bilgileri Dokümanının Hazırlanması	Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı oluşturulmalı ve periyodik olarak gözden geçirilmelidir. İletişim bilgileri dokümanı, iletişim kurulacak konu kapsamında iletişim kurulacak kişileri tanımlamalıdır.
3.1.10.4	1	Siber Tehdit Bildirimlerinin Yönetilmesi	Kurumlar siber olayların tespiti için gerekli altyapıları kurmalı, SGB ve olası diğer siber tehdit istihbarat kaynaklarından alınan bildirimler doğrultusunda gerekli önlemleri almalıdır.
3.1.10.5	1	Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması	Siber olaylar ile ilgili bildirim süresi ve rapora yansıtılacak bilgiler SGB tarafından belirlenen kriterler göz önünde bulundurularak belirlenmeli ve standart hale getirilmelidir. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu, kurum standartlarına göre hazırlanmalı, üst yönetim, SGB ve varsa bağlı olduğu Sektörel SOME'ye iletilmelidir.
3.1.10.6	1	Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri	Kurumların siber olay yönetimi kapsamındaki hizmetleri üçüncü taraflardan alması durumunda hizmetin güvenliği garanti altına alınmalıdır. Bk. Tedbir No: 3.5.3.3 Bk. Bölüm 4.3

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.10.7	2	SOME Personeli için Periyodik Siber Olay Tatbikatlarının Yapılması	SOME personelinin, gerçek dünyadaki tehditlere cevap verme konusundaki yeteneklerini arttırmak için rutin tatbikatlar planlanmalı ve uygulanmalıdır. Tatbikatlar iletişim kanallarını, karar mekanizmasını ve olaylara müdahale ekibinin teknik yeteneklerini test etmelidir. Tatbikat sonrasında tatbikat sonuçları ve öğrenilmiş dersler değerlendirilmeli ve kayıt altına alınmalıdır.
3.1.10.8	3	Siber Olay Yönetimi Puanlama ve Önceliklendirme	Olaylar, kuruma potansiyel etkileri göz önünde bulundurularak puanlanmalı ve olayların giderilmesi için hazırlanan aksiyon planında önceliklendirme için risk temelli bir model kullanılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.10.1	Siber Olaylara Müdahale Planlarının Hazırlanması	Mülakat, Gözden Geçirme	Siber olaylara müdahale planları; uygulanması gereken akış, rol ve sorumlulukları içerecek şekilde dokümante edilmekte midir?
3.1.10.2	Siber Olay Yönetimi Kapsamında Görev Alacak Personelin Belirlenmesi	Mülakat, Gözden Geçirme	Siber olayların yönetimi aşamalarında görev alacak personel, rol ve sorumlulukları ile birlikte tanımlanmakta mıdır? Personele olay müdahale için gerekli teknik alt yapı sağlanmakta mıdır? Siber olay yönetimi kapsamında görev alacak personel Kurumsal SOME Kurulum ve Yönetim Rehberi kriterlerine uygun olarak belirlenmekte midir? Görev alacak personel listesi periyodik olarak gözden geçirilmekte midir?
3.1.10.3	İletişim Bilgileri Dokümanının Hazırlanması	Mülakat, Gözden Geçirme	Siber olay bildirimi yapılacak resmi kurumlara ilişkin iletişim bilgileri dokümanı mevcut mudur? İletişim bilgileri dokümanı periyodik olarak gözden geçirilmekte midir?
3.1.10.4	Siber Tehdit Bildirimlerinin Yönetilmesi	Mülakat	Siber tehdit bildirimlerinin takibi için hangi istihbarat kaynaklarından yararlanılmaktadır?
3.1.10.5	Siber Olayların Raporlarının Standardize Edilmesi ve Yayınlanması	Mülakat, Gözden Geçirme	Siber olay bildirim süresi ve bildirimde verilecek bilgiler kurum içinde standart mıdır? Siber olaylara müdahale adımları detaylı bir şekilde raporlanmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.10.6	Üçüncü Taraflardan Alınan Siber Olay Yönetim Hizmetleri	Mülakat, Güvenlik Denetimi	Siber olay yönetim hizmetlerinin tamamı kurum tarafından mı karşılanmaktadır? Üçüncü taraflardan alınan siber olay yönetim fonksiyonları hangileridir? Üçüncü tarafın söz konusu hizmetleri rehberin yönlendirdiği şekliyle sağladığı denetlenmekte midir? Sözleşme, teknik şartname vb. hizmet alım dokümanlarında bu hususlar mevcut mudur? Denetim kayıtları var mıdır?
3.1.10.7	SOME Personeli için Periyodik Siber Olay Tatbikatlarının Yapılması	Mülakat, Gözden Geçirme	Kurumda periyodik olarak siber olay tatbikatları yapılmakta mıdır? Tatbikat senaryoları dokümante edilmekte midir? Tatbikat ile hangi yeterlilikler test edilmektedir? Tatbikat sonrasında tatbikat sonuçları ve öğrenilmiş dersler değerlendirilmekte ve kayıt altına alınmakta mıdır?
3.1.10.8	Siber Olay Yönetimi Puanlama ve Önceliklendirme	Mülakat	Siber olaylar, kuruma potansiyel etkileri göz önünde bulundurularak puanlanmakta ve olayların giderilmesi için hazırlanan aksiyon planında önceliklendirme risk temelli bir model kullanılarak yapılmakta mıdır?

3.1.11. Sızma Testleri ve Güvenlik Denetimleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.11.1	1	Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi	Kurum sistemlerinin güvenlik açıklarını ve saldırı yüzeyini belirlemek için düzenli aralıklarla harici ve dâhili sızma testleri ve güvenlik denetimleri gerçekleştirilmelidir. Sızma testleri ve güvenlik denetimleri gerçekleştirilmeden önce testi gerçekleştirecek taraftan, test süresince elde edilen hiçbir verinin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınmalıdır. Sızma testi ve güvenlik denetimi kapsamı tanımlanmalı ve dokümante edilmelidir. Sosyal mühendislik testleri de sızma testi kapsamına dâhil edilmelidir.
3.1.11.2	1	Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	Sağlıklı ve gerçek hayata uygun bir sızma testi için testler sırasında anonim kullanıcılar, misafir kullanıcılar, çalışanlar, kurumdan hizmet alan kullanıcılar ve kuruma destek veren kullanıcılar gibi farklı yetki seviyesindeki kullanıcı profilleri kullanılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.11.3	1	Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	Operasyonel ortamda olup sızma testi yapılması mümkün olmayan veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmalıdır.
3.1.11.4	1	Sızma Testi için Oluşturulan Hesapların Yönetimi	Sızma testini gerçekleştirmek için kullanılan herhangi bir kullanıcı veya sistem hesabı, yalnızca meşru amaçlar için kullanıldığından emin olmak için kontrol edilmeli, izlenmeli, kayıt altına alınmalı ve test bittikten sonra pasif hale getirilmelidir.
3.1.11.5	1	Doğrulama Testlerinin Yaptırılması	Kapatılan güvenlik açıklarına yönelik doğrulama testleri görevlerin ayrılığı ilkesi doğrultusunda yapılmalıdır.
3.1.11.6	1	Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	Sızma testi ve güvenlik denetimi bulguları karşılaştırılabilir bir puanlama yöntemi dikkate alınarak raporlanmalıdır.
3.1.11.7	2	Test Ortamlarının Hazırlanması	Canlı ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için gerçeğine benzer test ortamları oluşturulmalıdır. Test ortamının oluşturulması mümkün olmayan her bir bileşen için 3.1.11.3 numaralı tedbir maddesi uygulanmalıdır.
3.1.11.8	2	Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	Sızma testleri ve güvenlik denetimleri yılda en az 1 defa yapılmalıdır.
3.1.11.9	3	Düzenli Kırmızı Takım Tatbikatlarının Yapılması	Siber saldırılara karşı kurumsal hazırlığı test etmek adına düzenli kırmızı takım tatbikatları yapılmalı veya yaptırılmalıdır. Tatbikat sonuçları kurum içi dokümante edilerek raporlanmalıdır. Rapor sonuçlarına göre kurumda gerekli iyileştirmeler sağlanmalıdır.
3.1.11.10	3	Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü	Kurum ağına eklenecek donanıma veya yazılıma, ağa dâhil edilmeden önce zafiyet taraması ve güvenlik denetimi yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.11.1	Sızma Testleri ve Güvenlik Denetimlerinin Gerçekleştirilmesi	Mülakat, Gözden Geçirme	Kurum bünyesinde sızma testleri ve güvenlik denetimleri düzenli olarak yapılmakta mıdır? Sızma testi ve güvenlik denetimleri öncesinde testi gerçekleştirecek taraftan test süresince elde edilen verilerin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınmakta mıdır? Sızma testi ve güvenlik denetimleri kapsamı tanımlanmakta ve dokümante edilmekte midir? Kurumda sızma testi yapılmadan önce tüm sistemler için zafiyet taramaları yapılmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.11.2	Sızma Testlerinin Kullanıcı Profillerine Göre Gerçekleştirilmesi	Mülakat	Sızma testleri, farklı yetki seviyesindeki bütün kullanıcı profillerini içerecek şekilde gerçekleştirilmekte midir?
3.1.11.3	Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi	Mülakat	Operasyonel ortamda olup sızma testi yapılması mümkün olmayan ve/veya yüksek risk içeren sistemler için güvenlik denetimleri ve güvenlik sıkılaştırmaları düzenli olarak yapılmakta mıdır?
3.1.11.4	Sızma Testi için Oluşturulan Hesapların Yönetimi	Mülakat, Güvenlik Denetimi	Kurumda sızma testi için kullanılan hesaplar kontrol edilmekte midir? Bu hesaplar test sonrasında pasif hale getirilmekte midir?
3.1.11.5	Doğrulama Testlerinin Yaptırılması	Mülakat, Sızma Testi	Kapatılan güvenlik açıklarının doğrulama testleri yapılmakta mıdır?
3.1.11.6	Sızma Testi ve Güvenlik Denetimi Bulgularının Seviyelendirilmesi	Mülakat, Gözden Geçirme	Sızma testi ve güvenlik denetimi bulguları standart bir şekilde raporlanmakta mıdır?
3.1.11.7	Test Ortamlarının Hazırlanması	Mülakat, Gözden Geçirme	Canlı ortamda olup test edilmesi sakıncalı sistemler için benzer test ortamları oluşturulmakta mıdır? Test ortamının oluşturulması mümkün olmayan bileşenler için nasıl bir yol izlenmektedir?
3.1.11.8	Sızma Testleri ve Güvenlik Denetimlerinin Periyodu	Mülakat, Gözden Geçirme	Sızma testleri ve güvenlik denetimleri ne kadar sürede bir gerçekleştirilmektedir?
3.1.11.9	Düzenli Kırmızı Takım Tatbikatlarının Yapılması	Mülakat, Gözden Geçirme	Kurumda düzenli aralıklarla kırmızı takım tatbikatları yapılmakta mıdır? Tatbikat sonuçları kayıt altına alınmakta ve dokümante edilmekte midir?
3.1.11.10	Kurum Ağına Eklenen Yazılımın ve Donanımın Kontrolü	Mülakat, Gözden Geçirme	Yazılım ve donanımlar kurum ağına dâhil edilmeden önce zafiyet taraması ve güvenlik denetiminden geçmekte midir?

3.1.12. Kimlik Doğrulama ve Erişim Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.1	1	Erişim Kontrol Politikasının Oluşturulması ve Uygulanması	Erişim kontrol politikaları oluşturulmalı, uygulamaya alınmalı ve güncelliği periyodik olarak kontrol edilmelidir. Kullanıcı (sistem yöneticisi ve sisteme işlem amacıyla erişen kullanıcılar) hesap işlemleri (açma, kapama, değişiklik) ve erişim talepleri tanımlı bir süreç ile takip edilmeli ve kayıt altına alınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.2	1	Kullanıcı Hesaplarının Yönetimi	Her kullanıcı için kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabı tanımlanmalı, tüm kullanıcı hesaplarına ait bir parola ataması yapılmalıdır. Kullanıcı hesaplarına ait parolalar belirlenirken dikkat edilmesi gereken kurallar tanımlanmalı ve uygulanmalıdır.
3.1.12.3	1	Başarısız Oturum Açma Denemelerinin Yönetimi	Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla uygun güvenlik önlemleri (istek sınırlandırma, IP bloklama, CAPTCHA vb.) alınmalıdır. Başarısız oturum açma denemeleri kayıt altına alınmalıdır.
3.1.12.4	1	Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi	Kurum bilgi sistemindeki herhangi bir varlıkta varsayılan kullanıcı adı ve parolalar kullanılmamalıdır. Test ortamlarında kullanımda olan tüm varsayılan kullanıcılar ve parolalar, canlıya alınmadan önce silinmeli veya değiştirilmelidir.
3.1.12.5	1	Yönetici Hesaplarının Kullanımı	Sistem yöneticilerinin yüksek haklar gerektiren işlemleri yapmak için ayrı bir hesapları olmalıdır. Yönetici hesaplarıyla yapılan işlemler için denetim kayıtları oluşturulmalıdır.
3.1.12.6	1	İşlem Yapılmayan Oturumların Sonlandırılması	İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmalıdır.
3.1.12.7	1	Kimlik Doğrulama	Kurum kaynaklarına erişimlerde kimlik doğrulama mekanizmaları kullanılmalıdır.
3.1.12.8	1	Kullanıcı Yetkilerinin Güncellenmesi	Sistem yöneticilerinin ve kullanıcılarının yetkileri düzenli olarak gözden geçirilmeli, görev değişikliklerinde erişim yetkileri güncellenmelidir. Bir personelin veya yüklenicinin sorumluluklarının değişmesinden hemen sonra hesapları devre dışı bırakmak ve sistem erişimini iptal etmek için süreç oluşturulmalı ve uygulanmalıdır. Bu hesaplar devre dışı bırakılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.9	1	Kurum Dışı Paydaşların Uzaktan Erişimi	Kurum dışı paydaşların kurum kaynaklarına uzaktan erişimine, ilgili kurum personelinin onayı dışında izin verilmemelidir. Uzaktan erişimin gerçekleştiği durumlarda ise aşağıdaki kurallar uygulanmalıdır: • Erişim yetkisi sınırlı ve belirli bir süreyle tanımlanmalıdır. Oturum zaman aşımı süresi belirlenmeli ve süre sonunda kullanıcı kimlik doğrulamaya zorlanmalıdır. • Çok faktörlü kimlik doğrulama metotları aktif edilmelidir. • Erişimin gerçekleştiği hedefler ile erişimin yapıldığı kaynaklar için kısıtlama yapılmalıdır. • Erişimlere ilişkin iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1 • Herhangi bir anomali ve ihlal durumuna karşın gerekli izleme ve alarm mekanizmaları aktifleştirilmelidir. • Gerektiği durumlarda video kayıt ve personel gözetimi metotları işletilmelidir. • Erişim yolu şifreli ve güvenli olmalıdır.
3.1.12.10	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	Belirli bir süre kullanılmayan, bir iş süreci veya kurum personeli ile ilişkilendirilemeyen tüm hesaplar otomatik olarak devre dışı bırakılmalıdır.
3.1.12.11	2	Yönetici Hesaplarının İşletimi	Etki alanı ve yerel hesaplar dâhil tüm yönetim hesaplarını yönetmek için otomatik araçlar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabı oluşturulduğunda veya silindiğinde kayıt tutacak ve alarm oluşturacak şekilde yapılandırılmalıdır. Tüm yönetici hesap erişimleri için çok faktörlü kimlik doğrulama ve şifreli kanallar kullanılmalıdır. Kurumdaki sistemler bir yönetici hesabından giriş denemesi yapıldığında kayıt tutmalı ve giriş denemesi yapılması durumunda alarm oluşturacak şekilde yapılandırılmalıdır.
3.1.12.12	2	Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	Betik dosyası oluşturma araçlarına (PowerShell ve Python gibi) erişim, yalnızca iş amaçları doğrultusunda bu özelliklere erişmesi gereken hesaplar ile sınırlandırılmalıdır.
3.1.12.13	2	Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik doğrulama sistemlerinin ve bu sistemlerle entegre uygulamaların envanteri tutulmalıdır.
3.1.12.14	2	Merkezi Kimlik Doğrulama	Kimlik doğrulama merkezi olarak yapılmalıdır. Merkezi kimlik yönetim ve doğrulama sisteminin kullanılamadığı durumlarda, risk analizi çalışması doğrultusunda telafi edici önlemler alınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.12.15	2	Çok Faktörlü Kimlik Doğrulama Yapılması	Kurum ağına dışarıdan yapılan erişimler çok faktörlü kimlik doğrulaması ile sağlanmalıdır.
3.1.12.16	2	Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması	Tüm kimlik doğrulama bilgileri güçlü kriptografik algoritmalar kullanılarak saklanmalı ve şifreli kanallar kullanılarak iletilmelidir.
3.1.12.17	2	Servis Hesaplarının Yönetimi	Servis hesapları en az yetki prensibi göz önünde bulundurularak oluşturulmalıdır. Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmamalıdır. Servis hesaplarının kurum içerisinde bir sahibi olmalı ve periyodik olarak gözden geçirilmelidir.
3.1.12.18	3	Hesap Giriş Davranışlarında Değişikliklerin Saptanması	Kullanıcı davranışları, kullanıcı rolü ve yetki seviyesi değişiklikleri güvenlik ihlal durumlarına karşı izlenmeli ve alarm mekanizmaları devreye alınmalıdır.
3.1.12.19	3	Oturum Kayıtlarının Tutulması	Gizlilik dereceli verilerin saklandığı/işlendiği sistemler üzerinde sistem yönetimi amacıyla açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınmalı ve alınan kayıtların doğrulaması yapılmalıdır.
3.1.12.20	3	Sistem Yöneticisi Görevlerinin Güvenliği	Tüm sistem yöneticisi görevleri belirli IP adresleri kullanılarak yapılmalıdır. Yönetim işlemlerini gerçekleştiren sistem yöneticileri, sadece yönetimsel haklar gerektiren işler için ilgili hesapları kullanmalıdır. Yetkilendirmelerin senede en az 1 kez olacak şekilde gözden geçirilmesi, gereksinimi kalmamış yetkilerin geri alınması sağlanmalıdır.
3.1.12.21	3	Veri ve Parola Güvenliğinin Sağlanması	Veri ve parolaların güvenliğinin sağlanması gerektiğinde otomatik parola yönetim aracı (password vault) kullanılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.12.1	Erişim Kontrol Politikasının Oluşturulması ve Uygulanması	Mülakat, Gözden Geçirme	Erişim kontrol politikaları oluşturulmakta mıdır? Politika kapsamında kullanıcı hesap işlemleri ve erişim taleplerinin yönetilmesine ilişkin nasıl bir süreç tanımlanmaktadır?
3.1.12.2	Kullanıcı Hesaplarının Yönetimi	Mülakat, Güvenlik Denetimi	Kullanıcı hesaplarının yönetimine ilişkin hangi bilgi güvenliği kontrolleri uygulanmaktadır?
3.1.12.3	Başarısız Oturum Açma Denemelerinin Yönetimi	Mülakat, Sızma Testi	Oturum açma mekanizmasına yapılacak saldırıları engellemek amacıyla hangi güvenlik önlemleri alınmaktadır? Başarısız oturum açma denemeleri kayıt altına alınmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.12.4	Varsayılan Kullanıcıların ve Parolaların Değiştirilmesi	Mülakat, Sızma Testi	Kurum bilgi sistemlerinde yer alan varlıkların varsayılan parolaları değiştirilmekte midir? Test çalışmalarında varsayılan parolalar değiştirilmekte midir? Kullanılmayan varsayılan hesaplar silinmekte midir?
3.1.12.5	Yönetici Hesaplarının Kullanımı	Mülakat, Sızma Testi	Kurumda sistem yöneticileri, yönetimsel işlemler için ayrı bir hesap kullanmakta mıdır? Yöneticiler hedef cihazlara nasıl erişim sağlamaktadırlar?
3.1.12.6	İşlem Yapılmayan Oturumların Sonlandırılması	Mülakat, Sızma Testi	İşlem yapılmayan oturumlar belirli bir süre sonra sonlandırılmakta mıdır?
3.1.12.7	Kimlik Doğrulama	Mülakat, Sızma Testi	Kurum kaynaklarına erişimlerde hangi kimlik doğrulama mekanizmaları kullanılmaktadır?
3.1.12.8	Kullanıcı Yetkilerinin Güncellenmesi	Mülakat, Gözden Geçirme	Sistem yöneticilerinin ve kullanıcılarının hakları düzenli aralıklarla gözden geçirilmekte midir? Kimlik doğrulama sistemi tarafından düzenlenen tüm hesapların envanteri tutulmakta mıdır? Görevi sona eren hesaplar devre dışı bırakılmakta mıdır? Bu işlem için otomatik bir süreç oluşturulmuş mudur? Devre dışı bırakılan hesaplara yapılan erişim denemeleri izlenip, kayıt altına alınmakta mıdır?
3.1.12.9	Kurum Dışı Paydaşların Uzaktan Erişimi	Mülakat, Güvenlik Denetimi	Kurum dışı paydaşların kurum sistemlerine uzaktan erişimi kapsamında hangi güvenlik kontrolleri uygulanmaktadır?
3.1.12.10	Kullanılmayan Hesapların Devre Dışı Bırakılması	Mülakat, Güvenlik Denetimi	Bir iş süreci veya kurum çalışanı ile ilişkilendirilemeyen tüm hesaplar devre dışı bırakılmakta mıdır?
3.1.12.11	Yönetici Hesaplarının İşletimi	Mülakat	Kurumda yönetim hesaplarının envanteri tutulmakta mıdır? Bu işlem otomatik araçlarla mı yapılmaktadır? Yönetici hesap erişimleri nasıl yapılmaktadır?
3.1.12.12	Betik Dillerinin Kullanımına Yönelik Erişimin Sınırlandırılması	Mülakat, Güvenlik Denetimi	Kurum bilgisayarlarında betik çalıştırma yetkisi hangi kullanıcılara verilmektedir?
3.1.12.13	Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	Mülakat, Gözden Geçirme	Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik sağlayıcılarının envanteri tutulmakta mıdır?
3.1.12.14	Merkezi Kimlik Doğrulama	Mülakat, Güvenlik Denetimi, Sızma Testi	Kurum mümkün olan tüm durumlarda kimlik denetimini merkezi olarak yapmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.12.15	Çok Faktörlü Kimlik Doğrulama Yapılması	Mülakat, Güvenlik Denetimi	Kurum tarafından yapılan kimlik denetimlerinde çok faktörlü kimlik doğrulama mekanizmasının uygulanmadığı yerler var mıdır?
3.1.12.16	Kimlik Doğrulama Bilgilerinin Güvenli Olarak Saklanması	Mülakat, Güvenlik Denetimi	Kimlik doğrulama bilgilerinin saklanmasına yönelik hangi güvenlik önlemleri alınmaktadır? Kurumun tüm kimlik doğrulama bilgileri şifreli kanallar üzerinden iletilmekte midir? Alınan önlemler yetkili kurumlarca test edilmiş midir?
3.1.12.17	Servis Hesaplarının Yönetimi	Mülakat, Güvenlik Denetimi	Servis hesapları erişim yetkileri nasıl tanımlanmaktadır? Servis hesaplarına yönelik gözden geçirme süreci nasıl işletilmektedir? Kullanıcı veya yetkili hesaplar servis hesabı olarak kullanılmakta mıdır?
3.1.12.18	Hesap Giriş Davranışlarında Değişikliklerin Saptanması	Mülakat	Kullanıcı hesap giriş davranışları düzenli olarak izlenmekte midir? Kullanıcı rolü ve yetki seviyesi değişiklikleri gibi durumlarda alarm oluşturulmakta mıdır?
3.1.12.19	Oturum Kayıtlarının Tutulması	Mülakat, Güvenlik Denetimi	Gizlilik dereceli verilerin saklandığı/işlendiği sistemler üzerinde açılan oturumlar sırasında gerçekleştirilen faaliyetler kayıt altına alınmakta mıdır? Alınan kayıtların doğrulaması nasıl yapılmaktadır?
3.1.12.20	Sistem Yöneticisi Görevlerinin Güvenliği	Mülakat, Güvenlik Denetimi	Tüm yönetimsel görevler yönetim dışı faaliyetler için kullanılmayan belirli bilgisayarlar üzerinden mi yapılmaktadır? Yetkilendirmeler periyodik olarak gözden geçirilmekte midir?
3.1.12.21	Veri ve Parola Güvenliğinin Sağlanması	Mülakat, Sızma Testi	Veri ve parolaların güvenliği için otomatik parola yönetim aracı (password vault) kullanılmakta mıdır?

3.1.13. Felaket Kurtarma ve İş Sürekliliği Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.13.1	1	Yedekleme Planının Oluşturulması	Kurum bünyesinde iş süreçlerinde kullanılan ve iş süreçlerini destekleyen tüm sistemler göz önünde bulundurularak yedekleme ihtiyacı olan sistemler tespit edilmeli ve dokümante edilmiş bir yedekleme planı üzerinden yedekleme yönetimi yapılmalıdır. Yedekleme planı en az aşağıdaki başlıkları içerecek şekilde oluşturulmalıdır: • Yedeği alınan sistemler • Yedekleme işleminin adı • Yedekleme işlemi başlangıç tarih ve saat bilgisi • Yedekleme tipi • Yedekleme periyodu • Yedekleme süreçlerinde versiyonlama
3.1.13.2	1	Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi	Yedekleme planı, yedekleme ihtiyaçları göz önünde bulundurularak yılda en az bir kere gözden geçirilmelidir. Bu gözden geçirme kapsamında iş birimleri ile de görüşülerek yedekleme ihtiyacı ortadan kalkan sistemler tespit edilmeli, yedekleme işleminden çıkarılmalı ve yedekleme işleminde olmayan fakat dâhil edilmesi gereken sistemler tespit edilerek yedekleme işlemine dâhil edilmelidir.
3.1.13.3	1	Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması	Yedekleme işlemlerine ilişkin iz kayıtları oluşturulmalı, bu kayıtlar bilgi güvenliği gereklilikleri ve ilgili mevzuat göz önünde bulundurularak tanımlanmış süre kadar tutulmalı ve zaman damgası ile korunmalıdır. Bk. Tedbir No: 3.1.8.1
3.1.13.4	1	Yedekten Geri Dönüş Testleri	Yedekleme ortamlarının çalıştığından ve geri dönülebilir olduğundan emin olmak adına; kapsamdaki sistemlerin, uygulamaların ve verinin yedekleri düzenli olarak geri dönüş testlerine tabi tutulmalı ve gerçekleştirilen geri dönüş testlerine yönelik kayıtlar oluşturulmalıdır. Bu kayıtlar en az aşağıdaki bilgileri içermelidir: • Testin gerçekleştirildiği gün ve saat bilgisi • Testi yapılan sistemler • Testin gerçekleştirildiğini kanıtlayan ekran görüntüleri • Testin başarılı sonuçlanıp sonuçlanmadığı • Test sırasında karşılaşılan sorunlar ve çıkarılan dersler.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.13.5	1	Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası	Yedekleme medyalarının envanteri tutulmalı ve envanter periyodik olarak gözden geçirilmelidir. Yedekleme medyaları, fiziksel olarak güvenli ve yedek alınan bölgeden farklı bir konumda saklanmalıdır. Yedeklenen verinin; ana sistemlerin bulunduğu ortamla benzer riskleri içermeyen başka bir ortamda saklandığı teyit edilmelidir. Yedeklenen veri tesis/yerleşke dışına taşınırken güvenliğinin sağlandığı ve bulunduğu ortamın fiziksel ve mantıksal güvenliğinin sağlanmış olduğu teyit edilmelidir. Yedekler kullanım süresinin sona ermesi sonrasında ulusal/uluslararası standartlara uygun olarak güvenli bir şekilde imha edilmeli ve imha kayıtları tutulmalıdır.
3.1.13.6	2	İş Sürekliliği Kapsamının Tanımlanması	Kurumun faaliyet alanı ile yasal ya da sözleşmelerden doğan yükümlülükleri de göz önünde bulundurularak iş sürekliliği çalışmaları kapsamında ele alınması gereken hizmetler, birimler ve lokasyonlar tanımlanmalıdır.
3.1.13.7	2	İş Sürekliliği Planlarının Hazırlanması	Kapsam dâhilinde yer alan hizmetler, birimler ve lokasyonlar göz önünde bulundurularak iş sürekliliği planları hazırlanmalı ve belirli aralıklarla gözden geçirilmelidir.
3.1.13.8	2	İş Sürekliliği Kapsamında Rol ve Sorumlulukların Tanımlanması	İş sürekliliği kapsamında olan tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
3.1.13.9	2	İş Sürekliliği Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	İş sürekliliği planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile birlikte tedarik edilen hizmetlerin süreklilik kriterleri de dikkate alınmalıdır.
3.1.13.10	2	İş Sürekliliği Planlarının Test Edilmesi	Süreklilik yönetimi dâhilinde tüm planlar kurum tarafından belirlenen periyotlarda test edilmeli ve test sonuçları kayıt altına alınmalıdır.
3.1.13.11	2	İş Sürekliliği Planlarının Güvenli Muhafazası	Süreklilik yönetimi dâhilindeki planların, acil durum müdahale prosedürlerinin ve gerekli diğer dokümanların güncel versiyonlarının kurumun yerleşkesi içinde ve mümkünse kurum binası dışında belirlenecek bir yerde tutulması ve her türlü felaket senaryosu sırasında erişilebilir olması sağlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.13.12	2	Felaket Kurtarma Planlarının Hazırlanması	İş sürekliliği planları göz önünde bulundurularak kritik bilgi sistemleri bileşenlerine yönelik felaket kurtarma planları oluşturulmalıdır. Plan içerisinde aşağıdaki konular göz önünde bulundurulmalıdır: • Felaket kurtarma planı yapılan yerleşkenin felaket kurtarma merkezinde manuel olarak devreye alınması için gerekli minimum envanter gereksinimi • Felaket sonrası normale dönüş planı kapsamında uygulanacak adımlar • Felaket sonrası adı geçen servise ait verinin aktarma işlemi tamamlandığında kabul edilebilir kayıp veri miktarı ve niteliği, maksimum kesinti süresi ile yedekten geri dönüş süresi
3.1.13.13	2	Felaket Kurtarma Planları Kapsamında Rol ve Sorumlulukların Tanımlanması	Felaket kurtarma planlarının devreye alınması aşamasında yer alacak tüm paydaşların ve süreç içinde yer alacak personelin görev ve sorumlulukları dokümante edilmeli ve ilgili taraflara bildirilmelidir.
3.1.13.14	2	Felaket Kurtarma Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Felaket kurtarma planları kapsamında; hizmet alınan üçüncü tarafların rol ve sorumlulukları ile tedarik edilen hizmetlerin sürekliliği dikkate alınmalıdır.
3.1.13.15	2	Felaket Kurtarma Planlarının Test Edilmesi	Felaket kurtarma çalışmaları dâhilindeki tüm planlar yılda en az bir kez test edilmeli ve test sonuçları kayıt altına alınmalıdır.
3.1.13.16	2	Felaket Kurtarma Planlarının Güvenli Muhafazası	Felaket kurtarma çalışmaları dâhilindeki planların güncel versiyonları her türlü felaket senaryosu sırasında erişilebilir olmalıdır.
3.1.13.17	3	Kritik Sistem Sürekliliğinin Sağlanması	Kurum tarafından kritik olarak belirlenen sistem, servis, uygulama ve altyapının hizmet sürekliliğini sağlamak amacıyla gerekli yedeklilik yapıları oluşturulmalıdır. Hizmetler devreye alınırken yedeklilik testleri yapılmalıdır. Hizmet seviye taahhütleri oluşturulmalı, ölçülmeli ve raporlanmalıdır.
3.1.13.18	3	Felaket Kurtarma Merkezi Oluşturulması	Herhangi bir felaket anında bilgi sistemleri işlevlerinin sürdürülebilmesi için bir felaket kurtarma merkezi kurulmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.13.1	Yedekleme Planının Oluşturulması	Mülakat, Gözden Geçirme	Yedekleme ile ilgili nasıl bir süreç işletilmektedir? Yedeği alınacak sistemler nasıl belirlenmektedir? Yedekleme ihtiyaçlarının belirlenmesine yönelik hangi çalışmalar yapılmaktadır? Yedekleme planları oluşturulmakta mıdır? Yedeklemelerin hangi sıklıkta alınacağı nasıl belirlenmektedir?
3.1.13.2	Yedekleme Planının Periyodik Olarak Gözden Geçirilmesi	Mülakat, Gözden Geçirme	Yedekleme planları yılda en az bir kere gözden geçirilmekte midir? Yapılan gözden geçirmeler kayıt altına alınmakta mıdır? Planların gözden geçirilmesi çalışmaları için iş birimlerinden geri dönüş alınmakta mıdır?
3.1.13.3	Yedekleme İşlemleri için İz Kayıtlarının Oluşturulması	Mülakat, Gözden Geçirme	Yedekleme işlemlerine yönelik iz kayıtları tutulmakta mıdır? İz kayıtları yedekleme işlemlerine yönelik hangi bilgileri içermektedir? İz kayıtları ne kadar süre tutulmaktadır? İz kayıtları zaman damgası ile korunmakta mıdır?
3.1.13.4	Yedekten Geri Dönüş Testleri	Mülakat, Gözden Geçirme	Yedekten geri dönüş testleri yapılmakta mıdır? Geri dönüş testlerine yönelik bir zaman planı hazırlanmakta mıdır? Geri dönüş testlerinin kapsamı nasıl belirlenmektedir? Geri dönüş testlerine yönelik oluşturulmuş kayıtlar nelerdir?
3.1.13.5	Yedekleme Medyalarının Saklanması, Güvenliği ve İmhası	Mülakat, Gözden Geçirme	Yedekleme medyalarına ait envanter bulunmakta mıdır? Envanter belirli aralıklara gözden geçirilmekte midir? Yedekleme sistemi, yedekleme ile ilgili kasetler ve sunucu nerede bulunmaktadır? Kullanım ömrünü tamamlamış olan yedekler nasıl imha edilmektedir?
3.1.13.6	İş Sürekliliği Kapsamının Tanımlanması	Mülakat, Gözden Geçirme	Hangi sistemler iş sürekliliği planları kapsamında yer almaktadır? Kapsama alınacak sistemler nasıl belirlenmektedir?
3.1.13.7	İş Sürekliliği Planlarının Hazırlanması	Mülakat, Gözden Geçirme	İş sürekliliği ile ilgili planlar hazırlanmış ve belirli aralıklarla gözden geçirilmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.13.8	İş Sürekliliği Kapsamında Rol ve Sorumlulukların Tanımlanması	Mülakat, Gözden Geçirme	İş sürekliliği planı hazırlanırken rol ve sorumluluklar tanımlanmakta mıdır? İş sürekliliği planlarında yer alan kilit personel kimlerdir? Bu personelin bulunmaması durumunda yedek personel tanımlaması yapılmış mıdır? Acil durumlar için kimlerin aranacağına ve kimlerle iletişim kurulacağına yönelik bir iletişim listesi var mıdır? Bu liste hangi sıklıkla gözden geçirilmektedir?
3.1.13.9	İş Sürekliliği Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Mülakat, Gözden Geçirme	İş sürekliliği planlarında, üçüncü taraflardan alınan hizmetler de değerlendirilmekte midir? Bu kapsamda üçüncü tarafların rol ve sorumlulukları tanımlanmakta mıdır?
3.1.13.10	İş Sürekliliği Planlarının Test Edilmesi	Mülakat, Gözden Geçirme	İş sürekliliği planlarına yönelik testler yapılmakta mıdır? Test kayıtları tutulmakta mıdır? Testler hangi aralıklarla gerçekleştirilmektedir?
3.1.13.11	İş Sürekliliği Planlarının Güvenli Muhafazası	Mülakat, Gözden Geçirme	İş sürekliliği planları nerede muhafaza edilmektedir?
3.1.13.12	Felaket Kurtarma Planlarının Hazırlanması	Mülakat, Gözden Geçirme	Felaket kurtarma planları yazılı hale getirilmekte midir? Felaket kurtarma planı içeriğinde hangi konular ele alınmaktadır?
3.1.13.13	Felaket Kurtarma Planları Kapsamında Rol ve Sorumlulukların Tanımlanması	Mülakat, Gözden Geçirme	Felaket kurtarma planları hazırlanırken rol ve sorumluluklar tanımlanmakta mıdır? Felaket kurtarma planlarında yer alan kilit personel ve bu personelin bulunmaması durumunda yedeği olacak personel belirlenmiş midir? Acil durumlar için kimlerin aranacağına ve kimlerle iletişim kurulacağına yönelik bir iletişim listesi var mıdır? Bu liste hangi aralıklarla güncellenmektedir?
3.1.13.14	Felaket Kurtarma Çalışmalarında Üçüncü Taraf Hizmetlerin Dikkate Alınması	Mülakat, Gözden Geçirme	Felaket kurtarma planlarında, üçüncü taraflardan alınan hizmetler değerlendirilmekte midir? Bu kapsamda üçüncü tarafların rol ve sorumlulukları tanımlanmakta mıdır?
3.1.13.15	Felaket Kurtarma Planlarının Test Edilmesi	Mülakat, Gözden Geçirme	Felaket kurtarma planları periyodik olarak test edilmekte midir? Test sonuçları kayıt altına alınmakta mıdır?
3.1.13.16	Felaket Kurtarma Planlarının Güvenli Muhafazası	Mülakat, Gözden Geçirme	Felaket kurtarma planları nerede muhafaza edilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.13.17	Kritik Sistem Sürekliliğinin Sağlanması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Üzerinde kritik veri bulunan, kritik servis sunulan, kurumlar tarafından kritik olarak belirlenen altyapı ve sistemlerin hizmet sürekliliği nasıl sağlanmaktadır? Cihaz, enerji, personel, ağ vb. yedekliliği nasıl kurgulanmaktadır? Hizmetler devreye alınırken yedeklilik testleri yapılmakta mıdır? Hizmet seviye taahhütleri var mıdır? Hizmet seviyesi nasıl ve hangi aralıklarla ölçülmekte ve raporlanmaktadır?
3.1.13.18	Felaket Kurtarma Merkezi Oluşturulması	Mülakat, Gözden Geçirme	Felaket kurtarma merkezi var mıdır? Felaket kurtarma merkezinin bilgi güvenliği kriterleri kurumun bilgi güvenliği gereksinimlerini karşılamakta mıdır? Felaket kurtarma merkezi, kurumun asıl sistemlerine göre nasıl konumlandırılmıştır?

3.1.14. Uzaktan Çalışma

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.14.1	1	Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	Kurum tarafından uzaktan çalışma faaliyetlerinde uygulanması gereken şartları ve kısıtlamaları tanımlayan bir politika hazırlanmalı ve uygulanmalıdır. Hazırlanan politika asgari olarak aşağıdaki hususları içermelidir. • Önerilen uzaktan çalışma ortamı • Zararlı yazılımlardan korunma ve güvenlik duvarı gereksinimleri • Yetkisiz erişimin engellenmesi • Kablosuz ağ hizmetlerinin kullanımı • Yedekleme gereksinimleri • Fiziksel güvenlik • Kişilere ait teçhizatlar üzerinde geliştirilen işlere ait fikri mülkiyet hakları ile ilgili anlaşmazlıklar • Uzaktan çalışmanın sona ermesi durumunda; yetki ve erişim haklarının iptali ve kullanılan teçhizatın iadesi
3.1.14.2	1	Ekipman Güvenliğinin Sağlanması	Kurum personeli, uzaktan çalışma faaliyetlerinde yalnızca kurum tarafından sağlanan ve/veya yapılandırma ayarları kurumun bilgi güvenliği gereksinimlerine uygun olan cihazları kullanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.14.3	1	Dosya Paylaşımı	Uzaktan çalışma faaliyetlerinde, çalışma dosyalarını paylaşmak için kurumsal kaynaklar kullanılmalıdır.
3.1.14.4	1	Farkındalık Eğitimlerinin Verilmesi	Uzaktan çalışan kurum personeline özellikle güçlü parola kullanımı, sosyal mühendislik ve kimlik avı/oltalama saldırıları gibi konularda farkındalık eğitimleri verilmelidir. Bk. Tedbir No: 3.5.2.1
3.1.14.5	1	Zararlı Yazılımdan Korunma Uygulamaları	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazlarda zararlı yazılımdan korunma uygulaması kullanılmalı ve zararlı yazılımdan korunma uygulamalarında en güncel yama dosyalarının bulunması ve imza veri tabanının güncel olması sağlanmalıdır. Bk. Tedbir No: 3.1.5.1 Bk. Tedbir No: 3.1.5.4
3.1.14.6	1	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Uzaktan çalışma kapsamında kurum bilgilerinin işleneceği cihazların işletim sistemlerinin ve kullanılan uygulamaların güncel olması sağlanmalı, güvenlik yamaları yüklü olmalıdır. Bk. Bölüm 5.1
3.1.14.7	1	Kurum Kaynaklarına Uzaktan Erişim	Uzaktan çalışma kapsamında kurum kaynaklarına erişim VPN teknolojileri ve çok faktörlü kimlik doğrulama ile sağlanmalıdır. Erişimler kurum politikalarına göre en az yetki prensibine göre sınırlandırılmalıdır. Bk. Tedbir No: 3.1.6.8
3.1.14.8	1	Video Konferans Uygulamalarının Kullanımı	Video konferans uygulamaları kurum içerisinde barındırılmalıdır. Kurum içerisinde barındırılmayan üçüncü taraf bir uygulama kullanılacak ise uygulama açık kaynak kodlu olmalıdır.
3.1.14.9	1	Güçlü Parola Kullanımı	Uzaktan çalışma kapsamında kurumun politikalarına uygun güçlü parolaların kullanılması sağlanmalıdır.
3.1.14.10	1	Güncel Video Konferans Uygulamalarının Kullanılması	Video konferans uygulamasının güncel olması ve uygulamada en güncel yamaların yüklü olması sağlanmalıdır.
3.1.14.11	1	Video Konferans Görüşmelerine Yetkisiz Katılım	Video konferans görüşmelerine sadece toplantı bağlantı adresi kullanılarak yapılabilecek yetkisiz erişimler engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.1.14.12	1	Video Konferans Paylaşım İşlemleri ve Sohbet Özelliği	Video konferans uygulaması üzerinden toplantı sırasında toplantı moderatörü/yardımcı moderatör onayı ile; • İstenilen kullanıcının ekran paylaşımı durdurulabilmeli, • Sohbet (chat) özelliği devre dışı bırakılabilmeli, • Dosya paylaşımı özelliği devre dışı bırakılabilmelidir. Video konferans uygulaması üzerinden yapılacak dosya paylaşımlarında dosya kontrolü yapılmalıdır. Dosya kontrolü yapılamıyorsa video konferans uygulaması üzerinden dosya paylaşımı yapılması engellenmelidir. Bk. Tedbir No: 3.2.4.5 Video konferans uygulaması üzerinden yapılan görüşmeler (dosya paylaşımı, ses, video, chat) uçtan uca şifreli olmalıdır.
3.1.14.13	1	Video Konferans Katılımcı Yönetimi	Video konferans uygulaması üzerinden toplantıya erişimin toplantı moderatöründen önce sağlanması engellenmelidir.
3.1.14.14	1	Video Konferans Toplantı Odası İsimlendirmeleri	Video konferans uygulaması üzerinde yapılan toplantılarda, toplantı odası isimlendirmeleri karmaşık olarak oluşturulmalıdır.
3.1.14.15	1	Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması	Uzaktan çalışan kullanıcı bilgisayarlarında güvenlik duvarı yazılımları aktif durumda olmalıdır. Bk. Tedbir No: 3.1.6.11
3.1.14.16	2	Bekleme Odası Özelliğinin Bulunması	Video konferans uygulaması bekleme odası özelliği içermelidir. Katılımcılar, konferansı organize eden kişinin manuel onayı ile katılım sağlamalıdır.
3.1.14.17	3	Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi	Uzaktan çalışan kullanıcı bilgisayarlarında olası veri sızıntısını engellemek amaçlı uç nokta seviyesinde veri sızıntısını önlemeye yönelik güvenlik önlemleri alınmalıdır. Bk. Tedbir Başlık No: 3.1.7
3.1.14.18	3	Erişimin Kurum Bilgisayarları ile Sınırlandırılması	Uzaktan çalışma kapsamında sadece kurum cihazları üzerinden erişim sağlanmalıdır. VPN erişiminde kurum tarafından sağlanan cihazlar için oluşturulan sertifikaların kullanılması sağlanmalıdır.
3.1.14.19	3	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Bk. Tedbir No: 3.1.6.32

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.14.1	Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması	Mülakat, Gözden Geçirme	Kurum tarafından uzaktan çalışma faaliyetlerinde uygulanması gereken şartları ve kısıtlamaları tanımlayan bir politika tanımlanmış mıdır? İlgili politika uygulanmakta mıdır? Uzaktan çalışma politikası kapsamında hangi konular ele alınmaktadır?
3.1.14.2	Ekipman Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kurum personeli tarafından uzaktan çalışma faaliyetlerinde kullanılacak cihazlara yönelik tanımlanan bilgi güvenliği gereksinimleri nelerdir? Cihazlara yönelik tanımlanan bilgi güvenliği gereksinimlerine uyum nasıl kontrol edilmektedir?
3.1.14.3	Dosya Paylaşımı	Mülakat, Güvenlik Denetimi	Uzaktan çalışma faaliyetlerinde çalışma dosyalarını paylaşmak amacıyla hangi kaynaklar kullanılmaktadır?
3.1.14.4	Farkındalık Eğitimlerinin Verilmesi	Mülakat	Bilgi güvenliği farkındalık eğitimleri kapsamında uzaktan çalışma faaliyetleri ile ilgili hangi konular ele alınmaktadır?
3.1.14.5	Zararlı Yazılımdan Korunma Uygulamaları	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kullanılan cihazlarda hangi zararlı yazılımdan korunma programları kullanılmaktadır? Kullanımda olan zararlı yazılımdan korunma programları versiyonları nelerdir? Güncelleme durumu nasıl kontrol edilmektedir? Zararlı yazılımdan korunma politikaları nasıl yönetilmektedir?
3.1.14.6	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kullanılan cihazlarda yer alan işletim sistemlerine ait versiyonlar nedir? Kullanılan uygulamalar güncel midir? Güncellik durumu nasıl takip edilmektedir?
3.1.14.7	Kurum Kaynaklarına Uzaktan Erişim	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kurum kaynaklarına erişim nasıl sağlanmaktadır? Kullanıcı kimlik doğrulama nasıl yapılmaktadır? Erişimler sınırlandırılmakta mıdır?
3.1.14.8	Video Konferans Uygulamalarının Kullanımı	Mülakat, Güvenlik Denetimi	Kurum hangi video konferans uygulamasını kullanmaktadır? Kurum içerisinde barındırılan video konferans uygulaması var mıdır?
3.1.14.9	Güçlü Parola Kullanımı	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında dikkate alınması gereken bir parola politikası tanımlanmış mıdır? Parola politikası hangi kurallara uyumu zorunlu kılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.1.14.10	Güncel Video Konferans Uygulamalarının Kullanılması	Mülakat, Güvenlik Denetimi	Video konferans uygulaması güncel midir? Kontrolü nasıl sağlanmaktadır?
3.1.14.11	Video Konferans Görüşmelerine Yetkisiz Katılım	Mülakat, Güvenlik Denetimi	Video konferans görüşmelerine yetkisiz katılımı engellemek için hangi kontroller uygulanmaktadır?
3.1.14.12	Video Konferans Paylaşım İşlemleri ve Sohbet Özelliği	Mülakat, Güvenlik Denetimi	Video konferans uygulaması üzerinden toplantı sırasında ekran paylaşımlarının yönetimine ilişkin hangi işlemler yapılabilmektedir? Video konferans uygulaması sohbet özelliği devre dışı bırakılabilmekte midir? Video konferans uygulaması üzerinden dosya paylaşımı özelliği devre dışı bırakılabilmekte midir? Video konferans uygulaması tarafından dosya paylaşım imkânının sunulması durumunda, dosya kontrolü nasıl yapılmaktadır? Video konferans uygulaması üzerinden yapılan görüşmeler uçtan uca şifreli olarak sağlanmakta mıdır?
3.1.14.13	Video Konferans Katılımcı Yönetimi	Mülakat, Güvenlik Denetimi	Video konferans uygulaması üzerinden katılımcıların toplantıya erişimleri, ancak toplantı moderatörünün erişimi sonrasında olacak şekilde ayarlanmakta mıdır?
3.1.14.14	Video Konferans Toplantı Odası İsimlendirmeleri	Mülakat, Güvenlik Denetimi	Video konferans uygulaması üzerinden oluşturulan toplantı odası isimlendirmeleri karmaşık olarak oluşturulmakta mıdır?
3.1.14.15	Kullanıcı Bilgisayarında Güvenlik Duvarının Aktif Olması	Mülakat, Güvenlik Denetimi	Uzaktan çalışan kullanıcı bilgisayarlarında güvenlik duvarı yazılım aktif olarak kullanılmakta mıdır?
3.1.14.16	Bekleme Odası Özelliğinin Bulunması	Mülakat, Güvenlik Denetimi	Video konferans başladıktan sonra sadece yetkili kullanıcıların katılımının sağlanabilmesi için hangi kontroller uygulanmaktadır?
3.1.14.17	Uç Nokta Seviyesinde Veri Sızıntısının Önlenmesi	Mülakat, Güvenlik Denetimi	Uzaktan çalışan kullanıcı bilgisayarlarında veri sızıntısı nasıl önlenmektedir?
3.1.14.18	Erişimin Kurum Bilgisayarları ile Sınırlandırılması	Mülakat, Güvenlik Denetimi	Uzaktan çalışma kapsamında kurum cihazları dışında bir erişim imkânı bulunmakta mıdır?
3.1.14.19	Kuruma Uzaktan Bağlanan Cihazların Yönetimi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.6.32

3.2. Uygulama ve Veri Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, uygulama ve veri güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Uygulama ve Veri Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Kimlik Doğrulama
- Oturum Yönetimi
- Yetkilendirme
- Dosyaların ve Kaynakların Güvenliği
- Güvenli Kurulum ve Yapılandırma
- Güvenli Yazılım Geliştirme
- Veri Tabanı ve Kayıt Yönetimi
- Hata Ele Alma ve Kayıt Yönetimi
- İletişim Güvenliği
- Kötücül İşlemleri Engelleme
- Dış Sistem Entegrasyonlarının Güvenliği

3.2.1. Kimlik Doğrulama

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.1.1	1	Kullanıcı Yönetiminin Yapılabilmesi	Uygulamalar kullanıcı hesaplarının yönetimini sağlayan arayüzlere sahip olmalı ve bu arayüzlere yalnızca yetkili kullanıcıların erişebilmesi sağlanmalıdır. Kullanıcı hesapları, geçici (belirli bir süre, koşul vb. boyunca) veya kalıcı (aksi belirtilmedikçe sürekli) olarak kilitlenebilmelidir. Kalıcı olarak kilitlenen hesap, üzerindeki geçici kilit kaldırılsa dahi kilitli kalmalıdır.
3.2.1.2	1	Ortak Hesap Kullanılmaması	Kullanıcı tanımlamaları, yapılan işlemlerin izlenebilirliğini sağlayacak ve tekil olarak kişi veya sistemi işaret edecek şekilde yapılmalıdır.
3.2.1.3	1	Kimlik Doğrulama İşlemleri için İz Kayıtlarının Oluşturulması	Tüm başarılı ve başarısız kimlik doğrulama girişimleri için özet veri içerecek şekilde iz kaydı oluşturulmalıdır. Bk. Tedbir No: 3.1.8.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.1.4	1	Kimlik Doğrulama Bilgilerinin Güvenliği	Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası varsayılan olarak maskelenmeli ve açık olarak görünmemelidir. Unutulan parola işlevi ve diğer kurtarma yolları geçerli parolayı açığa çıkarmamalı ve yeni parola kullanıcıya açık metin olarak gönderilmemelidir. Kimlik doğrulama bilgileri sadece güvenli kanallar üzerinden taşınmalıdır. Parola veya diğer kimlik doğrulama bilgileri açık metin olarak saklanmamalıdır. Bu bilgileri korumak için kaba kuvvet saldırılarına dayanıklı, güçlü kriptografik yöntemler (şifreleme, tuzlama, özet alma) kullanılmalıdır.
3.2.1.5	1	İlk Parolanın Belirlenmesi	İlk parola belirleme işlemi kullanıcı tarafından yapılmayacak ise, güvenli bir parola belirleme mekanizması ve üretilmiş bu parolaların güvenli olarak taşınması için iletme mekanizması oluşturulmalıdır. Ayrıca, bu parolalar ilk kullanımda değiştirilmeye zorlanmalıdır.
3.2.1.6	1	Varsayılan Kullanıcı Adı ve Parolaların Kullanılmaması	Tüm yazılım bileşenlerinde (veri tabanı, uygulama sunucu, paket program vb.) varsayılan veya tahmin edilebilir kullanıcı adı ve parolalar değiştirilmelidir. Bu gibi bilgilere sahip hesaplar kaldırılarak kullanılmaması sağlanmalıdır. Tahmin edilebilir bilgilere sahip veya varsayılan hesapların kullanılmasının zorunluluk olduğu durumlarda ilgili parolalar değiştirilerek kullanılmalı ve hesaplara ait her aktivite izlenmelidir. Bu hesapların parolaları periyodik olarak veya her kullanım sonrasında güncellenmelidir.
3.2.1.7	1	Kaynak Kodda Kimlik Doğrulama Bilgilerinin Bulunmaması	Kaynak kodda veya kaynak kod depolarında gizli bilgiler, API anahtarları ve parolalar yer almamalıdır. Kullanılan tüm kimlik doğrulama bilgileri şifrelenmeli ve korunan bir yerde depolanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa özel anahtara sadece yetkili kullanıcının erişimine izin verecek mekanizmalar mevcut olmalıdır.
3.2.1.8	1	Parola Yönetimi	Parola giriş alanları uzun ve karmaşık bir parola girilmesini engellememeli, parola cümle (deyimsel parola) kullanımına izin vermeli ya da teşvik etmelidir. Kurumlar güvenlik gereksinimlerine göre parola politikası belirlemelidir. Ayrıca parolalar için bir en uzun geçerlilik süresi tanımlanmış olmalıdır. Değişen parola fonksiyonu eski parolayı, yeni parolayı ve bir parola onayını kapsamalıdır. Kimlik doğrulama için bilgi sorgulayan sorular (gizli sorular) kullanılmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.1.9	1	Kimlik Doğrulama Fonksiyonlarına Yapılacak Saldırılara Karşı Önlem Alınması	Oturum açma, parola sıfırlama ya da hesap unutma gibi işlevler sıralı denemelerle bilgi edinmeye olanak vermemelidir. Kaba kuvvet saldırılarını önlemek amacıyla (istek sınırlandırma, IP bloklama, CAPTCHA vb.) etkin güvenlik yöntemleri uygulanmalıdır. Kimlik doğrulama işlemlerinin başarılı olup olmadığı paket boyutu gibi değerler üzerinden anlaşılamamalıdır. Hesaplara erişim için yeniden oynatma (replay) saldırılarına dayanıklı bir kimlik doğrulama mekanizması kullanılmalıdır.
3.2.1.10	2	Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi	Unutulan parolanın sıfırlaması kullanıcı adının unutulması vb. durumlar için; kısa ileti, e-posta onayı, mobil onay, çevrimdışı onay vb. yöntemler kullanılmalıdır. İlgili yöntemler kullanılırken sahip olunan, bilinen ve biyometrik faktörlerin en az ikisinden yararlanılmalıdır. Hassas işlevler gerçekleştirilmeden önce, yeniden kimlik doğrulama, daha güçlü bir mekanizmayla kimlik doğrulama, çok faktörlü kimlik doğrulama veya işlem imzalama gibi yöntemler uygulanmalıdır. Uygulamanın ilgili yönetim arayüzlerine yalnızca yetkili kullanıcılar tarafından erişim sağlanmalıdır. Açık anahtar altyapısı tabanlı kimlik doğrulama kullanılıyorsa sertifika yolu doğrulanmalı ve kullanıcının sertifikası sistem üzerindeki geçerli kullanıcı veya grup bilgisi ile eşleştirilmelidir.
3.2.1.11	2	Hesap Kurtarma Seçeneklerinin Güvenliği	Hesaba yeniden erişebilecek tüm hesap kimlik doğrulama işlevleri (parola güncelleme, parolamı unuttum, devre dışı/kayıp simge (token), süresi dolmuş parolanın güncellenmesi, yardım masası vb.) en az ana kimlik doğrulama mekanizması kadar güvenli olmalıdır.
3.2.1.12	2	Kullanılmayan Hesapların Tespiti	Uygulama, belirli bir süre boyunca hiç kullanılmamış olan hesapları raporlayabilmelidir. Bu hesaplar pasif duruma getirilmeli veya silinmelidir.
3.2.1.13	3	Merkezi Kimlik Doğrulama Mekanizmalarının Kullanılması	Kurumsal merkezi kimlik yönetim ve doğrulama sistemleri kullanılmalı veya e-Devlet sistemi ile entegrasyon sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.1.1	Kullanıcı Yönetiminin Yapılabilmesi	Mülakat, Gözden Geçirme	Uygulamalarda kullanılan bir kimlik doğrulama mekanizması mevcut mu? Tasarım dokümanında kullanıcı yönetimi için süreç/işlev tanımlanmış mı? Uygulamalar, kullanıcı hesaplarını yönetmek için ilgili arayüzlere sahip mi? Kullanıcı hesapları geçici veya kalıcı olarak kilitlenebiliyor mu? Uygulamalar üzerinden geçici/kalıcı olarak kilitlenmiş hesaplar tespit edilebiliyor mu?
3.2.1.2	Ortak Hesap Kullanılmaması	Mülakat, Güvenlik Denetimi	Kullanıcıların yerine işlem yapan yazılımsal süreçler (web servisleri, kurumsal yazılımlar vb.) kullanıcı olarak tanımlanabiliyor mu? Kullanıcıların yerine işlem yapan yazılımsal süreçlerin (web servisleri, kurumsal yazılımlar vb.) gerçekleştirdiği işlemlerin kaydı oluşturuluyor mu? Aynı hesabın birden fazla kullanıcı tarafından kullanılmasını (ortak hesap) önlemek adına tekil kullanıcılar tanımlanmakta mıdır?
3.2.1.3	Kimlik Doğrulama İşlemleri için İz Kayıtlarının Oluşturulması	Mülakat, Gözden Geçirme	Kullanıcıların oturum açma istekleri ve ilgili isteklere verilen yanıtlar/işlem sonuçları kayıt altına alınıyor mu? Şüpheli kimlik doğrulama işlemleri kayıt altına alınıyor mu? İz ne kadar süre için saklanıyor?
3.2.1.4	Kimlik Doğrulama Bilgilerinin Güvenliği	Mülakat, Gözden Geçirme, Kaynak Kod Analizi	Kullanıcı parolaları oluşturulurken veya güncellenirken giriş yapılan parolalar nasıl görüntülenmektedir? Parola sıfırlama süreci tasarım dokümanında tanımlanmış mıdır? Parola sıfırlama işlemi kapsamında yeni parola nasıl oluşturulmaktadır? Parolalar veri tabanında hangi kriptografik yöntemler kullanılarak saklanmaktadır? Bu kriptografik yöntemler ulusal ve/veya uluslararası standartlar tarafından güvenli kabul ediliyor mu? Kritik bilgilerin taşınması esnasında ifşa olmaması için iletişimde ne gibi önlemler alınmaktadır?
3.2.1.5	İlk Parolanın Belirlenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Parola belirleme süreci tasarım dokümanında tanımlanmış mıdır? Parola belirleme sürecinde ilk parolanın güvenli olarak oluşturulmasında ve iletiminde hangi yöntemler kullanılmaktadır? Kullanıcı, ilk parolasını kendisi oluşturmadığında ilgili parolayı ilk kullanımda değiştirmeye zorlanıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.1.6	Varsayılan Kullanıcı Adı ve Parolaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Uygulamaya erişim için varsayılan kullanıcılar tanımlanmış mıdır? Uygulamanın kullandığı veri tabanı ve uygulama sunucularında varsayılan kullanıcı bulunmakta mıdır? Varsayılan kullanıcıların aktiviteleri izlenmekte midir? Parola değişim periyodu politikada nasıl tanımlanmıştır?
3.2.1.7	Kaynak Kodda Kimlik Doğrulama Bilgilerinin Bulunmaması	Mülakat, Gözden Geçirme, Kaynak Kod Analizi	Uygulama kodlarında herhangi bir kullanıcıya ait bilgiler (kullanıcı adı, parola, anahtar vb.) yer almakta mıdır? Uygulamanın diğer hizmetlere erişmek için kullandığı kimlik doğrulama bilgileri nasıl depolanmakta ve kullanılmaktadır?
3.2.1.8	Parola Yönetimi	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama hesaplarının parolalarında kullanmak üzere mevcut bir parola politikası tanımlanmış mıdır? Bu parola politikasının işletilmesini uygulama destekliyor mu? Uygulama, parola değiştirme işlemi esnasında kullanıcının mevcut parolası üzerinden doğrulama yapıyor mu? Uygulamada, parola değiştirme işlemi esnasında yeni parolanın tekrar girilmesi (parola onayı) istenerek istenmeyen/bilinmeyen bir değer ile parolanın değiştirilmesi engelleniyor mu?
3.2.1.9	Kimlik Doğrulama Fonksiyonlarına Yapılacak Saldırılara Karşı Önlem Alınması	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama yaygın kimlik doğrulama saldırılarına karşı (sürekli istek gönderme, yeniden oynatma, şüpheli aktivitelere ait sürekli alarmlar ürettirme vb.) zafiyet içermekte midir? Araçlarla otomatik yapılan yaygın kimlik doğrulama saldırılarını önlemek için hangi önlemler alınmıştır? Bu saldırılara karşı neler yapılacağı dokümante edilmiş midir?
3.2.1.10	Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama kimlik doğrulamak için hangi ek güvenlik önlemlerini kullanıcılarına sunmaktadır? Kimlik doğrulama mekanizmalarında elektronik imza gibi güçlü yöntemlerin kullanılabilmesi için seçenek sağlanıyor mu? Uygulamanın yönetim arayüzlerine güvenilmeyen taraflarca erişilmesini engellemek için kimlik doğrulama, yetkilendirme vb. mekanizmalar tanımlanmış mı? Kimlik doğrulama mekanizmasında kullanılan açık anahtar altyapısının sertifika yolu doğrulanmakta mıdır? Unutulan parola ve diğer kurtarma işlemleri nasıl gerçekleştiriliyor?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.1.11	Hesap Kurtarma Seçeneklerinin Güvenliği	Mülakat, Güvenlik Denetimi, Sızma Testi	Profil güncelleme, parolamı unuttum, devre dışı/kayıp simge (token), süresi dolmuş parolanın güncellenmesi ve yardım masası ile hesap kurtarma yöntemlerinin güvenliği nasıl sağlanmıştır? Uygulama kullanıcı bilgilerinin değişmesi ile sonuçlanacak tüm durumlar için iz kaydı oluşturmakta mıdır?
3.2.1.12	Kullanılmayan Hesapların Tespiti	Mülakat, Güvenlik Denetimi	Uygulama, belirli bir süre boyunca hiç kullanılmamış olan hesapları raporlayabilmekte midir? Bu hesapların yönetimi için nasıl bir yol izlenmektedir?
3.2.1.13	Merkezi Kimlik Doğrulama Mekanizmalarının Kullanılması	Mülakat, Güvenlik Denetimi	Merkezi kimlik yönetim ve doğrulama sistemi kullanılıyor mu? Kimlik doğrulama için E-Devlet sistemi ile entegrasyon sağlanmış mıdır?

3.2.2. Oturum Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.2.1	1	Kimlik Doğrulama İşlemleri Sonrasında Yeni Bir Oturum ve Yeni Bir Oturum Kimliğinin Üretilmesi	Tüm kimlik doğrulama ve yeniden kimlik doğrulama işlemleri sonucunda yeni bir oturum ve yeni bir oturum kimliği üretilmelidir. Oturum kimlikleri yeterince uzun olmalı, rastgele olmalı ve etkin oturumlar içerisinde tekil olmalıdır. Oluşturulan oturum kimliği yalnızca bir kez kullanılmalıdır.
3.2.2.2	1	Oturum Kimliğinin Doğrulanması ve Güvenliğinin Sağlanması	Yalnızca uygulama tarafından üretilen oturum kimliklerinin uygulamada aktif oturum kimliği olarak kullanıldığı doğrulanmalıdır. Oturum kimliğinin URL, hata mesajları ve iz kayıtları içerisinde yer almaması sağlanmalıdır. URL içerisinde oturum kimliğinin yeniden yazılması engellenmelidir.
3.2.2.3	1	Kullanıcı Oturumlarının Sonlandırılması	Kimlik doğrulamayla erişilen tüm sayfalardan oturum kapatma işlevine erişilebilmelidir. Buna ek olarak, oluşturulan oturum kimliğinin geçerlilik süresi belirlenmelidir. İlgili süre sonunda, belirli süre etkinlik olmadığında veya kullanıcı oturumu kapattığında oturum geçersiz hale gelmelidir. İlgili sürelerin güncellenmesi sürecinde yetkilendirme mekanizmasından faydalanılmalıdır. Ayrıca oturumun geçersiz olmasına sebep olacak bilgilerin değişmesi durumunda (kullanıcı parolasının güncellenmesi, yetkilerin güncellenmesi vb.) etkin oturumların sonlandırılması sağlanmalıdır. Oturum sonlandığında istemci ve sunucuda oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.2.4	1	Oturum Güvenlik Mekanizmalarının Kullanılması	Kullanılan çatının, programlama dilinin ve iletişim protokolünün sağladığı oturum güvenlik mekanizmaları kullanılmalıdır. Web uygulamalarının oturum çerezlerinde HTTPOnly, Secure, SameSite vb. bayraklar kullanılmalıdır. Tanımlama bilgilerinde depolanan oturum kimliklerinin yolları, uygulama için uygun kısıtlayıcı bir değere ayarlanmalıdır.
3.2.2.5	3	Kullanıcıların Aktif Oturumlarını Yönetebilmesi	Kullanıcılar uygulamadaki etkin oturumlarını görüntüleyebilmeli ve aktif oturumlarından istediğini sonlandırabilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.2.1	Kimlik Doğrulama İşlemleri Sonrasında Yeni Bir Oturum ve Yeni Bir Oturum Kimliğinin Üretilmesi	Mülakat, Gözden Geçirme, Sızma Testi	Yeni oturum açıldığında yeni bir kimlik (oturum anahtar değeri) oluşturuluyor mu? Kullanılan çatı ve geliştirme platformu, yeni oturum açıldığında yeni kimlik (oturum anahtar değeri) oluşturulmasını destekliyor mu? Kimlik doğrulama yapmak amacıyla kullanılan bileşenler üzerinde her oturum açıldığında farklı bir kimliğin oluşturulduğunu kontrol için sızma testi gerçekleştirildi mi?
3.2.2.2	Oturum Kimliğinin Doğrulanması ve Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme, Kaynak Kod Analizi	Uygulama tarafından üretilmemiş ancak farklı yöntemlerle/farklı uygulamalarla oluşturulmuş oturum kimliklerinin sistemde kullanılamadığı test edildi mi? Uygulama, farklı yöntemlerle/farklı uygulamalarla oluşturulmuş oturum kimliklerinin kullanıldığı durumda nasıl davranmaktadır? Oturum kimliğinin güvenliğinin sağlanması için uygulama içerisinde güvenlik önlemi tanımlanmış mıdır? Hata mesajlarının ve iz kayıtlarının hangi bilgileri içereceği / içeremeyeceği tasarım dokümanında tanımlanmış mıdır?
3.2.2.3	Kullanıcı Oturumlarının Sonlandırılması	Mülakat, Gözden Geçirme, Sızma Testi	Kullanıcı oturumu kapattığında oturumun sonlandığı test edilmiş midir? İşlem yapılmadan beklenecek süre ve/veya oturum kimliğinin geçerlilik süresi yetkisiz güncellenebiliyor mu? Oluşturulan oturum kimliğinin geçerlilik süresi belirlenmiş midir? İşlem yapılmadan beklenen geçerlilik süresi sonunda oturum sonlandırılıyor mu? Kullanıcı, oturumun geçersiz olmasına sebep olacak bilgilerini değiştirdikten sonra etkin olan tüm oturumlarını sonlandırabiliyor mu? Oturum sonlandığında oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından siliniyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.2.4	Oturum Güvenlik Mekanizmalarının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın geliştirme platformunun hangi güvenlik mekanizmaları kullanılmaktadır? Veri taşıma için hangi protokoller (HTTP, FTP vb.) kullanılmaktadır? Bu protokollerin güvenliği için hangi önlemler alınmaktadır?
3.2.2.5	Kullanıcıların Aktif Oturumlarını Yönetebilmesi	Mülakat, Güvenlik Denetimi	Uygulama arayüzleri kullanılarak etkin olan oturumlar listelenebiliyor mu? Uygulama arayüzleri kullanılarak etkin olan oturumlar sonlandırılabiliyor mu?

3.2.3. Yetkilendirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.3.1	1	Yetki Denetimi	Kullanıcıların uygulamaya erişimlerini tanımlayan yetki matrisi oluşturulmalı ve belirli aralıklarla güncellenmelidir. Kullanıcı sadece yetkilendirildiği uygulama bileşenlerine ve kaynaklara erişebilmeli ve bunları kullanabilmelidir. Uygulamaya yapılan her istek için yetki denetimi kontrolü uygulanmalıdır.
3.2.3.2	1	Kritik Veriye ve Kaynaklara Erişimlerin Kayıt Altına Alınması	Uygulama, yönettiği veriye ve kaynaklara erişimleri kayıt altına alabilmek için denetim kayıtları üretebilmelidir. Bk. Tedbir No: 3.1.8.1
3.2.3.3	1	En Az Yetki Prensibinin Uygulanması	Kullanıcılara verilecek yetkiler, yürütülen görevler ve ihtiyaçlar doğrultusunda belirlenmelidir. En az yetki prensibine göre kullanıcının gerçekleştirebileceği ilgili işlemler için gereken asgari yetkilerin haricinde bir ayrıcalık tanımlanmamalıdır.
3.2.3.4	3	İçerik Duyarlı ve Gelişmiş Erişim Denetimi	Uygulama içerik duyarlı (zaman, konum, IP adresi gibi öznitelikler) erişim denetimi yapabilmelidir. Uygulama; fonksiyonlara, kaynaklara, veriye erişim sürelerini, kullanım oranlarını veya kullanım sıklığını sınırlandırabilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.3.1	Yetki Denetimi	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamalara erişimi tanımlayan yetki matrisi oluşturulmuş ve belirli aralıklara güncellenmekte midir? Uygulamada kullanıcının yalnızca ilgili olduğu uygulama bileşenlerine ve kaynaklara erişebilmesini sağlayacak bir yetkilendirme mekanizması tanımlanmış mı? Uygulamada kullanıcıların diğer kullanıcılara ait kritik bilgilere erişmesini engellemek için nasıl bir yetkilendirme mekanizması tanımlanmıştır? Uygulamaya gelen her istek için yetki denetimi kontrolü yapılmakta mıdır?
3.2.3.2	Kritik Veriye ve Kaynaklara Erişimlerin Kayıt Altına Alınması	Mülakat, Gözden Geçirme, Sızma Testi	Veri akışı ve kaynaklara erişim için iz ve denetim kayıtları oluşturuluyor mu? Kayıtlar hangi bilgileri içeriyor? Kayıtlar kullanıcı arayüzünden sorgulanabiliyor mu? Kayıtlar silinebiliyor veya değiştirilebiliyor mu? Kayıtlar ne kadar süre ile saklanıyor?
3.2.3.3	En Az Yetki Prensibinin Uygulanması	Mülakat, Güvenlik Denetimi	Kullanıcılara verilen yetkiler, yürütülen görevler ve ihtiyaçlar doğrultusunda mı belirlenmektedir?
3.2.3.4	İçerik Duyarlı ve Gelişmiş Erişim Denetimi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulamada yetkilendirmeler zaman, konum, kullanılan ağ, IP adresi gibi özelliklere göre sınırlandırılabiliyor mu? Uygulama yetkilendirme ile erişimleri erişim süresi, kullanım sıklığı gibi parametrelere göre sınırlandırabiliyor mu? Uygulama erişim denetleme mekanizmasında içeriğe duyarlı kontroller ve yetkilendirmeler tanımlanabiliyor mu?

3.2.4. Dosyaların ve Kaynakların Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.4.1	1	Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması	Uygulamanın sahip olduğu sistem ve yapılandırma dosyaları ile denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verisiyle aynı konumda (dizin, sistem bölümü vb.) depolanmamalıdır. Bk. Tedbir No: 3.1.8.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.4.2	1	Uygulama Bileşenlerine Dış Kaynaklardan Erişimin Kısıtlanması	Uygulamanın bileşenlerinin çalıştığı sunuculardan (web sunucusu, uygulama sunucusu vb.), kendi sınırları dışında bulunan / kendi kontrolünde bulunmayan veya ilişkili olmayan kaynak ve sistemlere uzak bağlantı ve erişim varsayılan olarak engellenmelidir. Aynı şekilde uygulama bileşenlerinin bulunduğu sunuculara uzaktan erişim izni kontrollü sağlanmalıdır.
3.2.4.3	1	İstemci Ön Bellekleme İşlevinin Kritik Veri için Kapatılması	Tüm formlarda istemci tarafında yapılan ön bellekleme işlevselliği kritik veri için kapatılmalıdır.
3.2.4.4	1	Uygulamanın Kullandığı Kaynakların Güvensiz Ortamlarda Saklanmaması	Uygulama kullandığı veya ürettiği kayıtları (resimler, ofis dosyaları, iz kayıtları vb.) güvensiz ortamlarda (ortak dizin, USB disk vb.) saklamamalıdır.
3.2.4.5	1	Güvenilmeyen Kaynaklardan Alınan Dosyaların Denetlenmesi	Güvenilmeyen kaynaklardan alınan dosyaların öncelikle türü ve içeriği doğrulanmalı, güvenlik açığına sebep olabilecek bir içeriğe sahip olup olmadığı kontrol edilmelidir. Bu dosyalar kısıtlı izinlerle uygulama ana dizini dışında depolanmalıdır. Bu dosyaların çalıştırılmasına ve çalıştırılan koda dâhil edilmesine (parametre, eklenti vb. olarak) izin verilmemelidir.
3.2.4.6	1	Kaynaklara Erişimin Kısıtlanması	Kökler arası kaynak paylaşımında (CORS) güvenilmeyen kaynakların uygulamanın verilerine erişmesi engellenmelidir. URL yeniden yönlendirmelerinin sadece bilinen beyaz liste adreslerine yapılması, bilinmeyen adreslere yönlendirme gerekiyorsa kullanıcının uyarılarak onayının alınması sağlanmalıdır.
3.2.4.7	2	Açık Kaynak Kod Tabanının Kurum Bünyesinde Tutulması	Açık kaynak kod tabanın zafiyete neden olacak şekilde değiştirilmesini engellemek için kod tabanı kurum bünyesinde barındırılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.4.1	Yapılandırma Dosyaları, Denetim Kayıtları, İz Kayıtları vb. Bilgilerin Kullanıcı Verisiyle Aynı Konumda Depolanmaması	Mülakat, Güvenlik Denetimi	Uygulamanın yapılandırmasını ve ayarlarını içeren bilgiler nerede saklanmaktadır? Uygulamanın ürettiği denetim kayıtları ve iz kayıtları nerede saklanmaktadır? Uygulamanın sahip olduğu yapılandırma dosyaları, denetim kayıtları ve iz kayıtları gibi bilgiler kullanıcı verileri ile ayrı yerde mi saklanıyor? Uygulamanın yönettiği veri nerede saklanmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.4.2	Uygulama Bileşenlerine Dış Kaynaklardan Erişimin Kısıtlanması	Gözden Geçirme, Sızma Testi	Uygulamanın çalıştığı sunuculardan veri tabanına/dış kaynaklara uzaktan bağlantı ve erişim sağlanabilmekte midir? Uygulamanın çalıştığı sunuculardan uygulama ile ilişkili olmayan kaynak ve sistemlere uzaktan bağlantı ve erişim engelleniyor mu? Uygulama sunucularına her yerden uzak masaüstü ile erişilebilmekte midir?
3.2.4.3	İstemci Ön Bellekleme İşlevinin Kritik Veri için Kapatılması	Mülakat, Gözden Geçirme, Sızma Testi	İstemci tarafında önbellekte kritik bilgiler tutuluyor mu?
3.2.4.4	Uygulamanın Kullandığı Kaynakların Güvensiz Ortamlarda Saklanmaması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın kullandığı kayıtların hangi ortamlarda saklanabileceği tasarım dokümanında tanımlanmış mı?
3.2.4.5	Güvenilmeyen Kaynaklardan Alınan Dosyaların Denetlenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Kullanıcıdan ve güvenilmeyen kaynaklardan alınan dosyalar nerede depolanmaktadır? Bu dosyalar depolanmadan önce dosya türü nasıl doğrulanmaktadır ve zararlı içeriğe sahip olup olmadığı nasıl kontrol edilmektedir? Çalıştırılacak komutlara girdi olarak verilen dosyalar ile çalıştırılan komutların ürettiği dosyaların içeriği saldırılara maruz kalmamak için kullanılmadan önce denetleniyor mu? Denetim yapılan ortamın güvenliği nasıl sağlanıyor?
3.2.4.6	Kaynaklara Erişimin Kısıtlanması	Gözden Geçirme, Sızma Testi	URL yeniden yönlendirme işleminden önce hangi kontroller yapılıyor? Yönlendirilebilir güvenilir URL adresleri listesi tutuluyor mu? Listede olmayan adreslerle karşılaştığında uygulama nasıl karşılık vermektedir? Uygulamada kökler arası kaynak paylaşımında (CORS) güvenlik önlemleri tanımlanmış mıdır?
3.2.4.7	Açık Kaynak Kod Tabanının Kurum Bünyesinde Tutulması	Mülakat, Gözden Geçirme	Açık kaynaklı kod kullanarak yazılım geliştirilirken kod tabanı geliştirme yapan kurum bünyesinde tutuluyor mu?

3.2.5. Güvenli Kurulum ve Yapılandırma

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.5.1	1	Uygulamada Güvenlik Güncellemeleri ve Yamaları Yüklenmiş Bileşenlerin Kullanılması	Uygulama, güvenlik güncellemeleri ve yamaları yapılmış bileşenlerden oluşmalıdır. Bk. Tedbir No: 5.3.1.1
3.2.5.2	1	Kaynak Paylaşım ve İçerik Güvenliği Sıkılaştırmaları	Uygulamanın güvenliğini artırmak ve istemci tarafında yer alan kaynakların güvenliğini sağlamak amacıyla güvenli HTTP başlıkları (X-Frame-Options, Content-Security-Policy vb.) kullanılmalıdır. Uygulamanın diğer sistemler, uygulamalar veya kişiler ile paylaştığı dosya, veri veya kaynaklar için erişim kontrolleri yapılmalıdır. Bk. Tedbir No: 5.3.1.17
3.2.5.3	1	Kurulumların Korumalı ve Ayrıştırılmış Şekilde Yapılması	Uygulama kurulumları, korumalı ve ayrıştırılmış şekilde yapılmalıdır. Bu kapsamda yöneticiler için hazırlanmış kullanıcı kılavuzları ürünlerin güvenli kurulumları ve yapılandırılmaları ile ilgili talimatlar içermelidir. Uygulama çok katmanlı mimari (multitier architecture) kullanılarak tasarlanmalı ve her katman için güvenlik mekanizmaları oluşturulmalıdır. Uygulamanın kullandığı veri tabanları ve kayıtlar, internetten doğrudan erişilemeyecek şekilde yapılandırılmalıdır. İnternete açık olarak çalışan sunucular (uygulama sunucusu, web sunucu, e-posta sunucuları vb.) DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulmalıdır.
3.2.5.4	1	Sunuculara ve Çalışma Ortamlarına Sadece Uygulamanın ve Yetkili Kullanıcıların Erişebilmesi	Sunuculara ve çalışma ortamlarına (veri tabanı, dosya sistemi, servisler vb.) sadece uygulamanın ve yetkili kullanıcıların erişebileceği şekilde gerekli güvenlik yapılandırmaları uygulanmalıdır.
3.2.5.5	1	Sunucular Arası İletişimde İhtiyaç Duyulan En Az Yetkiye Sahip Hesapların Kullanılması	Uygulama sunucuları ve veri tabanı sunucuları gibi bileşenlerin arasındaki iletişimde ihtiyaç duyulan en az yetkiye sahip hesaplar kullanılmalıdır. Bk. Tedbir No: 3.2.3.3
3.2.5.6	1	İşletimdeki Sistemler Üzerinde Uygulama Kurulumu	İşletimdeki sistemler üzerine derleyiciler ve diğer geliştirme araçları kurulmamalıdır.
3.2.5.7	2	Güvenli Derleme	Sistem seviyesinde erişimi olan diller ile geliştirilmiş uygulamalar, güvenlik bayrakları (ASLR, DEP, hata ayıklama kapalı vb.) etkin olacak şekilde derlenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.5.8	2	Yapılandırma Değişikliklerinin İzlenmesi	Uygulama, yapılandırma değişiklikleri ile ilgili erişimleri kısıtlamalı ve yapılandırma değişiklikleri için iz kayıtları oluşturmalıdır. Çalışan uygulamanın kodlarının değiştirilmemesini sağlayacak önlemler (kaynak kodun özetinin saklanması, kaynak kodun konfigürasyon yönetim aracında bulunan sürüm numarasının (build number) saklanması vb.) alınmalıdır. Bk. Tedbir No: 3.1.8.1
3.2.5.9	2	Sistem Kaynaklarının Azalması Durumunda Uyarı Verilmesi	Sistem kaynakların azalması durumunda yöneticiye uyarı verilebilecek altyapı oluşturulmalıdır. Bu kapsamda ilgili altyapı, uyarı üretebilmeli veya üretilmiş uyarıları yöneticiye iletebilmelidir.
3.2.5.10	2	Anahtarlar ve Parolaların Değiştirilebilir Olması	Tüm anahtar ve parolalar değiştirilebilir olmalıdır ve kurulum esnasında oluşturulmalı veya değiştirilmelidir.
3.2.5.11	3	Sunucular Arası İletişimin Şifreli Olması	Uygulama sunucuları ile bağlantı kurduğu sunucular arasındaki iletişim şifreli olmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.5.1	Uygulamada Güvenlik Güncellemeleri ve Yamaları Yüklenmiş Bileşenlerin Kullanılması	Mülakat, Gözden Geçirme	Belirli aralıklarla mevcut uygulama bileşenlerinin güncelliği kontrol ediliyor mu? Mevcut uygulama bileşenlerinin eski versiyona sahip olduğu tespit edildiğinde ne gibi faaliyetler gerçekleştirilmektedir? Bu faaliyetler dokümanlarda tanımlanmış mıdır?
3.2.5.2	Kaynak Paylaşım ve İçerik Güvenliği Sıkılaştırmaları	Mülakat, Güvenlik Denetim, Sızma Testi	http güvenlik başlıkları kullanılıyor mu? CORS yapılandırması güvenli mi?
3.2.5.3	Kurulumların Korumalı ve Ayrıştırılmış Şekilde Yapılması	Mülakat, Gözden Geçirme	Kurulumun yapıldığı sunucu ve ağların ayrıştırılmış ve korunaklı olabilmesi için nasıl bir yöntem izlenmektedir? Bu yöntem için adımlar tanımlanmış ve dokümante edilmiş midir? Yöneticiler için hazırlanmış kullanıcı kılavuzları ürünlerin güvenli kurulumları ve yapılandırılmaları ile ilgili talimatlar içeriyor mu? İnternete açık olarak çalışan sunucuların çeşitli saldırılar sonucunda ele geçirilmesi durumunda kurum yerel ağının ve ilgili ağda bulunan diğer sunucuların güvenliğinin sağlanması için ne gibi önlemler alınıyor? Kurulum yapmaya yetkili kullanıcılar kimlerdir? Sadece yetkili kullanıcılar mı uygulama kurulumlarını yapıyor?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.5.4	Sunuculara ve Çalışma Ortamlarına Sadece Uygulamanın ve Yetkili Kullanıcıların Erişebilmesi	Mülakat, Gözden Geçirme	Yalnızca uygulamanın ve yetkili kullanıcıların sunuculara ve çalışma ortamlarına erişebileceği şekilde gerekli güvenlik yapılandırmaları uygulanmış mıdır?
3.2.5.5	Sunucular Arası İletişimde İhtiyaç Duyulan En Az Yetkiye Sahip Hesapların Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama ana bileşenleri (sunucular, servisler vb.) arası iletişimde kullanılacak hesapların yetkileri ihtiyaç duyacağı en az yetkiye göre yapılandırılmış mıdır?
3.2.5.6	İşletimdeki Sistemler Üzerinde Uygulama Kurulumu	Mülakat, Gözden Geçirme, Güvenlik Denetimi	İşletimdeki sistemler üzerinde derleyici veya geliştirme araçları bulunmakta mıdır?
3.2.5.7	Güvenli Derleme	Gözden Geçirme, Sızma Testi, Kaynak Kod Analizi	Derleme aşamasında kullanılan güvenlik bayrakları nelerdir?
3.2.5.8	Yapılandırma Değişikliklerinin İzlenmesi	Mülakat, Gözden Geçirme	Uygulamada yapılan yapılandırma değişiklikleri için iz kaydı (işletim sistemi, ağ veya uygulama seviyesinde) tutuluyor mu? Yapılandırma değişikliklerini yapabilecek kullanıcıların yetkilendirmesine yönelik bir süreç tanımlanmış ve uygulanmakta mıdır? Bu yetkilere sahip olan kullanıcıların listesi periyodik olarak gözden geçirilmekte midir?
3.2.5.9	Sistem Kaynaklarının Azalması Durumunda Uyarı Verilmesi	Mülakat, Gözden Geçirme	Uygulamanın kullandığı mevcut sistem kaynakları takip edilebiliyor mu? Uygulamanın kullandığı mevcut sistem kaynaklarının belirli bir sınır altına düşmesi durumunda yönetici/ilgili personel uygulama tarafından otomatik olarak bilgilendiriliyor mu?
3.2.5.10	Anahtarlar ve Parolaların Değiştirilebilir Olması	Mülakat, Gözden Geçirme	Uygulamada kullanılan tüm parola, şifre ve anahtarlar uygulamanın tekrar derlenmesi, kurulması vb. işlemlere ihtiyaç duyulmadan değiştirilebiliyor mu?
3.2.5.11	Sunucular Arası İletişimin Şifreli Olması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama sunucuları ve bağlantı kurduğu sunucular arasındaki iletişimin güvenliği nasıl sağlanmaktadır?

3.2.6. Güvenli Yazılım Geliştirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.6.1	1	Güvenlik Gereksinimleri ve Tasarımı	Yazılım geliştirme sürecinde güvenlik gereksinimleri tanımlanmalı ve bu gereksinimler göz önünde bulundurularak tasarım yapılmalıdır. Tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların teknik şartnamelerinde güvenlik gereksinimlerine yer verilmelidir.
3.2.6.2	1	Test ve Geliştirme Ortamında Gerçek Veri Kullanılmaması	Geliştirme ve/veya test ortamında kullanılacak veriler gerçek veri olmamalıdır. Bu kapsamda, ilgili ortamlarda kullanılması için amaca uygun veriler üretilmelidir.
3.2.6.3	1	Tedarik Edilen Uygulamalarda Kullanım Amacına Uygun Olmayan Özellik/Arka Kapı Bulunmaması	Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınmalıdır. Bk. EK-C.6: Taahhütname Örneği
3.2.6.4	1	Arayüzün Türkçe Dil Desteğine Sahip Olması	Bk. Tedbir No: 4.6.1.4
3.2.6.5	1	Güncel İstemci ve Sunucu Teknolojilerinin Kullanılması	Üretici tarafından sunulan teknik desteği sona ermiş, güvenlik açığı barındıran veya teknolojisi zaman aşımına uğramış sunucu veya istemci teknolojileri kullanılmamalıdır.
3.2.6.6	1	Uygulama Güvenlik Testlerinin Yapılması	Devreye alınan veya güncellenen uygulamalarda sızma testleri ve uygulama güvenliği testleri yapılmalıdır. Tedarik edilen uygulamalar üzerinde sızma testleri gerçekleştirilmelidir. Bk. Tedbir Başlık No: 3.1.11
3.2.6.7	2	Kaynak Kod Güvenlik Analizlerinin Yapılması	Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmelidir.
3.2.6.8	2	Güvenli Yazılım Geliştirme Süreçlerinin Uygulanması	Güvenli yazılım geliştirme süreçleri ve olgunluk modellerinden faydalanılarak kurumsal yazılım geliştirme süreçleri güncellenmeli ve güvenli yazılım geliştirme yaşam döngüsü uygulanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.6.1	Güvenlik Gereksinimleri ve Tasarımı	Mülakat, Gözden Geçirme	Tasarım, tanımlanmış yazılım güvenlik gereksinimlerine göre yapılmış mı? Yazılım güvenlik gereksinimleri, tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların teknik şartnamelerinde yer alıyor mu?
3.2.6.2	Test ve Geliştirme Ortamında Gerçek Veri Kullanılmaması	Mülakat	Geliştirme ve/veya test ortamlarında kullanılan veriler hangi yöntem ile / nasıl oluşturuldu? Yazılım için geliştirme ve test süreçlerinde hangi veriler kullanılıyor?
3.2.6.3	Tedarik Edilen Uygulamalarda Kullanım Amacına Uygun Olmayan Özellik/Arka Kapı Bulunmaması	Mülakat, Gözden Geçirme	Tedarik edilen veya hizmet alımı ile geliştirilen uygulamaların; yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınıyor mu?
3.2.6.4	Arayüzün Türkçe Dil Desteğine Sahip Olması	Mülakat	Bk. Denetim No: 4.6.1.4
3.2.6.5	Güncel İstemci ve Sunucu Teknolojilerinin Kullanılması	Mülakat, Gözden Geçirme	Belirli aralıklarla kullanılan istemci ve sunucu teknolojilerinin mevcut sürümlerinin bilinen zafiyet içerip içermediği kontrol ediliyor mu? Mevcut istemci ve sunucu teknolojilerinin eski versiyona sahip olduğu ya da kullanılan teknolojilerin bilinen zafiyet içerdiği tespit edildiğinde ne gibi önlemler alınmaktadır?
3.2.6.6	Uygulama Güvenlik Testlerinin Yapılması	Mülakat, Gözden Geçirme	Devreye alınan, güncellenen veya kaynak kodları ile tedarik edilen uygulamalar için sızma testleri gerçekleştiriliyor mu? İlgili testler neticesinde elde edilmiş sonuçlara göre düzeltici/önleyici tedbirler alınıyor mu?
3.2.6.7	Kaynak Kod Güvenlik Analizlerinin Yapılması	Mülakat, Gözden Geçirme	Kurumun kaynak koduna sahip olduğu tüm uygulamalar devreye alım öncesinde kaynak kod analizinden geçirilmekte midir?
3.2.6.8	Güvenli Yazılım Geliştirme Süreçlerinin Uygulanması	Mülakat, Gözden Geçirme	Güvenli yazılım geliştirme süreçleri ve/veya olgunluk modelleri uygulanıyor mu? Kurumsal yazılım geliştirme süreçleri güvenli yazılım geliştirme yaşam döngüsü süreçleri ve modellerinden faydalanılarak güncelleniyor mu?

3.2.7. Veri Tabanı ve Kayıt Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.7.1	1	Ortak Hesap Kullanılmaması ve En Az Yetki Prensibinin Uygulanması	Her veri tabanı kullanıcısı (kullanıcı, yönetici, uygulama vb.) için ayrı hesaplar tanımlanarak ortak hesap kullanılmamalıdır. En az ayrıcalık ilkesi kapsamında, kullanıcılara veri tabanı üzerinde gerçekleştirebilecekleri işlemler için gereken minimum yetkilerin haricinde bir ayrıcalık tanımlanmamalıdır. Bk. Tedbir No: 5.2.1.7
3.2.7.2	1	Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması	Kurumların kendi özel sistemleri veya yurt içinde yerleşik kurum kontrolündeki hizmet sağlayıcılar hariç olmak üzere kurumsal kritik verilerin saklanması/depolanması amacıyla bulut depolama hizmetleri kullanılmamalıdır. Bk. Tedbir No: 4.3.1.1
3.2.7.3	1	Veri Tabanlarına ve Verinin Saklandığı Ortamlara Yalnızca Yetkili Kullanıcıların Erişebilmesi	Veri tabanlarına ve verinin saklandığı ortamlara erişimin sadece yetkili kullanıcılar tarafından gerçekleştirilebilmesi için ilgili kaynaklar (güvenlik duvarı, işletim sistemi vb.) üzerinde yetkilendirme ve ayarlar yapılmalıdır.
3.2.7.4	1	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Veri tabanının dışarıya aktarımı (dosya olarak kaydetme, yerel veya uzak uygulamalara transfer etme vb.) sadece yetkili olan hesaplarla yapılmalıdır.
3.2.7.5	1	Veri Tabanlarında Varsayılan Kullanıcı ve Parolaların Kullanılmaması	Bk. Tedbir No: 5.2.1.3
3.2.7.6	1	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Bk. Tedbir No: 5.2.1.4
3.2.7.7	1	Test ve Geliştirme Ortamında Kullanılan Veri Tabanı Üzerinde Gerçek Veri Bulundurulmaması	Gerçek veri, test verisi olarak kullanılmamalıdır. Bu kapsamda geliştirme ve/veya test ortamlarında bulunan veri tabanı, gerçek veri barındırmamalıdır. Bunun yerine ilgili işlemler için özel üretilmiş veriler kullanılmalıdır. Bk. Tedbir No: 3.2.6.2
3.2.7.8	1	Kullanıcıların Denetim Kayıtları Üzerinde Değişiklik Yapmasının Engellenmesi	Kullanıcıların denetim kayıtları üzerinde değişiklik yapması engellenmelidir. Bunun için kullanıcıların ilgili kaynaklar (tablo, dosya vb.) üzerindeki yetkilerinin sınırlandırılması, kayıtların güvenli olarak farklı bir lokasyona kopyalanması vb. yöntemler kullanılabilir.
3.2.7.9	1	Veri Tabanı Versiyonunun Güncel ve Güvenlik Yamalarının Yüklü Olması	Bk. Tedbir No: 5.2.1.1
3.2.7.10	1	Veri Tabanı Üzerinde Özel Nitelikli Kişisel Verinin Açık Metin Olarak Tutulmaması	Veri tabanı üzerinde yer alan özel nitelikli kişisel veriler açık metin olarak tutulmamalıdır. İlgili bilgiler, ulusal ve/veya uluslararası standartlar tarafından kabul görmüş kriptografik yöntemlerden faydalanılarak saklanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.7.11	1	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Bk. Tedbir No: 5.2.1.5
3.2.7.12	1	Ayrıcalıkların Roller ve/veya Profiller Üzerinden Verilmesi	Tüm ayrıcalıklar veri tabanının sunduğu imkânlar dâhilinde en az yetki prensibine uyularak kullanıcılar yerine rollere ve/veya profillere tanımlanmalıdır. Kullanıcılar için mümkün olduğunca varsayılan roller ve profiller tercih edilmemeli, en uygun rol ve/veya profil ilgili kullanıcıya atanmalıdır. Bk. Tedbir No: 5.2.1.8
3.2.7.13	1	Veri Kurtarma Prosedürünün Hazırlanması	Verilerin yanlışlıkla silinmesine karşı verinin geri döndürülebilmesi için veri tabanı yönetim sisteminin sağladığı yedekleme ve kurtarma mekanizmaları önceden kurulmalıdır. Düzenli veri tabanı yedeği alınmalıdır.
3.2.7.14	1	Yedeklerin Güvenliğinin Sağlanması	Bk. Tedbir No: 5.2.1.11
3.2.7.15	1	Varsayılan Yapılandırmaların Kullanılmaması	Veri tabanlarında varsayılan güvensiz yapılandırmalar (iletişim protokolü, ihtiyaç duyulmayan veri tabanı özellikleri, varsayılan olarak güvensiz yapılandırılmış parametreler vb.) kullanılmamalıdır. Bk. Tedbir No: 5.2.1.2
3.2.7.16	2	Yetkili Kullanıcı İşlemlerinin Kaydedilmesi	Veri tabanı üzerinde yetkili kullanıcılar tarafından gerçekleştirilen işlemler için denetim kayıtları oluşturulmalıdır. Bu kapsamda ilgili denetim politikaları/prosedürleri kurum ihtiyaçları doğrultusunda belirlenerek veri tabanı üzerinde uygulanmalıdır.
3.2.7.17	2	Kritik Tablolar ve Görüntüler Üzerindeki Yetkilerin Denetlenmesi	Kritik veri tabanı tabloları ve görüntüleri (view) üzerindeki yetkiler periyodik olarak gözden geçirilmeli ve denetlenmelidir.
3.2.7.18	3	Tüm Kullanıcı İşlemlerinin Kaydedilmesi	Veri tabanı üzerinde bulunan tüm kullanıcılar tarafından gerçekleştirilen işlemler için denetim kayıtları oluşturulmalıdır. Bu kapsamda ilgili denetim politikaları/prosedürleri kurum ihtiyaçları doğrultusunda belirlenerek veri tabanı üzerinde uygulanmalıdır.
3.2.7.19	3	Saklama Gereksinimi Sona Eren Kritik Verinin Güvenli Silinmesi	Saklama gereksinimi sona eren kritik veri geri getirilemeyecek şekilde silinmelidir.
3.2.7.20	3	İşlenmesi Asıl Amaç Olmayan Verilerin Veri Tabanı Sunucusundan Maskelenerek Sunulması	İşlenmesi asıl amaç olmadığı durumlarda maskelenmesine ihtiyaç duyulan veriler dokümante edilerek belirlenmelidir. Bu kapsamda dokümante edilmiş ilgili veriler, işlenmesi asıl amaç olmadığında kullanıcının yetkisi doğrultusunda veri tabanı sunucusundan maskelenerek sunulmalıdır.
3.2.7.21	3	Veri Tabanına Gönderilen Sorguların Kontrol Edilmesi	Veri tabanına gönderilen tüm sorgular içerik ve yazım açısından denetlenmeli, olası enjeksiyon saldırıları engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.7.22	3	Kritik Veri İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Bk. Tedbir No: 5.2.1.20

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.7.1	Ortak Hesap Kullanılmaması ve En Az Yetki Prensibinin Uygulanması	Mülakat, Sızma Testi	Her veri tabanı kullanıcısı için ayrı hesap tanımlanıyor mu? Kullanıcılar üzerinde, veri tabanında gerçekleştirebilecekleri işlemler için gereken minimum yetkilerin haricinde bir ayrıcalık mevcut mu?
3.2.7.2	Bulut Depolama Hizmetlerinde Kurumsal Verilerin Bulundurulmaması	Mülakat, Gözden Geçirme	Kurumların kendi özel sistemleri üzerinde veya yurt içinde yerleşik hizmet sağlayıcılar hariç olmak üzere bulut depolama hizmetlerinde veriler saklanmakta veya depolanmakta mıdır?
3.2.7.3	Veri Tabanlarına ve Verinin Saklandığı Ortamlara Yalnızca Yetkili Kullanıcıların Erişebilmesi	Mülakat, Güvenlik Denetimi	Veri tabanlarına ve verinin saklandığı ortamlara erişimde yetkilendirme mekanizması kullanılıyor mu?
3.2.7.4	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Mülakat, Güvenlik Denetimi	Hangi kullanıcılar veri tabanının dışarıya aktarımında kullanılabilir? Veri tabanının dışarıya aktarımında yetkilendirilmiş olan hesapların hangileri olduğu periyodik denetleniyor mu?
3.2.7.5	Veri Tabanlarında Varsayılan Kullanıcı ve Parolaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Veri tabanında varsayılan hesaplar ve/veya varsayılan parolalar kullanılıyor mu?
3.2.7.6	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Mülakat, Güvenlik Denetimi	Veri tabanı kullanıcıları için parola politikaları tanımlanmış mı?
3.2.7.7	Test ve Geliştirme Ortamında Kullanılan Veri Tabanı Üzerinde Gerçek Veri Bulundurulmaması	Mülakat, Güvenlik Denetimi	Geliştirme ve/veya test ortamlarında bulunan veri tabanı, gerçek veri barındırıyor mu? İlgili ortamlarda kullanılan/kullanılacak veriler nasıl oluşturulmaktadır?
3.2.7.8	Kullanıcıların Denetim Kayıtları Üzerinde Değişiklik Yapmasının Engellenmesi	Mülakat, Güvenlik Denetimi	Kullanıcıların denetim kayıtları üzerinde değişiklik yapabilmesinin önüne geçmek adına hangi önlemler alınmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.7.9	Veri Tabanı Versiyonunun Güncel ve Güvenlik Yamalarının Yüklü Olması	Mülakat, Sızma Testi	Veri tabanı için güncelleştirmeler ve güvenlik yamaları belirli periyotlar ile kontrol edilerek uygulanıyor mu?
3.2.7.10	Veri Tabanı Üzerinde Özel Nitelikli Kişisel Verinin Açık Metin Olarak Tutulmaması	Mülakat, Gözden Geçirme	Veri tabanı üzerinde yer alan özel nitelikli kişisel veriler kriptografik yöntemler kullanılarak saklanmakta mıdır?
3.2.7.11	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Veri tabanı sunucularına yapılan uzak bağlantıların güvenliği nasıl sağlanıyor?
3.2.7.12	Ayrıcalıkların Roller ve/veya Profiller Üzerinden Verilmesi	Mülakat, Güvenlik Denetimi	Kullanıcılara ayrıcalıklar doğrudan atanıyor mu? Varsayılan roller ve profiller kullanılıyor mu?
3.2.7.13	Veri Kurtarma Prosedürünün Hazırlanması	Mülakat, Gözden Geçirme	Olası veri kayıplarına karşı nasıl bir önlem alınmıştır? Düzenli olarak yedek alınmakta mıdır? Yedekler nerede ve nasıl muhafaza edilmektedir?
3.2.7.14	Yedeklerin Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme, Sızma Testi	Yedek dosyalarına yetkisiz erişimleri engellemek adına hangi önlemler alınmaktadır?
3.2.7.15	Varsayılan Yapılandırmaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Veri tabanında, varsayılan güvensiz yapılandırmalar (iletişim protokolü, ihtiyaç duyulmayan veri tabanı özellikleri, varsayılan olarak güvensiz yapılandırılmış parametreler vb.) bilinen güvenli değerler/yöntemler ile değiştirilerek oluşabilecek zafiyetlere karşı önlemler alınıyor mu?
3.2.7.16	Yetkili Kullanıcı İşlemlerinin Kaydedilmesi	Mülakat, Güvenlik Denetimi	Veri tabanı denetleme mekanizması aktif mi? Veri tabanı denetim kayıtları, hangi denetim politikaları/prosedürleri göz önünde bulundurularak oluşturulmaktadır? Veri tabanında yetkili kullanıcıların yaptığı işlemler kayıt altına alınıyor mu?
3.2.7.17	Kritik Tablolar ve Görüntüler Üzerindeki Yetkilerin Denetlenmesi	Mülakat, Güvenlik Denetimi	Periyodik olarak kritik veri tabanı tabloları ve görüntüleri (view) üzerinde yetkilere sahip olan kullanıcılar/roller analiz ediliyor mu?
3.2.7.18	Tüm Kullanıcı İşlemlerinin Kaydedilmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Veri tabanı denetleme mekanizması aktif mi? Veri tabanı denetim kayıtları, hangi denetim politikaları/prosedürleri göz önünde bulundurularak oluşturulmaktadır? Veri tabanında tüm kullanıcıların yaptığı işlemler kayıt altına alınıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.7.19	Saklama Gereksinimi Sona Eren Kritik Verinin Güvenli Silinmesi	Mülakat, Gözden Geçirme	Kritik verinin kullanımları tamamlandığında üzerlerinde ne gibi işlemlerin uygulanacağı tanımlanmış mıdır? Tanımlanmış faaliyetler nasıl uygulanmaktadır?
3.2.7.20	İşlenmesi Asıl Amaç Olmayan Verilerin Veri Tabanı Sunucusundan Maskelenerek Sunulması	Mülakat, Sızma Testi	Hangi verilerin maskelenerek kullanılacağı dokümante edilmiş midir? Veri tabanı üzerinde bulunan ilgili veriler, işlenmesi asıl amaç olmadığında kullanıcı yetkisi doğrultusunda maskelenerek sunulmakta mıdır?
3.2.7.21	Veri Tabanına Gönderilen Sorguların Kontrol Edilmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Veri tabanına gönderilen tüm sorgular için uygulamadan bağımsız olarak içerik ve yazım denetimi yapılmakta mıdır?
3.2.7.22	Kritik Veri İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kritik veri içeren veri tabanı sunucularında bulunan durağan verinin güvenliğinin sağlanmasında hangi yöntemler kullanılmaktadır?

3.2.8. Hata Ele Alma ve Kayıt Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.8.1	1	Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi	Uygulamalar, tüm oluşabilecek hataları yakalayabilecek ve hata durumlarında varsayılan olarak güvenli durumlara geçecek şekilde tasarlanmış olmalıdır. Örneğin, yetkilendirme esnasında hata oluşması durumunda uygulama ilgili işlemi durdurmalı ve kullanıcı yetkilendirilmemelidir. Kimlik doğrulama işlemi sırasında hata ile karşılaşıldığında ise kullanıcının uygulamaya girişi engellenmelidir. Hata durumu ile ilgili detaylar kullanıcıya gösterilmemelidir.
3.2.8.2	1	Hataların ve Tanımlanan Olayların İz Kayıtlarının Oluşturulabilmesi	Uygulama, tanımlanan güvenlik olaylarının/işlemlerinin (yetki değişiklikleri, kullanıcı değişiklikleri, kimlik doğrulama işlemleri) başarılı ve başarısızlık durumları için iz kayıtları oluşturabilmelidir. İz kaydı minimum şu bilgileri içermelidir: • İşlemi yapan kullanıcı (gerçek kişi veya yazılımsal süreç için tanımlanmış kullanıcı) bilgisi • İşlem zamanı • Kaynak ve hedef sistem tanımlayıcı bilgileri (ip, sunucu adı vb.) • İşlem özeti (başarılı işlem, başarısız işlem vb.) Bk. Tedbir No: 3.1.8.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.8.3	1	Özel Nitelikli Kişisel Veri İçeren Hata Mesajının veya İz Kaydının Üretilmemesi	Uygulama, özel nitelikli kişisel veri içeren hata mesajı veya iz kaydı üretmemelidir.
3.2.8.4	1	İz Kayıtlarında Olayların Zaman Bilgisinin Yer Alması	İz kayıtlarında olayların zaman sıralamasına ilişkin araştırma yapılabilecek şekilde zaman bilgisi yer almalıdır. Bk. Tedbir No: 3.1.8.3
3.2.8.5	1	İz Kayıtlarının Güvenliğinin Sağlanması	Uygulama, uygulama sunucusu ele geçirildiğinde iz kayıtlarının güvenliğini sağlamak amacıyla değiştirilmesine veya silinmesine izin vermemelidir. Bk. Tedbir No: 3.1.8.1
3.2.8.6	1	İz Kayıtlarının Saldırı Vektörü Olarak Kullanımının Engellenmesi	Kayıtların doğruluğunu sağlamak ve bütünlüğünün bozulmasını (log forging) engellemek için iz kayıtları oluşturulurken kullanılan girdiler üzerinde girdi denetimi yapılmalıdır. Kayıtlar görüntülenirken oluşabilecek zafiyetlere (XSS vb.) karşı ise karakter kodlama ve filtreleme gibi tedbirler uygulanmalıdır. Bk. Tedbir No: 3.2.10.12

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.8.1	Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi	Mülakat, Sızma Testi	Uygulamalarda hata ile karşılaşılması durumunda takip edilecek adımlar/faaliyetler tanımlanmış mıdır?
3.2.8.2	Hataların ve Tanımlanan Olayların İz Kayıtlarının Oluşturulabilmesi	Mülakat, Gözden Geçirme	Uygulama için önceden tanımlanan güvenlik olayları için hem başarılı hem de başarısız işlemler kayıt altına alınabilmekte midir? Oluşturulan iz kayıtlarında hangi bilgiler yer almaktadır?
3.2.8.3	Özel Nitelikli Kişisel Veri İçeren Hata Mesajının veya İz Kaydının Üretilmemesi	Mülakat, Gözden Geçirme	Hata mesajlarının ve iz kayıtlarının hangi bilgileri içereceği dokümante ediliyor mu? Hata mesajlarının ve iz kayıtlarının içereceği bilgiler arasında önceden tanımlanmış olan özel nitelikli kişisel veri bulunmakta mıdır?
3.2.8.4	İz Kayıtlarında Olayların Zaman Bilgisinin Yer Alması	Mülakat, Gözden Geçirme	Oluşturulan iz kayıtlarında doğru zaman bilgisi mevcut mudur? Oluşturulan iz kayıtlarında kullanılan zaman bilgisi formatı/biçimi tanımlanmış mıdır?
3.2.8.5	İz Kayıtlarının Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme	İz kayıtlarının güvenliğinin sağlanması için uygulanabilir adımlar/süreçler tasarım dokümanında tanımlanmış mı? İz kayıtları için mevcut bir yetkilendirme mekanizması kullanılıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.8.6	İz Kayıtlarının Saldırı Vektörü Olarak Kullanımının Engellenmesi	Mülakat, Gözden Geçirme, Sızma Testi	İz kayıtlarının veri yapısı ve veri sınırlaması tanımlanmış mıdır? İz kayıtlarında saldırı için kullanılabilecek kullanıcı girdisi üzerinde girdi denetimi yapılmakta mıdır?

3.2.9. İletişim Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.9.1	1	SSL/TLS Protokolünün Güvenli Kullanılması	Kimlik doğrulaması yapılmış, kritik veri ya da işlevler içeren tüm bağlantılar SSL/TLS protokolünün bilinen zafiyet içermeyen güvenilir sürümü ile yapılmalıdır. Sertifikalarda ve sertifikanın tüm hiyerarşisinde ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş güçlü algoritmalar ve protokoller kullanılmalıdır.
3.2.9.2	1	Sertifika Denetimlerinin Yapılması	Güvenilen bir sertifika otoritesinden her Transport Layer Security (TLS) sunucu sertifikasına bir güven zinciri oluşturulabilmeli ve internet üzerinden erişilebilen her sunucu sertifikası geçerli olmalıdır. Uygulama, Çevrimiçi Sertifika Durum Protokolü Damgalama (OCSP stapling) gibi yöntemlerle sertifika iptal denetimi gerçekleştirebilecek şekilde yapılandırılmalıdır.
3.2.9.3	2	HSTS Kullanılması	Web sayfalarına gerçekleştirilecek bağlantıların ve kullanılacak kaynakların güvenliği için HSTS kullanılmalıdır.
3.2.9.4	3	Hatalı Sertifikaların Tespiti	Uygulama adına oluşturulabilecek hatalı sertifikalar için sertifika şeffaflığı logları (Certificate Transparency Logs) üzerinde düzenli olarak kontroller yapılmalıdır.
3.2.9.5	3	SSL/TLS Hata İz Kayıtları	SSL/TLS bağlantı hatası durumları için iz kaydı oluşturulmalıdır.
3.2.9.6	3	Kritik Verinin Şifrelenmesi	Ulusal düzeyde kritik veri işleyen uygulamalar tarafından oluşturulan trafikten kripto analiz yöntemleri ile bilginin ifşası için yapılabilecek saldırılar engellenmelidir. Bu veri şifreli trafik üzerinden ayrıca şifrelenerek taşınmalıdır.
3.2.9.7	3	Kurum Tarafından Onaylanmış Sertifikaların Kullanılması	Yazılımlarda kullanılmak üzere üretilmiş sertifikaların kaynağı kontrol edilmelidir. Yazılımlarda sadece kurum tarafından belirlenen kaynak/otorite tarafından üretilmiş sertifikaların kullanılması sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.9.1	SSL/TLS Protokolünün Güvenli Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Şifreli iletişim için hangi protokol versiyonu kullanılıyor? Sertifikalarda kullanılabilecek algoritmalar ve protokoller tanımlanmış mı? Sertifikalarda kullanılan algoritmalar ve protokoller ulusal ve/veya uluslararası otoriteler tarafından güvenli/uygulanabilir olarak kabul ediliyor mu?
3.2.9.2	Sertifika Denetimlerinin Yapılması	Mülakat, Gözden Geçirme	Mevcut sunucuların sertifikalarının geçerliliği belirli zamanlarda kontrol ediliyor mu? Otomatik olarak sertifika iptal denetimi gerçekleştirilebiliyor mu?
3.2.9.3	HSTS Kullanılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Gerçekleştirilecek bağlantıların ve kullanılacak kaynakların güvenliği için HSTS kullanılıyor mu?
3.2.9.4	Hatalı Sertifikaların Tespiti	Mülakat, Gözden Geçirme	Uygulama adına oluşturulabilecek hatalı sertifikalar için sertifika şeffaflığı logları (Certificate Transparency Logs) üzerinde düzenli olarak kontroller yapılıyor mu?
3.2.9.5	SSL/TLS Hata İz Kayıtları	Mülakat, Gözden Geçirme	SSL/TLS bağlantı hatası durumlarında iz kaydı oluşturuluyor mu?
3.2.9.6	Kritik Verinin Şifrelenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Ulusal düzeyde kritik uygulama verisinin taşınmasında ne gibi güvenlik önlemleri alınıyor?
3.2.9.7	Kurum Tarafından Onaylanmış Sertifikaların Kullanılması	Mülakat, Gözden Geçirme	Kurum tarafından yetkilendirilmiş sertifika otoriteleri/üreticileri belirlenmiş ve dokümante edilmiş midir? Onaylı olmayan sertifikaların cihazlara ve yazılımı kurulumunu engellemek amacıyla hangi yöntemler kullanılmaktadır? Kurumda sertifika üretme/temin etme konusunda görevlendirilmiş personel bulunmakta mıdır?

3.2.10. Kötücül İşlemleri Engelleme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.10.1	1	Sunucu Tarafında Girdi Doğrulama Denetiminin Yapılması	Uygulama sunucu tarafında, kabul edilen her bir veri tipi için girdi doğrulama denetimi yapmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.10.2	1	Girdi Doğrulama Hataları için İz Kaydının Oluşturulması	Sistemlerde (sunucu, uygulama vb.) yapılan girdi doğrulama işlemi sırasında oluşan hatalar için iz kayıtları oluşturulmalı ve ilgili istek reddedilmelidir. Bk. Tedbir No: 3.1.8.1
3.2.10.3	1	Uygulamanın Yetkisiz Olarak Program Çalıştırmasının Engellenmesi	Uygulamanın fonksiyonel gereksinimlerini karşılamak amacıyla ihtiyaç duyduğu programlar haricinde program/uygulama çalıştırması engellenmelidir.
3.2.10.4	1	Kritik Bilgilerin Formlarda Bulunan Gizli Alanlarda Saklanmaması	Form yapısını kullanan uygulamalar, kritik bilgileri formlarda bulunan gizli alanlarda saklamamalıdır.
3.2.10.5	1	CSRF Saldırılarına Karşı Önlem Alınması	Siteler arası istek sahteciliği (CSRF) zafiyetine karşı gerekli güvenlik önlemleri (CSRF token, SameSite bayrağı vb.) alınmalıdır.
3.2.10.6	1	Veri Tabanına Erişimde Kullanılan Dile Karşı Enjeksiyon Saldırılarının Önlenmesi	Bütün veri tabanı sorguları, parametrik olarak yapılmalı ve veri tabanına erişimde kullanılan dile karşı (SQL, NoSQL vb.) enjeksiyon saldırılarını engelleyebilecek güvenlik önlemleri alınmalıdır.
3.2.10.7	1	İşletim Sistemi Komut Enjeksiyonu Açıklarının Önlenmesi	İşletim sistemi komut enjeksiyonu açıklarına karşı güvenlik önlemleri alınmalıdır.
3.2.10.8	1	Bellek Taşması Saldırılarının Önlenmesi	Uygulama ve uygulamanın çalışma ortamında bellek taşması saldırılarına karşı önlem alınmalıdır.
3.2.10.9	1	Dosya İçerme Açıklarının Önlenmesi	Uygulama, dosya yolunu girdi olarak alıyor ise uzak ya da yerel dosya içerme açıklarını önleyici güvenlik denetimlerini yapmalıdır.
3.2.10.10	1	XML Tabanlı Saldırıların Önlenmesi	Uygulama, XML açıklarını (XPath sorgu saldırıları, XML harici öğe saldırıları, XML enjeksiyonu vb.) önleyici güvenlik denetimlerini yapmalıdır.
3.2.10.11	1	Yapısal Olmayan Veri için Karakterlerin Denetlenmesi	Yapısal olmayan veriler (belirli bir formata/biçime sahip olmayan) için izin verilen karakterler ve uzunluklar belirlenerek verinin içeriğinde olabilecek olası zararlı karakterlere karşı girdi kontrolü yapılmalıdır.
3.2.10.12	1	Girdi Denetimi Yapılması	HTML form alanlarının veri girdileri, REST çağrıları, HTTP üst başlıkları, çerezler, toplu işlem dosyaları gibi veri girdileri için doğrulama denetimi yapılmalıdır.
3.2.10.13	1	Yüklenen Dosyaların Denetlenmesi	Bk. Tedbir No: 3.2.4.5
3.2.10.14	2	İsteklerin Öngörülmeyen Büyüklükte Olup Olmadığının Kontrol Edilebilmesi	Uygulama sunucusuna gelen isteklerin öngörülmeyen bir sayıda ya da büyüklükte olup olmadığı kontrol edilebilmelidir. Bk. Tedbir No: 5.3.1.8

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.10.15	3	TS ISO/IEC 19790-24759 Onaylı Kriptografik Modüllerin ve Rastgele Sayı Üreteçlerinin Kullanılması	Uygulamada şifreleme, anahtar değişimi, dijital imzalama veya özet alma gibi fonksiyonlar bulunuyorsa TS ISO/IEC 19790-24759 onaylı kriptografik modüller ve rastgele sayı üreteçleri kullanılmalıdır.
3.2.10.16	3	Karakter Kodlamasının Tespiti	Girdi-çıktı denetimi yapılmadan önce veri üzerinde karakter kodlaması (character encoding) yapılıp yapılmadığı tespit edilmelidir. Tespit edilen kodlamaya göre denetimler gerçekleştirilmelidir.
3.2.10.17	3	Uygulama Seviyesi Servis Dışı Bırakma Saldırılarının Engellenmesi	Uygulamalara servis dışı bırakma saldırılarını önlemek için güvenlik mekanizmaları (tasarım seviyesinde önlem, uygulama seviyesi DoS çözümleri, web uygulama güvenlik duvarı kullanımı vb.) hayata geçirilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.10.1	Sunucu Tarafında Girdi Doğrulama Denetiminin Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamada kullanılan mevcut bir girdi doğrulama mekanizması var mı? Girdi doğrulama mekanizması her veri tipi için kullanılıyor mu?
3.2.10.2	Girdi Doğrulama Hataları İçin İz Kaydının Oluşturulması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın hata ile karşılaşması durumunda takip edeceği adımlar/faaliyetler tasarım dokümanında tanımlanmış mı? Girdi doğrulama işlemi esnasında karşılaşılan hatalar kayıt altına alınıyor mu?
3.2.10.3	Uygulamanın Yetkisiz Olarak Program Çalıştırmasının Engellenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın fonksiyonel gereksinimlerini karşılamak amacıyla ihtiyaç duyduğu programlar haricinde program/uygulama çalıştırmaması engelleniyor mu? Program/uygulama çalıştırmaması amacıyla uygulanan yöntem/mekanizmalar nelerdir?
3.2.10.4	Kritik Bilgilerin Formlarda Bulunan Gizli Alanlarda Saklanmaması	Mülakat, Gözden Geçirme, Sızma Testi	Kritik bilgiler formlarda bulunan gizli alanlarda saklanıyor mu?
3.2.10.5	CSRF Saldırılarına Karşı Önlem Alınması	Mülakat, Gözden Geçirme, Sızma Testi	CSRF kaynaklı zafiyetleri önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? CSRF kaynaklı zafiyetlere karşı açığın bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda CSRF zafiyetlerine karşı açığı bulunan uygulama için hangi önlemler alındı?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.10.6	Veri Tabanına Erişimde Kullanılan Dile Karşı Enjeksiyon Saldırılarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Veri tabanı işlemleri için parametrik sorgular mı kullanılıyor? Veri tabanına erişimde kullanılan dile karşı enjeksiyon saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Veri tabanına erişimde kullanılan dile karşı enjeksiyon saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda veri tabanına erişimde kullanılan dile karşı enjeksiyon saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.7	İşletim Sistemi Komut Enjeksiyonu Açıklarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Komut enjeksiyonu saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Komut enjeksiyonu saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda komut enjeksiyonu saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.8	Bellek Taşması Saldırılarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Bellek taşması saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Bellek taşması saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda bellek taşması saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.9	Dosya İçerme Açıklarının Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Uzak ya da yerel dosya içerme saldırılarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? Uzak ya da yerel dosya içerme saldırılarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda uzak ya da yerel dosya içerme saldırılarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.10	XML Tabanlı Saldırıların Önlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	XML açıklarını önlemek için nelerin yapılacağı tasarım dokümanında tanımlanmış mı? XML açıklarına karşı zafiyetin bulunup bulunmadığını tespit etmek için analiz yapıldı mı? Analizler sonucunda XML açıklarına karşı zafiyetli bulunan uygulama için hangi önlemler alındı?
3.2.10.11	Yapısal Olmayan Veri için Karakterlerin Denetlenmesi	Mülakat, Sızma Testi, Kaynak Kod Analizi	Uygulamada kullanılan mevcut bir girdi doğrulama mekanizması var mı? Mevcut girdi doğrulama mekanizması yapısal olmayan veri için kullanılabiliyor mu? Yapısal olmayan verinin girdi doğrulamasında hangi faaliyetler/yöntemler uygulanıyor?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.10.12	Girdi Denetimi Yapılması	Mülakat, Sızma Testi, Kaynak Kod Analizi	Uygulamada kullanılan mevcut bir girdi doğrulama mekanizması var mı? HTML girdilerinin işleme alınmadan önce kontrol edilmesi için girdi doğrulama mekanizması kullanılıyor mu?
3.2.10.13	Yüklenen Dosyaların Denetlenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Bk. Denetim No: 3.2.4.5
3.2.10.14	İsteklerin Öngörülmeyen Büyüklükte Olup Olmadığının Kontrol Edilebilmesi	Gözden Geçirme, Sızma Testi	Uygulamaya gelen isteklerin ve yüklenecek dosyaların üst sınır büyüklükleri belirlenmiş midir? Bu sınırlar uygulama tarafından kontrol edilmekte midir?
3.2.10.15	TS ISO/IEC 19790-24759 Onaylı Kriptografik Modüllerin ve Rastgele Sayı Üreteçlerinin Kullanılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Kullanılan kriptografik modüller/rastgele sayı üreteçleri TS ISO/IEC 19790-24759 onaylı mıdır?
3.2.10.16	Karakter Kodlamasının Tespiti	Mülakat, Sızma Testi, Kaynak Kod Analizi	Girdi-çıktı denetimi yapılmadan önce gerçekleştirilecek faaliyetler tasarım dokümanında tanımlanmakta mıdır? Girdi-çıktı denetimi yapılmadan önce karakter kodlaması doğrulaması yapılmakta mıdır?
3.2.10.17	Uygulama Seviyesi Servis Dışı Bırakma Saldırılarının Engellenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Uygulama seviyesinde oluşabilecek servis dışı bırakma saldırılarını önlemek için hangi güvenlik mekanizmaları kullanılmaktadır?

3.2.11. Dış Sistem Entegrasyonlarının Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.11.1	1	Web Servislerinin Güvenli Protokol Üzerinden Sunulması	Dışarıya açılan web servisleri; iyi yapılandırılmış, bilinen zafiyet içermeyen, güncel SSL/TLS versiyonlarını destekleyen bir protokol ile sunacak şekilde tasarlanmalıdır. Bk. Tedbir No: 3.2.9.1
3.2.11.2	1	Web Servisi Yapılandırmalarının Yetkili Kullanıcılar Tarafından Yapılması ve Yönetilmesi	Web Servisi yapılandırmaları (konumlandırma, açılacak servis portlarının tahsisi, ağ yapılandırması vb.) yetkili kullanıcılar tarafından yapılmalı ve yönetilmelidir. Varsayılan olarak yapılandırmalar güvenliği en üst düzeyde sağlayacak şekilde belirlenmelidir.
3.2.11.3	1	Web Servis Çağrılarında Kimlik Doğrulama ve Yetkilendirme Kontrolü	Her servis çağrısı için kimlik doğrulama ve yetkilendirme kontrolü yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.2.11.4	1	Sunulan Web Servislerin Girdi-Çıktı Denetimlerinin Yapılması	Sunulan web servisleri, girdi-çıktı denetimlerinin eksikliğinden kaynaklı saldırı çeşitlerine (XSS, uzak kod çalıştırma vb.) karşı önlem alacak şekilde geliştirilmeli ve konumlandırılmalıdır. Web servisi geliştirme aşamasında bilinen zafiyet içeren bileşenler (çatı, kütüphane, yazılım modülleri vb.) kullanılmamalıdır. Bk. Tedbir Başlık No: 3.2.10
3.2.11.5	1	Web Servis Yapılandırma ve Yönetim İşlemleri	Uygulama, web servis yapılandırma ve yönetim işlevlerine sadece yetkili kullanıcıların erişebilmesini sağlamalıdır.
3.2.11.6	2	Entegre Olunan Sistemin Web Servislerinin Beklenen Şekilde Çalıştığının Doğrulanması	Mevcut sistemde entegre olunan sistemden kaynaklanan hataların tolere edilebilmesi için gerekli önlemler (eşik değerinin aşılması, veri uyuşmazlığının olması vb. durumda uyarı mekanizmalarının aktif edilmesi) alınmalıdır.
3.2.11.7	2	Uygulamanın Kararlılığının Sağlanması	Uygulamanın entegre olunan sisteme ulaşamaması veya sistemin hata dönmesi durumlarında, uygulama kararlı ve güvenli şekilde işlemlerini devam ettirebilecek şekilde tasarlanmalıdır. Uygulama bu durumlarda hizmet sürekliliğini sağlayacak fonksiyonlara sahip olmalıdır.
3.2.11.8	2	Web Servisi Çağrı Sayısının ve Kaynak Kullanımının Sınırlandırılması	Kullanıcıların belirli bir süre içinde yapabilecekleri çağrı sayısı ve maksimum kaynak kullanımı her bir kullanıcı için belirlenebilmelidir. Sınır aşımında çağrılara cevap verilmemeli veya çağrılar engellenmelidir.
3.2.11.9	3	Dış Sistemler / Uygulamalar Arası Çağrıların Kayıt Altına Alınması	Dış sistemler ve uygulamalar arasındaki çağrıların girdi parametreleri ve sonuçları çağrıyı yapan ve sunan uygulamalar tarafından kayıt altına alınmalıdır.
3.2.11.10	3	Kritik Altyapı Sistemleri ile Güvenli İletişimin Sağlanması	Kritik altyapı sistemleri ile entegrasyonda özel hatlar (kiralık hat, özel güvenli ağ vb.) kullanılmalı ve yedekliliği için altyapı hazırlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.11.1	Web Servislerinin Güvenli Protokol Üzerinden Sunulması	Mülakat, Gözden Geçirme, Sızma Testi	Güvenli iletişim için kullanılan mevcut SSL/TLS protokolü ilgili zafiyet ve saldırılara karşı analiz edildi mi? Güvenli iletişim için kullanılan mevcut SSL/TLS protokolü yapılandırması ulusal ve/veya uluslararası otoriteler tarafından güvenli/uygulanabilir olarak kabul ediliyor mu?
3.2.11.2	Web Servisi Yapılandırmalarının Yetkili Kullanıcılar Tarafından Yapılması ve Yönetilmesi	Mülakat, Gözden Geçirme	Web servis yapılandırma ve yönetim işlevleri için mevcut bir yetkilendirme mekanizması kullanılıyor mu?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.2.11.3	Web Servis Çağrılarında Kimlik Doğrulama ve Yetkilendirme Kontrolü	Gözden Geçirme, Sızma Testi	Web servislerinde her çağrı için kimlik doğrulama ve yetkilendirme kontrolü yapılıyor mu?
3.2.11.4	Sunulan Web Servislerin Girdi-Çıktı Denetimlerinin Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamada kullanılan mevcut bir girdi-çıktı denetim mekanizması var mı? Mevcut girdi-çıktı denetim mekanizması web servis girdileri/çıktıları için kullanılabiliyor mu? Web servis girdileri/çıktıları için yapılan girdi-çıktı denetimlerinde hangi faaliyetler/yöntemler uygulanıyor? Yazılımda kullanılan bileşenler (çatı, kütüphane, yazılım modülleri vb.) ve uygulanan yamalar bilinen zafiyet içeriyor mu?
3.2.11.5	Web Servis Yapılandırma ve Yönetim İşlemleri	Mülakat, Gözden Geçirme, Sızma Testi	Uygulama üzerinden sunulan web servis yapılandırma ve yönetim işlevleri için mevcut bir yetkilendirme mekanizması kullanılıyor mu?
3.2.11.6	Entegre Olunan Sistemin Web Servislerinin Beklenen Şekilde Çalıştığının Doğrulanması	Mülakat, Gözden Geçirme, Sızma Testi	Entegre olunan sistemin web servislerinin beklenen şekilde çalıştığının doğrulaması nasıl yapılıyor?
3.2.11.7	Uygulamanın Kararlılığının Sağlanması	Mülakat, Gözden Geçirme, Sızma Testi	Entegre olunan sistemin web servislerine ulaşılamaması veya web servislerinin hata sonucu dönmesi durumlarında uygulamanın kararlılığı nasıl sağlanıyor? İlgili durumda ne gibi faaliyetlerin/süreçlerin uygulanacağı tanımlanmış mı?
3.2.11.8	Web Servisi Çağrı Sayısının ve Kaynak Kullanımının Sınırlandırılması	Mülakat, Gözden Geçirme, Sızma Testi	Web servisi mevcut kaynaklarının kasıtlı olarak tüketilmesini engellemek için ne gibi önlemler alınıyor?
3.2.11.9	Dış Sistemler / Uygulamalar Arası Çağrıların Kayıt Altına Alınması	Mülakat, Gözden Geçirme	Dış sistemler / uygulamalar arası çağrılar kayıt altına alınıyor mu? İlgili çağrılar için tutulmuş kayıtlar üzerinde geçmişe dönük analizler/denetimler gerçekleştiriliyor mu?
3.2.11.10	Kritik Altyapı Sistemleri ile Güvenli İletişimin Sağlanması	Mülakat, Gözden Geçirme	Kritik altyapı sistemleri ile entegrasyonda hangi iletişim altyapıları kullanılıyor?

3.3. Taşınabilir Cihaz ve Ortam Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, taşınabilir cihaz ve ortam güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "Taşınabilir Cihaz ve Ortam Güvenliği" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Akıllı Telefon ve Tablet Güvenliği
- Taşınabilir Bilgisayar Güvenliği
- Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)

3.3.1. Akıllı Telefon ve Tablet Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.1.1	1	Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı	Mobil cihazların kurum içinde kullanılabilmesi için taşınabilir cihazların kullanımı, uygunluğu ve uzaktan yönetimi ile ilgili aşağıdaki hususları içeren mobil cihaz kullanım politikası hazırlanmalı ve uygulanmalıdır. • Fiziksel koruma ile ilgili gereksinimler, • Parola tanımlama, • Yazılım kurulum kısıtları, • İşletim sistemi ve uygulama güncelleme politikası • Uzaktan devre dışı bırakma, silme ya da kilitleme • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Kurum, mobil cihaz üzerinden e-posta ve/veya VPN gibi kurumsal servislere erişim izni vermeden önce politikayı çalışana tebliğ etmelidir. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmamalıdır.
3.3.1.2	1	Mobil Cihazlarda Jailbreak veya Rootlama İşleminin Yapılmaması	Kurum bünyesinde geliştirilen uygulamalar rootlanmış/jailbreak yapılmış cihazlarda çalışmayı reddetmelidir. Kurum tarafından sağlanan telefon ve tabletler üzerinde jailbreak veya rootlama işlemi yapılmamalıdır.
3.3.1.3	1	Kullanıcılara Uygulama İzinleri Hakkında Eğitim Verilmesi	Mobil cihaz kullanıcılarına uygulamaların istedikleri izinler ve bu izinlerin riskleri hakkında eğitim verilmelidir. Bk. Tedbir No: 3.5.2.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.1.4	1	Mobil Cihaz Envanterinin Tutulması	Kuruma ait mobil cihazların yazılım ve donanım envanteri tutulmalıdır. Bk. Tedbir No: 3.1.1.1 Bk. Tedbir No: 3.1.2.1
3.3.1.5	1	Halka Açık Şarj İstasyonlarının Kullanılmaması	Çalışanlar mobil cihazlarını halka açık şarj istasyonlarında şarj etmemeleri konusunda bilgilendirilmelidir.
3.3.1.6	2	Cihazın Uzaktan Fabrika Ayarlarına Döndürülmesi	Cihazı uzaktan fabrika ayarlarına döndürüp içindeki veriyi silebilecek bir mekanizma kullanılmalıdır.
3.3.1.7	2	Tamire Verilen Cihazlarda Bulunan Verinin Silinmesi	Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek cihazlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler silinmelidir. Cihaz içindeki veri silinemeyecek durumda ise cihaz imha edilmelidir.
3.3.1.8	3	Güvenlik Yazılımlarının Yüklenmesi	Zararlı yazılımları tespit eden ve önleyen güvenlik uygulamaları kullanılmalıdır.
3.3.1.9	3	Taşınabilir Cihaz Yönetimi	Kritik veriye erişen kişisel ve kurumsal cihazlar uzaktan yönetilebilmeli, cihazlara güvenlik politikaları uygulanabilmeli ve gerek duyulduğunda politikalar uzaktan güncellenebilmelidir.
3.3.1.10	3	Taşınabilir Cihazların Ayrı Sistemlerde Kullanılması	Kritik seviyeli ağlarda kullanılan taşınabilir cihazlar, internete bağlı veya kurum dışı sistemlerde kullanılmamalıdır.
3.3.1.11	3	Parola Politikaları	Taşınabilir cihazlar için parola politikaları belirlenmeli ve ekran kilitleri için bu politikanın uygulanması zorunlu tutulmalıdır.
3.3.1.12	3	Çok Sayıda Hatalı Giriş Denemesi Yapılması Halinde Cihaz İçindeki Verinin Silinmesi	Kaba kuvvet saldırılarından korunmak için, kurum tarafından belirlenecek sayıda hatalı giriş denemesi sonrası cihaz belleğinde bulunan veriler silinmelidir.
3.3.1.13	3	Desteklenen Cihaz Listesinin Oluşturulması	Kurum bünyesinde kullanılacak cihazların listesi çıkartılmalı ve bu liste dışında bulunan cihazların kurum sistemlerine erişimi engellenmelidir.
3.3.1.14	3	Güncel Olmayan Cihazların Sistemlere Erişiminin Engellenmesi	Güncelleme almayan veya bilinen zafiyete sahip olan işletim sistemi veya uygulama barındıran cihazların kurum sistemlerine erişimi engellenmelidir.
3.3.1.15	3	Seyahat Kullanım Politikasının Tanımlanması	Yurt dışı seyahatleri sırasında kullanılacak cihazlar için bir kullanım politikası hazırlanmalı, cihazlar seyahat sonrası bu politikaya göre kontrol edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.1.1	Akıllı Telefon ve Tabletlerin Kabul Edilebilir Kullanımı	Mülakat, Gözden Geçirme	Kurum verisine erişen kişisel cihazlar için tanımlanmış bir mobil cihaz kullanım politikası var mıdır? Politika içeriğinde aşağıdaki konular ele alınmakta mıdır? • İşletim sisteminin ve uygulamaların güncel tutulması gerektiği belirtilmiş midir? • Güncelleme almayan cihazalar için ne gibi önlemler tanımlanmıştır? • Hangi bulut servislerinin kullanılabileceği belirtilmiş midir? • Kullanımda olmayan kablosuz teknolojilerin (wifi, hotspot, airdrop vb.) kapalı tutulması gerektiği belirtilmiş midir? • Güvensiz kablosuz ağların (Otel, havalimanı vb.) kullanımına kısıtlama getirilmiş midir? • Cihazlarda ekran kilidi olması zorunlu tutulmuş mudur? • Root ve Jailbreak yapılması yasaklanmış mıdır? • Uygulamaların hangi kaynaklardan kurulması gerektiği belirtilmiş midir? • Uzaktan cihaz yönetimine izin veren fonksiyonların kullanımı ile ilgili maddeler var mıdır? Politika çalışanlara tebliğ edilmiş midir?
3.3.1.2	Mobil Cihazlarda Jailbreak veya Rootlama İşleminin Yapılmaması	Mülakat, Güvenlik Denetimi	Kurum için geliştirilen uygulamalar root veya jailbreak yapılmış cihazlarda çalışmayı reddetmekte midir? Mobil cihaz kullanım politikasında root veya jailbreak yapılmış cihazlar için hangi önlemler tanımlanmıştır?
3.3.1.3	Kullanıcılara Uygulama İzinleri Hakkında Eğitim Verilmesi	Mülakat	Kullanıcılara mobil cihaz güvenliği eğitimi verilmekte midir? Genel farkındalık eğitimleri içinde mobil cihaz güvenliğinden bahsedilmekte midir?
3.3.1.4	Mobil Cihaz Envanterinin Tutulması	Mülakat, Gözden Geçirme	Kurumun sahibi olduğu cihazların yazılım ve donanım envanteri tutulmakta mıdır?
3.3.1.5	Halka Açık Şarj İstasyonlarının Kullanılmaması	Mülakat, Güvenlik Denetimi	Mobil cihaz kullanım politikasında kullanıcılara halka açık şarj istasyonlarını kullanmamaları gerektiği bildirilmiş midir?
3.3.1.6	Cihazın Uzaktan Fabrika Ayarlarına Döndürülmesi	Mülakat	Mobil cihaz kullanım politikasında kurum çalışanlarının cihazlarını uzaktan fabrika ayarlarına döndürmelerini sağlayacak ayarları yapmaları istenmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.1.7	Tamire Verilen Cihazlarda Bulunan Verinin Silinmesi	Mülakat	Kuruma ait mobil cihazlar tamire verilmeden önce fabrika ayarlarına döndürülmekte midir? Fabrika ayarlarına döndürülemeyen cihazlar için imha prosedürü tanımlanmış mıdır? Mobil cihaz kullanım politikasında kullanıcılara kendi cihazlarını fabrika ayarlarına döndürmeden üçüncü kişilere satmaması veya tamire vermemesi gerektiği belirtilmiş midir?
3.3.1.8	Güvenlik Yazılımlarının Yüklenmesi	Mülakat, Güvenlik Denetimi	Zararlı yazılımları tespit eden ve önleyen uygulamalar kullanılmakta mıdır?
3.3.1.9	Taşınabilir Cihaz Yönetimi	Mülakat, Güvenlik Denetimi	Kurum kritik veriye erişen cihazlarını merkezi olarak yönetebilmekte midir? Mobil cihaz kullanım politikasında listelenen tedbirleri kapsayan bir güvenlik politikası belirlenmiş midir? Güvenlik politikası kritik veriye erişen cihazlara yüklenmiş midir?
3.3.1.10	Taşınabilir Cihazların Ayrı Sistemlerde Kullanılması	Mülakat, Güvenlik Denetimi	Kritik seviyeli ağlarda kullanılan taşınabilir cihazlar kurum dışı veya internete bağlı ağlarda kullanılmakta mıdır?
3.3.1.11	Parola Politikaları	Mülakat, Güvenlik Denetimi	Kurumun güvenlik ihtiyaçlarına göre bir mobil cihaz parola politikası belirlenmiş midir? Politikanın kullanımı merkezi yönetim yazılımı ile zorunlu kılınmış mıdır?
3.3.1.12	Çok Sayıda Hatalı Giriş Denemesi Yapılması Halinde Cihaz İçindeki Verinin Silinmesi	Mülakat, Güvenlik Denetimi	Kilit ekranında çok sayıda hatalı giriş denemesi yapılan cihazların fabrika ayarlarına dönmesini sağlayan bir politika oluşturulmuş mudur? Politikanın kullanımı merkezi yönetim yazılımı ile zorunlu kılınmış mıdır? Mobil cihazlar kaç hatalı deneme sonrasında fabrika ayarlarına dönecek şekilde yapılandırılmıştır?
3.3.1.13	Desteklenen Cihaz Listesinin Oluşturulması	Mülakat, Güvenlik Denetimi	Kurumda kullanılmasına izin verilen cihazların listesi oluşturulmuş mudur? Cihaz seçiminde hangi kriterler kullanılmıştır?
3.3.1.14	Güncel Olmayan Cihazların Sistemlere Erişiminin Engellenmesi	Mülakat, Güvenlik Denetimi	Merkezi yönetim sistemi, güvenlik yamaları yüklenmemiş ya da üzerinde kara listeye alınmış uygulama/uygulama sürümü barındıran cihazların sisteme erişimini engelliyor mudur?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.1.15	Seyahat Kullanım Politikasının Tanımlanması	Mülakat	Yurt dışı seyahatleri sırasında kullanılacak cihazlar için bir kullanım politikası hazırlanmış mıdır? Yurt dışına giden personelin yurda dönüşte mobil cihazları incelemeye alınmakta mıdır? İncelemeye alınan cihazlar için hangi kontroller uygulanmaktadır?

3.3.2. Taşınabilir Bilgisayar Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.2.1	1	Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı	Taşınabilir bilgisayarların kurum bünyesinde kullanılabilmesi için taşınabilir bilgisayarların kullanımı, uygunluğu ve uzaktan yönetimi ile ilgili aşağıdaki hususları içeren kullanım politikası hazırlanmalı ve uygulanmalıdır. • Fiziksel koruma ile ilgili gereksinimler • Parola tanımlama • Yazılım kurulum kısıtları • İşletim sistemi ve uygulama güncelleme politikası • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Kurum, taşınabilir bilgisayarın temini öncesinde politikayı çalışana tebliğ etmelidir. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda bulundurulmamalıdır.
3.3.2.2	1	Güvenlik Yazılımlarının Yüklenmesi	Zararlı yazılımları tespit eden ve önleyen güvenlik yazılımları kullanılmalıdır. Bk. Tedbir No: 3.1.5.1 Bk. Tedbir No: 3.1.5.4
3.3.2.3	1	Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi	Onarım/tadilat için üçüncü kişilere (yetkisi servis vb.) verilecek taşınabilir bilgisayarlar fabrika ayarlarına döndürülmeli ve içindeki kurumsal veriler güvenli yöntemler kullanılarak silinmelidir.
3.3.2.4	2	Disk Şifreleme	Taşınabilir bilgisayarlara, çalınma ve kaybolma riskine karşı disk şifreleme uygulanmalıdır. Kullanıcıların disk şifreleme özelliğini devre dışı bırakmaları engellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.2.5	3	Harici Depolama Ortamlarına Erişimin Yönetimi	Taşınabilir bilgisayarlarda, harici depolama ortamlarına okuma ve yazma izinleri varsayılan olarak devre dışı bırakılmalıdır. İş gereksinimleri doğrultusunda gerekli onayların alınması durumunda okuma ve yazma izinleri devreye alınmalı, yapılan işlemler izlenmelidir.
3.3.2.6	3	Taşınabilir Bilgisayar Yönetimi	Taşınabilir bilgisayarlar uzaktan yönetilebilmeli, cihazlara güvenlik politikaları uygulanabilmeli ve gerek duyulduğunda politikalar uzaktan güncellenebilmelidir.
3.3.2.7	3	Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi	Güncel olmayan işletim sistemi ve/veya güvenlik yazılımları barındıran bilgisayarların kurum sistemlerine erişimi engellenmelidir.
3.3.2.8	3	Seyahat Kullanım Politikasının Tanımlanması	Yurt dışı seyahatleri sırasında kullanılacak bilgisayarlar için bir kullanım politikası hazırlanmalı, bilgisayarlar seyahat sonrası bu politikaya göre kontrol edilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.2.1	Taşınabilir Bilgisayarların Kabul Edilebilir Kullanımı	Mülakat	Kurum verisine erişen taşınabilir bilgisayarlar için tanımlanmış bir kullanım politikası var mıdır? Politika içeriğinde aşağıdaki konular ele alınmakta mıdır? • Fiziksel koruma ile ilgili gereksinimler • Parola tanımlama • Yazılım kurulum kısıtları • İşletim sistemi ve uygulama güncelleme politikası • Yedekleme • Bulut servislerinin kullanımı • Kablosuz ağların kullanımı • El değiştirme ve imha Politika çalışanlara tebliğ edilmiş midir?
3.3.2.2	Güvenlik Yazılımlarının Yüklenmesi	Mülakat, Güvenlik Denetimi	Taşınabilir bilgisayarlara hangi güvenlik yazılımları kurulmaktadır?
3.3.2.3	Tamire Verilen Taşınabilir Bilgisayarlarda Bulunan Verinin Silinmesi	Mülakat	Kuruma ait mobil cihazlar tamire verilmeden önce hangi güvenlik önlemleri uygulanmaktadır?
3.3.2.4	Disk Şifreleme	Mülakat, Güvenlik Denetimi	Taşınabilir bilgisayarlar için çalınma ve kaybolma riskine karşı ne gibi önlemler alınmaktadır?
3.3.2.5	Harici Depolama Ortamlarına Erişimin Yönetimi	Mülakat, Güvenlik Denetimi	Kritik veriye erişim imkânı olan taşınabilir bilgisayarlarda, harici depolama ortamlarını okuma ve yazma özellikleri devre dışı bırakılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.2.6	Taşınabilir Bilgisayar Yönetimi	Mülakat, Güvenlik Denetimi	Kurum kritik veriye erişen cihazlarını merkezi olarak yönetebilmekte midir? Mobil cihaz kullanım politikasında listelenen tedbirleri kapsayan bir güvenlik politikası oluşturulmuş mudur? Güvenlik politikası kritik veriye erişen cihazlara yüklenmiş midir?
3.3.2.7	Güncel Olmayan Bilgisayarların Sistemlere Erişiminin Engellenmesi	Mülakat, Güvenlik Denetimi	Merkezi yönetim sistemi, güvenlik yamaları yüklenmemiş ya da üzerinde kara listeye alınmış uygulama/uygulama sürümü barındıran taşınabilir bilgisayarların sisteme erişimini engellemekte midir?
3.3.2.8	Seyahat Kullanım Politikasının Tanımlanması	Mülakat	Yurt dışı seyahatleri sırasında kullanılacak taşınabilir bilgisayarlar için bir kullanım politikası hazırlanmış mıdır? Yurt dışına giden personelin yurda dönüşte taşınabilir bilgisayarları incelemeye alınmakta mıdır? İncelemeye alınan bilgisayarlar için hangi kontroller uygulanmaktadır?

3.3.3. Taşınabilir Ortam Güvenliği (CD/DVD, Taşınabilir Bellek Ortamları)

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.3.3.1	1	Taşınabilir Ortamların Kabul Edilebilir Kullanımı	Taşınabilir ortam yönetimine ilişkin en az fiziksel koruma ve saklama ile ilgili gereksinimler, yedekleme, el değiştirme ve imha hususlarını içeren kullanım politikası hazırlanmalı ve uygulanmalıdır.
3.3.3.2	1	Taşınabilir Ortamların Saklama ve Kullanım Koşulları	Tüm taşınabilir ortamlar, olumsuz fiziksel etkilere karşı üretici tarafından tavsiye edilen saklama ve kullanım koşullarına uyumlu olarak kullanılmalıdır.
3.3.3.3	2	Taşınabilir Ortamların Barındırdığı Verilerin Güvenliği	Taşınabilir ortamlar üzerinde yer alan kritik bilgi/veri şifreli olarak saklanmalıdır.
3.3.3.4	2	Taşınabilir Ortamların Güvenli İmhası	Kullanım süresi dolmuş taşınabilir ortamlar veri sızıntılarını önlemek amacıyla güvenli olarak imha edilmelidir.
3.3.3.5	2	Taşınabilir Ortam Bilgisinin Yedeklenmesi	Taşınabilir ortam içindeki bilgi/veri saklanması gereken süre göz önünde bulundurularak güvenli şekilde yedeklenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.3.3.1	Taşınabilir Ortamların Kabul Edilebilir Kullanımı	Mülakat	Kurum verisini barındıran taşınabilir ortamlar için tanımlanmış bir kullanım politikası var mıdır? Kabul edilebilir kullanım politikası içeriğinde hangi konular ele alınmaktadır? Politika çalışanlara tebliğ edilmiş midir?
3.3.3.2	Taşınabilir Ortamların Saklama ve Kullanım Koşulları	Mülakat	Taşınabilir ortamların güvenliğine yönelik hangi kontroller uygulanmaktadır?
3.3.3.3	Taşınabilir Ortamların Barındırdığı Verilerin Güvenliği	Mülakat, Güvenlik Denetimi	Taşınabilir ortamların barındırdığı verilerin güvenliği nasıl sağlanmaktadır?
3.3.3.4	Taşınabilir Ortamların Güvenli İmhası	Mülakat, Güvenlik Denetimi	Taşınabilir ortamların imhasına yönelik nasıl bir prosedür işletilmektedir?
3.3.3.5	Taşınabilir Ortam Bilgisinin Yedeklenmesi	Mülakat, Güvenlik Denetimi	Taşınabilir ortamların barındırdığı verilere yönelik yedekleme prosedürü nasıl işletilmektedir?

3.4. Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, nesnelerin interneti cihazlarının güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Ağ Servisleri ve İletişimi
- Dâhili Veri Depolama
- Kimlik Doğrulama ve Yetkilendirme
- API ve Bağlantı Güvenliği
- Diğer Güvenlik Tedbirleri

3.4.1. Ağ Servisleri ve İletişimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.1.1	1	Ağ Portlarının Kısıtlanması	Cihazlarda sadece ilgili fiziksel ve mantıksal portlar ile servisler açık bırakılmalıdır.
3.4.1.2	1	Ağ Servislerinin Güvenlik Kontrolleri	Gerekli tüm ağ servislerinin açıklara ve saldırılara karşı kontrolleri periyodik olarak yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.1.3	1	Güvenli Yapılandırma	Cihaza yönelik aşağıda yer alan işlemlerin yapılması ve işlemler sırasında gerekli tüm bilgilerin güvenli bir şekilde aktarılması sağlanmalıdır. • Cihaz kurulumu • Konfigürasyon güncellemeleri • Sistem yazılımı güncellemeleri • İşletim sistemi ve kütüphane güncellemeleri IoT cihazlarının kurulumu ve yapılandırılması, yeniden başlatma ve kurtarma işlemleri vb. operasyonel ve yönetsel faaliyetlere ilişkin işletim prosedürleri hazırlanmalıdır.
3.4.1.4	1	Cihazın Güvenli İmhası veya Tekrar Kullanımı	Cihazın depolama ortamı içeren tüm parçaları elden çıkarılmadan veya yeniden kullanılmadan önce, herhangi bir kritik veri ve/veya lisanslı yazılım varsa kaldırılmasını veya güvenli şekilde üzerine yazılmasını sağlamak için kontrol edilmelidir. Verinin ve veri içeren ortamların güvenli imhası için işletilecek yöntemler verinin kritikliği göz önünde bulundurularak sınıflandırılmalı, yazılı hale getirilmeli ve uygulamaya alınmalıdır.
3.4.1.5	1	Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi	IoT cihazlarının izin alınmadan ağa bağlanmalarını ve yer değiştirmelerini engellemek amacıyla gerekli önlemler alınmalıdır.
3.4.1.6	2	Cihaz Güvenlik Duvarının Aktifleştirilmesi	Cihazlarda varsa güvenlik duvarı aktifleştirilmeli ve IoT sistemlerini kritik BT sistemlerinden izole etmek için güvenlik duvarları kullanılmalıdır.
3.4.1.7	2	Kablosuz Erişim Noktalarına Güvenli Bağlantı	Cihazların kablosuz erişim noktalarına bağlantıları güvenli erişim protokolleri ile desteklenmelidir.
3.4.1.8	2	Cihazların Merkezi Yönetimi	Cihazlar, merkezi bir yazılım üzerinden yönetilmelidir.
3.4.1.9	3	Ağ Üzerinden Gönderilen Verinin Şifrelenmesi	Cihazın ağ üzerinden veri gönderimi sırasında, kritik veri cihazın desteklediği şifreleme algoritmalarıyla şifrelenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.1.1	Ağ Portlarının Kısıtlanması	Güvenlik Denetimi, Sızma Testi	Cihazlarda gerektiğinden fazla port açık mıdır? Cihazın ağ portları ve servisleri internet üzerinden erişilebilir midir?
3.4.1.2	Ağ Servislerinin Güvenlik Kontrolleri	Mülakat, Gözden Geçirme	Ağ servisleri üzerinde zafiyet taramaları periyodik olarak yapılmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.1.3	Güvenli Yapılandırma	Mülakat, Güvenlik Denetimi	Cihaz üzerine aktarılacak konfigürasyon verisinin güvenli bir şekilde iletildiği nasıl garanti altına alınmaktadır? IoT cihazlarının kurulumu ve yapılandırılması, yeniden başlatma ve kurtarma işlemleri vb. operasyonel ve yönetsel faaliyetlere ilişkin işletim prosedürleri hazırlanmakta mıdır?
3.4.1.4	Cihazın Güvenli İmhası veya Tekrar Kullanımı	Mülakat, Gözden Geçirme	Verinin ve veri içeren ortamların güvenli imhası veya tekrar kullanımı için işletilecek yöntemler yazılı hale getirilmiş ve uygulanmakta mıdır? İmha işleminde bilgilerin açığa çıkmaması ve başkalarının eline geçmemesi için ne gibi önlemler alınmaktadır?
3.4.1.5	Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Yetkisiz cihazların kurum ağına bağlanmasını engellemek üzere ne gibi önlemler alınmaktadır?
3.4.1.6	Cihaz Güvenlik Duvarının Aktifleştirilmesi	Güvenlik Denetimi	Güvenlik duvarı imkânı olan cihazlarda, güvenlik duvarı aktif olarak kullanılmakta mıdır? Güvenlik duvarının konfigürasyonu yapılmış mıdır?
3.4.1.7	Kablosuz Erişim Noktalarına Güvenli Bağlantı	Güvenlik Denetimi	Cihazların kablosuz erişim noktalarına erişimleri güvenli erişim protokolleri ile desteklenmekte midir?
3.4.1.8	Cihazların Merkezi Yönetimi	Güvenlik Denetimi	Cihazların yönetilmesi için merkezi bir yazılım kullanılmakta mıdır?
3.4.1.9	Ağ Üzerinden Gönderilen Verinin Şifrelenmesi	Mülakat, Güvenlik Denetimi	Cihazlardan gönderilen kritik veri şifreli gönderilmekte midir? Kullanılan şifreleme algoritmaları nelerdir?

3.4.2. Dâhili Veri Depolama

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.2.1	1	Veri Yedekleme	Cihaz üzerinde yer alan veri, bilgi güvenliği ve yedekleme ihtiyaçları doğrultusunda düzenli olarak yedeklenmelidir.
3.4.2.2	1	Verilere Yetkili Erişim	IoT sistemlerinde depolanan verilerin güvenliğinin sağlanması için yetkilendirme sağlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.2.3	3	Kullanılan Cihazlardan Kritik Verinin Temizlenmesi	Bilgi güvenliği gereksinimleri göz önünde bulundurularak, kullanımına ihtiyaç kalmayan veya farklı alanlarda kullanılacak cihazlar üzerindeki kritik veri geri döndürülemeyecek şekilde silinmelidir. Kritik verinin cihaz üzerinden güvenli silinmesinin mümkün olmadığı durumlarda cihaz ulusal/uluslararası kabul görmüş yöntemlere uygun şekilde imha edilmelidir. Bk. Tedbir No: 3.4.1.4

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.2.1	Veri Yedekleme	Mülakat, Gözden Geçirme	Cihaz üzerinde yer alan veri hangi aralıklarla yedeklenmektedir? Yedekleme periyotları kurumun bilgi güvenliği gereksinimleri ile uyumlu mudur?
3.4.2.2	Verilere Yetkili Erişim	Mülakat, Güvenlik Denetimi	IoT sistemlerinde depolanan verilerin güvenliğinin sağlanması için erişim yetkilendirme sağlanmakta mıdır?
3.4.2.3	Kullanılan Cihazlardan Kritik Verinin Temizlenmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kritik verilerin cihazlardan geri döndürülemeyecek şekilde silinmesi amacıyla bir prosedür belirlenmiş ve uygulanmakta mıdır? Cihaz üzerinden kritik verinin silinmesinin mümkün olmadığı durumlarda hangi yöntemler uygulanmaktadır? Cihazların imhasına yönelik tanımlanmış prosedür var mıdır? İmha sürecinde hangi yöntemlerden faydalanılmaktadır?

3.4.3. Kimlik Doğrulama ve Yetkilendirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.3.1	1	Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi	Sistemde tanımlı ise oturum sonlandırma işlemleri aktifleştirilmelidir. Bilgi güvenliğini tehdit eden bir durumun ortaya çıkması halinde oturum sonlandırma ve cihazı pasife alma işlemleri uzaktan yapılabilmelidir.
3.4.3.2	1	Kimlik Doğrulama Politikası	Güçlü kimlik doğrulama politikası tanımlanmalı ve uygulanmalıdır. Cihazın içinde iletişim için kullanılan kimlik bilgileri güvenli bir şekilde tutulmalıdır.
3.4.3.3	1	Kullanıcı Yetki Sınırlaması	Kullanıcı hesapları tekil olacak şekilde oluşturulmalı, bilgi güvenliği gereksinimleri ve cihazın yetenekleri doğrultusunda erişim yetkileri asgari düzeyde tanımlanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.3.4	1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Ön tanımlı parolalar ve kullanıcı isimleri, kullanım öncesinde mutlaka değiştirilmeli ve kullanılan parolaların güvenli bir alanda muhafaza edilmesi sağlanmalıdır.
3.4.3.5	1	Sıfırlama Mekanizmaları	Cihaz üzerinde sıfırlama mekanizması bulunmalı ve bu mekanizmaya yetkisiz erişim engellenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.3.1	Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi	Güvenlik Denetimi	Giriş yapılan hesaplarda isteğe bağlı veya otomatik olarak oturum sonlandırılmakta mıdır? Bilgi güvenliğini tehdit eden bir durumun ortaya çıkması halinde oturum sonlandırma ve cihazı pasife alma işlemleri gerçekleştirilebilmekte midir?
3.4.3.2	Kimlik Doğrulama Politikası	Güvenlik Denetimi	Sistemde güçlü parola politikası aktif olarak kullanılmakta mıdır? Sistemde teknik olarak parola yenileme politikası mevcut ise aktif midir? Sistemde iki adımlı doğrulama mekanizması mevcut ise aktif midir?
3.4.3.3	Kullanıcı Yetki Sınırlaması	Güvenlik Denetimi	Sistemde kullanıcılar asgari düzeyde yetkiye sahip midir? Kullanıcıları sorumlu tutacak şekilde her kullanıcıya özel bir kullanıcı adı tanımlanmakta mıdır ve bu kullanıcı işlemlerinin kayıtları tutulmakta mıdır?
3.4.3.4	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Güvenlik Denetimi, Sızma Testi	Kurulum aşamasından sonra ön tanımlı parolalar değiştirilmekte midir? Parolalar nerede tutulmaktadır?
3.4.3.5	Sıfırlama Mekanizmaları	Güvenlik Denetimi	Cihaz üzerinde sıfırlama mekanizması bulunmakta mıdır? Bu mekanizmaya yetkisiz erişim nasıl engellenmektedir?

3.4.4. API ve Bağlantı Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.4.1	1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Sistemde yerel veya bulut tabanlı web uygulamalarının varsayılan kimlik doğrulama bilgisi değiştirilmelidir. Bk. Tedbir No: 3.2.1.6
3.4.4.2	1	API ve Bağlantı Güvenliği	API ve bağlantılarda IP kısıtlaması yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.4.3	2	Web Uygulama Güvenlik Duvarı Kullanımı	Sistemde web uygulama güvenlik duvarı mevcut ise nesnelerin interneti cihazları için aktifleştirilmelidir.
3.4.4.4	2	Sistem API'lerinde Güvenli Haberleşme Protokolü Kullanımı	API'ler cihazın desteklediği bilinen zafiyet içermeyen güvenilir sürüme sahip bir haberleşme protokolü üzerinden haberleşmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.4.1	Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi	Güvenlik Denetimi	Sistemde kullanılan yerel veya bulut tabanlı web uygulamalarına ait varsayılan kimlik doğrulama bilgileri değiştirilmekte midir?
3.4.4.2	API ve Bağlantı Güvenliği	Mülakat, Güvenlik Denetimi	API ve bağlantılarda IP kısıtlama yapılmakta mıdır?
3.4.4.3	Web Uygulama Güvenlik Duvarı Kullanımı	Mülakat, Güvenlik Denetimi	IoT sistemleri için web uygulama güvenlik duvarı kullanılmakta mıdır?
3.4.4.4	Sistem API'lerinde Güvenli Haberleşme Protokolü Kullanımı	Mülakat, Güvenlik Denetimi	Sistem API'leri cihazın desteklediği güvenli bir haberleşme protokolü kullanmakta mıdır? Kullanılan protokoller nelerdir?

3.4.5. Diğer Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.5.1	1	Güncellemelerin Kontrolü	Sistemde varsa yeni güncelleme alma özelliği aktifleştirilmeli ve güncellemeler güvenilir kaynaklardan periyodik olarak alınmalıdır.
3.4.5.2	1	Cihazlara Fiziksel Erişimin Kısıtlanması	Cihazlara sadece yetkili kişiler fiziksel erişim sağlamalıdır. Yetkisiz kişilerin fiziksel erişimini engelleyecek güvenlik tedbirleri alınmalıdır.
3.4.5.3	3	Gömülü İşletim Sistemi İçin Kod Analiz Raporu Alınması	Gömülü işletim sistemi için mümkünse onaylanmış kod analiz raporu alınmalıdır.
3.4.5.4	3	Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması	Cihaza yönelik elektromanyetik sızıntılara karşı gerekli güvenlik önlemleri alınmalıdır.
3.4.5.5	3	Tersine Mühendisliğe Karşı Koruma	Cihazın donanımı ve yazılımı tersine mühendisliği zorlaştıracak şekilde tasarlanmış olmalı ve tersine mühendisliğe karşı korunmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.4.5.6	3	Güvenli Önyükleme	Cihaz güvenli önyükleme (secure boot) özelliğine sahip olmalıdır.
3.4.5.7	3	Güncellemelerin Güvenilir Kanallar Üzerinden Yapılması	Dışarıdan cihaza gelen güncellemeler cihazın desteklediği ölçüde imza doğrulaması yapılarak kontrol edilmelidir. Eğer cihaz güncelleme kaynağının doğruluğunu kontrol edebilecek bir mekanizma desteklemiyorsa, güncellemeler sadece yetkili kişiler tarafından fiziksel olarak yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.4.5.1	Güncellemelerin Kontrolü	Mülakat, Güvenlik Denetimi	Sistem üzerinde güncellemeler düzenli olarak alınmakta mıdır? Güncellemelere yönelik kontroller nasıl yapılmaktadır?
3.4.5.2	Cihazlara Fiziksel Erişimin Kısıtlanması	Mülakat, Güvenlik Denetimi	Cihazlara fiziksel erişim güvenliğini sağlamak için ne gibi önlemler alınmaktadır? Herhangi bir güvenlik ihlali durumunda işletilmesi planlanan eylem planı bulunmakta mıdır?
3.4.5.3	Gömülü İşletim Sistemi İçin Kod Analiz Raporu Alınması	Güvenlik Denetimi	Gömülü işletim sistemi için onaylanmış kod analiz raporu alınmakta mıdır?
3.4.5.4	Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması	Güvelik Analizi	Cihaza yönelik elektromanyetik sızıntılara karşı hangi güvenlik tedbirleri alınmaktadır?
3.4.5.5	Tersine Mühendisliğe Karşı Koruma	Güvenlik Denetimi	Cihazın tersine mühendisliğe karşı korumak amacıyla ne gibi önlemler alınmaktadır? Cihazın donanım ve yazılım bileşenleri tersine mühendisliği zorlaştıracak şekilde tasarlanmış mıdır?
3.4.5.6	Güvenli Önyükleme	Güvenlik Denetimi	Cihaz güvenli önyükleme (secure boot) özelliğine sahip midir?
3.4.5.7	Güncellemelerin Güvenilir Kanallar Üzerinden Yapılması	Mülakat, Güvenlik Denetimi	Cihaz güncellemeleri nasıl yapılmaktadır? Güncelleme yapılmadan önce güncellemenin geldiği kaynak kontrol edilmekte midir? Eğer güncelleme kaynağı kontrol edilemiyorsa, güncellemeler sadece fiziksel olarak yetkili kişiler tarafından mı yapılmaktadır?

3.5. Personel Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, personel güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Personel Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri
- Eğitim ve Farkındalık Faaliyetleri
- Tedarikçi İlişkileri Güvenliği

3.5.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.1.1	1	Güvenlik Soruşturmalarının Yapılması	İşe alım aşamasında, yasal düzenlemeler ve iş gereksinimleri göz önünde bulundurularak tüm aday personel için akademik bilgilerin ve geçmiş iş tecrübelerinin doğruluğu, referanslar ve sahip olunan sertifikaların geçerliliği kontrol edilmeli, adli sicil kaydı sorgulaması yapılmalıdır.
3.5.1.2	1	Varlıkların Kabul Edilebilir Kullanım Kurallarının Tanımlanması	Kurum varlıklarının kabul edilebilir kullanım politikası belirlenerek kurum personelinin ve yüklenicilerin bu kurallara uyum sağlaması taahhüt altına alınmalıdır.
3.5.1.3	1	Temiz Masa Temiz Ekran Politikasının Tanımlanması	Fiziksel ortam, taşınabilir bilgi/veri depolama ortamları ve diğer bilgi işleme olanaklarını kapsayan temiz masa temiz ekran politikası tanımlanmalı ve uygulanmalıdır.
3.5.1.4	1	Sözleşmelerde Bilgi Güvenliği Hususlarının Yer Alması	Personel ve yüklenicilerin kurum varlıklarına erişimi sağlanmadan önce, kendileriyle yapılan sözleşmelerde bilgi güvenliği sorumlulukları belirtilmelidir.
3.5.1.5	1	Sosyal Medya Kullanım Politikasının Uygulanması	Sosyal medya kullanım politikası oluşturulmalı ve bu kapsamda personel tarafından sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmaması garanti altına alınmalıdır.
3.5.1.6	1	Bilgi Güvenliği İhlal Olayına Yönelik Disiplin Sürecinin Tanımlanması	Bilgi güvenliği ihlal olaylarını yönetmek amacıyla ilgili yasalar, iş sözleşmeleri vb. unsurlar göz önünde bulundurularak bir disiplin süreci tanımlanmalı ve uygulanmalıdır.
3.5.1.7	1	Rol, Sorumluluk ve Asgari Yetkinliklerin Tanımlanması	Kurum personeli tarafından gerçekleştirilen işin tanımı ve gereklilikleri göz önünde bulundurularak, ilgili personelin kurum bünyesindeki bilgi güvenliği rolü, sorumlulukları ve sahip olması gereken asgari yetkinlikler tanımlanmalı ve yazılı hale getirilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.1.8	1	İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi	İstihdam sorumlulukları değişen personel/yükleniciye yeni bilgi güvenliği sorumlulukları ve görevleri; istihdamı sonlandırılan personel/yükleniciye ise istihdamın sona ermesinden sonra devam edecek bilgi güvenliği sorumlulukları bildirilmelidir.
3.5.1.9	1	Gizlilik ile İlgili Gereksinimlerin Personele Tebliğ Edilmesi	Kurumun bilgi güvenliği gereksinimleri göz önünde bulundurularak personel veya yüklenicilerin uyması gereken politika, prosedür, talimat gibi dokümanlar ilgili personel/yükleniciye tebliğ edilmelidir. İlgili dokümanların içeriği bilgi güvenliği gereksinimlerinde değişiklik olması durumunda güncellenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.1.1	Güvenlik Soruşturmalarının Yapılması	Mülakat, Gözden Geçirme	İşe başvuru yapan personel tarafından beyan edilen akademik bilgilerin ve sertifikaların geçerliliği nasıl kontrol edilmektedir? Doğrulama kontrolleri kapsamında adli sicil kaydı, geçmiş iş tecrübeleri ve ilişkili referansların kontrolü yapılmakta mıdır? Doğrulama kontrollerine yönelik değerlendirme sonuçları nasıl ve nerede tutulmaktadır?
3.5.1.2	Varlıkların Kabul Edilebilir Kullanım Kurallarının Tanımlanması	Mülakat, Gözden Geçirme	Varlıkların kabul edilebilir kullanım politikası belirlenmiş midir? Varlıkların kabul edilebilir kullanım politikası kurum personeli ve yüklenicilere duyurulmuş mudur? Kurum personeli ve yüklenicilerin varlıkların kabul edilebilir kullanım politikasına uyum sağlamaları hususu taahhüt altına alınmış mıdır?
3.5.1.3	Temiz Masa Temiz Ekran Politikasının Tanımlanması	Mülakat, Gözden Geçirme	Fiziksel ortam, taşınabilir bilgi/veri depolama ortamları ve diğer bilgi işleme olanaklarını kapsayan temiz masa temiz ekran politikası tanımlanmış mıdır? Temiz masa temiz ekran politikası personel ve yüklenicilere nasıl bildirilmektedir? Temiz masa temiz ekran politikasının ihlal edilmesi durumunda işletilecek süreç tanımlanmış mıdır?
3.5.1.4	Sözleşmelerde Bilgi Güvenliği Hususlarının Yer Alması	Mülakat, Gözden Geçirme	İşe yeni başlayan personel ve yüklenicilerle yapılan sözleşme içeriklerinde bilgi güvenliği hususları yer almakta mıdır? Sözleşme içerikleri kapsamında bilgi güvenliği ile ilgili gerekliliklerin yeterli düzeyde ele alındığının kontrolü düzenli olarak yapılmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.1.5	Sosyal Medya Kullanım Politikasının Uygulanması	Mülakat, Gözden Geçirme	Sosyal medya kullanım politikası oluşturulmuş mudur? Sosyal medya kullanım politikası içeriğinde hangi konular ele alınmıştır? Gizlilik dereceli verinin personel tarafından sosyal medya üzerinden paylaşılmaması hususu nasıl garanti altına alınmaktadır?
3.5.1.6	Bilgi Güvenliği İhlal Olayına Yönelik Disiplin Sürecinin Tanımlanması	Mülakat, Gözden Geçirme	Bilgi güvenliği ihlal olayını gerçekleştiren personel/yükleniciye yönelik ilgili yasalar, iş sözleşmeleri vb. unsurlar göz önünde bulundurularak oluşturulmuş bir disiplin süreci var mıdır?
3.5.1.7	Rol, Sorumluluk ve Asgari Yetkinliklerin Tanımlanması	Mülakat, Gözden Geçirme	Kurum personeli tarafından gerçekleştirilen işin tanımı ve gereklilikleri göz önünde bulundurularak, personelin kurum bünyesindeki bilgi güvenliği rolü, sorumlulukları ve sahip olması gereken asgari yetkinlikler tanımlanmakta mıdır?
3.5.1.8	İstihdam Sorumluluklarının Sonlandırılması veya Değiştirilmesi	Mülakat, Gözden Geçirme	Personel ve yüklenici sözleşmelerinde, istihdamın sona ermesinden sonra da geçerli olacak hükümlere yer verilmiş midir? İstihdamın sonlandırılmasından sonra veya istihdam koşullarının değiştirilmesinden sonra ilgili personele/yükleniciye, uymaları gereken bilgi güvenliği sorumlulukları nasıl bildirilmektedir?
3.5.1.9	Gizlilik ile İlgili Gereksinimlerin Personele Tebliğ Edilmesi	Mülakat, Gözden Geçirme	Personel veya yüklenicilerin uyması gereken bilgi güvenliği politikaları, prosedürleri, talimatları tanımlanarak tebliğ edilmiş midir? İlgili dokümanlar kurumun bilgi güvenliği gereksinimlerini karşılamakta mıdır? Bilgi güvenliği gereksinimlerinde herhangi bir değişiklik olması durumunda dokümanlar güncellenmekte midir?

3.5.2. Eğitim ve Farkındalık Faaliyetleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.2.1	1	Farkındalık Eğitimleri Verilmesi	Tüm kurum personeline düzenli aralıklarla; • Bilgi güvenliği ve siber güvenlik temel kavramları, • Kurumsal bilgi güvenliği ve siber güvenlik politikaları, • Parola güvenliği, • E-posta kullanımında güvenlik, • İnternet kullanımında güvenlik, • Mobil güvenlik, • Fiziksel güvenlik, • Sosyal ağların riskleri ve güvenli kullanımı, • Kişisel verilerin güvenliği, • Bilinen ve yaygın kullanılan sosyal mühendislik yöntemleri ve bu yöntemlere karşı alınacak önlemler, • Lisanslı ürün kullanımı gibi temel ve güncel konuları içerecek şekilde bilgi güvenliği ve siber güvenlik farkındalık eğitimleri verilmelidir. Farkındalık eğitimlerinin etkinliğine yönelik ölçümler (eğitim öncesi ve sonrası yazılı sınav, sosyal mühendislik saldırıları vb.) yapılmalı ve ölçüm sonucu doğrultusunda aksiyonlar planlanmalıdır.
3.5.2.2	1	Olayların Tespiti ve Raporlanmasına Yönelik Eğitimlerin Verilmesi	Bilgi güvenliği ve SOME personeline, siber olay veya bilgi güvenliği ihlal olayı tespiti ve raporlanması konularında eğitim verilmelidir.
3.5.2.3	2	Yetenek İhtiyaç Analizi Yapılması	Bilgi güvenliği ve siber güvenlik alanında görev yapan personel için yetenek ihtiyaç analizi yapılmalıdır. Yetenek ihtiyaç analizi çıktıları doğrultusunda eğitim yol haritası çıkarılmalı ve uygulamaya alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.2.1	Farkındalık Eğitimleri Verilmesi	Mülakat, Gözden Geçirme	Kurum personeline bilgi güvenliği ve siber güvenlik farkındalık eğitimleri verilmekte midir? Eğitim içeriğinde hangi konular ele alınmaktadır? Eğitim içerikleri periyodik olarak güncellenmekte midir? Eğitimin etkinliği nasıl değerlendirilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.2.2	Olayların Tespiti ve Raporlanmasına Yönelik Eğitimlerin Verilmesi	Mülakat	Bilgi güvenliği ve SOME personeline, siber olay veya bilgi güvenliği ihlal olayı tespiti ve raporlamasının nasıl yapılacağına yönelik eğitim verilmekte midir? Verilen eğitimlerde hangi konular ele alınmaktadır?
3.5.2.3	Yetenek İhtiyaç Analizi Yapılması	Mülakat, Gözden Geçirme	Bilgi güvenliği ve siber güvenlik alanında görev yapan personele yönelik yetenek ihtiyaç analizleri yapılmakta mıdır? Analiz sonuçları göz önünde bulundurularak personel için eğitim yol haritası hazırlanmakta mıdır? Eğitim yol haritası doğrultusunda kurum çalışanlarına düzenli olarak eğitimler verilmekte midir?

3.5.3. Tedarikçi İlişkileri Güvenliği

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.3.1	1	Tedarikçi İlişkilerinde Bilgi Güvenliği Politikasının Tanımlanması	Tedarikçiler tarafından erişilen kurum varlıklarının korunmasını sağlamak, tedarikçilerin kurumun bilgi varlıklarına erişimi ile ilgili riskleri azaltmak ve bilgi güvenliği gereksinimlerini karşılamak amacıyla politika tanımlanmalı ve uygulanmalıdır.
3.5.3.2	1	Demo ve Kavram İspatı Çalışmalarında Gizlilik Taahhütnamesi	Kurumun bilgi güvenliği gereksinimleri göz önünde bulundurularak üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, üçüncü tarafın sorumluluklarını içeren gizlilik taahhütnamesi hazırlanmalı ve imza altına alınmalıdır. İlgili taahhütname içeriği periyodik olarak gözden geçirilmelidir.
3.5.3.3	1	Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele Alınması	Kurum varlıklarına erişebilen, işletebilen, depolayabilen, iletebilen veya kurumun bilgi teknolojileri altyapı bileşenlerini temin eden tedarikçilerin her biri ile yapılacak sözleşmelere bilgi güvenliği gereksinimleri eklenmelidir.
3.5.3.4	1	Tedarik Zinciri Güvenliği	Yükleniciler ile yapılan sözleşmelerde, tedarik edilen bilgi ve iletişim teknolojileri ürün ve hizmetleri için tedarik zinciri ile ilişkili riskler göz önünde bulundurulmalı ve ilgili güvenlik gereksinimleri sözleşme içeriklerine eklenmelidir. Bu kapsamda, birlikte çalışılacak kişi ve/veya kuruluşlardan tedarik zinciri güvenliğinin temin edileceğine dair yazılı belge alınmalıdır.
3.5.3.5	1	Kabul Kriterlerinin Belirlenmesi	Tedarik edilen ürünün istenilen güvenlik kriterleri dâhilinde teslim edilmiş olduğunun doğrulanabilmesi için kabul kriterleri belirlenmeli, izleme ve doğrulama metotları tanımlanmalı ve yüklenici ile üzerinde anlaşılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.5.3.6	1	İletişim Metotlarının Belirlenmesi	Garanti süreci dâhil tedarik sürecinin tamamında bilgilendirme amaçlı ya da olası herhangi bir anormal durum ile ilgili olarak kimler ile nasıl iletişime geçileceği, hangi kuralların geçerli olacağı tanımlanmalı ve yüklenici ile üzerinde anlaşılmalıdır.
3.5.3.7	1	Yüklenici Tarafından Tedarik Edilen Ürün/Hizmet Değişikliklerinin Yönetimi	Yüklenici tarafından sağlanan hizmet ve ürün tedariki kapsamında bir değişiklik olması durumu göz önünde bulundurularak hizmet alınan faaliyetin kritikliği ve riskleri gözden geçirilmelidir. Bu değerlendirme hesaba katılarak, yüklenici ile yapılan sözleşmeye gereklilikler yansıtılmalı, bu gibi değişiklik durumlarının nasıl ele alınacağı net bir şekilde tanımlanmalıdır.
3.5.3.8	1	Ana Yüklenici ve Alt Yüklenici Sorumluluklarının Netleştirilmesi	Ana yüklenicinin, tedarik edilen ürün ve hizmetleri sunabilmek için tedarik süresince bir alt yüklenici kullanması durumunda; ana yüklenici ile alt yüklenici rol ve sorumluluklarının dokümante edildiği, bilgi güvenliği gereksinimlerine tedarik sürecinin tamamında alt yüklenici tarafından da uyulacağının taahhüdü ana yükleniciden alınmalıdır.
3.5.3.9	1	Tedarikçi Hizmetlerinin İzlenmesi	Bilgi güvenliği şartlarının sağlandığını garanti altına almak amacıyla tedarikçi hizmetleri düzenli aralıklarla gözden geçirilmeli ve dokümante edilmelidir.
3.5.3.10	2	Tedarik Zinciri İzleme Sürecinin Oluşturulması	Yüklenici tarafından güvenlik gereksinimlerine uyumun garanti altına alınması amacıyla; tedarik zinciri süresince, tedarik edilen hizmet/ürüne yönelik kritik bileşenlerin durumunun izlenebilirliği sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.3.1	Tedarikçi İlişkilerinde Bilgi Güvenliği Politikasının Tanımlanması	Mülakat, Gözden Geçirme	Tedarikçi ilişkilerinde bilgi güvenliği gereksinimlerini karşılamak amacıyla bir politika tanımlanmış mıdır? Bilgi güvenliği politikası hangi hususları içermektedir?
3.5.3.2	Demo ve Kavram İspatı Çalışmalarında Gizlilik Taahhütnamesi	Mülakat, Gözden Geçirme	Üçüncü taraflar ile yapılan demo ve kavram ispatı (PoC) çalışmalarında, üçüncü taraflara gizlilik taahhütnamesi imzalatılmakta mıdır? Taahhütname kurumun bilgi güvenliği gereksinimlerine uygun olarak hazırlanmış mıdır?
3.5.3.3	Tedarikçi Sözleşmelerinde Bilgi Güvenliğinin Ele Alınması	Mülakat, Gözden Geçirme	Tedarikçiler ile yapılan sözleşmelere bilgi güvenliği gereksinimleri eklenmiş midir? Sözleşmelerde yer alan bilgi güvenliği gereksinimleri hangi hususları içermektedir?
3.5.3.4	Tedarik Zinciri Güvenliği	Mülakat, Gözden Geçirme	Yükleniciler ile yapılan sözleşmelerde, tedarik zinciri güvenliğine yönelik maddeler yer almakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.5.3.5	Kabul Kriterlerinin Belirlenmesi	Mülakat, Gözden Geçirme	Tedarik edilecek ürüne yönelik kabul kriterleri belirlenmekte midir? Tedarik edilen ürünün istenilen güvenlik kriterleri ile uyumlu şekilde teslim edilmiş olduğunun doğrulanabilmesi için nasıl bir yöntem izlenmektedir?
3.5.3.6	İletişim Metotlarının Belirlenmesi	Mülakat, Gözden Geçirme	Garanti süreci dâhil tedarik sürecinin tamamında olası herhangi bir anormal durum ile ilgili nasıl iletişime geçileceği ve hangi kuralların geçerli olacağı tanımlanmakta mıdır?
3.5.3.7	Yüklenici Tarafından Tedarik Edilen Ürün/Hizmet Değişikliklerinin Yönetimi	Mülakat, Gözden Geçirme	Yüklenici tarafından sağlanan hizmet ve ürün tedarik süreci kapsamında yaşanan değişikliklerin yönetimi nasıl yapılmaktadır? Yüklenici ile yapılan sözleşmelerde ürün/hizmet değişikliklerinin yönetimine ilişkin gereklilikler yer almakta mıdır?
3.5.3.8	Ana Yüklenici ve Alt Yüklenici Sorumluluklarının Netleştirilmesi	Mülakat, Gözden Geçirme	Ana yüklenicinin, tedarik süresince alt yüklenici kullanması durumunda; ilgili tüm tarafların rol ve sorumluluklarının tanımlandığı, alt yüklenici tarafından bilgi güvenliği gerekliliklerinin yerine getirileceğini garanti altına alan taahhüt ana yükleniciden alınmakta mıdır?
3.5.3.9	Tedarikçi Hizmetlerinin İzlenmesi	Mülakat, Gözden Geçirme	Bilgi güvenliği şartlarının sağlandığını garanti altına almak amacıyla tedarikçi hizmetleri düzenli aralıklarla gözden geçirilmekte midir?
3.5.3.10	Tedarik Zinciri İzleme Sürecinin Oluşturulması	Mülakat, Gözden Geçirme	Tedarik zinciri süresince, tedarik edilen hizmet/ürüne yönelik kritik bileşenlerin durumu izlenebilmekte midir?

3.6. Fiziksel Mekânların Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, fiziksel mekânların güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Fiziksel Mekânların Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri
- Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri
- Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)

3.6.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.1	1	Fiziksel Güvenlik Sınırı	Kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmalıdır. Kurum tesislerine girişte ve çıkışta, güvenlik biriminin yer aldığı güvenlik kontrol noktası olmalı ve kuruma fiziksel erişimler yalnızca yetkilendirilmiş personel ile sınırlandırılmalıdır.
3.6.1.2	1	Güvenlik Biriminin Yeterliliği	Tesisin büyüklüğü, bulunduğu coğrafi alan ve var olan izleme sistemleri ile orantılı düzeyde ve bilgi seviyesinde güvenlik personeli bulundurulmalıdır. Güvenlik personelinin görevini tam olarak yerine getirip getirmediği düzenli olarak kontrol edilmelidir.
3.6.1.3	1	Fiziksel Giriş ve Çıkış Kontrolleri	Personelin fiziksel erişimini iş gereksinimleri doğrultusunda sınırlayan, tüm giriş/çıkışları kayıt altına alan kimlik kontrol mekanizması olmalıdır. Personel ve araç giriş kontrolü, güvenlik birimi tarafından yapılmalı ve kuruma giriş/çıkış noktaları sınırlı olmalıdır. Yetkisiz kişilerin tesise giriş yapabileceği; otopark girişleri, teslimat ve yükleme alanları gibi erişim noktaları ve olası diğer noktalar kontrol edilmeli, mümkünse yetkisiz erişimi engellemek için bilgi işleme olanaklarının bulunduğu alanlardan ayrılmalıdır.
3.6.1.4	1	Dış Güvenlik Unsurlarının Kontrolü	Tüm dış güvenlik unsurları (Ör. demir parmaklık, tel örgü, duvarlar, kamera sistemi, alarm sistemi vb.) düzenli olarak sabotaj, hasar veya bozulmalara karşı kontrol edilmelidir. Binalara ait bütün pencereler, kapılar, dış duvarlar ve güvenlik altına alınması gereken yerler yeterli gözetleme ve kontrol tedbirleri ile takip edilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.5	1	Ziyaretçi Giriş Çıkış Kontrolleri	Ziyaretçilerin fiziksel erişimini iş gereksinimleri doğrultusunda sınırlayan, giriş ve çıkışlarını kayıt altına alan kimlik kontrol mekanizması olmalıdır. En az aşağıda yer alan ziyaretçi karşılama tedbirleri uygulanmalıdır: • Kuruma gelen ziyaretçilere yönelik kayıtlar; ad, soyad, geliş amacı ve tarihi, refakat eden kişi bilgisi, giriş ve çıkış saati bilgilerini içermek üzere tutulmalıdır. • Ziyaretçi tarafından sunulan resmi kimlik kartlarının güvenlik birimi tarafından teyit edilmesi sonrasında ziyaretçi erişimi için giriş kartı verilmelidir. • Ziyaretçilerin verilen giriş kartını tesis içerisinde bulunduğu süre boyunca üzerinde görünür biçimde taşıması sağlanmalıdır. • Ziyaretçilerin tesis içerisinde refakatçi personel olmadan dolaşmasına izin verilmemelidir. • Ziyaretçi taşıtlarının tesislere giriş ve çıkışı izlenmelidir.
3.6.1.6	1	Yetkisiz Fiziksel Erişim Durumunda İzlenecek Sürecin Tanımlanması	Tesislere yetkisiz girdiğinden şüphelenilen kişi ve araçların tespiti, ihbarı ve gerekli müdahalenin gerçekleştirilmesi için yöntemler, rol ve sorumluluklar tanımlanmalıdır. Bu kapsamda; • Şüpheli durumların nasıl bildirileceği tanımlanmalıdır. (Kurum içi bir telefon numarası veya telsiz kanalının tahsis edilmesi ve bunun tesislerde görülebilecek yerlerde duyurulması vb.), • Bu tip durumlara müdahalenin kim tarafından ve nasıl yapılacağı belirlenmelidir.
3.6.1.7	1	Kablolama Güvenliği	Tüm kablolar yapısal kablo kanallarından geçirilmelidir. Karışmayı engellemek için güç kabloları, haberleşme kablolarından mümkün mertebe ayrılmalıdır. Kablolara yetkisiz aygıtların eklenmesine (fiziksel olarak araya girme saldırılarına karşı) izin verilmemelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.8	1	Dış ve Çevresel Tehditlere Karşı Koruma	Kurumun faaliyet gösterdiği binalar için depreme karşı dayanıklılık testi yapılmış olmalı ve bu durum belgelendirilmelidir. Kurumun faaliyet gösterdiği binalarda yangın söndürme sistemi olanakları ve acil durumda aranacaklar listesi bulunmalıdır. Acil durumda aranacaklar listesi periyodik olarak gözden geçirilmeli ve herkes tarafından görülebilecek uygun yerlerde asılı olmalıdır. Periyodik yangın ve deprem tatbikatları yapılmalı ve tatbikat sonuçları kayıt altına alınmalıdır. Su baskını ve yangın ihtimalini azaltmak için mutfak ve tuvaletlerin kritik bilgi bulunan yerlere uzak olmasına dikkat edilmelidir. Yangın, su baskını, duman tespiti için dedektörler konumlandırılmalı ve merkezi bir uyarı sistemiyle 7/24 gözlenmelidir. Periyodik olarak binanın topraklama kontrolleri yapılmalı ve kayıt altına alınmalıdır. Bina için yeterli koruma seviyesine sahip bir paratoner kullanılmalı, paratonerin bakımları periyodik olarak yapılmalı ve bakım sonuçları kayıt altına alınmalıdır. Elektrik, su, gaz ve diğer destekleyici altyapı hizmetlerini kesmek için kullanılan acil durum anahtarları ve vanalar acil çıkışların veya ekipman odalarının yakınında konumlandırılmalıdır.
3.6.1.9	1	Kamera Sistemleri	Kurum binasına giriş noktaları, bina içindeki koridorlar, bina çevresi, sistem odası, veri merkezi, kontrollü erişim noktaları ve güvenli alanlar kapalı devre kamera sistemi tarafından izlenip kayıt altına alınmalıdır. Kameralarla izlenmeyen noktalar tespit edilmeli ve periyodik olarak kontrolü sağlanmalıdır. Kamera kayıtlarına yalnızca yetkili personel erişmeli ve bu kayıtlar ilgili sistem odası/veri merkezi haricinde güvenli bir ortamda saklanmalıdır. Kamera kayıtları bilgi güvenliği gereklilikleri göz önünde bulundurularak belirlenmiş süre kadar muhafaza edilmelidir. Kamera sistemleri, dış ağlara açık olmamalıdır.
3.6.1.10	2	Çalışma Alanlarının Güvenliği	Binalarda ziyaretçilerin kabul edileceği lobi ve toplantı odaları, personelin çalışma alanlarından ayrı bir bölgede olmalıdır. İki bölge arasındaki geçiş kontrollü olarak sağlanmalıdır. Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.1.11	2	Destekleyici Altyapı Hizmetleri	Çalışma alanlarına gelen elektrik enerji hattı yedekli olmalıdır. Jeneratör ve UPS sistemleri bulunmalı, yedekliliği sağlanmalı ve düzenli bakımı (akülerin kontrolü, yeterli mazot bulundurma vb.) yapılmalıdır. Jeneratör ve UPS bakımı, onarımı ve testi için yapılan tüm işlemler kayıt altına alınmalıdır.
3.6.1.12	3	Fiziksel Güvenlik Sistemleri Verilerinin Siber Olay Tespitinde Kullanılması	Kurumda yaşanabilecek siber olayların tespitine girdi sağlamak amacı ile fiziksel güvenlik sistemlerinin desteklemesi durumunda alarm, hata mesajları vb. kayıtlar siber olay tespit sistemlerine iletilmelidir. Bk. Tedbir No: 3.6.2.13
3.6.1.13	3	Ziyaretçi Fiziksel Erişim Güvenliği	Ziyaretçi giriş ve çıkışı refakatçi ile sağlanmalıdır. Ziyaretçi giriş kartı yalnızca ilgili alanlara erişim sağlayacak şekilde tanımlanmalıdır. Ziyaretçilerin tesis içerisinde refakatçi personel olmadan dolaşmasına izin verilmemelidir. Ziyaretçilerin giriş ve çıkışlarda üstleri ve eşyaları uygun yöntemlerle (elle arama, x-ray vb.) aranmalıdır. Ziyaretçilerin bilgisayar, cep telefonu, akıllı saat vb. elektronik cihazları istisnai izne tabi olmalıdır. Bu cihazların kurum içerisine alınmasına izin verilmeden önce, güvenlik birimi tarafından kuruma girişi yapılacak cihazın seri numarası, marka, modeli ve hangi amaçla kullanılacağı bilgileri kayıt altına alınmalıdır.
3.6.1.14	3	Fiziksel Erişim Güvenliği	Personelin hangi bölgelere erişebileceği konusunda bir tanımlama yapılmalıdır. Emniyet ve güvenlik açısından önem taşıyan yerlere girişte güvenlik birimine ek güvenlik önlemlerinin olması (kartlı giriş sistemi, biyometrik veriler ile kimlik doğrulama sistemi vb.) sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.1	Fiziksel Güvenlik Sınırı	Mülakat, Gözden Geçirme	Kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırları tanımlanmış mıdır? Bu alanlara giriş ve çıkış noktalarında güvenlik kontrol mekanizması bulunmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.2	Güvenlik Biriminin Yeterliliği	Mülakat, Gözden Geçirme	Tesis içerisinde güvenlik kontrollerini sağlayabilecek yetkinlikte ve yeterli sayıda güvenlik personeli görevlendirilmekte midir? Güvenlik birimi tarafından gerçekleştirilen işlemler periyodik olarak denetlenmekte midir? Güvenlik biriminde çalışan personel, bilgi güvenliği farkındalık eğitimlerine katılım sağlamakta mıdır?
3.6.1.3	Fiziksel Giriş ve Çıkış Kontrolleri	Mülakat, Gözden Geçirme	Kuruma fiziksel giriş/çıkış işlemlerinin güvenliği sağlamak için hangi tedbirler alınmaktadır? Kargo ve kurye gibi özel teslimat hizmeti veren tarafların kuruma giriş yetkileri var mıdır? Kargo ve kuryelerin kuruma giriş/çıkış faaliyetleri nasıl gerçekleştirilmektedir? Kurumda dağıtım ve yükleme ile ilgili belirlenmiş özel alanlar var mıdır? Bu alanlara girişler ve bu alanların kullanımı ile ilgili kontroller nasıl yapılmaktadır?
3.6.1.4	Dış Güvenlik Unsurlarının Kontrolü	Mülakat, Gözden Geçirme	Binalara ait bütün pencereler, kapılar, dış duvarlar ve güvenlik altına alınması gereken yerler gözetleme veya diğer güvenlik kontrolleri ile takip edilmekte midir?
3.6.1.5	Ziyaretçi Giriş Çıkış Kontrolleri	Mülakat, Gözden Geçirme	Binaya girişte ziyaretçi bilgileri kayıt altına alınmakta mıdır? İlgili kayıtlar ne kadar süre saklanmaktadır? Bu kayıtlara kimlerin erişim yetkisi bulunmaktadır? Bina içerisindeki ziyaretçi hareketleri nasıl takip edilmektedir? Otoparktan girişler nasıl kontrol edilmektedir? Binaya giriş yapan kişilerin üzerinde ve araçlarında herhangi bir sakıncalı, şüpheli, yanıcı ve patlayıcı madde bulunup bulunmadığı yönünde tarama yapılmakta mıdır? Bina girişi, otopark girişi gibi alanlarda güvenliği sağlamaya yönelik hangi kontroller alınmaktadır?
3.6.1.6	Yetkisiz Fiziksel Erişim Durumunda İzlenecek Sürecin Tanımlanması	Mülakat, Gözden Geçirme	Yetkisiz giriş tespit edildiğinde izlenecek adımlar, bildirim yapılacak kişiler ve bu tip durumlarda müdahalenin kim tarafından gerçekleştirileceği tanımlanmış ve kurum içerisinde duyurulmuş mudur?
3.6.1.7	Kablolama Güvenliği	Mülakat, Gözden Geçirme	Kablolama güvenliğini sağlamak için hangi kontroller uygulanmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.8	Dış ve Çevresel Tehditlere Karşı Koruma	Mülakat, Gözden Geçirme	Bina çevresinde güvenliği tehdit edebilecek yerler (petrol istasyonu, yüksek voltaj elektrik dağıtım hatları, sıkıştırılmış gaz istasyonları vb.) bulunmakta mıdır? Yangın, sel, deprem, saldırı vb. felaket durumlarında kurum personeli tarafından yapılması gerekenler tanımlanmış mıdır? Acil durumlarda aranacaklar listesi oluşturulmuş mudur, oluşturulan liste güncel midir? Liste herkes tarafından görünür bir şekilde tutulmakta mıdır? Paratoner ve topraklama ile ilgili periyodik kontroller yapılmakta mıdır? Yapılan kontroller kayıt altına alınmakta mıdır?
3.6.1.9	Kamera Sistemleri	Mülakat, Gözden Geçirme	Kapalı devre kamera sistemi tesis edilmiş midir? Kameralarla izlenmeyen noktalar tespit edilmekte ve periyodik olarak kontrolü sağlanmakta mıdır? Kamera sistemi tarafından hangi alanlar izlenmektedir? Kamera kayıtları ne kadar süre tutulmaktadır? Kamera kayıtları nerede muhafaza edilmektedir? Kamera kayıtlarına kimler erişim sağlamaktadır?
3.6.1.10	Çalışma Alanlarının Güvenliği	Mülakat, Gözden Geçirme	Binalarda ziyaretçilerin kabul edileceği lobi ve toplantı odaları, personelin çalışma alanlarından ayrı ve fiziksel erişimin kontrollü olduğu bir bölgede midir? Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında; mobil cihazlar ve veri transferi özelliğine sahip cihazların olup olmadığına yönelik kontrol yapılmakta mıdır?
3.6.1.11	Destekleyici Altyapı Hizmetleri	Mülakat, Gözden Geçirme	Periyodik bakım listesinde hangi teçhizatlar bulunmaktadır? Bakım kayıtları tutulmakta mıdır?
3.6.1.12	Fiziksel Güvenlik Sistemleri Verilerinin Siber Olay Tespitinde Kullanılması	Mülakat, Güvenlik Denetimi	Fiziksel güvenlik sistemlerinin hangi kayıtları siber olay tespit sistemlerine aktarılmaktadır? Aktarılan kayıtlar aracılığıyla hangi senaryoların tespiti sağlanmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.1.13	Ziyaretçi Fiziksel Erişim Güvenliği	Mülakat, Gözden Geçirme	Kurum bünyesinde işletilen bir ziyaretçi kabul prosedürü bulunmakta mıdır? Ziyaretçilerin kuruma giriş ve çıkışları refakatçi eşliğinde sağlanmakta mıdır? Ziyaretçiler giriş ve çıkışlarda uygun yöntemlerle aranmakta mıdır? Ziyaretçilerin bilgisayar, cep telefonu, akıllı saat vb. elektronik cihazları kurum içerisine alınmadan önce yetkili kişilerden izin alınmakta mıdır? Kurum içerisine alınacak cihazların hangi bilgileri kayıt altına alınmaktadır?
3.6.1.14	Fiziksel Erişim Güvenliği	Mülakat, Gözden Geçirme	Personelin hangi bölgelere erişebileceği konusunda bir tanımlama yapılmış mıdır? Fiziksel erişim yetkileri hangi zaman aralıklarında, nasıl kontrol edilmektedir? Emniyet ve güvenlik açısından önem taşıyan yerlere girişte yeterli seviyede güvenlik kontrolleri uygulanmakta mıdır?

3.6.2. Sistem Odası/Veri Merkezine Yönelik Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.2.1	1	Sistem Odası/Veri Merkezi Güvenliği Politikası	Güvenli çalışma alanları oluşturmak amacıyla sistem odası/veri merkezi güvenliği politikası oluşturulmalı ve periyodik olarak gözden geçirilmelidir.
3.6.2.2	1	Fiziksel Varlıkların Sistem Odası/Veri Merkezi Dışına Transferi	Sistem odası/veri merkezinde bulunan varlıkların sistem odası/veri merkezi dışına transferi durumunda, bilgi güvenliği gereksinimleri çerçevesinde gerekli onay ve yetkilendirme işlemleri tamamlanmalıdır.
3.6.2.3	1	Güvenli Alan Yetkilendirmesinin Yapılması	Bilgi güvenliği kontrollerinin yeterli seviyede sağlanmasının büyük öneme sahip olduğu, kilitlenmiş bir büro veya içinde birçok oda bulunan alan, içinde kilitlenebilir dolaplar veya korumalar içeren fiziki bir güvenlik çevresi olarak tanımlanan güvenli alanlarda çalışma için yetkilendirme ve izleme prosedürleri oluşturulmalı, erişim kontrol mekanizmaları devreye alınmalıdır. Güvenli alanlara erişim yetkileri düzenli olarak gözden geçirilmelidir.
3.6.2.4	1	Üçüncü Taraf Hizmetlerin Güvenliği	Güvenli alanlara veya kritik bilgi işleme ortamlarına; destek, bakım gibi hizmetler için gelen üçüncü taraf personeline, yetkili kurum personeli nezaretinde sınırlandırılmış şekilde erişim izni verilmelidir. Ziyaretçilere yönelik; ad, soyad, geliş amacı ve tarihi, refakat eden personel, giriş/çıkış saat bilgilerini içeren kayıt tutulmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.2.5	1	Ortam Koşullarının Kontrolü	Sistem odası/veri merkezinde; su, elektrik, nem, sıcaklık ve duman kontrolünü düzenli olarak yapacak sistemler devreye alınmalıdır. Bu sistemlerin normal ve eşik değerleri belirlenmeli, bu eşik değerlerin aşılması durumunda ilgili personele uyarı mesajlarının gönderileceği bir alarm mekanizması kurulmalıdır. Ortam izleme sistemleri uzaktan izleme ve denetim amacıyla dışarıya açık olarak kurulmamalıdır.
3.6.2.6	1	Kamera Sistemleri	Bk. Tedbir No: 3.6.1.9
3.6.2.7	1	Destekleyici Altyapı Hizmetleri	Sistem odası/veri merkezine gelen elektrik enerji hattı yedekli olmalıdır. Elektrik kesintilerinde jeneratör devreye girinceye kadar sistem odası beslemesi UPS tarafından sağlanmalı ve bu UPS sistemine başka cihazlar bağlanmamalıdır. UPS'lerin periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır. Jeneratör(lerin) periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır. Jeneratör yakıt deposu her zaman dolu ve yedekli olmalıdır. Belli periyotlarda ve uzun süreli jeneratör kullanımlarında düzenli olarak jeneratör yakıt durumu kontrol edilerek kayıt altına alınmalıdır. Sistem odası/veri merkezi destekleyici servisler arasında yer alan UPS, jeneratör, klima vb. olanakların bakımları üreticileri tarafından tavsiye edilen aralıklarda konusunda yetkin uzmanlar tarafından yapılmalı ve ilgili tüm işlemler kayıt altına alınmalıdır. Veri merkezi topraklama ölçümleri periyodik olarak yapılmalı ve sonuçlar kayıt altına alınmalıdır.
3.6.2.8	1	Dış ve Çevresel Tehditlere Karşı Koruma	Sistem odası/veri merkezi duvarları ve zemini neme ve aleve dayanıklı yalıtım malzemeleri ile kapatılmalıdır. Sistem odası/veri merkezi; ısı, nem ve hava yalıtımı için oda içerisinde açıklık kalmayacak şekilde kapatılmalıdır. Sistem odası/veri merkezi; yemekhane, su, havalandırma, atık su gideri, sulu yangın söndürme, havalandırma kanalları ve üniteleri, doğal gaz ve yanıcı bileşenlerin depolandığı yerler gibi risk teşkil edecek noktalardan mümkün olabildiğince uzakta konumlandırılmalıdır. Sistem odası/veri merkezinin depreme karşı dayanıklılık testi yapılmış olmalı ve bu durum belgelendirilmelidir. Veri merkezi yerleşkesinde, gerekli yıldırım koruma tertibatı sağlanmalıdır. Sistem odası/ veri merkezinde yanıcı, yakıcı, parlayıcı ve toz oluşturan maddeler bulundurulmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.2.9	1	Donanım Bakımı ve Güvenliği	Bilgisayar, iletişim cihazları ve veri depolama donanımları kullanım veya depolama amacıyla yerleştirilirken; donanım üreticisinin belirttiği teknik standartlara uygun ortamlar sağlanmalıdır. Donanım bakımları üreticileri tarafından tavsiye edilen aralıklarda konusunda yetkin uzmanlar tarafından yapılmalı ve ilgili tüm işlemler kayıt altına alınmalıdır.
3.6.2.10	1	Kablolama Güvenliği	Kablolama düzgün ve kolay ayırt edilecek şekilde yapılmalı, bütün kablolar tek tek etiketlenmeli ve kayıt altına alınmalıdır. Sistem/veri merkezi odasında yer alan kablolar ayrı kablo kanalları içerisinden geçirilmelidir.
3.6.2.11	1	Fiziksel Giriş Kontrolleri	Sistem odası/veri merkezine giriş ve çıkış işlemlerinde kimlik doğrulama mekanizmaları kullanılmalıdır. Sistem/veri merkezine gerçekleştirilen giriş/çıkışlar kayıt altına alınmalıdır.
3.6.2.12	2	Ortam Koşullarının Gerçek Zamanlı İzlenmesi	Sistem odası/veri merkezindeki su, nem, sıcaklık ve duman kontrolü için üretilen veri gerçek zamanlı izlenebilmeli, merkezi izleme sistemlerine güvenli bir protokolle aktarılabilmelidir.
3.6.2.13	2	Siber Olay Tespitinde İz Kayıtlarının Kullanılması	Siber olay tespitinde; gerekli olması durumunda, sistem odası/veri merkezi fiziksel güvenlik ve ortam kontrolü yapılarına ait iz kayıtları, girdi olarak kullanılabilmelidir.
3.6.2.14	3	Kontrollü Erişim Noktalarının Oluşturulması	Kritik veriyi ve bilgi sistemlerini korumak adına kontrollü erişim noktaları tanımlanmalı, yetkisiz erişimi engelleyecek önlemler alınmalıdır.
3.6.2.15	3	İklimlendirme Kontrolü	Sistem odası/veri merkezinde yedekli olacak şekilde hassas kontrollü klima bulunmalıdır. Klimalardan bir tanesi bekleme konumunda çalışmalı ve diğer klima herhangi bir sebepten devre dışı kaldığında ya da gerekli soğutmayı yapamadığında bekleme konumundaki klima otomatik olarak devreye girmelidir. Hassas kontrollü klimalar sistem odası/veri merkezi kapasitesine uygun olarak seçilmeli, tam otomatik elektronik kontrollü olmalıdır. Arızalara yönelik alarm üretebilmeli, enerjinin herhangi bir anda kesilip gelmesiyle otomatik olarak devreye girebilmelidir. Klimaların periyodik bakım, ölçüm ve test işlemleri gerçekleştirilmeli ve kayıt altına alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.2.1	Sistem Odası/Veri Merkezi Güvenliği Politikası	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi güvenliği politikası hazırlanmış mıdır? Sistem odası/veri merkezi güvenliği politikası ne kadar sürede bir gözden geçirilmektedir? Sistem odası/veri merkezi güvenliği politikasının ihlali durumunda nasıl bir yöntem izlenmektedir?
3.6.2.2	Fiziksel Varlıkların Sistem Odası/Veri Merkezi Dışına Transferi	Mülakat, Gözden Geçirme	Sistem odası/veri merkezinde yer alan varlıkların sistem odası/veri merkezi dışına transferi durumunda gerekli onay ve yetkilendirme işlemi yapılmakta mıdır? Sistem odası/veri merkezi dışına transfer edilen varlıklara ait kayıt bulunmakta mıdır?
3.6.2.3	Güvenli Alan Yetkilendirmesinin Yapılması	Mülakat, Gözden Geçirme	Güvenli alanlar nasıl belirlenmektedir? Güvenli alanlar için yetkilendirme mekanizması nasıl işletilmektedir? Güvenli alanlara giriş yetkisi olan personel yetkileri periyodik olarak gözden geçirilmekte midir?
3.6.2.4	Üçüncü Taraf Hizmetlerin Güvenliği	Mülakat, Gözden Geçirme	Destek, bakım gibi hizmetler için gelen üçüncü taraf personeline refakat edilmekte midir? Üçüncü taraf personeli tarafından yapılan işlemler kayıt altına alınmakta mıdır?
3.6.2.5	Ortam Koşullarının Kontrolü	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi nem, sıcaklık ve duman kontrolü nasıl yapılmaktadır? Merkezi izleme sistemi kullanılmakta mıdır?
3.6.2.6	Kamera Sistemleri	Mülakat, Gözden Geçirme	Bk. Denetim No: 3.6.1.9
3.6.2.7	Destekleyici Altyapı Hizmetleri	Mülakat, Gözden Geçirme	Periyodik bakım listesinde hangi teçhizatlar bulunmaktadır? Teçhizat bakımlarına yönelik yapılan işlemler ve sonuçları kayıt altına alınmakta mıdır? Topraklama ölçümleri ne kadar sıklıkta bir yaptırılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.2.8	Dış ve Çevresel Tehditlere Karşı Koruma	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi duvarları neme ve aleve dayanıklı malzeme ile kaplanmış mıdır? Sistem odası/veri merkezi; ısı, nem ve hava yalıtımı için oda içerisinde açıklık kalmayacak şekilde yapılandırılmış mıdır? Sistem odası/veri merkezi yerleşimi yapılırken hangi konular dikkate alınmıştır? Veri merkezi çevresinde güvenliği tehdit edebilecek alanlar bulunmakta mıdır? Veri merkezi yerleşkesinde, gerekli yıldırım koruma tertibatı sağlanmakta mıdır?
3.6.2.9	Donanım Bakımı ve Güvenliği	Mülakat, Gözden Geçirme	Bilgisayar, iletişim cihazları ve veri depolama donanımları, kullanım veya depolama amacıyla yerleştirilirken; donanım üreticisinin belirttiği teknik standartlara uygun ortamlar sağlanmakta mıdır? Donanım bakımlarına yönelik yapılan işlemler kayıt altına alınmakta mıdır?
3.6.2.10	Kablolama Güvenliği	Mülakat, Gözden Geçirme	Kablolama güvenliğini sağlamak için ne gibi kontroller uygulanmaktadır?
3.6.2.11	Fiziksel Giriş Kontrolleri	Mülakat, Gözden Geçirme	Sistem odasına/veri merkezine giriş ve çıkışlara yönelik güvenliği sağlamak için hangi kontroller uygulanmaktadır? Sistem odası/veri merkezine giriş ve çıkış kayıtları tutulmakta mıdır? Bu kayıtlar düzenli olarak gözden geçirilmekte midir?
3.6.2.12	Ortam Koşullarının Gerçek Zamanlı İzlenmesi	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi su, nem, sıcaklık ve duman kontrolü için üretilen veri gerçek zamanlı izlenebilmekte midir?
3.6.2.13	Siber Olay Tespitinde İz Kayıtlarının Kullanılması	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi fiziksel güvenlik ve ortam kontrolü yapılarına ait iz kayıtları, siber olay tespitine girdi sağlayacak şekilde tutulmakta mıdır?
3.6.2.14	Kontrollü Erişim Noktalarının Oluşturulması	Mülakat, Gözden Geçirme	Kontrollü erişim noktaları nasıl belirlenmektedir? Kontrollü erişim noktaları için alınan güvenlik önlemleri nelerdir?
3.6.2.15	İklimlendirme Kontrolü	Mülakat, Gözden Geçirme	Sistem odası/veri merkezi iklimlendirmesi için ne tip klima kullanılmaktadır? Sistem odası/veri merkezinde kullanılan klimalar yedekli midir? Klimaların periyodik olarak bakımları yapılmakta mıdır? Bakımlarına yönelik kayıtlar tutulmakta mıdır?

3.6.3. Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
3.6.3.1	1	Sistem Odası/Veri Merkezi Cihaz Yerleşim Planı	Sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların hangi odalarda/bölümlerde kullanıldığını gösteren bir liste tutulmalıdır.
3.6.3.2	2	Gizlilik Seviyeli Bilgi İşleyen Cihazların TEMPEST Onayı	Sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların TEMPEST onayları olmalıdır. TEMPEST onayı bulunan cihazların envanteri tutulmalıdır.
3.6.3.3	3	TEMPEST Tesisat Kurallarına Uyum	Sistem odası/veri merkezindeki cihazların bulunduğu odalarda/bölümlerde elektromanyetik bilgi kaçaklarına karşı TEMPEST tesisat kurallarına/ilgili mevzuatlara uygun önlemler alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
3.6.3.1	Sistem Odası/Veri Merkezi Cihaz Yerleşim Planı	Mülakat, Gözden Geçirme	Kurumda sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazların hangi odalarda/bölümlerde kullanıldığını gösteren bir liste bulunmakta mıdır?
3.6.3.2	Gizlilik Seviyeli Bilgi İşleyen Cihazların TEMPEST Onayı	Mülakat, Gözden Geçirme	Sistem odası/veri merkezinde kullanılan gizlilik seviyeli bilgi işleyen cihazların TEMPEST onayları bulunmakta mıdır? TEMPEST onayı bulunan cihazların envanteri tutulmakta mıdır?
3.6.3.3	TEMPEST Tesisat Kurallarına Uyum	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistem odası/veri merkezindeki cihazların bulunduğu odalarda/bölümlerde elektromanyetik bilgi kaçaklarına karşı TEMPEST tesisat kurallarına uygun önlemler alınmakta mıdır?

UYGULAMA VE TEKNOLOJİ ALANLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

4. BÖLÜM

4. UYGULAMA VE TEKNOLOJİ ALANLARINA YÖNELİK GÜVENLİK TEDBİRLERİ

4.1. Kişisel Verilerin Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, kişisel verilerin güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Kişisel Verilerin Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Kayıt Yönetimi
- Erişim Kayıtları Yönetimi
- Yetkilendirme
- Şifreleme
- Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme
- Aydınlatma Yönetimi
- Açık Rıza Yönetimi
- Kişisel Veri Yönetim Sürecinin İşletilmesi

4.1.1. Kayıt Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.1.1	1	Kişisel Veri İşleme Envanterinin Hazırlanması ve Yönetimi	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirdikleri kişisel veri işleme faaliyetlerini; • Kişisel veri işleme amaçları ve hukuki dayanağını, • Veri kategorisini, • Aktarılan alıcı grubunu, • Kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, • Yabancı ülkelere aktarımı öngörülen kişisel verileri, • Veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları kişisel veri envanteri oluşturulmalı ve belirli periyotlarda güncellenmelidir. Hazırlanan envanter, Veri Sorumluları Sicili Hakkında Yönetmelik’e uygun olmalıdır.
4.1.1.2	1	Kişisel Veri Saklama ve İmha Politikasının Hazırlanması	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik’e uygun olarak ve kurum tarafından hazırlanan kişisel veri işleme envanteri göz önünde bulundurularak kişisel veri saklama ve imha politikası hazırlanmalıdır.
4.1.1.3	1	Kişisel Verilerin Veri Tabanlarında Birincil Anahtar Olarak Kullanılmaması	Veri tabanı tablolarının tasarımında kişisel veriler (T.C. kimlik numarası, pasaport numarası vb.) birincil anahtar olarak kullanılmamalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.1.4	1	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Kişisel veri barındıran veri tabanının dışarıya aktarımı (dosya olarak kaydetme, yerel veya uzak uygulamalara transfer etme vb.) yalnızca yetkilendirilmiş kullanıcılar tarafından yapılmalıdır. Bk. Tedbir No: 3.2.7.4
4.1.1.5	1	Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması	Kişisel veri barındıran kayıtlar (resimler, ofis dosyaları vb.) güvensiz ortamlarda (yetkisiz erişim sağlanabilen ortak dizin, harici bellek, disk vb.) saklanmamalıdır. Kayıtların saklanmasının zorunlu olduğu durumlarda ulusal/uluslararası standartlar/otoriteler tarafından kabul edilen güvenli yöntemlerden yararlanılmalıdır.
4.1.1.6	1	Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması	Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmalıdır. Bk. Tedbir Başlık No: 3.2.10
4.1.1.7	1	Kişisel Verinin Gizli Alanlarda Saklanmaması	İlgili kişinin açık rızası olmadan kişisel veri web sayfalarının gizli alanlarında saklanmamalıdır. Kişisel veri, tarayıcı ön belleğinde (cache) saklanmamalıdır. Uygulamada kullanılan çerezlerin kişisel veri içermesi zorunluluk ise secure bayrağı (secure flag) kullanılmalıdır. Ayrıca, istemci tarafında web depolama (web storage) özelliği ile kişisel veriler kayıt altına alınmamalıdır.
4.1.1.8	1	Hata Mesajlarında Mahremiyetin Korunması	Bk. Tedbir No: 3.2.8.3
4.1.1.9	1	Özel Nitelikli Kişisel Verinin Saklanması	Özel nitelikli kişisel veriyi barındıran kayıtlar ulusal/uluslararası kabul görmüş güvenli yöntemlerle (şifreli metin olarak, güçlü şifreleme algoritmaları kullanarak, disk seviyesinde şifreleme vb.) saklanmalıdır. Bk. Tedbir No: 3.2.7.10
4.1.1.10	1	Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi	İstemci ve sunucu uygulamalarında dosyalarda ve çerezlerde geçici olarak tutulan kişisel verilerin işleme gereksinimi veya kanuni saklama süresi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde (geri getirilemeyecek, tekrar elde edilemeyecek vb.) yok edilmelidir.
4.1.1.11	2	Veri Tabanı Tasarımı	Veri tabanı tasarımı kişisel verilerin yedekleme, anonimleştirme ve veri aktarımı işlemlerini kolaylaştıracak şekilde yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.1.1	Kişisel Veri İşleme Envanterinin Hazırlanması ve Yönetimi	Mülakat, Gözden Geçirme	Veri Sorumluları Sicili Hakkında Yönetmelik'e uygun kişisel veri işleme envanteri hazırlanmış mıdır? Envanter belirli periyotlarda güncellenmekte midir?
4.1.1.2	Kişisel Veri Saklama ve İmha Politikasının Hazırlanması	Mülakat, Gözden Geçirme	Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'e uygun kişisel veri saklama ve imha politikası hazırlanmış, ilgili taraflara duyurulmuş ve uygulanıyor mu?
4.1.1.3	Kişisel Verilerin Veri Tabanlarında Birincil Anahtar Olarak Kullanılmaması	Mülakat, Gözden Geçirme	Veri tabanı tablolarının tasarımında kişisel veriler (T.C. kimlik numarası, pasaport numarası vb.) birincil anahtar olarak kullanılmakta mıdır?
4.1.1.4	Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması	Mülakat, Güvenlik Denetimi	Veri tabanı işlemlerinde kullanılan hesaplarda minimum yetki prensibi uygulanmakta mıdır? Veri tabanının kısmen/tamamen dışa aktarımı için hangi hesap(lar) kullanılmaktadır?
4.1.1.5	Kişisel Verilerin Güvensiz Ortamlarda Saklanmaması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kişisel verinin hangi ortamlarda saklanabileceği tanımlanmış mıdır? Tanımlanan ortamlarda ulusal/uluslararası standartlara uygun güvenlik önlemleri alınmakta mıdır?
4.1.1.6	Kişisel Veri Üzerinde Girdi/Çıktı Denetimi Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Uygulamanın girdi olarak kullandığı kişisel veri üzerinde girdi/çıktı doğrulama eksikliğinden kaynaklı zafiyetlere karşı güvenlik kontrolleri uygulanmakta mıdır?
4.1.1.7	Kişisel Verinin Gizli Alanlarda Saklanmaması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veriler web sayfalarının gizli alanlarında ya da web depolama özelliği üzerinde saklanmakta mıdır? Kişisel veriler tarayıcı ön belleğinde saklanmakta mıdır? Çerezlerde bulunan kişisel verinin güvenliği nasıl sağlanmaktadır?
4.1.1.8	Hata Mesajlarında Mahremiyetin Korunması	Mülakat, Gözden Geçirme	Hata mesajlarında mahremiyetin korunması amacı ile hangi önlemler alınmaktadır?
4.1.1.9	Özel Nitelikli Kişisel Verinin Saklanması	Mülakat, Gözden Geçirme, Sızma Testi	Özel nitelikli kişisel veri barındıran kayıtların güvenliği için ne gibi önlemler alınıyor? Alınan önlemler ulusal ve/veya uluslararası kabul görmüş uygulamalar mıdır?
4.1.1.10	Geçici Olarak Tutulan Kişisel Verinin Yok Edilmesi	Mülakat, Gözden Geçirme, Sızma Testi	İstemci ve sunucu uygulamalarında kişisel verinin geçici kopyalarının yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) amacıyla yöntemler/süreçler belirlenmiş midir? Belirlenen yöntemler/süreçler uygulanmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.1.11	Veri Tabanı Tasarımı	Mülakat, Gözden Geçirme	Kişisel verilerin yedekleme, anonimleştirme ve veri aktarımı işlemlerini kolaylaştırmak için veri tabanı tasarımında hangi adımlar atılmıştır?

4.1.2. Erişim Kayıtları Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.2.1	1	Erişimlerin Kayıt Altına Alınması	Kişisel veri barındıran ortamlara yapılan başarılı ve başarısız erişimler kayıt altına alınmalıdır.
4.1.2.2	1	Erişim Kayıtlarının Arşivlenmesi	Kişisel verilere gerçekleştirilen erişim kayıtları, kurumun tabi olduğu ilgili mevzuata ve ikincil düzenlemelere uygun şekilde arşivlenmelidir.
4.1.2.3	1	Erişim Kayıtlarının Güvenliğinin Sağlanması	Kişisel veriye gerçekleştirilen erişim kayıtlarının yetkisiz okunması, değiştirilmesi veya silinmesi önlenmelidir. Bk. Tedbir No: 3.1.8.1
4.1.2.4	1	Erişim Kayıtlarının Aktarımı	Kişisel veriye gerçekleştirilen erişim kayıtları dışarı ve içeri aktarılabilir olmalıdır. Çalışan sistem üzerinde yapılacak içeri aktarma işlemi mevcut kayıtları yok etmemeli veya değiştirmemelidir.
4.1.2.5	2	Yetkisiz Erişimlerin Tespiti	Kişisel veriye gerçekleştirilen yetkisiz işlemleri tespit edebilmek için erişim kayıtları analiz edilmelidir.
4.1.2.6	3	Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması	Erişim kayıtları özel nitelikli kişisel veri barındırmamalıdır. Kayıtlarda özel nitelikli kişisel verinin bulundurulmasının zorunlu olduğu durumlarda, işlem detayının anlaşılabileceği şekilde kişisel verilerin güvenliği maskeleme vb. yöntemler ile sağlanmalıdır. Bk. Tedbir No: 3.2.8.3

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.2.1	Erişimlerin Kayıt Altına Alınması	Mülakat, Gözden Geçirme	Kişisel veri barındıran ortamlara yapılan başarılı ve başarısız erişimler kayıt altına alınmakta mıdır? Alınan kayıtlar hangi periyotlarda gözden geçirilmektedir?
4.1.2.2	Erişim Kayıtlarının Arşivlenmesi	Mülakat, Gözden Geçirme	Kişisel verilere gerçekleştirilen erişim kayıtları ilgili mevzuatlara ve ikincil düzenlemelere uygun şekilde arşivlenmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.2.3	Erişim Kayıtlarının Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme	Kişisel veriye gerçekleştirilen erişim kayıtlarının güvenliği nasıl sağlanmaktadır?
4.1.2.4	Erişim Kayıtlarının Aktarımı	Mülakat, Gözden Geçirme	Erişim kayıtlarının dışarı/içeri aktarılması için bir mekanizma mevcut mudur? Erişim kayıtlarının dışarı/içeri aktarılması için kullanılan mekanizmada mevcut kayıtların güvenliğini sağlamak için ne gibi önlemler alınmaktadır?
4.1.2.5	Yetkisiz Erişimlerin Tespiti	Mülakat, Gözden Geçirme	Erişim kayıtları üzerinden yetkisiz işlemleri tespit edebilmek amacıyla analiz faaliyetleri gerçekleştirilmekte midir?
4.1.2.6	Erişim Kayıtlarında Özel Nitelikli Kişisel Veri Bulundurulmaması	Mülakat, Gözden Geçirme	Erişim kayıtlarının hangi bilgileri içereceği tanımlanmış mı? Erişim kayıtları özel nitelikli kişisel veri barındırıyor mu?

4.1.3. Yetkilendirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.3.1	1	Yetkilendirme Mekanizmasının Kullanılması	Kullanıcıların sadece erişim yetki matrislerinde yetkilendirildiği kişisel veriye erişmesi sağlanmalıdır. Yetkisiz erişim durumunda veya beklenmeyen bir durum oluştuğunda kişisel veriye erişim varsayılan olarak engellenmelidir. Bk. Tedbir No: 3.2.3.1 Bk. Tedbir No: 3.2.8.1
4.1.3.2	1	Kimlik Doğrulama Mekanizmasının Kullanılması	Kişisel veri barındıran tüm ortamlara (web sayfası, dosya vb.) erişim için kimlik doğrulaması yapılmalıdır.
4.1.3.3	1	Erişimin Sınırlandırılması	Kişisel veri barındıran ortamlara (veri tabanı sunucusu, dosya sunucusu vb.) sadece uygulamadan erişim sağlanmalı ve bu ortamlara alternatif ve güvenli olmayan yöntemler (veri tabanı istemcileri ile doğrudan erişim, güvenli olmayan protokoller ile erişim vb.) ile yapılabilecek yetkisiz erişimler engellenmelidir.
4.1.3.4	1	Erişim Denetim Politikalarının Oluşturulması	Kişisel verilerin bulunduğu ortamlar/kaynaklar belirlenmelidir. Belirlenen ortamlar/kaynaklar için erişim denetim politikaları oluşturulmalıdır. Bu politikalarda, kullanıcı rolleri ve erişim yetkilerini açıklayan matris tanımlanmalıdır.
4.1.3.5	2	Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması	Özel nitelikli kişisel verilerin tutulduğu ortamlara erişim için çok faktörlü kimlik doğrulaması yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.3.6	2	Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması	Dış sistemler/uygulamalar arası kişisel veri akışı için erişim doğrulama kontrolü yapılmalıdır. Dış sistemler ve uygulamalar arasındaki kişisel veri akışlarında erişim ile ilgili girdi parametreleri ve sonuçlar kayıt altına alınmalıdır.
4.1.3.7	3	Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması	Sistem içi kişisel verinin akışı için erişim doğrulama kontrolü yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.3.1	Yetkilendirme Mekanizmasının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veriye erişim istekleri için yetkilendirme mekanizması kullanılmakta mıdır? Kişisel veriye erişim isteklerinde kullanılan yetkilendirme mekanizmasında hangi kurallar uygulanmaktadır? Kişisel veriye yetkisiz erişimi engellemek amacıyla hangi önlemler alınmaktadır?
4.1.3.2	Kimlik Doğrulama Mekanizmasının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veri barındıran ortamlara (web sayfası, dosya vb.) erişimde kimlik doğrulama mekanizması kullanılıyor mu?
4.1.3.3	Erişimin Sınırlandırılması	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel veri barındıran ortamlara hangi yöntemlerle erişim sağlanmaktadır? Belirlenen yöntemler kullanılmadan gerçekleştirilmek istenen erişimlerin engellenmesi amacıyla hangi önlemler alınmaktadır?
4.1.3.4	Erişim Denetim Politikalarının Oluşturulması	Mülakat, Gözden Geçirme	Kişisel verilerin bulunduğu ortamlara/kaynaklara yapılacak erişimleri denetlemek amacıyla politika oluşturulmuş mudur? Belirlenen politika hangi hususları içermektedir?
4.1.3.5	Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması	Mülakat, Gözden Geçirme, Sızma Testi	Özel nitelikli kişisel veri barındıran ortamlara erişim için kullanılan kimlik doğrulama mekanizmaları nelerdir?
4.1.3.6	Dış Sistemler / Uygulamalar Arası Veri Akışı için Erişimlerin Doğrulanması	Mülakat, Gözden Geçirme, Sızma Testi	Dış sistemler/uygulamalar arası kişisel veri akışı için erişim doğrulama kontrolü yapılmakta mıdır? Erişim ile ilgili girdi parametreleri ve sonuçlar kayıt altına alınmakta mıdır?
4.1.3.7	Alt Bileşenler Arasında Veri Akışı için Erişimlerin Doğrulanması	Mülakat, Gözden Geçirme, Sızma Testi	Sistem içi kişisel verinin akışı için erişim doğrulama kontrolü yapılmakta mıdır?

4.1.4. Şifreleme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.4.1	1	İletişimin Şifrelenmesi	Kişisel verinin paylaşımında sistemler (kurum uygulamaları, dış web servisler) arası iletişim şifreli olarak gerçekleştirilmelidir. Bk. Tedbir No: 3.2.9.1
4.1.4.2	2	Verinin Maskelenmesi	Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda (Adres bilgileri güncellenirken T.C. kimlik numarasının maskelenmesi, hesap numarasına havale işleminde alıcının adının maskelenmesi vb.) uygulama kişisel veriyi maskeleyerek göstermelidir.
4.1.4.3	2	Verinin Bütünlüğünün Korunması	Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için uygun kriptografik yöntemler uygulanmalıdır.
4.1.4.4	3	Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması	Bk. Tedbir No: 3.2.5.11

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.4.1	İletişimin Şifrelenmesi	Mülakat, Gözden Geçirme, Sızma Testi	Kişisel verinin paylaşımında sistemler arası iletişim şifreli olarak gerçekleştirilmekte midir?
4.1.4.2	Verinin Maskelenmesi	Mülakat, Güvenlik Denetimi	Kişisel veri üzerinde işlem yapılması ana amaç olmayan durumlarda verinin mahremiyeti için hangi önlemler alınmaktadır? Alınan önlemlerde maskeleme yöntemleri kullanılmakta mıdır? Kullanılan maskeleme yöntemleri nelerdir?
4.1.4.3	Verinin Bütünlüğünün Korunması	Mülakat, Gözden Geçirme	Kişisel verinin yetkisiz bir şekilde değiştirilmesini engellemek için hangi yöntemler kullanılmaktadır? Kullanılan yöntemlerde kriptografik kontroller yer almakta mıdır?
4.1.4.4	Sistemin Alt Bileşenleri Arasındaki İletişimin Şifreli Yapılması	Mülakat, Gözden Geçirme, Sızma Testi	Bk. Denetim No: 3.2.5.11

4.1.5. Yedekleme, Silme, Yok Etme ve Anonim Hale Getirme

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.5.1	1	Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması	Kişisel veri barındıran sistem yedeklerinin sadece yetkili kullanıcılar tarafından alınması sağlanmalıdır. İlgili yedekleme işlemlerine ait iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1
4.1.5.2	1	Kişisel Verilerin Silinmesi	Silme işlemine konu teşkil edecek kişisel verilerin belirlenerek, bu verilere erişim yetkisi olan ilgili kullanıcıların tespit edilmesi ve ilgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ortadan kaldırılması amacıyla gerekli süreçler tanımlanmalı ve uygulanmalıdır.
4.1.5.3	1	Kişisel Verilerin Yok Edilmesi	İşleme süresi biten kişisel verilerin hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi amacıyla gerekli süreçler tanımlanmalı ve uygulanmalıdır.
4.1.5.4	1	Kişisel Verilerin Anonim Hale Getirilmesi	Kişisel veri saklama ve imha politikası çerçevesinde, saklama süresi dolan ve anonim hale getirilmesi uygun görülen kişisel veriler ile gerçek ortam hariç test, eğitim ve geliştirme gibi ortamlarda kullanılacak kişisel veriler ulusal/uluslararası standartlar/otoriteler tarafından kabul görmüş yöntemlerle anonim hale getirilmelidir.
4.1.5.5	1	Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması	Kişisel veriyi barındıran yedekler etkin güvenlik kontrollerinin uygulandığı ortamlarda saklanmalıdır. Kişisel veri barındıran yedeklerin yetkisiz okunması, değiştirilmesi veya silinmesi engellenmelidir. Yedeklere yapılan erişimlerin iz kayıtları tutulmalıdır. Bk. Tedbir No: 3.1.8.1
4.1.5.6	2	Kişisel Veri Barındıran Yedeklerin Yok Edilmesi	Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi (geri getirilemeyecek, tekrar elde edilemeyecek vb. şekilde silme) için gerekli süreç tanımlanmalı ve uygulanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.5.1	Sistem Yedeklerinin Yetkili Kullanıcılar Tarafından Alınması	Mülakat, Güvenlik Denetimi	Kişisel veri barından sistem yedeklerini almak amacıyla yetkilendirilmiş kullanıcılar bulunmakta mıdır? Yedekleme işlemlerine ait iz kayıtları tutulmakta mıdır? Tutulan kayıtlar ne kadar süre ile muhafaza edilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.5.2	Kişisel Verilerin Silinmesi	Mülakat, Gözden Geçirme	Kişisel verilerin silinmesine yönelik süreç tanımlanmış ve uygulanmakta mıdır?
4.1.5.3	Kişisel Verilerin Yok Edilmesi	Mülakat, Gözden Geçirme	İşleme süresi biten kişisel veriler nasıl belirlenmektedir? Kişisel verilerin saklanmasına ve imhasına yönelik politika oluşturulmuş ve uygulanmakta mıdır?
4.1.5.4	Kişisel Verilerin Anonim Hale Getirilmesi	Mülakat, Gözden Geçirme, Sızma Testi	Anonim hale getirilmesi planlanan kişisel veriler nasıl belirlenmektedir? Kişisel verileri anonim hale getirmek amacıyla hangi yöntemlerden faydalanılmaktadır? Test, geliştirme vb. ortamlarda kullanılan kişisel veriler anonim hale getirilmekte midir?
4.1.5.5	Kişisel Veri Barındıran Yedeklerin Güvenliğinin Sağlanması	Mülakat, Gözden Geçirme	Kişisel veri barındıran yedeklerin güvenliğinin sağlanması için uygulanacak faaliyetler/süreçler belirlenmiş midir? Yedeklere yapılan erişimlerin iz kayıtları tutulmakta mıdır?
4.1.5.6	Kişisel Veri Barındıran Yedeklerin Yok Edilmesi	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Kişisel veri barındıran yedeklerin güvenli şekilde yok edilmesi amacıyla bir mekanizma/süreç uygulanmakta mıdır?

4.1.6. Aydınlatma Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.6.1	1	Aydınlatmanın Doğru Zamanda Yapılması	İlgili kişiden elde edilecek kişisel verilerle ilgili işleme faaliyetine başlamadan önce ilgili kişinin talebine bağlı olmadan aydınlatma yapılmalıdır. Kişisel veri ilgili kişiden elde edilmiyorsa; • Kişisel verilerin elde edilmesinden itibaren makul bir süre içerisinde, • Kişisel verilerin ilgili kişi ile iletişim amacıyla kullanılacak olması durumunda, ilk iletişim kurulması esnasında, • Kişisel verilerin aktarılacak olması halinde, en geç kişisel verilerin ilk kez aktarımının yapılacağı esnada ilgili kişi aydınlatılmalıdır. Aydınlatma ile ilgili yükümlülüğün yerine getirilmesi süreci Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'e uygun olarak yürütülmelidir.
4.1.6.2	1	Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi	Aydınlatma metninin ilgili kişi tarafından okunup anlaşıldığına dair kayıtlar tutulmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.6.3	2	Uygulama Üzerinden Aydınlatma Metninin Güncellenmesi	Aydınlatma metni, yetkili kullanıcılar tarafından uygulama üzerinden güncellenebilmelidir. Aydınlatma metninin güncelleme işlemi öncesi durumu kayıt altına alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.6.1	Aydınlatmanın Doğru Zamanda Yapılması	Mülakat, Gözden Geçirme	İlgili kişilere aydınlatmanın doğru zamanda yapılması amacıyla bir süreç oluşturulmuş mudur?
4.1.6.2	Aydınlatmanın Yerine Getirildiğinin İspat Edilmesi	Mülakat, Gözden Geçirme	Aydınlatmanın yerine getirildiğini ispat edecek bir mekanizma oluşturulmuş mudur?
4.1.6.3	Uygulama Üzerinden Aydınlatma Metninin Güncellenmesi	Mülakat, Gözden Geçirme	Aydınlatma metni uygulama üzerinden güncellenebilmekte midir? Aydınlatma metninin güncelleme işlemi öncesi durumu kayıt altına alınmakta mıdır?

4.1.7. Açık Rıza Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.7.1	1	Açık Rıza Unsurlarının Belirlenmesi	Kişisel verilerin işlenmesi amacıyla açık rıza alınması gereken durumlarda, kişisel veri işleme amacının açıkça ifade edildiği açık rıza metni hazırlanmalı ve ilgili kişilere sunulmalıdır. Kişisel verilerin yurt içi veya yurt dışı aktarımı söz konusu ise bu husus açık rıza metninde ifade edilerek ayrı bir bölüm halinde düzenlenmeli ve ilgili kişilerden ayrı bir açık rıza alınmalıdır. Kişisel verilerin farklı işleme amaçları varsa her biri için ayrı açık rıza alınmalıdır.
4.1.7.2	1	Açık Rızanın Kayıt Altına Alınması	İlgili kişiden alınmış açık rızanın inkâr edilemezliğini sağlamak amacıyla alınan açık rıza kayıt zaman damgası ile kayıt altına alınmalıdır. Bk. Tedbir No: 3.1.8.4
4.1.7.3	1	Açık Rıza Durumunun Sorgulanması	Açık rıza metninin onay tarihi ve onay durumu saklanmalıdır. İlgili kişiye ait açık rıza durumu ilgili kişi ve yetkili kişi(ler) tarafından görüntülenebilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.7.4	3	Uygulama Üzerinden Açık Rıza Alınması	Özel nitelikli kişisel verinin işlenmesi ve kişisel verinin üçüncü kişilere aktarılması durumunda açık rıza uygulama üzerinden alınmalı ve açık rıza beyan durumu sorgulanabilmelidir.
4.1.7.5	3	Açık Rıza Metninin Güncellenmesi	Uygulama üzerinde açık rıza metni yetkili kişiler tarafından güncellenebilmelidir. Güncelleme öncesindeki açık rıza metinleri saklanmalıdır. Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınması sağlanmalıdır.
4.1.7.6	3	Açık Rıza ile İlgili Taleplerin Yönetilmesi	İlgili kişi, açık rızasını geri alma talebini uygulama üzerinden gerçekleştirebilmelidir. İlgili kişinin açık rızasını geri alma talebi veri sorumlusu tarafından uygulanmalı ve ilgili kişinin açık rızasına dayanarak yapılan veri işleme faaliyetleri durdurulmalıdır.
4.1.7.7	3	Islak İmzalı Açık Rıza Metninin Saklanması	İlgili kişiden alınmış ıslak imzalı (fiziksel) açık rıza metninin aslı ya da taranmış kopyası saklanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.7.1	Açık Rıza Unsurlarının Belirlenmesi	Mülakat, Gözden Geçirme	Kişisel verilerin işlenmesi amacıyla açık rıza alınması gereken durumlar belirlenmiş midir? Açık rıza alınması amacıyla aydınlatma metni hazırlanarak ilgili kişilere sunulmakta mıdır?
4.1.7.2	Açık Rızanın Kayıt Altına Alınması	Mülakat, Gözden Geçirme	Açık rızanın kayıt altına alınması için bir mekanizma/süreç işletilmekte midir?
4.1.7.3	Açık Rıza Durumunun Sorgulanması	Mülakat, Gözden Geçirme	İlgili kişiye ait açık rıza metninin onay durumu, onay tarihi saklanmakta mıdır? İlgili kişi tarafından açık rıza durumu sorgulanabilmekte midir? Yetkili kişi(ler)ce hangi kullanıcılardan açık rıza alındığı sorgulanabilmekte midir?
4.1.7.4	Uygulama Üzerinden Açık Rıza Alınması	Mülakat, Gözden Geçirme	Uygulama üzerinden açık rızanın alınması ve açık rıza beyan durumunun sorgulanması için bir mekanizma/süreç işletilmekte midir?
4.1.7.5	Açık Rıza Metninin Güncellenmesi	Mülakat, Gözden Geçirme	Uygulama üzerinde açık rıza metninin güncellenebilmesi için bir mekanizma/süreç tanımlanmış mıdır? Güncelleme öncesindeki açık rıza metinleri saklanmakta mıdır? Güncellenen açık rıza metinleri için kullanıcılardan tekrar açık rıza alınmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.7.6	Açık Rıza ile İlgili Taleplerin Yönetilmesi	Mülakat, Gözden Geçirme	Uygulama üzerinden açık rıza ile ilgili taleplerin yönetimi sağlanabilmekte midir?
4.1.7.7	Islak İmzalı Açık Rıza Metninin Saklanması	Mülakat, Gözden Geçirme	Islak imzalı açık rıza metinlerinin taranmış halinin saklanması amacıyla bir süreç işletilmekte midir?

4.1.8. Kişisel Veri Yönetim Sürecinin İşletilmesi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.1.8.1	1	İlgili Kişinin Başvuru Hakkının Yönetilmesi	İlgili kişinin veri sorumlusuna başvuruda bulunabilmesi ve bu başvuruya süresinde cevap verilebilmesi için bir süreç oluşturulmalıdır. Bu süreç Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olmalıdır.
4.1.8.2	1	Kişisel Veriye Yapılan İşlemlerin Elde Edilmesi	İlgili kişinin, kişisel verisine yapılan işlemleri öğrenme talebine istinaden veri sorumlusu tarafından bu işlemler elde edilmelidir. Bk. Tedbir No: 4.1.8.1
4.1.8.3	1	Güncelleme, Anonimleştirme, Silme ve Yok Etme İşlemlerinin Gerçekleştirilmesi	İlgili kişi tarafından talep edilen; güncelleme, anonimleştirme, silme, yok etme işlemleri gerçekleştirilmelidir. Talep edilmesi durumunda bu işlemler kişisel verinin aktarıldığı üçüncü taraflara da iletilmelidir. Yapılacak işlemlerle ilgili bilgilendirme Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'e uygun olarak gerçekleştirilmelidir. Bk. Tedbir No: 4.1.8.1
4.1.8.4	1	Kişisel Verinin Aktarıldığı Üçüncü Tarafların Tespit Edilmesi	Kişisel verinin kimlere aktarıldığı, aktarılma amacı ve aktarılma tarihine ait bilgiler kayıt altına alınmalı ve bu bilgiler talep edilmesi durumunda ilgili kişiye bildirilmelidir. Bk. Tedbir No: 4.1.8.1
4.1.8.5	2	Kişisel Verisi Etkilenen veya Etkilenmesi Muhtemel Kişilerin Bilgilendirilmesi	Kişisel verinin kanuni olmayan yollarla başkaları tarafından ele geçirilmesi, yayımlanması, ifşa edilmesi veya bütünlüğünün bozulması durumunda ilgili kişi ve mevzuat gereği bilgilendirilmesi gereken kurum ve kuruluşlar bilgilendirilmelidir. İlgili kişiye yapılacak bildirimler uygun yöntemlerle (internet sayfası, e-posta, SMS vb.) gerçekleştirilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.1.8.1	İlgili Kişinin Başvuru Hakkının Yönetilmesi	Mülakat, Gözden Geçirme	İlgili kişinin veri sorumlusuna başvuru hakkının yönetilmesi amacıyla bir süreç işletilmekte midir? Bu süreç yürürlükte olan ilgili mevzuata uygun mudur?
4.1.8.2	Kişisel Veriye Yapılan İşlemlerin Elde Edilmesi	Mülakat, Gözden Geçirme	İlgili kişinin verisine yapılan işlemler kayıt altında tutulmakta mıdır?
4.1.8.3	Güncelleme, Anonimleştirme, Silme ve Yok Etme İşlemlerinin Gerçekleştirilmesi	Mülakat, Gözden Geçirme	İlgili kişi tarafından talep edilen güncelleme, anonimleştirme, silme ve yok etme işlemlerinin yapılabilmesi amacıyla bir süreç işletilmekte midir? Tanımlanan süreç yürürlükte olan mevzuata uygun mudur?
4.1.8.4	Kişisel Verinin Aktarıldığı Üçüncü Tarafların Tespit Edilmesi	Mülakat, Gözden Geçirme	Kişisel veriler üçüncü taraflara aktarıldığında aktarım işlemi ile ilgili hangi bilgiler kayıt altına alınmaktadır?
4.1.8.5	Kişisel Verisi Etkilenen veya Etkilenmesi Muhtemel Kişilerin Bilgilendirilmesi	Mülakat, Gözden Geçirme	Kişisel veri ihlalinin kamuoyuna, yetkili kurum ve kuruluşlar ile ilgili kişiye bildirilmesi amacıyla bir süreç işletilmekte midir?

4.2. Anlık Mesajlaşma Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, anlık mesajlaşma güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Anlık Mesajlaşma Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri

4.2.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.2.1.1	1	Mesajlaşma Uygulaması Seçimi	Kurumsal haberleşme amacıyla sunucuları kurum kontrolünde olan mesajlaşma uygulamaları kullanılmalıdır. Kurumun kendine ait bir haberleşme uygulaması yoksa mesajlaşma amacıyla sunucuları yurt içinde bulunan yerli ve milli uygulamalar tercih edilmelidir.
4.2.1.2	1	İletim Ortamı Güvenliği	Mesajlaşma uygulamasının iletim katmanı güvenliği, bilinen zafiyetleri olmayan, güncel bir SSL/TLS sürümü ile sağlanmalıdır ve uygulamada SSL Pinning kullanılmalıdır. Bk. Tedbir No: 3.2.9.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.2.1.3	1	Gizlilik Dereceli Veri Paylaşımı	Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere mobil uygulamalar üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmamalıdır.
4.2.1.4	1	Çoklu Cihaz Kullanımı	Uygulama birden fazla mobil cihaz üzerinde eş zamanlı olarak çalışmamalıdır. Hesaba farklı bir mobil cihazdan giriş yapılmak istendiğinde kullanıcı kimlik doğrulamaya zorlanmalı, başarılı kimlik doğrulama sonrası uygulama sadece yeni giriş yapılan cihaz üzerinde kullanılabilmelidir.
4.2.1.5	2	Uçtan Uca Şifreleme	Uygulamadan gönderilen tüm mesajlar ve uygulama kullanılarak yapılan tüm sesli ve görüntülü aramalar uçtan uca şifrelenmelidir.
4.2.1.6	2	Şifreleme Anahtarlarının Saklanması	Uygulama şifreleme için kullandığı anahtarları işletim sisteminin güvenli depolama alanlarında (TEE, HSM, keystore, keychain vb.) tutmalıdır.
4.2.1.7	2	Yönetim Arayüzüne Erişim	Mesajlaşma sistemlerine ait yönetim arayüzlerine yetkili tarafların erişimi, yeterli en düşük haklarla güvenli bir şekilde yapılmalıdır. Yönetim arayüzüne erişilerek yapılan işlemlere ait denetim izleri tutulmalıdır. Bk. Tedbir No: 3.1.8.1
4.2.1.8	3	Cihaz Üzerindeki Verinin Şifrelenmesi	Uygulama cihaz üzerinde sakladığı tüm veriyi şifreli olarak tutmalıdır.
4.2.1.9	3	Kritik Haberleşmenin Güvenliği	Kritik veri içeren her türlü sesli, yazılı ve görüntülü haberleşme uygulamalarında, kaynak kodları kurum tarafından talep edildiğinde denetlenebilen, işletmesi ve yönetimi yerel olarak yapılabilen yerli ve milli uygulamalar tercih edilmelidir.

Denetim Maddeleri

Tedbir No.	Denetim Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.2.1.1	Mesajlaşma Uygulaması Seçimi	Mülakat, Güvenlik Denetimi	Kurum içi mesajlaşma için hangi uygulama kullanılmaktadır?
4.2.1.2	İletim Ortamı Güvenliği	Mülakat, Güvenlik Denetimi	Mesajlaşma sistemlerinde iletim ortamı güvenliği nasıl sağlanmaktadır? Kullanılan protokol ve sürümleri nelerdir? Bilinen ve yayımlanmış zafiyetleri var mıdır? Kullanılan algoritma takımları ve anahtarlar yeterli güvenlik seviyesinde midir?
4.2.1.3	Gizlilik Dereceli Veri Paylaşımı	Mülakat, Güvenlik Denetimi	Mobil uygulamalar üzerinden gizlilik dereceli veri paylaşımı ve haberleşmesi nasıl engellenmektedir?

Tedbir No.	Denetim Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.2.1.4	Çoklu Cihaz Kullanımı	Mülakat, Güvenlik Denetimi	Kullanıcı hesabına aynı anda birden fazla mobil cihaz üzerinden erişilebiliyor mu? Yeni cihaz üzerine kurulum yapılırken kimlik doğrulaması yapılıyor mu?
4.2.1.5	Uçtan Uca Şifreleme	Mülakat, Güvenlik Denetimi, Sızma Testi	Anlık mesajlaşma uygulaması mesajları uçtan uca şifrelemekte midir?
4.2.1.6	Şifreleme Anahtarlarının Saklanması	Mülakat, Güvenlik Denetimi, Sızma Testi	Mesajlaşma uygulaması şifreleme anahtarlarını nasıl saklamaktadır? Anahtarlar cihazdan çıkartılabilir mi?
4.2.1.7	Yönetim Arayüzüne Erişim	Mülakat, Güvenlik Denetimi, Sızma Testi	Mesajlaşma sistemleri yönetim arayüzlerine güvenli erişim nasıl sağlanmaktadır? Erişim yetkileri, bilgi güvenliği gereksinimleri doğrultusunda bilmesi gereken prensibi göz önünde bulundurularak tanımlanmakta mıdır? Yönetim arayüzüne erişilerek gerçekleştirilen işlemler kayıt altına alınmakta mıdır? Eğer kullanılıyor ise kullanıcıların gizli anahtarı, biyometrik bilgisi güvenli bir şekilde tutulmakta mıdır?
4.2.1.8	Cihaz Üzerindeki Verinin Şifrelenmesi	Güvenlik Denetimi, Sızma Testi	Uygulama çalıştığı cihaz üzerinde hangi bilgileri tutmaktadır? Cihaz üzerinde tutulan veri şifreli olarak saklanmakta mıdır? Şifreli veriyi çözmek için gerekli anahtar nerede saklanmaktadır?
4.2.1.9	Kritik Haberleşmenin Güvenliği	Mülakat, Güvenlik Denetimi	Kritik veri iletimini sağlayan uygulamanın yönetimi ve işletimi yerel olarak yapılmakta mıdır? Kaynak kodları talep halinde denetlenebilmekte midir?

4.3. Bulut Bilişim Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, bulut bilişim güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Bulut Bilişim Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri

4.3.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.3.1.1	1	Bulut Hizmeti Kullanımı	Kritik verilerin yurt içinde depolandığı ve yurt dışında barındırılmayacağı garanti altına alınmalıdır. Kurumlara ait özel bulut sistemleri haricinde, bulut servis sağlayıcılardan yer, sunucu veya servis tabanlı bulut hizmeti kullanılacaksa, • Erişen personel, yetki ve yetkinlik düzeyleri • Erişim, işlem ve ağ trafiği iz kayıtlarının izlenmesi • Güncelleme durum alarmları • Siber olay alarmları • Performans ve kapasite göstergeleri kurum tarafından kontrol edilmelidir.
4.3.1.2	1	Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi	Bulut bilişim hizmeti kapsamında hizmet alınan taraf ile hizmet alan kurum arasında, karşılıklı yükümlülükleri ve gizlilik maddelerini içeren bir sözleşme yapılmalıdır. Alınan hizmetin kapsamı sözleşme içerisinde tam olarak belirtilmeli ve hizmet kapsamında işlenen verinin kritikliği doğrultusunda yeterli seviyede güvenlik önlemleri alınmalıdır. İlgili sözleşmenin geçerlilik süresi belirlenmeli ve periyodik olarak gözden geçirilmesi sağlanmalıdır. Bk. Tedbir No: 3.5.3.1 Bk. Tedbir No: 3.5.3.3
4.3.1.3	1	Veri İletimi Güvenliği	Bulut bilişim kapsamında çalışan tüm sistemler arasındaki veri trafiği zafiyet içermeyen güvenli ve güncel iletişim protokolleriyle gerçekleştirilmelidir. Bulut ortamına doğru veri iletimi sağlanırken iletimin tek yönlü olması sağlanmalı, kurumsal ağ bulut ortamından gelecek tehditlere karşı izole olmalıdır.
4.3.1.4	1	Kaynakların İzole Edilmesi	Aynı bulut ortamını kullanan kurumların sistemleri ağ seviyesinde birbirlerinden mantıksal ve/veya fiziksel olarak izole edilmelidir. Kurumların yalnızca kendilerine ait veriye erişim imkânı sağlanmalıdır.
4.3.1.5	1	İmajların İmha Edilmesi	Bulut hizmeti kapsamında, ihtiyaç olması durumunda şablon olarak kullanılan imajların geri döndürülemeyecek şekilde silinmesine servis sağlayıcı tarafından imkân tanınmalıdır.
4.3.1.6	1	Sanal Makineye Ait Belleklerin İmhası	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.3.1.7	1	Bulut Ortamı Güvenliği	Servis sağlayıcılar kendi kaynaklarını DDoS saldırılarına karşı koruyabilmeli ve kapasitesinin üzerinde gelen yüksek boyutlu DDoS saldırılarına karşı iş ve hizmet sürekliliğini sağlayabilmelidir. Hizmet alan taraf ile imzalanan sözleşme ve taahhütlerde bu husus yer almalıdır. Servis sağlayıcılar, servis verdikleri herhangi bir hizmet alanına gelen bir siber saldırıdan (servis dışı bırakma, zararlı yazılım vb.) veya saldırının sistemlerde oluşturabileceği performans problemlerinden diğer hizmet alanlarının etkilenmemesi için güvenlik duvarı, saldırı tespit sistemi gibi güvenlik önlemlerini almalıdır. Servis sağlayıcıların verdikleri hizmetler ile ilgili hizmet seviye taahhüt koşulları belirlenmeli, ölçülmeli ve raporlanabilmelidir. Kurumlar, varlık gruplarının kritiklik derecesine uygun güvenlik tedbirlerini uygulayan ve periyodik güvenlik denetimlerini gerçekleştiren bulut hizmeti sağlayıcılarından hizmet almalıdır. Operatörler tarafından sunuculara erişimde trafiğin yurt içinde kalmasına yönelik tedbirler uygulanmalıdır. Bulut hizmeti kullanımında kuruma ait şifreleme anahtarları hizmeti alan kurum tarafından yönetilmelidir. Bulut yönetim arayüzü üzerinden işlem yapmak için IPSec veya SSL VPN geçidi kullanılmalı ve bulut yönetim arayüzüne erişim sadece bu kanallardan yapılmalıdır.
4.3.1.8	1	Sanal Makineye Ait Disk Bölgelerinin İmhası	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir.
4.3.1.9	1	İş Sürekliliğinin Sağlanması	Bulut bilişim hizmeti sunacak servis sağlayıcı iş sürekliliğini sağlamak amacıyla felaket kurtarma merkezi veya yedekleme mekanizmaları ile ilgili yeterlilikleri kurumun bilgi güvenliği gereksinimlerine uygun olarak sağlamalıdır. Bk. Tedbir Başlık No: 3.1.13
4.3.1.10	1	Erişim Yetkilerinin Yönetiminin Sağlanması	Bulut hizmet sağlayıcısının, hizmet alan kurumun sistemine giriş yapması gerektiğinde önceden belirlenmiş kurum yetkililerinden onay almalıdır. Yetkilendirme süreli olmalı ve sorun giderildiğinde erişim yetkisi kaldırılmalıdır. Hizmet sağlayıcı bu süreçte yapılan tüm işlemleri kayıt altına almalı ve bunları raporlamalıdır. Hizmet sağlayıcının bu süreci sistem üzerinde yönetecek ve raporlayacak özellikleri ve tanımlı süreçleri olmalıdır.
4.3.1.11	1	Hizmetin Sonlandırılması Hususları	Paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir. Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.3.1.12	2	Güvenli Veri Depolama Politikasının Uygulanması	Bulut bilişim hizmeti sunacak servis sağlayıcının veri güvenliğini (ifşa, değiştirme, bozulma vb. durumlara karşı) sağlamak adına güvenli veri depolama politikası bulunmalıdır.
4.3.1.13	2	Bulut Ortamı İşlem Kayıtlarının Tutulması	Bulut sistemlerde gerçekleştirilen yönetimsel işlemler kayıt altına alınmalı ve değişmezliği sağlanmalıdır. Bk. Tedbir No: 3.1.8.1
4.3.1.14	3	Kaynakların Fiziksel Olarak İzole Edilmesi	Bulut sistemler üzerinde kuruma ait kritik veri bulundurulacaksa, kritik veriler kurum dışı başka kaynaklar ile aynı fiziksel cihaz üzerinde bulundurulmamalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.3.1.1	Bulut Hizmeti Kullanımı	Mülakat, Gözden Geçirme	Kuruma ait hangi veriler bulut sistemler üzerinde tutulmaktadır? Bulut hizmet sağlayıcı tarafından kuruma hangi kontroller sağlanmaktadır?
4.3.1.2	Hizmet Kapsamı ile Rol ve Sorumlulukların Belirlenmesi	Mülakat, Gözden Geçirme	Bulut bilişim hizmeti kapsamında, hizmet alınan taraf ile hizmet alan kurum arasında, karşılıklı yükümlülükleri ve gizlilik maddelerini içeren bir sözleşme var mıdır? Sözleşme içeriği, geçerlilik süresi boyunca düzenli olarak gözden geçirilmekte midir?
4.3.1.3	Veri İletimi Güvenliği	Mülakat, Güvenlik Denetimi	Bulut bilişim kapsamında çalışan sistemler arasındaki veri trafiği için hangi şifreli iletim protokolü kullanılmaktadır? Bulut ortamından kuruma yönelik trafiğe izin verilmekte midir?
4.3.1.4	Kaynakların İzole Edilmesi	Mülakat, Güvenlik Denetimi	Aynı bulut ortamını kullanan kurumların sistemleri birbirlerinden mantıksal ve/veya fiziksel olarak izole edilmekte midir?
4.3.1.5	İmajların İmha Edilmesi	Mülakat, Güvenlik Denetimi	Bulut hizmeti kapsamında, ihtiyaç olması durumunda şablon olarak kullanılan imajlar geri döndürülemeyecek şekilde silinebilmekte midir?
4.3.1.6	Sanal Makineye Ait Belleklerin İmhası	Mülakat, Güvenlik Denetimi	Herhangi bir sanal makine hizmetinin sonlandırılması ile birlikte, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri servis sağlayıcı tarafından geri döndürülemeyecek şekilde otomatik olarak silinmekte midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.3.1.7	Bulut Ortamı Güvenliği	Mülakat, Güvenlik Denetimi, Sızma Testi	Bulut ortamı internet güvenliğine yönelik hangi uygulamalar devrededir? Alınan bulut hizmetlerinde varlık gruplarının kritiklik derecesine uygun güvenlik tedbirlerinin tesis edildiği kontrol edilmekte midir? Hizmet alınan servis sağlayıcı kendi kaynaklarını DDoS saldırılarına karşı nasıl koruyabilmektedir, yüksek boyutlu DDoS saldırılarına karşı iş ve hizmet sürekliliğini nasıl sağlanmaktadır? Hizmet alan taraf ile imzalanan sözleşme ve taahhütlerde bu husus nasıl yer almaktadır? Hizmet alınan servis sağlayıcı, herhangi bir hizmet alanına gelen bir siber saldırıdan (servis dışı bırakma, zararlı yazılım vb.) veya saldırının sistemlerde oluşturabileceği performans problemlerinden diğer hizmet alanların etkilenmemesi için nasıl önlem almışlardır? Hizmet alınan servis sağlayıcıların verdikleri hizmetler ile ilgili hizmet seviye taahhüt koşulları net belirlenmiş, ölçülüyor ve raporlanabiliyor durumda mıdır?
4.3.1.8	Sanal Makineye Ait Disk Bölgelerinin İmhası	Mülakat, Güvenlik Denetimi	Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmekte midir?
4.3.1.9	İş Sürekliliğinin Sağlanması	Mülakat, Gözden Geçirme	Bulut bilişim hizmeti sunan servis sağlayıcı iş sürekliliğini sağlamak amacıyla hangi kontrolleri uygulamaktadır? Uygulanan kontroller kurumun bilgi güvenliği gereksinimleri ile örtüşmekte midir?
4.3.1.10	Erişim Yetkilerinin Yönetiminin Sağlanması	Mülakat, Gözden Geçirme	Bulut hizmet sağlayıcısının, hizmet alan kurumun sistemine giriş yapması gerektiği durumlarda kurum tarafında onay alınması gereken yetkililer belirlenmiş midir? Bulut hizmet sağlayıcısı tarafından kurum sistemine erişilmesi durumunda gerçekleştirilen tüm işlemler kayıt altına alınmakta mıdır? Alınan kayıtlara ilişkin bir rapor oluşturularak kurum ile paylaşılmakta mıdır?
4.3.1.11	Hizmetin Sonlandırılması Hususları	Mülakat, Gözden Geçirme	Bulut hizmet sağlayıcıdan alınan hizmetin sonlandırılması durumunda kuruma ait veriler sistemlerden geri getirilemeyecek şekilde silinmekte midir? Güvenli silme işlemi için hangi yöntemler kullanılmaktadır? Bulut hizmet sağlayıcıdan alınan hizmetin sonlanması durumunda kuruma ait profil ayarları, hizmet raporları vb. bilgilerin hizmet sağlayıcı tarafından silindiği garanti altına alınmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.3.1.12	Güvenli Veri Depolama Politikasının Uygulanması	Mülakat, Gözden Geçirme	Bulut bilişim hizmet sağlayıcı tarafından güvenli veri depolama politikası hazırlanmış mıdır? Politika düzenli olarak gözden geçirilmekte midir? Politikanın ihlali durumunda hangi prosedür işletilmektedir?
4.3.1.13	Bulut Ortamı İşlem Kayıtlarının Tutulması	Mülakat, Gözden Geçirme	Bulut sistemler üzerinde gerçekleştirilen işlemler kayıt altına alınmakta mıdır? Kayıtların bütünlüğünü sağlamaya yönelik hangi kontroller uygulanmaktadır?
4.3.1.14	Kaynakların Fiziksel Olarak İzole Edilmesi	Mülakat, Gözden Geçirme	Bulut sistemler üzerinde tutulan kuruma ait kritik verilerin kurum dışı başka varlıklar ile aynı fiziksel cihazda bulundurulmaması garanti altına alınmakta mıdır?

4.4. Kripto Uygulamaları Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, kripto uygulamaları güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Kripto Uygulamaları Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Kriptografik Algoritmalar ve Kullanımı
- Şifreleme ve Anahtar Yönetimi
- Kriptografik Uygulamalar

4.4.1. Kriptografik Algoritmalar ve Kullanımı

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.1.1	1	Kriptografik Algoritma Tipinin Seçilmesi	Kriptografik algoritma seçimi; algoritma kullanım amacı, algoritmayı kullanacak taraflar ve bu kapsamda işlenecek bilgi/verinin kritiklik seviyesi göz önünde bulundurularak yapılmalıdır.
4.4.1.2	1	Kripto Uygulama, Cihaz ve Sistemlerin Kriptografik Algoritma Güvenliği	Kurum bünyesinde, standartlaştırılmış ve güvenli kriptografik algoritma takımında yer alan algoritmaları barındıran uygulama, cihaz ve sistemler kullanılmalıdır. Standartlaştırılmış ve güvenli kriptografik algoritmalara yönelik endüstri standartları ve en iyi uygulama örnekleri dikkate alınmalıdır. Standartlaştırılmış kriptografik algoritma takımında yer almayan kriptografik algoritmaların kullanımının gerekmesi durumunda kullanım öncesinde, yetkilendirilmiş kripto analiz laboratuvarı tarafından yeterli güvenlik seviyesinde olup olmadıklarının analizi ve değerlendirilmesi yapılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.1.3	1	Standart Kriptografik Algoritmaları İçeren Kripto Modüllerinin Güvenliği	Kullanılacak standart kriptografik algoritmaları içeren kripto modüllerinin uygun güvenlik hedefi veya koruma profili olan Ortak Kriterlere ve/veya TS ISO/EC 19790 – 24759 standardına uygunluğu yetkili laboratuvarlarca test edilmelidir. Bu testler sonucunda, kurum varlıklarının kritiklik derecesine uygun kripto modüller kullanılmalıdır.
4.4.1.4	3	Milli Kriptografik Algoritmaların Gerçeklendiği Kripto Cihazlarının Tedariki	Kritik bilgi/veri işleyen kurumların, kritiklik seviyesine uygun tipte milli kriptografik algoritmaların gerçeklendiği cihazlar temin edilmelidir. Yetkili kripto analiz laboratuvarından güvenli şekilde kullanılabileceğine dair kripto analiz raporu bulunan milli kriptografik algoritmaların donanımsal olarak gerçeklendiği bu kripto cihazların, yetkili laboratuvar tarafından yapılan COMSEC güvenlik testlerinden başarılı bir şekilde geçmiş olmaları gerekmektedir. COMSEC güvenlik testlerine tabi tutulan kripto modüller için Ortak Kriter ve/veya TS ISO/EC 19790 – 24759 standardına uyum gerekliliği bulunmamaktadır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.1.1	Kriptografik Algoritma Tipinin Seçilmesi	Mülakat, Gözden Geçirme	Kriptografik algoritma seçimi nasıl yapılmaktadır? Kriptografik algoritma seçiminde varlık grubuna ait kritiklik derecesi, kullanım amacı ve kullanım ortamı gereksinimleri dikkate alınmakta mıdır?
4.4.1.2	Kripto Uygulama, Cihaz ve Sistemlerin Kriptografik Algoritma Güvenliği	Mülakat, Gözden Geçirme	Kripto uygulama, cihaz ve sistemler tarafından kullanılan kriptografik algoritmalar standartlaştırılmış kriptografik algoritma takımında yer almakta mıdır? Standartlaştırılmış kriptografik algoritma takımında yer almayan kriptografik algoritmaların kullanılmadan önce yetkilendirilmiş kripto analiz laboratuvarı tarafından analiz ve değerlendirme işlemleri yapılmakta mıdır? Kripto algoritmalarının güvenlik seviyeleri düzenli aralıklarla gözden geçirilmekte midir?
4.4.1.3	Standart Kriptografik Algoritmaları İçeren Kripto Modüllerinin Güvenliği	Mülakat, Gözden Geçirme	Kullanılan kriptografik sistemde standart kriptografik algoritmaları içeren kripto modüllerinin güvenliği Ortak Kriter ve/veya TS ISO/IEC 19790-24759 onaylı mıdır?
4.4.1.4	Milli Kriptografik Algoritmaların Gerçeklendiği Kripto Cihazlarının Tedariki	Mülakat, Gözden Geçirme	Milli kriptografik algoritmalar, milli üreticilerden tedarik edilen cihazlarda mı gerçeklenmiştir? Yetkili kripto analiz laboratuvarı tarafından hazırlanan, ilgili cihazlarda kullanılan milli kriptografik algoritmaların güvenli bir şekilde kullanılabileceğine dair kripto analiz raporu bulunmaktadır? Bu algoritmaların gerçeklendiği kriptografik cihazlar, yetkili COMSEC laboratuvarı tarafından uygulanan güvenlik testlerinden başarılı bir şekilde geçmiş midir?

4.4.2. Şifreleme ve Anahtar Yönetimi

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.1	1	Kriptografik Anahtara İlişkin Güvenlik Gereksinimleri Analizi	Kriptografik anahtarlar üretilirken; kullanım amacına uygun, bilgi güvenliği gereksinimlerini karşılayacak seviyede, ulusal ve uluslararası düzeyde kabul görmüş anahtar uzunlukları kullanılmalıdır. Anahtar uzunlukları, bilgi güvenliği gereksinimleri doğrultusunda endüstri standartları ve en iyi uygulama örnekleri dikkate alınarak belirlenmelidir.
4.4.2.2	1	Kriptografik Anahtarların Üretilmesi	Anahtar üretim aşamasında, anahtarın tahmin edilebilir olmasını engellemek için anahtarın entropisinin anahtar boyundan daha düşük olmaması sağlanmalıdır. Üretim esnasında ulusal ve/veya uluslararası standartlar kapsamında kabul görmüş ve yetkili test ve değerlendirme merkezi tarafından güvenlik testleri yapılmış bir gerçek rassal sayı üreteci "True Random Number Generator (TRNG)" veya sanki rassal sayı üreteci "Pseudo Random Number Generator" kullanılmalıdır.
4.4.2.3	1	Anahtar Üretim ve Dağıtım Cihazlarına Erişim	Anahtar üretim ve dağıtım cihazlarının bulunduğu fiziksel ve elektronik ortamlara yalnızca erişim yetkisi olan tarafların erişimi mümkün kılınmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.
4.4.2.4	1	Güvenli Yedekleme	Anahtarın yedeğinin alındığı fiziksel ve elektronik ortamların güvenliği sağlanmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.
4.4.2.5	1	Kriptografik Anahtarlara Erişim Kontrolü	Kriptografik anahtarlara erişim sadece kullanım amacına özel olarak erişim yetkisi tanımlanmış personel ile sınırlandırılmalıdır. Tüm işlemlerin kayıtları alınmalı ve bu kayıtlar uygun güvenlik seviyesiyle korunmalıdır.
4.4.2.6	1	Kriptografik Anahtarların Revize Edilmesi	Kriptografik anahtarlar aşağıdaki maddelerin herhangi birisinin ortaya çıkması durumunda revize edilmelidir: • Kriptografik anahtar ile ilgili herhangi bir zafiyet durumu oluşması ya da zafiyet şüphesinin olması • Kriptografik anahtarlara erişim yetkisi olan personelin kurumdan ayrılması veya görev değiştirmesi • Kriptografik anahtarların, kullanım periyodunun tamamlanması ile birlikte geçerlilik sürelerinin dolması

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.7	1	Güvenli Anahtar Ulaştırma / İletimi	Anahtar dağıtım protokolünün analiz edilerek güvenli olması sağlanmalıdır. Gizli kriptografik anahtar bir ağ ortamından iletilecek ise trafik iki uç arasında şifreli ve araya girme saldırılarına karşı korumalı olmalıdır. Ayrıca, trafiğin şifrelemesi taşınan anahtarın gizlilik seviyesi ile uyumlu olmalıdır. Kullanım amacı ve içerdiği bilgi/verinin kritiklik derecesine göre anahtarın birden fazla parçaya ayrılarak farklı kanallarla iletilmesi sağlanmalıdır. Kriptografik anahtar dijital bir kanal ile iletilmiş ise iletilen anahtarın bütünlük kontrolü yapılmalı ve iletilen anahtarın orijinal anahtar ile aynı olduğu doğrulanmalıdır. Dijital kanal açık bir kanalsa, anahtarın şifrelenmesi de sağlanmalıdır. Anahtar dağıtımı ve üretimi için uygun görüldüğü durumlarda HSM tabanlı bir teknoloji tercih edilerek yukarıda bahsi geçen gereksinimler HSM aracılığı ile sağlanmalıdır. Bu durumda, HSM sistemi uygun şekilde yapılandırılmalı ve erişimleri kontrol altına alınmalıdır.
4.4.2.8	1	Anahtar Taşıma Cihazlarının Muhafazası ve Cihaza Erişim	Anahtar taşıma cihazları güvenli alanlarda muhafaza edilmelidir. Anahtar taşıma cihazlarına ve depolama medyasına sadece yetkilendirilmiş personelin ulaşabilmesi sağlanmalıdır. Tüm erişim kayıtları tutularak takibinin yapılması sağlanmalıdır.
4.4.2.9	1	Anahtar Üretim Ortamlarına Güvenli Erişim	Anahtar üretim ortamlarına erişim HTTPS, SSH gibi şifreleme desteği sunan protokoller kullanılarak yapılmalıdır.
4.4.2.10	1	İz Kayıtlarının Oluşturulması	Yasal yükümlülükleri yerine getirmek, şüpheli davranışları tespit etmek ve güvenlik ihlali durumunda adli soruşturma yetenekleri sağlamak için anahtarlar üzerinde gerçekleştirilen yetkilendirme, yetki değişikliği, iptal etme, silme, yedekleme vb. tüm işlemler kayıt altına alınmalıdır. Bk. Tedbir No: 3.1.8.1
4.4.2.11	1	Kriptografik Anahtarların İptal Edilmesi/Güvenli Yok Edilmesi	Kriptografik anahtarlar, kabul edilebilir sınırlı bir geçerlilik süresine ve/veya kullanım sayısına sahip olmalıdır. Yaşam süresi devam ederken kaybedilen ve/veya saldırgan tarafından kısmen ya da tamamen ele geçirilen bir kriptografik anahtarın iptal işlemi gerçekleştirilmelidir. Yetkisini yitirmiş kriptografik anahtar ve/veya akıllı kart, token vb. kriptografik anahtar ihtiva eden donanımlar geri dönülemez biçimde yok edilmelidir.
4.4.2.12	1	Kriptografik Anahtar Sorumlusu Zimmet Tutanağının Hazırlanması	Anahtar dağıtım ve teslim şeklinin imkân vermesi durumunda kriptografik anahtarların sadece gerekli ve geçerli iş amaçları için kullanılacağını, kriptografik anahtarlar ile yapılmış olan tüm işlemlerin sorumluluğunun kişiye ait olduğunu vurgulayan bir zimmet tutanağının hazırlanmalı, kriptografik anahtarların zimmetlendiği personele imzalatılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.13	1	Kriptografik Anahtar Yetkilendirme	Üretilen anahtarların kullanım kabiliyetleri (şifreleme, şifre çözme, imzalama, doğrulama vb.) dokümante edilmeli ve yetkilendirme bu doğrultuda yapılmalıdır.
4.4.2.14	1	Anahtarların Üretim Yerinden Sonra Kopyalanamaması ve Çoğaltılamaması	Anahtarların üretim yerinden sonra kontrolsüz şekilde kopyalanması ve çoğaltılması engellenmelidir. Anahtar kaç kopya üretildi ise o sayıda dağıtım ve kullanım sağlanmalıdır.
4.4.2.15	1	Anahtarlara Açık Metin Olarak Erişilmemesi	Anahtar malzemesi elektronik ortamda tutulduğu veri tabanında veya yayımlandığı taşıma ortamlarında açık olarak görülememelidir. (Anahtarı kullanan cihazlara aktarımın kâğıt üzerinde olması durumu kapsam dışıdır.) Açık anahtar görülmesi ihlal kapsamında değerlendirilmelidir ve anahtar kullanımdan çıkarılmalıdır.
4.4.2.16	1	İhlal Raporlama	Anahtarların ifşa olması ve anahtar kullanım süreçlerindeki ihlal durumlarını raporlama (compromise reporting) mekanizması kurulmalıdır.
4.4.2.17	1	Yedek Anahtar	Anahtar üretim ve dağıtımın hızlı olamadığı uygulamalarda, ihlal/ifşa durumlarında kullanılmak üzere yedek anahtarlar hazırlanmalıdır.
4.4.2.18	1	Anahtar Üretim ve Yönetim Sistemi Testi	Kullanılacak anahtar üretim ve yönetim sistemleri ile kripto cihazların yerli ve milli üreticilerden temini tercih edilmelidir. Kullanılacak anahtar üretim ve yönetim sisteminin uygun güvenlik hedefi veya koruma profili olan Ortak Kriterlere ve/veya TS ISO/IEC 19790 – 24759 standardına uygunluğu yetkili laboratuvarlarca test edilmelidir. Bu testler sonucunda, kurum varlıklarının kritiklik derecesine uygun kripto modüller kullanılmalıdır.
4.4.2.19	2	Güvenli Anahtar Saklama	Kriptografik anahtar şifreleme anahtarları ile veri şifreleme anahtarları birbirlerinden izole edilmiş ortamlarda saklanmalıdır. Her iki özellikteki anahtar da dışarıdan yapılabilecek müdahaleye karşı korunmuş modüllerde (TRSM) saklanmalıdır. Bu mümkün değilse bilgiyi parçalı olarak korumak gereklidir. Parçalı koruma işleminde parçalar ayrı yerlerde tutulmalı, bilgi kullanılacağı zaman bir araya gelmesi sağlanmalıdır. Üretilen anahtarlar özellikle güvenli saklama için tasarlanmış USB token, akıllı kart vb. teknolojilerde saklanmalıdır. Eğer yazılımsal token vb. bir teknoloji kullanılacak ise ilave olarak hard tokenda fiziksel olarak sağlanan sahip olma özelliğinin, kişinin bilgisayar, tablet vb. da sağlanması gerekmektedir. Soft token siber saldırılara karşı dayanıklı olmalı ve gizli anahtarı sızdırmamalıdır.
4.4.2.20	3	Anahtar Taşıma Cihazlarında Yapılan Tüm Anahtar İşlemlerinin Kaydının Tutulması	Anahtar taşıma cihazlarında yalnızca anahtar alma ve yayımlama yetkisi olan personel işlem yapabilmelidir. Yapılan tüm işlemler anahtar bilgisi ve işlemi gerçekleştiren kullanıcı ile birlikte kayıt altına alınmalıdır. Kayıtlar uygun şekilde korunmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.2.21	3	Anahtar Taşıma Cihazlarında Bulunan Anahtarın Onaylı Kriptografik Yöntemlerle Şifreli Olarak Tutulması	Anahtar taşıma cihazlarında bulunan anahtarlar bellek gölgesinde öznitelikleri listelenerek ulaşılacak şekilde, onaylı kriptografik yöntemlerle şifreli olarak tutulmalıdır ve sadece yüklenirken açılmalıdır.
4.4.2.22	3	Anahtar Alma ve Depolama İşlemlerinde Bütünlük Hatası Oluşması Durumunda Anahtar Malzemesinin İmha Edilmesi	Anahtar alma işleminde bütünlük hatası tespit edilirse veya depolanan anahtarda bütünlük hatası oluşması durumunda anahtar malzemesi hemen imha edilmeli ve işlem kayıt altına alınmalıdır.
4.4.2.23	3	Kripto Güvenlik Belgesi Kontrolü	Kriptografik anahtarlara erişim sadece yetki sahibi kleranslı (kripto güvenlik belgesi) personel ile sınırlanlandırılmalıdır.
4.4.2.24	3	Anahtar Kimliği	Anahtarlar mümkünse tekil olarak adreslenebilir olmalıdır. Örneğin, anahtarların üzerinde veya yanlarında kimlik bilgisi bulunmalıdır. Anahtarın kimliği kullanılarak, alınan kayıtlar üzerinden anahtarın geçmişine ulaşılabilmelidir.
4.4.2.25	3	Anahtar Sayımı	Planlı veya plansız olarak anahtar sayımı yapılmalıdır.
4.4.2.26	3	Anahtar Üretim ve Yönetim Sistemi Testi	Anahtar üretim ve yönetim sistemleri için kullanılacak kripto cihazlar milli üreticilerden temin edilmelidir. Kripto cihazların kullanımı öncesinde, yetkili kripto analiz laboratuvarı tarafından COMSEC güvenlik testleri yapılmalı ve test sonuçlarının onaylanması durumunda kullanıma alınmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.2.1	Kriptografik Anahtara İlişkin Güvenlik Gereksinimleri Analizi	Mülakat, Gözden Geçirme	Kriptografik anahtarlar; kullanım amacına uygun güvenlik gereksinimlerini karşılayacak şekilde, ulusal ve uluslararası düzeyde kabul görmüş anahtar uzunlukları kullanılarak mı üretilmektedir?
4.4.2.2	Kriptografik Anahtarların Üretilmesi	Mülakat, Gözden Geçirme	Anahtar üretim aşamasında, anahtarın tahmin edilebilir olmasını engellemek için hangi kontroller uygulanmaktadır? Anahtar üretilirken kullanılan TRNG ve/veya PRNG ulusal ve/veya uluslararası standartları sağlamakta olan, testleri (COMSEC veya ISO) ulusal bir laboratuvarda yapılmış bir cihaz mıdır?
4.4.2.3	Anahtar Üretim ve Dağıtım Cihazlarına Erişim	Mülakat, Gözden Geçirme	Anahtar üretim ve dağıtım cihazları fiziksel tedbirler alınmış yalnızca yetkili kişilerin girebildiği korumalı alanda tutulmakta mıdır?
4.4.2.4	Güvenli Yedekleme	Mülakat, Gözden Geçirme	Sayısal sertifika ve anahtarın yedeğinin alındığı ortamlar nasıl korunmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.2.5	Kriptografik Anahtarlara Erişim Kontrolü	Mülakat, Gözden Geçirme	Kriptografik anahtarlara erişim yetkileri nasıl verilmektedir?
4.4.2.6	Kriptografik Anahtarların Revize Edilmesi	Mülakat, Gözden Geçirme	Anahtarlara erişim yetkisi olan personelin kurumdan ayrılması veya görev değiştirmesi durumunda nasıl bir yol izlenmektedir?
4.4.2.7	Güvenli Anahtar Ulaştırma / İletimi	Mülakat, Güvenlik Denetimi	Gizli kriptografik anahtar bir ağ ortamından iletilecek ise bu iletim aşamasının güvenli gerçekleştirildiğine yönelik ne gibi önlemler alınmaktadır? Kriptografik anahtarın fiziksel olarak ulaştırılması esnasında alınan fiziksel güvenlik önlemler nelerdir?
4.4.2.8	Anahtar Taşıma Cihazlarının Muhafazası ve Cihaza Erişim	Mülakat, Güvenlik Denetimi	Anahtar taşıma cihazlarına ve depolama medyasına erişim kontrolü nasıl sağlanmaktadır? Erişim kayıtları tutulmakta mıdır ve bu kayıtların denetimi düzenli aralıklar ile yapılmakta mıdır?
4.4.2.9	Anahtar Üretim Ortamlarına Güvenli Erişim	Mülakat, Güvenlik Denetimi	Üretim ortamlarına erişimde hangi yöntemler kullanılmaktadır?
4.4.2.10	İz Kayıtlarının Oluşturulması	Mülakat, Gözden Geçirme	Kriptografik anahtarlar üzerinde gerçekleştirilen hangi işlemler kayıt altına alınmaktadır?
4.4.2.11	Kriptografik Anahtarların İptal Edilmesi/Güvenli Yok Edilmesi	Mülakat, Gözden Geçirme	Kriptografik anahtarlar için tanımlanmış bir imha periyodu var mıdır? Kriptografik anahtarların gizliliğinin ihlal edildiği durumlarda nasıl bir yöntem uygulanmaktadır?
4.4.2.12	Kriptografik Anahtar Sorumlusu Zimmet Tutanağının Hazırlanması	Mülakat, Gözden Geçirme	Kriptografik anahtarların zimmetlendiği personele sorumluluklarını tanımlayan bir tutanak ya da taahhütname imzalatılmakta mıdır?
4.4.2.13	Kriptografik Anahtar Yetkilendirme	Mülakat, Gözden Geçirme	Üretilen anahtarların kullanım kabiliyetleri dokümante edilmekte midir?
4.4.2.14	Anahtarların Üretim Yerinden Sonra Kopyalanamaması ve Çoğaltılamaması	Mülakat, Gözden Geçirme, Sızma Testi	Anahtarlar üretildikten sonra kopyalama ve çoğaltılmaya karşı önlem olarak hangi kontroller uygulanmaktadır? Dağıtım nasıl gerçekleştirilmektedir? Anahtar dağıtım kontrol süreçleri belirlenmiş midir?
4.4.2.15	Anahtarlara Açık Metin Olarak Erişilmemesi	Mülakat, Gözden Geçirme	Elektronik dağıtımı yapılan kripto malzemesinin çıktı alınıp görülebilmesi engellenmiş midir? Yetki ihlali teknik imkânlar la engellenmiş midir? Kaydedilmeyen, yakalanamayan ihlal olasılığı var mıdır?
4.4.2.16	İhlal Raporlama	Mülakat, Gözden Geçirme	Anahtarların ifşa olması ve anahtar süreçlerindeki ihlal durumlarını raporlamak için bir mekanizma bulunmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.2.17	Yedek Anahtar	Mülakat, Gözden Geçirme	Anahtar üretim ve dağıtımın hızlı olamadığı uygulamalarda, ihlal/ifşa durumlarında kullanmak üzere yedek anahtarlar bulunmakta mıdır?
4.4.2.18	Anahtar Üretim ve Yönetim Sistemi Testi	Mülakat, Gözden Geçirme	Anahtar üretim ve yönetim sistemi Ortak Kriterler ve/veya TS ISO/IEC 19790-24759 standardı ile uyumlu mudur?
4.4.2.19	Güvenli Anahtar Saklama	Mülakat, Gözden Geçirme	Kriptografik anahtar şifreleme anahtarları ile veri şifreleme anahtarları saklanırken nasıl bir yöntem izlenmektedir?
4.4.2.20	Anahtar Taşıma Cihazlarında Yapılan Tüm Anahtar İşlemlerinin Kaydının Tutulması	Mülakat, Gözden Geçirme	Anahtar taşıma cihazlarında yetkili kullanıcının yaptığı tüm işlemler kayıt altına alınmakta mıdır? Kayıtlar uygun güvenlik seviyesiyle korunmakta mıdır?
4.4.2.21	Anahtar Taşıma Cihazlarında Bulunan Anahtarın Onaylı Kriptografik Yöntemlerle Şifreli Olarak Tutulması	Mülakat, Gözden Geçirme	Anahtar taşıma cihazlarında bulunan anahtarlar onaylı kriptografik yöntemlerle şifreli olarak tutulmakta mıdır?
4.4.2.22	Anahtar Alma ve Depolama İşlemlerinde Bütünlük Hatası Oluşması Durumunda Anahtar Malzemesinin İmha Edilmesi	Mülakat, Gözden Geçirme	Anahtar alma işleminde bütünlük hatası tespit edilirse veya depolanan anahtarda bütünlük hatası oluşması durumunda nasıl bir yol izlenmektedir?
4.4.2.23	Kripto Güvenlik Belgesi Kontrolü	Mülakat, Gözden Geçirme	Kriptografik anahtarlara erişim yetkisi verilecek personel için kripto güvenlik belgesi kontrolü yapılmakta mıdır?
4.4.2.24	Anahtar Kimliği	Mülakat, Gözden Geçirme	Anahtarlar tekil olarak adreslenmekte ve yaşam çevrim aşamaları takip edilmekte midir?
4.4.2.25	Anahtar Sayımı	Mülakat, Gözden Geçirme	Planlı veya plansız anahtar sayımı yapılmakta mıdır?
4.4.2.26	Anahtar Üretim ve Yönetim Sistemi Testi	Mülakat, Gözden Geçirme	Anahtar üretim ve yönetim sistemi milli üreticilerden temin edilmekte midir? Yetkili kripto analiz laboratuvarı tarafından hazırlanmış, anahtar üretim ve yönetim sisteminin güvenli bir şekilde kullanılabileceğine dair kripto analiz raporu bulunmakta mıdır? Anahtar üretim ve yönetim sistemi, yetkili COMSEC laboratuvarı tarafından uygulanan güvenlik testlerinden başarılı şekilde geçmiş midir?

4.4.3. Kriptografik Uygulamalar

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.4.3.1	1	Güvensiz Ağlar Üzerinden Güvenli Haberleşme	Güvenli ağların, güvensiz bir ağ üzerinden haberleşmesinin gerekmesi durumunda VPN teknolojileri kullanılmalıdır.
4.4.3.2	1	Envanter Yönetimi	Kurumda aktif olarak kullanılan ve aktif olarak kullanılmayan tüm kriptografik ürünlerin güncel bir listesi tutulmalıdır. Liste içeriğinde kullanılan ürünlerin hangi işlemler için hangi amaçla kullanıldıkları tanımlanmalı, envantere yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.
4.4.3.3	1	Güvenlik Değerlendirme ve Onay Durumu Yönetimi	Kullanılan kriptografik ürünlerin işlediği verinin gizlilik derecesine uygun olarak kullanılmasını sağlamak amacıyla ilgili güvenlik değerlendirmesi ve gizlilik derecesi ile uyumlu olarak onay sürecinin işletilip işletilmediği kontrol edilmelidir.
4.4.3.4	2	Kripto Protokollerinin En Güncel ve Güvenilir Versiyonlarının Kullanımı	Kriptografik algoritmaların ve protokollerin en güncel ve güvenli olan versiyonlarının kullanımı sağlanmalıdır. Anahtar uzunlukları, bilgi güvenliği gereksinimleri doğrultusunda endüstri standartları ve en iyi uygulama örnekleri dikkate alınarak belirlenmelidir. Sistemde kullanılan taşıma katmanı protokollerine ait sürümler belirli aralıklarla değerlendirilmeli ve denetlenmelidir.
4.4.3.5	2	Envanter Yönetim Araçları ile Kriptografik Ürünlerin Yönetimi ve İzlenmesi	Kullanılan kriptografik ürünlerin kullanım durumları, versiyon kontrolü, güvenlik değerlendirmesi ve onay durumu gibi bilgilerin takibi ve raporlaması envanter yönetim sistemi ile yapılmalıdır. Envanter yönetim sistemine yalnızca yetkilendirilmiş personelin erişimi mümkün kılınmalıdır.
4.4.3.6	3	Kripto Cihazları TEMPEST Laboratuvar Onayı	Kritik bilgi/veri işleyen kurumlarda, bu bilgilerin işlenmesinde kullanılan kriptografik sistemler için kullanılan kripto cihazlarının TEMPEST testlerinin yapılmalıdır.
4.4.3.7	3	Kripto Cihazları Kripto Analiz Laboratuvar Onayı	Kritik bilgi/veri işleyen kurumlarda, bu bilgilerin işlenmesinde kullanılan kriptografik ürünlerin yetkili kripto analiz laboratuvarı tarafından kriptografik mimari ve algoritma analizi yapılmalıdır.
4.4.3.8	3	Kripto Cihazları COMSEC Laboratuvar Onayı	Kritik bilgi/veri işleyen kurumlarda, bu bilgilerin işlenmesinde kullanılan kriptografik ürünlere ait (milli veya standart algoritma içeren) kriptografik algoritmaların kullanacakları anahtarları üretecek, taşıyacak ve kullanacak sistem ve cihazlar, yetkili COMSEC laboratuvarında gerekli testlerden geçmeli ve güvenlik onayı almalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.4.3.1	Güvensiz Ağlar Üzerinden Güvenli Haberleşme	Mülakat, Güvenlik Denetimi	Güvenli ağların, güvensiz bir ağ üzerinden haberleşmesinin gerekmesi durumunda nasıl bir yöntem izlenmektedir?
4.4.3.2	Envanter Yönetimi	Mülakat, Gözden Geçirme	Kurumda kullanılan kriptografik ürünlerin envanteri tutulmakta mıdır? Envanter kapsamında hangi bilgiler yer almaktadır? Envanter nerede tutulmaktadır? Envantere erişim yetkileri düzenli aralıklar ile gözden geçirilmekte midir?
4.4.3.3	Güvenlik Değerlendirme ve Onay Durumu Yönetimi	Mülakat, Güvenlik Denetimi	Kurum tarafından hangi kriptografik ürünler kullanılmaktadır? Kullanılan kriptografik ürünler hangi gizlilik seviyelerinde veri işlemektedir? Kullanılan kriptografik ürünlere yönelik yapılan güvenlik değerlendirmeleri nelerdir? Kriptografik ürünlere yönelik hangi sertifikalar bulunmaktadır? Kriptografik ürünlerin işledikleri verilerin gizlilik seviyesine uygun olarak gerekli güvenlik değerlendirmeleri yapılmış ve ilgili onaylar alınmış mıdır?
4.4.3.4	Kripto Protokollerinin En Güncel ve Güvenilir Versiyonlarının Kullanımı	Mülakat, Güvenlik Denetimi	Güncel ve güvenilir kriptolama algoritmalarının kullanıldığı nasıl kontrol edilmektedir? Kriptografik protokollerin güvenli sürümleri desteklenmekte midir? Kriptografik protokollerin eski sürümleri ile yapılan iletişim istekleri reddedilmekte midir?
4.4.3.5	Envanter Yönetim Araçları ile Kriptografik Ürünlerin Yönetimi ve İzlenmesi	Mülakat, Gözden Geçirme	Envanter yönetimi amacıyla hangi araç kullanılmaktadır? Envantere hangi personel erişim sağlamaktadır?
4.4.3.6	Kripto Cihazları TEMPEST Laboratuvar Onayı	Mülakat, Güvenlik Denetimi	Kriptografik sistemler için kullanılan kripto cihazlarının TEMPEST testleri yapılmakta mıdır?
4.4.3.7	Kripto Cihazları Kripto Analiz Laboratuvar Onayı	Mülakat, Güvenlik Denetimi	Kriptografik sistemler için kriptografik mimari ve algoritma analizi yapılmış mıdır?
4.3.8	Kripto Cihazları COMSEC Laboratuvar Onayı	Mülakat, Güvenlik Denetimi	Kriptografik algoritmaların kullanacakları anahtarları üretecek, taşıyacak ve kullanacak sistemin kullanımı öncesinde; sistem, yetkili bir COMSEC laboratuvarında gerekli testlerden geçirilip güvenlik onayı alınmış mıdır?

4.5. Kritik Altyapılar Güvenliği

Amaç

Bu güvenlik tedbiri ana başlığının amacı, kritik altyapılar güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Kritik Altyapılar Güvenliği” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri
- Enerji Sektörü Özelinde Güvenlik Tedbirleri
- Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri

Kritik altyapılar güvenliği kapsamında uygulanacak enerji ve elektronik haberleşme sektörü özelindeki güvenlik tedbirlerinin yanı sıra varlık gruplarına yönelik güvenlik tedbirlerinin yer aldığı alt başlıklar da dikkate alınmalıdır.

4.5.1. Genel Güvenlik Tedbirleri

Tedbirler

Aşağıda listelenen rehber ana başlıklarında yer alan tedbirler uygulanır:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

Denetim Maddeleri

Aşağıda listelenen rehber ana başlıklarında yer alan denetim soru önerileri uygulanır:

- Ağ ve Sistem Güvenliği
- Uygulama ve Veri Güvenliği
- Taşınabilir Cihaz ve Ortam Güvenliği
- Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği
- Personel Güvenliği
- Fiziksel Mekânların Güvenliği

4.5.2. Enerji Sektörü Özelinde Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.2.1	1	Cihaz Konfigürasyonları	EKS içerisinde yer alan hiçbir cihaz varsayılan ayarlarıyla sistem içerisinde konumlandırılmamalıdır. Cihaz konfigürasyonları bilgi güvenliği gereksinimlerine uygun olarak yapılmalıdır.
4.5.2.2	1	Ağ Erişim Kontrolü	EKS ağı ve kurumsal BT ağı arasındaki iletişimler için erişim kontrolü sağlanmalı ve yetkisiz erişimler engellenmelidir.
4.5.2.3	1	Ağ Segmentasyonu	Operasyonel faaliyetlerin kritikliği değerlendirilmeli ve EKS ağı belirlenen kritiklik derecesine göre segmentlere ayrılmalıdır. Oluşturulan ağlar birbirlerinden izole edilmeli ve erişim güvenliğine yönelik kısıtlayıcı önlemler alınmalıdır.
4.5.2.4	1	Kimlik Doğrulama	EKS kullanıcıları ve kurum ağı kullanıcıları için ayrı kimlik doğrulama sistemi kullanılmalıdır.
4.5.2.5	1	Erişim Yönetimi	EKS ağı internete kapalı konumda tutulmalıdır. Söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise internet ve uzaktan erişim faaliyetlerine güvenlik güncellemeleri ve sıkılaştırma politikaları uygulanarak asgari seviyede izin verilmelidir.
4.5.2.6	1	Fiziksel Erişim Güvenliği	EKS ortamındaki herhangi bir bilgi varlığına, yetkisiz kişiler tarafından yapılacak aktif (hırsızlık, modifikasyon, manipülasyon) veya pasif (görsel gözlem, not alma, fotoğraf çekme) fiziksel erişimi sınırlamak amacıyla sistemlerin bulunduğu ortamlara erişimde; • Çok faktörlü kimlik doğrulama, • Kamera ve/veya hareket dedektörleri kullanımı • Ziyaretçi kabul kuralları için süreç tanımlanması ve uygulanması • Cihaz manipülasyonu için alarm mekanizmaları gibi güvenlik önlemleri alınmalıdır.
4.5.2.7	1	Sistem Sürekliliğinin Sağlanması	EKS sistem sürekliliğini sağlamak amacıyla sistem mimarisi dağıtık ve/veya yedekli bir yapıda oluşturulmalıdır.
4.5.2.8	1	Veri Manipülasyonunun Engellenmesi	EKS ağı pasif olarak (mirror trafik kullanılarak) izlenerek veri manipülasyonunu engellemeye yönelik önlemler alınmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.2.9	1	Kullanıcı Erişim Yönetimi	IED ve RTU cihazlarında hizmet veren web sunucusu olması durumunda, internet üzerinden sunucuya erişim kapatılmalı ve iç ağda kimlik doğrulama mekanizmaları doğrultusunda erişim sağlanmalıdır. Sunucuya internet üzerinden erişime ihtiyaç olduğu durumlarda VPN üzerinden erişim sağlanmalıdır. MMS protokolünde kimlik doğrulama özelliği aktif bir şekilde kullanılmalıdır.
4.5.2.10	1	SSL/TLS Korumalı İletişim	EKS ağındaki MMS protokolü ile sağlanan dikey iletişim, SSL/TLS üzerinden şifreli bir şekilde sağlanmalı, IED'lerde ve HMI/SCADA cihazlarında desteklenmesi durumunda SSL/TLS özelliği aktif hale getirilmelidir.
4.5.2.11	1	GPS İletişim ve Senkronizasyonunun Güvenliği	Enerji alt yapılarında kullanılan GPS teknolojileri spoofing saldırılarına karşı korunmalıdır.
4.5.2.12	1	Ekipman Güvenliğinin Sağlanması	Kullanılan ekipman, çevresel tehditlerden kaynaklanacak olumsuz etkilere karşı gerekli önlemler alınarak korunmalıdır.
4.5.2.13	1	Tehdit İstihbaratı Yönetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmaları yapılmalı ve tehdit istihbaratı verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmalıdır.
4.5.2.14	1	Otoritelerle İletişim	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmalıdır.
4.5.2.15	2	Veri İletimi	Ağ üzerindeki verilerin iletimi için güvenli aktarım yöntemleri (hava boşluğu, veri diyodu vb.) kullanılmalıdır. Bk. Tedbir No: 3.1.6.36

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.2.1	Cihaz Konfigürasyonları	Mülakat, Güvenlik Denetimi	EKS içerisinde yer alan tüm cihazların konfigürasyonları bilgi güvenliği gereksinimleri göz önünde bulundurularak yapılandırılmakta mıdır?
4.5.2.2	Ağ Erişim Kontrolü	Mülakat, Güvenlik Denetimi	KBS ağı ve EKS ağı doğrudan iletişim kurmakta mıdır? EKS ağı güvenliğini sağlamak amacıyla hangi kontroller uygulanmaktadır?
4.5.2.3	Ağ Segmentasyonu	Mülakat, Güvenlik Denetimi	Operasyonel faaliyetler göz önünde bulundurularak EKS ağı segmentlere ayrılmış mıdır? Segmentler arası erişim güvenliği nasıl sağlanmaktadır?
4.5.2.4	Kimlik Doğrulama	Mülakat, Güvenlik Denetimi	EKS kullanıcıları kapsamında kimlik doğrulama nasıl yapılmaktadır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.2.5	Erişim Yönetimi	Mülakat, Güvenlik Denetimi	EKS ağı internete kapalı mıdır? EKS ağına uzaktan erişim için hangi kontroller uygulanmaktadır?
4.5.2.6	Fiziksel Erişim Güvenliği	Mülakat, Güvenlik Denetimi	EKS ortamındaki herhangi bir bilgi varlığına, yetkisiz kişiler tarafından yapılacak aktif veya pasif fiziksel erişimi sınırlamak amacıyla hangi güvenlik kontrolleri uygulanmaktadır?
4.5.2.7	Sistem Sürekliliğinin Sağlanması	Mülakat, Güvenlik Denetimi	EKS merkezi ile hizmet verilen bölge arasında dağıtık ve/veya yedekli bir sistem mimarisi oluşturulmuş mudur?
4.5.2.8	Veri Manipülasyonunun Engellenmesi	Mülakat, Güvenlik Denetimi	EKS ağı düzenli olarak izlenmekte midir? Veri manipülasyonunu engellemek için hangi kontroller uygulanmaktadır?
4.5.2.9	Kullanıcı Erişim Yönetimi	Mülakat, Güvenlik Denetimi	Kimlik doğrulama mekanizmaları kullanılmakta mıdır? MMS protokolünde kimlik doğrulama mekanizmaları aktif midir?
4.5.2.10	SSL/TLS Korumalı İletişim	Mülakat, Güvenlik Denetimi	Trafo merkezleri içerisindeki MMS protokolü ile sağlanan dikey iletişim, SSL/TLS üzerinden şifreli bir şekilde sağlanmakta mıdır?
4.5.2.11	GPS İletişim ve Senkronizasyonunun Güvenliği	Mülakat, Güvenlik Denetimi	Enerji alt yapılarında kullanılan GPS teknolojileri spoofing saldırılarına karşı nasıl koruma altına alınmaktadır?
4.5.2.12	Ekipman Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Enerji sektörü özelinde kullanılan ekipmanı çevresel tehditler sebebi ile kaynaklanacak olumsuz etkilere karşı korumak amacıyla hangi önlemler alınmaktadır?
4.5.2.13	Tehdit İstihbaratı Yönetimi	Mülakat, Güvenlik Denetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için ne tür çalışmalar yapılmaktadır? Tehdit istihbarat verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmış mıdır?
4.5.2.14	Otoritelerle İletişim	Mülakat, Güvenlik Denetimi	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmış mıdır?
4.5.2.15	Veri İletimi	Mülakat, Güvenlik Denetimi	Ağ üzerindeki verilerin iletimi için hangi güvenli aktarım yöntemleri kullanılmaktadır?

4.5.3. Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.3.1	1	Hizmet Güvenliği ve Sürekliliği	Sağlanan iletişim hizmetlerinin güvenliğini ve sürekliliğini ele alan bir güvenlik politikası belirlenmeli ve uygulanmalıdır. Güvenlik politikası; geçmişte yaşanan güvenlik olayları ve ihlalleri, hizmet kesintileri ve sektördeki diğer sağlayıcıları etkileyen olaylar dikkate alınarak periyodik olarak güncellenmelidir. Özellikle kilit personelin belirlenen güvenlik politikasına yönelik farkındalığı arttırılmalıdır.
4.5.3.2	1	Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri	Üçüncü taraflardan temin edilen/hizmet alınan BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, yardım masalarına, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimleri sözleşmelerde detaylı olarak ele alınmalıdır. Bk. Tedbir No: 3.5.3.3
4.5.3.3	1	Altyapı Servislerinin Güvenliği	Haberleşme hizmetlerindeki altyapı servislerinin kötüye kullanımından kaynaklanacak ve müşterileri/diğer hizmet sağlayıcıları olumsuz olarak etkileyebilecek tehditler için gerekli önlemler alınmalıdır.
4.5.3.4	1	Sahtecilik İşlemlerini Tespit ve Önleme	Sinyalleşme trafiğindeki olası sahtecilik işlemlerini tanımlamak, tespit etmek ve önlemek için bir sistem kurulmalı ve işletilmelidir.
4.5.3.5	1	Sinyalleşme Trafiğinin Güvenliği	Sinyalleşme sistem ve protokollerindeki zafiyetler kullanılarak yapılabilecek saldırıların tespiti/önlenmesi amacıyla sinyalleşme trafiği izlenmeli, gizlilik ve bütünlüğünü tesis edecek önlemler alınmalıdır.
4.5.3.6	1	Güvenilir İletişimin Tesisi	Sağlanan iletişim hizmetlerinde müşterilerin kaynak IP adreslerinin doğrulanmasına olanak tanıyan sistemler kullanılmalı, hatalı, değiştirilmiş (spoofed) IP adreslerinin şebekede dolaşımını engellemek için gerekli önlemler alınmalıdır.
4.5.3.7	1	Sıkılaştırma Faaliyetleri	Sunucular, yönlendiriciler ve diğer şebeke elemanlarının saldırı yüzeyini azaltmak için gerekli sıkılaştırma kontrolleri uygulanmalıdır. Bk. Bölüm 5
4.5.3.8	1	Ekipman Arızalarının İzlenmesi	Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizması kurulmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.5.3.9	1	Ekipman Güvenliğinin Sağlanması	Haberleşme sistemlerinde kullanılan ekipmanı, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korumak amacıyla gerekli önlemler alınmalıdır.
4.5.3.10	1	Tehdit İstihbaratı Yönetimi	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için gerekli tehdit istihbaratı çalışmaları yapılmalı ve tehdit istihbaratı verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmalıdır.
4.5.3.11	1	Otoritelerle İletişim	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmalıdır.
4.5.3.12	1	Arayan Hat Bilgisi Kullanımı	Haberleşme hizmetinde, arayan numara manipülasyonunu (Caller ID Manipulation) engellemeye yönelik teknik ve hukuki tedbirler alınmalıdır.
4.5.3.13	1	İnternet Değişim Noktası	Yurt içi iletişim trafiğinin ülke sınırları içerisinde kalması sağlanmalı, bu trafiğin ve abone kayıtlarının yurt dışına çıkarılarak tekrar yurt içine yönlendirilmesi engellenmelidir.
4.5.3.14	3	Kritik Haberleşme Güvenliği	Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, bu kurumların merkez birimlerine ve talep edeceği diğer birimlerine doğrudan hizmet sağlayan haberleşme ve transmisyon altyapısında ilk toplama noktasına kadar radyolink vb. kablosuz teknolojiler kullanılmamalı, kullanımın zorunlu olması durumunda ihtiyaç duyulan gizlilik seviyesine uygun donanımsal veya yazılımsal milli kripto sistemleriyle birlikte kullanılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.3.1	Hizmet Güvenliği ve Sürekliliği	Mülakat, Gözden Geçirme	Sağlanan iletişim hizmetlerinin güvenliğini ve sürekliliğini ele alan bir güvenlik politikası belirlenmiş midir? Güvenlik politikası kapsamında hangi konular ele alınmaktadır? Güvenlik politikası hangi periyotlarda gözden geçirilmektedir?
4.5.3.2	Üçüncü Taraflara İlişkin Güvenlik Gereksinimleri	Mülakat, Gözden Geçirme	Üçüncü taraflardan temin edilen/hizmet alınan BT ürünlerine, BT hizmetlerine, dış kaynaklı iş süreçlerine, yardım masalarına, çağrı merkezlerine, ara bağlantılara, ortak tesislere vb. yönelik güvenlik gereksinimleri ilgili sözleşmelerde nasıl adreslenmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.5.3.3	Altyapı Servislerinin Güvenliği	Mülakat, Güvenlik Denetimi	Haberleşme hizmetlerindeki altyapı servislerinin kötüye kullanımından kaynaklanacak ve müşterileri / diğer hizmet sağlayıcıları olumsuz olarak etkileyebilecek tehditleri önlemek amacıyla hangi güvenlik kontrolleri uygulanmaktadır?
4.5.3.4	Sahtecilik İşlemlerini Tespit ve Önleme	Mülakat, Güvenlik Denetimi	Sinyalleşme trafiğindeki olası sahtecilik işlemlerini tanımlamak, tespit etmek ve önlemek için bir sistem kurulmuş mudur? İlgili sistem nasıl işletilmektedir?
4.5.3.5	Sinyalleşme Trafiğinin Güvenliği	Mülakat, Güvenlik Denetimi	Sinyalleşme sistem ve protokollerindeki zafiyetlere yönelik hangi önlemler alınmaktadır?
4.5.3.6	Güvenilir İletişimin Tesisi	Mülakat, Güvenlik Denetimi	Sağlanan iletişim hizmetlerinde, müşterilerin kendisine tahsis edilmemiş kaynak adresi üzerinden iletişim sağlamamasına yönelik hangi önlemler alınmaktadır?
4.5.3.7	Sıkılaştırma Faaliyetleri	Mülakat, Güvenlik Denetimi	Sunucular, yönlendiriciler ve diğer şebeke elemanlarının saldırı yüzeyini azaltmak amacıyla hangi sıkılaştırma kontrolleri uygulanmaktadır?
4.5.3.8	Ekipman Arızalarının İzlenmesi	Mülakat, Gözden Geçirme	Güvenlik ve iş sürekliliği gereksinimlerini sağlamak amacıyla altyapıda yer alan ekipmanlara ait arıza sinyallerinin izlenmesi için alarm mekanizması mevcut mudur?
4.5.3.9	Ekipman Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Haberleşme sistemlerinde kullanılan ekipmanı, çevresel tehditler ile enerji destek sistemlerinden kaynaklanacak olumsuz etkilere karşı korumak amacıyla hangi önlemler alınmaktadır?
4.5.3.10	Tehdit İstihbaratı Yönetimi	Mülakat, Gözden Geçirme	Siber güvenlik tehdit istihbaratı ile ilgili güncel ve güvenilir bilgiyi almak için ne tür çalışmalar yapılmaktadır? Tehdit istihbarat verilerini yönetmek amacıyla bir süreç/mekanizma tanımlanmış mıdır?
4.5.3.11	Otoritelerle İletişim	Mülakat, Gözden Geçirme	Tehdit yönetim faaliyetlerini destekleyecek otoritelere ilişkin iletişim listesi tanımlanmış mıdır?
4.5.3.12	Arayan Hat Bilgisi Kullanımı	Mülakat, Güvenlik Denetimi	Arayan numara manipülasyonunu engellemeye yönelik hangi tedbirler alınmaktadır?
4.5.3.13	İnternet Değişim Noktası	Mülakat, Güvenlik Denetimi	Yurt içi iletişim trafiğinin ülke sınırları içerisinde kalmasına yönelik ne tür çalışmalar yapılmaktadır?
4.5.3.14	Kritik Haberleşme Güvenliği	Mülakat, Güvenlik Denetimi	Kritik altyapı sektörlerinde faaliyet gösteren kurumlarda haberleşmesi ve transmisyon hizmeti nasıl sağlanmaktadır?

4.6. Yeni Geliştirmeler ve Tedarik

Amaç

Bu güvenlik tedbiri ana başlığının amacı, yeni geliştirmeler ve tedarik güvenliği çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Yeni Geliştirmeler ve Tedarik” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Güvenlik Tedbirleri

4.6.1. Genel Güvenlik Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
4.6.1.1	1	Politika ve Prosedürlerin Tanımlanması	Tedarik edilen yazılımların, donanımların ve sistem bileşenlerinin temini ve kabul aşamasında gerçekleştirilmesi gereken testlere yönelik politika ve prosedürler tanımlanmış olmalıdır. Bileşenler, sorumlu personelin/birimin onayı ile kurum envanterine eklenmelidir.
4.6.1.2	1	Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi	Bk. Tedbir No: 3.1.2.4
4.6.1.3	1	Donanım Varlık Envanterine Kayıt Edilmemiş Donanımların Yönetimi	Bk. Tedbir No: 3.1.1.3
4.6.1.4	1	Arayüzün Türkçe Dil Desteğine Sahip Olması	Geliştirilen uygulama/sistem kapsamında sunulan arayüzün kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteği sağlanmalı, tedarik edilen ürünlerde ise Türkçe dil desteği olan ürünler tercih edilmelidir.
4.6.1.5	2	Alt Yüklenici Yönetimi	Yeni geliştirmeler ve ürün/hizmet tedariki kapsamında alt yüklenici ile çalışılması durumunda işletilecek politika ve prosedürler tanımlanmış olmalıdır. Alt yüklenici tarafından gerçekleştirilecek değişiklik ve sürüm yönetimi faaliyetleri kurumun politika ve prosedürleri ile uyumlu olmalıdır.
4.6.1.6	2	Fonksiyonel ve Fonksiyonel Olmayan Testlerin Yapılması	Yeni geliştirmeler ve ürün/hizmet tedariki kapsamında kurumun fonksiyonel ve fonksiyonel olmayan testlere (yük, performans, güvenlik vb.) yönelik uygulanacak süreçleri tanımlı olmalı ve uygulanmalıdır. Bu süreçler düzenli olarak gözden geçirilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
4.6.1.1	Politika ve Prosedürlerin Tanımlanması	Mülakat, Gözden Geçirme	Tedarik edilen yeni ürünlerin alımıyla ilgili işleyişi ve kuralları içeren politika ve prosedürler tanımlı mıdır? Tedarik edilen yeni ürünler kurum envanterine sorumlu personelin/birimin onayı dâhilinde mi eklenmektedir?
4.6.1.2	Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.2.4
4.6.1.3	Donanım Varlık Envanterine Kayıt Edilmemiş Donanımların Yönetimi	Mülakat, Güvenlik Denetimi	Bk. Denetim No: 3.1.1.3
4.6.1.4	Arayüzün Türkçe Dil Desteğine Sahip Olması	Mülakat	Geliştirilen uygulama/sistem kapsamında sunulan arayüz, kullanıcılar tarafından açıkça anlaşılabilir olması adına Türkçe dil desteğine imkân sağlamakta mıdır?
4.6.1.5	Alt Yüklenici Yönetimi	Mülakat	Alt yüklenici ile çalışılma durumunda kurum tarafından işletilecek politika ve prosedürler tanımlanmış mıdır? Alt yüklenici tarafından gerçekleştirilen değişiklik ve sürüm yönetimi faaliyetleri kurumun politika ve prosedürleri ile uyumlu mudur?
4.6.1.6	Fonksiyonel ve Fonksiyonel Olmayan Testlerin Yapılması	Mülakat	Kurumun fonksiyonel ve fonksiyonel olmayan testlere yönelik uygulanacak süreçleri tanımlı mıdır? İlgili süreçler işletilmekte ve periyodik olarak gözden geçirilmekte midir?

SIKILAŞTIRMA TEDBİRLERİ

5. BÖLÜM

5. SIKILAŞTIRMA TEDBİRLERİ

5.1. İşletim Sistemi Sıkılaştırma Tedbirleri

Amaç

Bu güvenlik tedbiri ana başlığının amacı, işletim sistemi güvenlik sıkılaştırmaları çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. "İşletim Sistemi Sıkılaştırma Tedbirleri" ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Sıkılaştırma Tedbirleri
- Linux İşletim Sistemi Sıkılaştırma Tedbirleri
- Windows İşletim Sistemi Sıkılaştırma Tedbirleri

5.1.1. Genel Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.1	1	Kurulum Güvenliği	Kurulum esnasında kullanılan işletim sistemi dosyalarının özet bilgisi orijinal dağıtıcı özet değerleriyle teyit edilmelidir.
5.1.1.2	1	Servis Güvenliği	Sunucuların normal işleyişi için gerekli olmayan tüm servisler kapatılmalıdır. Sistemlerde çalışan servisler ihtiyaçları olan en az yetki ile çalışmalıdır. Servis kullanıcılarının yetkileri ayrıca kısıtlanmalıdır. Servislerin döndüğü başlık bilgileri (banner) bilgi ifşasına yol açmayacak şekilde değiştirilmelidir.
5.1.1.3	1	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Güncel ve güvenlik desteği devam eden işletim sistemleri kullanılmalıdır. Uygulama sürümleri periyodik olarak kontrol edilmelidir.
5.1.1.4	1	Şifreli Haberleşen Servislerin Kullanılması	Şifresiz kimlik doğrulama ve haberleşme kullanan servisler (Telnet, FTP, rlogin, HTTP, SMTP vb.), eğer varsa şifreli haberleşme imkânı sağlayan muadilleri (SSH, SFTP, HTTPS, SMTPS vb.) ile değiştirilmelidir.
5.1.1.5	1	Parola Politikasının Belirlenmesi	Tüm makinelerde kullanıcı parolaları için güçlü bir parola politikası belirlenmelidir. Kullanıcılar ilk girişten sonra parolalarını değiştirmeye zorlanmalı ve parolaların belirli bir süreden sonra geçerliliğini yitirip yenilenmesi sağlanmalıdır. Ayrıca belirli bir sayıda hatalı giriş denemesinden sonra kullanıcı hesapları kilitlenmelidir.
5.1.1.6	1	Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması	Kullanıcı bilgisayarlarında, bilgisayara ağ üzerinden erişim yetkisi, sadece yönetici hesapları ve uzak masaüstü kullanıcıları veya grupları ile sınırlandırılmalıdır.
5.1.1.7	1	Hata ve Sorun Bilgilerinin Üretici ile Paylaşılmaması	İşletim sistemi kurulumu ile gelen hata ve sorun bilgilerinin üretici ile paylaşılması özelliği pasif hale getirilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.8	1	Kablosuz Ağ Arayüzlerinin Kapatılması	Tüm sunucularda kullanılmayan kablosuz ağ arayüzleri pasif hale getirilmelidir.
5.1.1.9	1	Sistem Üzerinde Düzenli Olarak Zafiyet ve Zararlı Yazılım Taraması Yapılması	Sistemde düzenli olarak zafiyet taraması yapılmalı ve bu zafiyetlerin yönetimi gerçekleştirilmelidir. Sistem zararlı yazılımlara karşı düzenli olarak taranmalıdır. Bk. Tedbir No: 3.1.5.1
5.1.1.10	1	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Bk. Tedbir No: 3.1.6.11
5.1.1.11	1	Sunucularda Zaman Senkronizasyonunun Sağlanması	Sunucularda ilgili NTP ayarlamaları yapılarak tüm sunucularda zaman senkronizasyonu sağlanmalıdır.
5.1.1.12	1	Güvenli Süreç (Process) İşleme Ayarlarının Yapılması	İşletim sistemlerinin DEP, ASLR, XD/NX gibi savunma özellikleri istisnai durumlar haricinde aktif olmalıdır.
5.1.1.13	2	Kullanılmayan Uygulamaların Kaldırılması	Sistemlerde kullanılmayan uygulamalar belirlenerek kaldırılmalıdır.
5.1.1.14	2	Merkezi Güncelleme Sunucusu	İşletim sistemi güncellemeleri için merkezi bir güncelleme sunucusu oluşturulmalıdır.
5.1.1.15	2	IPv6 Pasif Hale Getirilmesi	Eğer kurum içerisinde IPv6 kullanılmıyorsa, IPv6 destekleyen tüm sunucularda IPv6 desteği pasif hale getirilmelidir.
5.1.1.16	2	Sistem İz Kayıtlarının Aktif Edilmesi	Tüm sunucu ve makinelerde iz kayıtları aktif edilmelidir. Sistem zaman ve tarih ayarları, kullanıcı hesapları, ağ yapılandırması, erişim kontrolleri üzerinde yapılan değişiklikler kayıt altına alınmalıdır. Ayrıca giriş ve çıkış bilgileri, yetkisiz dosya okuma denemeleri, dosya silme işlemleri ve sistem yöneticisi hareketleri de kayıt altına alınmalıdır. Bk. Tedbir No: 3.1.8.1
5.1.1.17	2	Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması	Sistemlerden syslog vb. araçlarla toplanan sistem iz kayıtları merkezi bir kayıt yönetim sistemine gönderilmelidir. Burada toplanan iz kayıtları kurum kritiklik seviyesi ve dinamiklerine uygun olarak işlenmelidir. Bk. Tedbir No: 3.1.8.6
5.1.1.18	2	Merkezi Kimlik Yönetimi Servisinin Kullanılması	Tüm makinelerde kullanıcı kimlik doğrulama için merkezi kimlik yönetimi servisi kullanılmalıdır.
5.1.1.19	3	Sunucularda Çalışan Servislerin Takibi	Sunucuların normal işleyişi için gerekli olan servisler dışında başka bir servisin sunucuda açılması halinde alarm üretilmeli ve ilgili servis kapatılmalıdır.
5.1.1.20	3	Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması	Makine özelinde saldırı tespit ve engelleme sistemi (HIDS/HIPS) kullanılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.1.21	3	Disk Kotalarının Belirlenmesi	Tüm makinelerde kullanıcılar için her dosya sistemine özel disk kota politikaları belirlenmeli ve etkinleştirilmelidir.
5.1.1.22	3	Disk Seviyesinde Şifreleme Yapılması	Kritik bilgi içeren ve/veya işleyen makinelerde disk seviyesinde şifreleme yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.1.1	Kurulum Güvenliği	Mülakat	Kurulumda kullanılan işletim sistemlerinin bütünlüğü, kurulumdan önce özetleri alınarak teyit edilmekte midir?
5.1.1.2	Servis Güvenliği	Mülakat, Güvenlik Denetimi, Sızma Testi	Sistemlerin döndüğü başlık bilgilerinde kısıtlamalar uygulanmakta mıdır? Bu kısıtlamalar nasıl belirlenmiştir? Sunucularda kullanılan ve kullanılmayan servisler belirlenmiş midir? Kullanılmayan servisler kapatılmış mıdır? Çalışan servislerin yetkileri nasıl belirlenmektedir? Yönetici hakları ile çalıştırılan servisler var mıdır?
5.1.1.3	Güncel İşletim Sistemi ve Uygulamaların Kullanılması	Mülakat, Güvenlik Denetimi	İşletim sistemi sürümleri ne sıklıkla güncellenmektedir? Kullanılan işletim sistemi sürümlerinin güncelliği sağlanmakta mıdır? İşletim sistemi üzerinde yer alan uygulamaların güncelliği kontrol edilmekte midir?
5.1.1.4	Şifreli Haberleşen Servislerin Kullanılması	Güvenlik Denetimi, Sızma Testi	Şifresiz haberleşen servisler, şifreli işlem yapan muadilleri ile değiştirilmiş midir?
5.1.1.5	Parola Politikasının Belirlenmesi	Mülakat, Güvenlik Denetimi	Tüm makineler için kullanıcı parolaları hangi prosedürlere göre belirlenmektedir? Parola değişimi ve yenileme hangi politikalara göre yapılmaktadır? Parola geçmişi tutulmakta ve hatalı giriş sayısına göre kullanıcı hesapları kilitlenmekte midir? Parolası olmayan hesaplar için nasıl bir prosedür uygulanmaktadır?
5.1.1.6	Son Kullanıcı Bilgisayarlarında Ağ Erişiminin Kısıtlanması	Güvenlik Denetimi	Son kullanıcı bilgisayarlarında ağ erişimi kısıtlaması yapılmış mıdır?
5.1.1.7	Hata ve Sorun Bilgilerinin Üretici ile Paylaşılmaması	Mülakat, Güvenlik Denetimi	İşletim sistemi kurulumu ile gelen hata ve sorun bilgilerinin üretici ile paylaşılması özelliği pasif hale getirilmiş midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.1.8	Kablosuz Ağ Arayüzlerinin Kapatılması	Mülakat, Güvenlik Denetimi	Tüm sunucularda kullanılmayan kablosuz ağ arayüzleri pasif hale getirilmiş midir?
5.1.1.9	Sistem Üzerinde Düzenli Olarak Zafiyet ve Zararlı Yazılım Taraması Yapılması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistemler için zafiyet yönetimi nasıl sağlanmaktadır? Bu işlem için hangi araçlardan faydalanılmaktadır? Sistemler üzerinde düzenli olarak zararlı yazılım taraması yapılmakta mıdır? Zararlı yazılım taramasında faydalanılan araçlar nelerdir?
5.1.1.10	Yerel Güvenlik Duvarı Ayarlarının Yapılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Tüm sunucularda yerel güvenlik duvarı aktif olarak çalışmakta mıdır? Güvenlik duvarı yapılandırması yaparken neler dikkate alınmaktadır? Güvenlik duvarı kurallarında varsayılan reddetme (deny) kuralı yer almakta mıdır?
5.1.1.11	Sunucularda Zaman Senkronizasyonunun Sağlanması	Mülakat, Güvenlik Denetimi	Sunucularda zaman senkronizasyonu sağlanmış mıdır ve güncel midir?
5.1.1.12	Güvenli Süreç (Process) İşleme Ayarlarının Yapılması	Mülakat, Güvenlik Denetimi	İşletim sistemlerinin DEP, ASLR vb. savunma mekanizmaları etkinleştirilmiş midir?
5.1.1.13	Kullanılmayan Uygulamaların Kaldırılması	Mülakat, Güvenlik Denetimi	Sistemlerde kullanılmayan uygulamaların tespiti nasıl gerçekleştirilmektedir? Sistemde kullanılmayan uygulamalar sistemlerden kaldırılmış mıdır?
5.1.1.14	Merkezi Güncelleme Sunucusu	Mülakat, Güvenlik Denetimi	Sistemlerin güncellik durumları nasıl kontrol edilmektedir? Güncelleştirme işlemleri için merkezi bir güncelleştirme sunucusu kullanılmakta mıdır?
5.1.1.15	IPv6 Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	Kurum içinde IPv6 kullanılmakta mıdır? Kullanılmıyorsa sunucularda IPv6 desteği pasif hale getirilmiş midir?
5.1.1.16	Sistem İz Kayıtlarının Aktif Edilmesi	Mülakat, Güvenlik Denetimi	Tüm sunucu ve makinelerde sistem iz kayıtları alınmakta mıdır? Hangi bilgiler kayıt altına alınmaktadır?
5.1.1.17	Sistem İz Kayıtlarının Merkezi Bir Sunucuda Toplanması	Mülakat, Güvenlik Denetimi	Sistem iz kayıtları merkezi bir kayıt sistemine gönderilmekte midir?
5.1.1.18	Merkezi Kimlik Yönetimi Servisinin Kullanılması	Mülakat, Güvenlik Denetimi	Merkezi bir kullanıcı yönetim sistemi kullanılmakta mıdır? Kullanılıyorsa, nasıl yönetilmektedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.1.19	Sunucularda Çalışan Servislerin Takibi	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucularda gerekli ve gereksiz servisler belirlenmiş midir? Gerekli ve gereksiz servisler nasıl belirlenmiştir? Listede olmayan bir servis başlatıldığında bunu engellemek/yönetmek için hangi araçlardan faydalanılmaktadır?
5.1.1.20	Bilgisayar Tabanlı Saldırı Tespit ve Engelleme Sistemlerinin Kullanılması	Mülakat, Güvenlik Denetimi	Sistem yerelinde saldırı tespit ve engelleme sistemi (HIDS/HIPS) kullanılmakta mıdır?
5.1.1.21	Disk Kotalarının Belirlenmesi	Mülakat, Güvenlik Denetimi	Kullanıcılar için disk kotaları belirlenmiş midir? Disk kota politikaları uygulanmakta mıdır?
5.1.1.22	Disk Seviyesinde Şifreleme Yapılması	Mülakat, Güvenlik Denetimi	Kritik bilgi içeren ve/veya işleyen makineler için disk seviyesinde şifreleme yapılmakta mıdır?

5.1.2. Linux İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.2.1	1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) pasif hale getirilmelidir.
5.1.2.2	1	Yetkili Kullanıcı Hesap Yönetimi	• Sisteme erişecek her kişi için ayrı bir kullanıcı hesabı oluşturulmalıdır. • Oluşturulan kullanıcılar için yetkiler belirlenmelidir. • Kullanılmayan hesaplar kaldırılmalıdır. • Sistem kullanıcılarının kabuğu /sbin/nologin olmalıdır. • Root login mümkünse engellenmelidir. • Tüm makinelerde UID değeri 0 olan tek kullanıcı root olmalıdır. • Ayrıca aynı isme veya UID değerine sahip kullanıcı veya grup bulunmamalıdır. • Servis ve sistem kullanıcıları hariç parolasız kullanıcılar bulunmamalıdır. • Sudoers kullanıcıları değişikliklere karşı takip edilmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.2.3	2	Dosya Sistemi Güvenli Erişim Düzenlemeleri	İçeriği değiştiğinde, silindiğinde veya taşındığında sistemin çalışmasını olumsuz yönde etkileyebilecek çalışma dosyalarının, kütüphanelerin ve yapılandırma dosyalarının (SUID ve SGID dosyaları, kayıt dosyaları, cron dosyaları, başlangıç betikleri, /etc/passwd, /etc/shadow vb.) yetkilendirmeleri amacına uygun şekilde düzenlenmeli ve kurum politikaları doğrultusunda denetlenmelidir. Varsayılan kullanıcı umask değeri en az yetki prensibine göre ayarlanmalıdır.
5.1.2.4	2	Güvenli Disk Bölümlendirme	İşletim sistemi dosyaları ile kullanıcı dosyaları, /home, /root, /boot, /tmp vb. birimler ayrı disk bölümlerinde tutulmalıdır.
5.1.2.5	2	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	CD/DVD ve USB gibi harici medyanın otomatik olarak mount edilmesini önlemek adına otomatik mount özelliği pasif hale getirilmelidir. Ayrıca /tmp dizini gibi mount noktalarında noexec, nodev, nosuid parametreleriyle çalıştırılabilir dosyalar pasif hale getirilmelidir.
5.1.2.6	2	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Önemli görülen dosyaların bütünlüğü düzenli olarak kontrol edilmelidir.
5.1.2.7	2	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Kullanılan makinelerde önyükleyici (bootloader) parolası belirlenmeli ve zorunlu tutulmalıdır. Ayrıca tek kullanıcı modu için kimlik doğrulaması yapılmalıdır. Boot edilebilir cihazlar listesi kısıtlanmalıdır. Kullanılmıyorsa USB, Firewire, Thunderbolt, PCMCIA vb. cihazlar iptal edilmelidir.
5.1.2.8	3	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	İşletim sistemi üzerinde erişim kontrolü, ilgili servisler (SELinux, AppArmor vb.) kullanılarak zorunlu erişim kontrolü (MAC) modeline göre yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.2.1	Kullanılmayan Dosya Sistemlerinin Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	Kullanılmayan dosya sistemleri (cramfs, freevxfs, hfs vb.) etkisiz hale getirilmiş midir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.2.2	Yetkili Kullanıcı Hesap Yönetimi	Mülakat, Güvenlik Denetimi	Kullanıcılar ve yetkileri nasıl yönetilmektedir? Gereksiz kullanıcılar bulunmakta mıdır? Sistem ve servis kullanıcıları hariç diğer kullanıcıların parolaları bulunmakta mıdır? Root ile uzaktan erişim mümkün müdür? UID değeri 0 olan kullanıcı bulunmakta mıdır? Aynı isme ve UID değerine sahip kullanıcılar ve gruplar bulunmakta mıdır? Sistem kullanıcıların kabuğu /sbin/nologin midir? Sudoers kullanıcıları değişikliklere karşı takip edilmekte midir?
5.1.2.3	Dosya Sistemi Güvenli Erişim Düzenlemeleri	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sistemlerde yer alan kritik dosyalar belirlenmiş midir? Dosya sistemlerine güvenli erişim kapsamında tanımlanmış bir politika var mıdır? Politika içeriğinde hangi hususlar ele alınmaktadır?
5.1.2.4	Güvenli Disk Bölümlendirme	Mülakat, Güvenlik Denetimi	Disk bölümlendirme nasıl yapılmaktadır?
5.1.2.5	Otomatik Başlatma (Mount) Özelliğinin Pasif Hale Getirilmesi	Mülakat, Güvenlik Denetimi	CD/DVD ve USB gibi medya cihazları otomatik olarak başlatılmakta mıdır? Bunu engellemek için ne gibi bir yapılandırma ayarı yapılmıştır?
5.1.2.6	Dosya Sistemi Bütünlük Kontrollerinin Düzenli Olarak Yapılması	Mülakat, Güvenlik Denetimi	Sistemlerde bütünlüğü kritik olan dosyalar belirlenmiş midir? Belirlenen bu dosyaların kontrolünü yapmak için hangi araçlardan/programlardan faydalanılmaktadır? Dosyaların bütünlüğünün bozulduğu durumlar için ne gibi bir süreç işletilmektedir?
5.1.2.7	Önyükleme (Boot) Ayarlarının Güvenli Şekilde Yapılandırılması	Mülakat, Güvenlik Denetimi	Önyükleyici için güvenli bir yapılandırma var mıdır? Boot cihazlarının yönetimi nasıl yapılmaktadır?
5.1.2.8	Zorunlu Erişim Kontrolünün (MAC) Aktif Edilmesi	Mülakat, Güvenlik Denetimi	Zorunlu erişim kontrolü (MAC) için hangi servilerden faydalanılmaktadır? Bu servislerin yönetimi nasıl sağlanmaktadır?

5.1.3. Windows İşletim Sistemi Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.3.1	1	Kullanıcı Haklarının Kısıtlanması	Kullanıcı hakları en az yetki prensibi göz önünde bulundurularak sadece ihtiyaç duyulan kullanıcı ve gruplara verilmelidir.
5.1.3.2	1	Otomatik Güncellemenin Aktif Olması	Tüm kullanıcı makinelerinde otomatik güncelleme özelliği aktif hale getirilmelidir.
5.1.3.3	1	SMB Protokolü Güvenliği	Windows işletim sistemlerinde SMB versiyon 1 protokolü yerine daha güvenli ve güncel SMB protokol versiyonları kullanılmalıdır.
5.1.3.4	1	Yerel Yönetici Hesapları Yönetimi	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmalıdır. Gerekli kullanıcılar için varsayılan olarak aynı tanımlanan yerel yönetici hesaplarının parolaları değiştirilmelidir.
5.1.3.5	1	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Etki alanı yöneticisi (Domain Admin) ve diğer yetkili hesapların (Enterprise Admin, Backup Admin ve Schema Admin) sayısı sınırlandırılmalıdır.
5.1.3.6	1	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Yetkili hesapların parola özetlerinin çalınmasının engellenmesi için: • Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında gerekli olmadıkça işlem yapılmamalı, işlem yapıldığı durumlarda kullanıcı bilgisayarlarının yeniden başlatılması sağlanmalıdır. • Yerel bilgisayarlarda parola özetleri tutulma sayısı 0 yapılmalıdır. • Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.
5.1.3.7	2	Kullanılmayan Hesapların Devre Dışı Bırakılması	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmalıdır. Bk. Tedbir No: 3.1.12.10
5.1.3.8	2	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Sistemlerde yer alan varsayılan yönetici ve misafir hesapları pasif hale getirilmelidir.
5.1.3.9	2	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Standart kullanıcıların betik çalıştırma motorlarına (Windows Script Host, Powershell, Command Prompt ve Microsoft HTML Application Host vb.) erişimi engellenmeli veya kısıtlanmalıdır.
5.1.3.10	2	Aktif Dizin Sorguları Güvenliği	Aktif dizin sorguları LDAP protokolü yerine güvenli LDAPs protokolü ile yapılacak şekilde konfigüre edilmelidir. Bk. Tedbir No: 3.2.9.1

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.1.3.11	2	Yönetici Hesaplarının İzlenmesi	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmelidir. Bk. Tedbir No: 3.1.12.11
5.1.3.12	2	Güvenli Yönetici İş İstasyonu Kullanımı	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.
5.1.3.13	2	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.3.1	Kullanıcı Haklarının Kısıtlanması	Mülakat, Güvenlik Denetimi	Kullanıcı haklarının kısıtlanması son kullanıcı bilgisayarlarına uygun olarak yapılandırılmış mıdır?
5.1.3.2	Otomatik Güncellemenin Aktif Olması	Mülakat, Güvenlik Denetimi	İşletim sisteminin otomatik güncelleme ayarı açık mıdır?
5.1.3.3	SMB Protokolü Güvenliği	Mülakat, Gözden Geçirme	SMB versiyon 1 protokolü sunucu ve istemcilerde kapatılmış mıdır, SMB protokolü hangi versiyon u kullanılmaktadır?
5.1.3.4	Yerel Yönetici Hesapları Yönetimi	Mülakat, Gözden Geçirme	Gerekli kullanıcılar dışında tüm kullanıcıların yerel yönetici hesapları devre dışı bırakılmış mıdır? Yerel yönetici hesaplarının parolaları nasıl değiştirilmektedir?
5.1.3.5	Ayrıcalıklı Hesap Sayılarının Sınırlandırılması	Mülakat, Gözden Geçirme	Ayrıcalıklı hesap sayıları sınırlandırılmakta mıdır?
5.1.3.6	Yetkili Hesapların Parola Özetlerinin Çalınmasının Engellenmesi	Mülakat, Gözden Geçirme	Etki alanı yöneticisi (domain admin) hesabıyla kullanıcı bilgisayarlarında ne sıklıkla ve ne gibi işlemler yapılmaktadır? Yerel bilgisayarlarda tutulan hesaplara ait parola özetlerinin tutulma sayısı 0 olarak ayarlanmış mıdır? Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) Grubuna alınmış mıdır?
5.1.3.7	Kullanılmayan Hesapların Devre Dışı Bırakılması	Mülakat, Gözden Geçirme	Aktif dizinde uzun süre kullanılmayan kullanıcı ve bilgisayar hesaplarını tespit etmek için bir yordam tanımlanmış mıdır?
5.1.3.8	Varsayılan Yönetici ve Misafir Hesaplarının Yapılandırılması	Mülakat, Güvenlik Denetimi	Varsayılan yönetici ve misafir hesaplarının yapılandırılması en iyi çözüm önerilerine uygun olarak yapılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.1.3.9	Standart Kullanıcıların Betik Çalıştırma Motorlarına Erişiminin Kısıtlanması	Mülakat, Güvenlik Denetimi	Cmd, powershell gibi betik çalıştırma motorlarına erişimler kısıtlandırılmış mıdır?
5.1.3.10	Aktif Dizin Sorguları Güvenliği	Mülakat, Gözden Geçirme	Aktif dizin sorguları güvenli LDAPs protokolü ile yapılmakta mıdır?
5.1.3.11	Yönetici Hesaplarının İzlenmesi	Mülakat, Gözden Geçirme	Ayrıcalıklı etki alanı gruplarına kullanıcı ekleme ve çıkarma işlemleri ve oturum açma kapama işlemleri izlenmekte midir?
5.1.3.12	Güvenli Yönetici İş İstasyonu Kullanımı	Mülakat, Gözden Geçirme	Yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu kullanılmakta mıdır?
5.1.3.13	Devre Dışı Bırakılan Hesabın Mail Erişiminin Engellenmesi	Mülakat, Gözden Geçirme	Aktif dizinde devre dışı bırakılan kullanıcı hesabı için activesync mail erişimi hemen kesilmekte midir?

5.2. Veri Tabanı Sıkılaştırma Tedbirleri

Amaç

Bu güvenlik tedbiri ana başlığının amacı, veri tabanı güvenlik sıkılaştırmaları çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Veri Tabanı Sıkılaştırma Tedbirleri” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Genel Sıkılaştırma Tedbirleri

5.2.1. Genel Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.2.1.1	1	Güncelleme ve Yama Yönetimi	Üretici tarafından desteklenmeyen sistemler zafiyet içerebileceğinden, veri tabanı bilinen en kararlı versiyon ile kullanılmalıdır. Bu kapsamda, belirli periyotlar ile sistemlerin güncelliği kontrol edilmeli ve gerekli güncelleştirmeler gerçekleştirilmelidir. Güvenlik yamaları, yayımlandıktan sonra mümkün olan en kısa zamanda ilgili sistemlere yüklenmelidir.
5.2.1.2	1	Veri Tabanı Parametrelerinin Güvenli Yapılandırılması	Veri tabanı için sunulan parametreler ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş yöntemler ile yapılandırılmalıdır. Ayrıca veri tabanı yönetim sistemi üreticisi tarafından yayımlanan güvenli kullanım önerileri uygulanmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.2.1.3	1	Varsayılan Hesap ve Parolaların Kullanılmaması	Veri tabanlarında varsayılan kullanıcı hesapları ve parolalar kullanılmamalıdır.
5.2.1.4	1	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Veri tabanı kullanıcıları için güçlü parola politikaları oluşturulmalı ve uygulanmalıdır.
5.2.1.5	1	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Veri tabanı sunucularına olan uzak bağlantı, mümkün olduğunca sınırlandırılarak yalnızca yetkili kullanıcıların ve/veya uygulamaların uzaktan erişimine olanak sağlayacak şekilde yapılandırılmalıdır. Bu kapsamda, ilgili sunucularda mevcut yapılandırmalar düzenlenmeli ve ağ katmanında gerekli önlemler alınmalıdır.
5.2.1.6	1	Kullanılmayan Hesapların Kapatılması	Düzenli olarak gerçekleştirecek denetimler ile belirli bir süre boyunca kullanılmayan kullanıcılar tespit edilerek pasif hale getirilmelidir.
5.2.1.7	1	Anonim Hesapların Bulunmaması	Veri tabanı kullanıcı hesapları, yapılan işlemlerin izlenebilirliğini sağlayacak ve tekil olarak kişi veya sistemi işaret edecek şekilde yapılmalıdır.
5.2.1.8	1	Veri Tabanı Rol ve Yetkilerinin Kısıtlanması	Tüm ayrıcalıklar, doğrudan kullanıcıya verilmek yerine kullanıcıların atanmış oldukları rollere/profillere tanımlanmalıdır. Düzenli aralıklarla veri tabanı rol ve yetkileri gözden geçirilmelidir. Kullanılmayan roller kaldırılmalı/pasif hale getirilmelidir. Ayrıca, kullanıcı hakları gözden geçirilerek gereksiz olarak tanımlanmış ve/veya ihtiyaç duyulmayan yetkiler kaldırılmalıdır.
5.2.1.9	1	Veri Tabanı Yönetim Sisteminin İşletim Sistemi Üzerindeki Ayrıcalıklarının Sınırlandırılması	Veri tabanının çalıştığı işletim sistemi üzerinde; komut çalıştırma, yerel dosya okuma/yazma vb. işlemlere imkân sağlayabilecek ayrıcalıkların sınırlandırılması için veri tabanı yönetim sistemi, desteklediği ölçüde yapılandırılmalıdır.
5.2.1.10	1	Komut/Sorgu Geçmişi Kayıtlarının Güvenliğinin Sağlanması	Veri tabanı tarafından, üzerinde çalıştırılmış komut/sorgu geçmişinin kayıt altına alındığı durumda ilgili kayıtların/dosyaların güvenliği sağlanmalıdır.
5.2.1.11	1	Yedeklerin Güvenliğinin Sağlanması	Yedek dosyalarına yetkisiz kullanıcıların erişmesini engellemek adına dosya izinlerinin yapılandırılması, şifreleme vb. yöntemler ile güvenlik sağlanmalıdır.
5.2.1.12	1	Adanmış Sunucu Kullanılması	Saldırı yüzeyini düşürmek amacıyla, veri tabanı yönetim sistemi adanmış bir sunucu üzerinde çalışmalıdır.
5.2.1.13	1	Kurulum Dosyalarının Güvenilir Kaynaklardan Temin Edilmesi	Kurulum dosyaları ve/veya kurulum için kullanılan paketler, güvenilir kaynaklardan elde edilmelidir.
5.2.1.14	1	Örnek Verilerin Silinmesi	Veri tabanından, kurulum ile gelen örnek veriler (örnek tablolar, kayıtlar, kullanıcılar vb.) silinmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.2.1.15	2	Veri Tabanı Sistem Dosyalarının ve İz Kayıtlarının Aynı Disk Bölümü Üzerinde Bulunmaması	Veri tabanı tarafından kullanılan sistem dosyaları ve üretilen iz kayıtları farklı disk bölümlerinde tutulmalıdır.
5.2.1.16	2	Veri Tabanında Tablo ve Nesne Düzeyinde Yetkilendirme Yapılması	Kritik veri içeren tablo ve nesneler için tablo ve/veya nesne bazında yetkilendirme yapılmalıdır.
5.2.1.17	2	İşletim Sistemi Üzerinde Veri Tabanı Servisi Çalıştıran Kullanıcıların Yönetici Haklarına Sahip Olmaması	İşletim sistemi üzerinde veri tabanı servis(ler)ini çalıştıran kullanıcılar için en az yetki prensibi uygulanmalıdır. Bu kapsamda ilgili kullanıcılar, ihtiyaç duyulmadığı takdirde yönetici haklarına sahip olmamalıdır.
5.2.1.18	2	Kümeleme veya Replikasyon İçinde Bulunan Veri Tabanı Sunucuları Arası İletişimin Güvenliğinin Sağlanması	Kümeleme (cluster) ve/veya replikasyon içinde bulunan veri tabanı sunucuları arasında gerçekleştirecekleri iletişim şifreli olarak yapılmalıdır. Buna ek olarak, ilgili süreçlerde kullanılacak hesaplar için en az yetki prensibi uygulanmalıdır. Bu kapsamda, replikasyon ve kümeleme faaliyetlerinde kullanılan hesaplar ihtiyaç duyulmadığı takdirde yönetici haklarına sahip olmamalıdır. Bk. Tedbir No: 5.2.1.8 Bk. Tedbir No: 3.2.5.11
5.2.1.19	2	Merkezi Kimlik Doğrulama Sisteminin Kullanılması	Veri tabanı yönetim sisteminin desteklediği ölçüde, merkezi kimlik doğrulama sistemi kullanılmalıdır.
5.2.1.20	3	Kritik Bilgi İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Veri tabanı sunucularında yer alan kritik verinin, depolama motoru (storage engine) ve/veya disk seviyesinde şifreleme gibi yöntemler ile güvenliği sağlanmalıdır. Bk. Tedbir No: 5.1.1.22
5.2.1.21	3	Veri Tabanı Sunucusu ile İstemci Arasındaki İletişimin Şifreli Olması	Veri tabanı sunucusu ile istemci arasındaki iletişim şifreli trafik üzerinden sağlanmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.2.1.1	Güncelleme ve Yama Yönetimi	Mülakat, Güvenlik Denetimi	Veri tabanının güncelliği ve güvenlik yamalarının mevcut olup olmadığı belirli periyotlar ile kontrol ediliyor mu? Yeni versiyonun veya güvenlik yamasının tespit edilmesi halinde güncelleştirmeler kontrollü bir şekilde devreye alınıyor mu?
5.2.1.2	Veri Tabanı Parametrelerinin Güvenli Yapılandırılması	Mülakat, Güvenlik Denetimi	Veri tabanı için sunulan parametreler, ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş yöntemler ile yapılandırılıyor mu?
5.2.1.3	Varsayılan Hesap ve Parolaların Kullanılmaması	Mülakat, Güvenlik Denetimi	Veri tabanında varsayılan hesaplar bulunmakta mıdır? Veri tabanı kullanıcıları arasında varsayılan parola kullanan hesap bulunmakta mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.2.1.4	Veri Tabanı Kullanıcıları için Parola Politikalarının Oluşturulması	Mülakat, Güvenlik Denetimi	Veri tabanı kullanıcılarını güçlü parola kullanmaya zorlayacak politikalar tanımlanmış mıdır? Tanımlanan politikalar tüm kullanıcılar için zorunlu tutulmakta mıdır?
5.2.1.5	Veri Tabanına Yapılan Uzak Bağlantıların Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Veri tabanı sunucularına yalnızca gerekli/yetkili kullanıcılar ve/veya uygulamalar tarafından uzaktan bağlantının sağlaması için hangi önlemler alınmaktadır?
5.2.1.6	Kullanılmayan Hesapların Kapatılması	Mülakat, Güvenlik Denetimi	Belirli bir süre boyunca kullanılmayan kullanıcılar tespit edilerek pasif hale getiriliyor mu?
5.2.1.7	Anonim Hesapların Bulunmaması	Mülakat, Güvenlik Denetimi	Aynı hesabın birden fazla kullanıcı tarafından kullanılmasını (ortak hesap) önlemek adına tekil kullanıcılar tanımlanmış mıdır?
5.2.1.8	Veri Tabanı Rol ve Yetkilerinin Kısıtlanması	Mülakat, Güvenlik Denetimi	Veri tabanı rol ve yetkileri düzenli aralıklarla gözden geçirilerek kullanılmayan roller pasif hale getiriliyor/kaldırılıyor mu? Kullanıcı hakları gözden geçirilerek gereksiz olarak tanımlanmış ve/veya ihtiyaç duyulmayan yetkiler kaldırılıyor mu?
5.2.1.9	Veri Tabanı Yönetim Sisteminin İşletim Sistemi Üzerindeki Ayrıcalıklarının Sınırlandırılması	Mülakat, Güvenlik Denetimi	Veri tabanının çalıştığı işletim sistemi üzerinde; komut çalıştırma, yerel dosya okuma/yazma vb. işlemlere imkân sağlayabilecek ayrıcalıkların sınırlandırılması için veri tabanı yönetim sistemi, desteklediği ölçüde yapılandırılmış mıdır?
5.2.1.10	Komut/Sorgu Geçmişi Kayıtlarının Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Veri tabanı tarafından, üzerinde çalıştırılmış komut/sorgu geçmişi kayıt altına alınıyor mu? Böyle bir durumda ilgili kayıtların/dosyaların güvenliği nasıl sağlanmaktadır?
5.2.1.11	Yedeklerin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Yedek dosyaların güvenliği hangi yöntemler ile sağlanmaktadır?
5.2.1.12	Adanmış Sunucu Kullanılması	Mülakat, Güvenlik Denetimi	İlgili veri tabanı sunucusu adanmış sunucu mudur?
5.2.1.13	Kurulum Dosyalarının Güvenilir Kaynaklardan Temin Edilmesi	Mülakat, Güvenlik Denetimi	Kurulum dosyalarının/kurulum için kullanılan paketlerin, güvenilir kaynaklardan alınmış olduğu kontrol ediliyor mu?
5.2.1.14	Örnek Verilerin Silinmesi	Mülakat, Güvenlik Denetimi	Veri tabanında, kurulum ile gelen örnek veriler (örnek tablolar, kayıtlar, kullanıcılar vb.) bulunuyor mu?
5.2.1.15	Veri Tabanı Sistem Dosyalarının ve İz Kayıtlarının Aynı Disk Bölümü Üzerinde Bulunmaması	Mülakat, Güvenlik Denetimi	Veri tabanı tarafından kullanılan sistem dosyaları hangi disk bölümü üzerinde bulunmaktadır? Veri tabanı tarafından üretilen iz kayıtları hangi disk bölümü üzerinde bulunmaktadır? Sistem bölümü, hangi disk bölümü üzerindedir?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.2.1.16	Veri Tabanında Tablo ve Nesne Düzeyinde Yetkilendirme Yapılması	Mülakat, Güvenlik Denetimi	Kritik veri içeren tablo ve nesneler için tablo ve/veya nesne bazında yetkilendirme kullanılıyor mu?
5.2.1.17	İşletim Sistemi Üzerinde Veri Tabanı Servisi Çalıştıran Kullanıcıların Yönetici Haklarına Sahip Olmaması	Mülakat, Güvenlik Denetimi	İşletim sistemi üzerinde veri tabanı servis(ler)ini çalıştıran kullanıcılar için en az yetki prensibi uygulanmış mıdır?
5.2.1.18	Kümeleme veya Replikasyon İçinde Bulunan Veri Tabanı Sunucuları Arası İletişimin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kümeleme ve/veya replikasyon içinde veri tabanı sunucuları mevcut mudur? Bu sunucular arasında gerçekleşen iletişim şifreli olarak mı yapılmaktadır? İlgili süreçlerde kullanılacak hesaplarda en az yetki prensibi uygulanmakta mıdır?
5.2.1.19	Merkezi Kimlik Doğrulama Sisteminin Kullanılması	Mülakat, Güvenlik Denetimi	Merkezi kimlik doğrulama sistemi kullanılmakta mıdır?
5.2.1.20	Kritik Bilgi İçeren Veri Tabanı Sunucularında Durağan Verinin Güvenliğinin Sağlanması	Mülakat, Güvenlik Denetimi	Kritik veri içeren veri tabanı sunucularında bulunan hareketsiz verinin (data at rest) güvenliği nasıl sağlanmaktadır?
5.2.1.21	Veri Tabanı Sunucusu ile İstemci Arasındaki İletişimin Şifreli Olması	Mülakat, Güvenlik Denetimi	Veri tabanı sunucusu ile istemci arasındaki iletişim şifreli trafik üzerinden mi sağlanmaktadır?

5.3. Sunucu Sıkılaştırma Tedbirleri

Amaç

Bu güvenlik tedbiri ana başlığının amacı, sunucu güvenlik sıkılaştırmaları çerçevesinde ele alınan tedbir listeleri ve denetim sorularını belirlemektir. “Sunucu Sıkılaştırma Tedbirleri” ana başlığı kapsamında ele alınan güvenlik tedbirleri alt başlıkları aşağıda yer almaktadır.

- Web Sunucusu Sıkılaştırma Tedbirleri
- Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

5.3.1. Web Sunucusu Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.1.1	1	Güncel Web Sunucu Yazılımlarının Kullanılması	Web sunucu yazılımlarının güncel, zafiyet içermeyen ve üreticisi tarafından desteği devam eden kararlı sürümleri kullanılmalıdır. Ayrıca, sunucuda kullanımda olan tüm araçların/paket programların güvenlik yamaları için düzenli aralıklarla kontrol yapılmalıdır.
5.3.1.2	1	WebDAV Desteğinin Kaldırılması	Web sunucusunun WebDAV (Web Distributed Authoring and Versioning) desteği kaldırılmalıdır. WebDAV ile ilgili modüller pasif hale getirilmelidir.
5.3.1.3	1	Web Sunucusu Kullanıcı Yönetimi	Web sunucu yazılımı yönetici hesabıyla değil, bu amaç için özel olarak oluşturulmuş bir hesap ile çalıştırılmalıdır. Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmalıdır.
5.3.1.4	1	Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması	Web sunucusu bilgi ifşalarını önleyecek şekilde yapılandırılmalıdır. Varsayılan hata ve kurulum sayfaları kaldırılmalıdır. Web sunucu teknolojisi hakkında bilgi ifşasına neden olan HTTP başlıkları kaldırılmalıdır. Hatalı HTTP isteklerine dönen cevaplarda bilgi ifşasına izin verilmemelidir.
5.3.1.5	1	Desteklenen HTTP Metotlarının Kısıtlanması	POST, GET, OPTIONS ve HEAD metotları dışında diğer HTTP metotları desteklenmemelidir. PUT, DELETE, PROPFIND gibi metotlar web servisi için kullanılıyorsa, kullanımlarının sadece web servis ihtiyaçları ile sınırlı olup olmadığı kontrol edilmelidir. Bu metotların dosya yükleme veya silme gibi farklı amaçlarla kullanımı engellenmelidir.
5.3.1.6	1	Dizin Listelemenin Pasif Hale Getirilmesi	Dizin listelemesi pasif hale getirilmelidir.
5.3.1.7	1	Debug Modunun Kapalı Olması	Web sunucu yazılımı debug (hata ayıklama) modunda çalıştırılmamalıdır.
5.3.1.8	1	İstek Limitlerinin Tanımlanması	Web sunucu yazılımının desteklediği ölçüde, istekler için limitler belirlenmelidir.
5.3.1.9	1	İz Kayıtlarının Alınması	Web sunucu yazılımına ilişkin iz kayıtları alınmalıdır. Bk. Tedbir No: 3.1.8.1
5.3.1.10	1	Yazma İzni Olan Dizinlerin Kısıtlanması	Yazma izni olan dizinler belirlenmeli, yazma yetkileri sadece dosya yükleme ihtiyacı olan dizinlere verilmelidir. Uygulama üzerinden yüklenen dosyalar için oluşturulmuş dizinlerde çalıştırma izni kaldırılmalıdır.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.1.11	1	SSL/TLS Kullanımı	Sunucu SSL/TLS kullanımına elverişli yapılandırılmalıdır. Bu kapsamda, sunucuda sadece, bilinen zafiyet içermeyen güvenilir sürüme sahip SSL/TLS versiyonları kullanılmalıdır. Bk. Tedbir No: 3.2.9.1
5.3.1.12	1	İsteklerin HTTP'den HTTPS'e Yönlendirilmesi	Web sunucusundaki herhangi bir HTTP bağlantı noktası, şifreleme kullanan bir sunucu bağlantı noktasına yönlendirmelidir.
5.3.1.13	1	Kullanılmayan Modüllerin Kaldırılması	Sunucuda sadece kullanılan modüllerin aktif olmalıdır.
5.3.1.14	1	Açık Portların Kısıtlanması	Web sunucusu yalnızca yetkili bağlantı noktalarındaki ağ bağlantılarını dinlemelidir. Kullanımda olmayan portlar kapatılmalıdır. Bk. Tedbir No: 5.1.1.2
5.3.1.15	1	Kaynak Kullanım Optimizasyonu	Uygulama seviyesinde yapılabilecek servis dışı bırakma saldırılarına karşı aşağıdaki sunucu üzerinde aşağıdaki sıkılaştırmalar yapılmalıdır: • Sunucunun kabul edebileceği maksimum kullanıcı sayısı artırılmalıdır. • Tek bir IP adresinden yapılabilecek bağlantı sayısı sınırlandırılmalıdır. • Her bir bağlantının kullanabileceği maksimum ve minimum transfer hızı belirlenmelidir. • Bağlantılar için zaman aşım değeri belirlenmeli, belirli bir süre açık kalan bağlantılar sonlandırılmalıdır.
5.3.1.16	1	Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu	İnternete açık olarak çalışan web sunucu ayrı bir bölgede (DMZ vb.) tutulmalıdır. Bk. Tedbir No: 3.2.5.3 Bk. Tedbir No: 3.1.6.6
5.3.1.17	1	Sunucuda Koruyucu HTTP Başlıklarının Kullanımı	Sunucu tarafında koruyucu HTTP başlıkları (X-Frame-Options, Strict-Transport-Security vb.) yapılandırılmalıdır.
5.3.1.18	1	Sunucunun Özel Anahtarının (Private Key) Korunması	Sunucunun özel anahtarına (private key) yapılacak yetkisiz erişimlere karşı önlemler alınmalıdır.
5.3.1.19	2	İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi	Web sunucularından alınan iz kayıtları merkezi bir kayıt sistemine gönderilmelidir. Bk. Tedbir No: 3.1.8.6

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.1.20	2	Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi	Sunucuya IP adresi üzerinden yapılan erişimler engellenmelidir.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.1.1	Güncel Web Sunucu Yazılımlarının Kullanılması	Mülakat, Güvenlik Denetimi	Web sunucu yazılımlarının güncel, zafiyet içermeyen ve üreticisi tarafından desteği devam eden kararlı sürümleri mi kullanılmaktadır?
5.3.1.2	WebDAV Desteğinin Kaldırılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Web sunucusunun WebDAV (Web Distributed Authoring and Versioning) desteği bulunmakta mıdır? WebDAV ile ilgili modullerden aktif durumda olan var mıdır?
5.3.1.3	Web Sunucusu Kullanıcı Yönetimi	Mülakat, Güvenlik Denetimi	Web sunucu yazılımı hangi kullanıcı hesabıyla çalıştırılmaktadır? Web sunucusunda bulunan varsayılan hesaplar/parolalar kullanım dışı bırakılmış mıdır?
5.3.1.4	Web Sunucusunun Bilgi İfşalarını Önleyecek Şekilde Yapılandırılması	Mülakat, Sızma Testi	Web sunucusu bilgi ifşalarını önleyecek şekilde yapılandırılmış mıdır? Web sunucu teknolojisi hakkında bilgi ifşasına neden olan HTTP başlıkları kaldırılmış mıdır? Olağan dışı (hatalı) HTTP isteklerine dönülen yanıtlarda bilgi ifşası olmaması için kontrol sağlanmış mıdır?
5.3.1.5	Desteklenen HTTP Metotlarının Kısıtlanması	Mülakat, Sızma Testi	Uygulama gereksinimleri dışındaki tüm HTTP metotları kısıtlanmış mıdır?
5.3.1.6	Dizin Listelemenin Pasif Hale Getirilmesi	Mülakat, Sızma Testi	Sunucuda dizin listelemesi pasif hale getirilmiş midir?
5.3.1.7	Debug Modunun Kapalı Olması	Mülakat, Gözden Geçirme, Sızma Testi	Web sunucu yazılımı debug modunda çalıştırılabilmekte midir?
5.3.1.8	İstek Limitlerinin Tanımlanması	Mülakat, Gözden Geçirme, Sızma Testi	Web sunucu yazılımının desteklediği ölçüde, istekler için limitler belirlenmiş midir?
5.3.1.9	İz Kayıtlarının Alınması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Web sunucu yazılımına ilişkin iz kayıtları alınmakta mıdır? Alınan iz kayıtları kurum politikaları ve ilgili mevzuatlarda belirtilen süre boyunca saklanmakta mıdır?
5.3.1.10	Yazma İzni Olan Dizinlerin Kısıtlanması	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucuda yazma izni olan dizin bulunuyor mudur? Bu dizinlerde düzenleme yapılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.1.11	SSL/TLS Kullanımı	Mülakat, Gözden Geçirme, Sızma Testi	Sunucu SSL/TLS kullanımına elverişli yapılandırılmış mıdır? Sunucuda hangi SSL/TLS sürümü kullanılmaktadır?
5.3.1.12	İsteklerin HTTP'den HTTPS'e Yönlendirilmesi	Mülakat, Gözden Geçirme, Sızma Testi	Web sunucusundaki tüm HTTP bağlantı noktaları şifreleme kullanan bir sunucu bağlantı noktasına yönlendiriliyor mudur?
5.3.1.13	Kullanılmayan Modüllerin Kaldırılması	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucuda kullanılmayan modüller kaldırılmış mıdır?
5.3.1.14	Açık Portların Kısıtlanması	Mülakat, Güvenlik Denetimi, Sızma Testi	Web sunucusunun yalnızca yetkili bağlantı noktalarındaki ağ bağlantıları mı dinlenmektedir? Kullanımda olmayan portlar kapatılmış mıdır?
5.3.1.15	Kaynak Kullanım Optimizasyonu	Mülakat, Sızma Testi	Tek bir IP adresi üzerinden yapılabilecek maksimum bağlantı sayısı belirlenmiş midir? Uzun süre açık kalan bağlantılar kapatılmakta mıdır? Bağlantılar için maksimum ve minimum transfer hızı belirlenmiş midir?
5.3.1.16	Sunucunun Korumalı ve Ayrıştırılmış Şekilde Kurulumu	Mülakat, Güvenlik Denetimi, Sızma Testi	İnternete açık olarak çalışan web sunucu DMZ (DeMilitarized Zone) gibi ayrı bir bölgede tutulmakta mıdır?
5.3.1.17	Sunucuda Koruyucu HTTP Başlıklarının Kullanımı	Mülakat, Sızma Testi	Olası saldırılara karşın önlem olarak sunucu tarafında koruyucu HTTP başlıkları yapılandırılmış mıdır?
5.3.1.18	Sunucunun Özel Anahtarının (Private Key) Korunması	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucunun özel anahtarı (private key) yetkisiz erişime karşı korunmakta mıdır?
5.3.1.19	İz Kayıtlarının Merkezi Kayıt Sistemine Gönderilmesi	Mülakat, Gözden Geçirme	Web sunucularından alınan iz kayıtları merkezi bir kayıt sistemine gönderiliyor mudur?
5.3.1.20	Sunucuya IP Adresi Üzerinden Erişimlerin Engellenmesi	Mülakat, Güvenlik Denetimi, Sızma Testi	Sunucuya IP adresi üzerinden erişimler engellenmiş midir?

5.3.2. Sanallaştırma Sunucusu Sıkılaştırma Tedbirleri

Tedbirler

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.2.1	1	Güncel Sanallaştırma Yazılımının Kullanılması	Sanallaştırma sunucusunda kullanılan sanallaştırma yazılımı güncel olmalı ve mevcut güvenlik yamaları yüklü olmalıdır.
5.3.2.2	1	Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması	Konteynerların/sanal makinelerin çalıştığı ana makine üzerinde sıkılaştırmalar yapılmalıdır. Bk. Bölüm 5.1
5.3.2.3	1	Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanması	Bk. Tedbir No: 5.1.1.11
5.3.2.4	1	Sanallaştırma Yazılımı Güvenlik Duvarının Aktif Olması	Sanallaştırma yazılımı ile beraber gelen güvenlik duvarı aktif olmalı ve sadece ihtiyaç duyulan portlar üzerinden ihtiyaç duyulan IP adreslerine erişime izin vermelidir.
5.3.2.5	1	Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması	Depolama alanı ağı (SAN) etkinliğini ayırmak için imar ve mantıksal birim numarası (LUN) maskeleme kullanılmalıdır.
5.3.2.6	1	Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması	Sanallaştırma ünitelerine erişim sağlayabilen kullanıcıların, sanal makinelerin sahibi olan kullanıcıların ekranlarını yetkisiz olarak görüntülemesi engellenmelidir. Ayrıca yetkisiz konsol erişimleri de engellenmelidir. Her kullanıcı kimlik doğrulaması sonrasında erişim sağlamalıdır.
5.3.2.7	1	Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme	Sanallaştırma ünitesinde kullanıcılar en az yetki prensibine uygun şekilde ilgili kullanıcı rollerine atanmalıdır.
5.3.2.8	1	Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması	Ana bilgisayardan ve sanal makinelerden gerekli olmayan tüm hizmetler/donanımlar kaldırılmalıdır. Örneğin, kullanılmayan sanal donanımlar (sürücüler, ağ adaptörleri vb.) devre dışı bırakılmalıdır. Ayrıca gereksiz hipervizör hizmetleri (pano paylaşımı, dosya paylaşımı vb.) devre dışı bırakılmalıdır.
5.3.2.9	1	Sanal Makineler Üzerindeki Diskler için Disk Küçültme Konfigürasyonuna Erişimin Kısıtlanması	Sanal disk küçültme (disk shrinking) işleminin sürekli olarak yapılması, sanal diskin kullanılamamasına ve veri kaybına sebebiyet verebileceği için bu ayarı yönetebilecek kullanıcılar belirlenerek, sadece bu kullanıcıların erişimine izin verilmelidir.
5.3.2.10	2	Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi	Sanallaştırma yazılımı çalıştığı tüm sunucularda merkezi olarak eş zamanlı güncellenmelidir.

Tedbir No.	Tedbir Seviyesi	Tedbir Adı	Tedbir Tanımı
5.3.2.11	2	Sanal Makineler için İz Kayıtlarının Yönetilmesi	Sanallaştırma ortamında çalışan sanal makineler için alınan iz kayıtları kalıcı bir şekilde saklanmalıdır. Ayrıca bu iz kayıtları merkezi bir kayıt sistemine gönderilmelidir. Bk. Tedbir No: 3.1.8.1 Bk. Tedbir No: 3.1.8.6
5.3.2.12	2	Sanal Makinelerin Güvenli İmhası	Sanal makineler silinmeden önce, sanal makineye ait disk dosyalarına sıfır yazılmalı ve daha sonrasında kalıcı silme işlemi yapılmalıdır.
5.3.2.13	2	Hipervizörler Tarafından Sunulan Bellek Paylaşımı Özelliklerinin Kullanımı	Bellek paylaşımı (memory sharing) kullanılmıyor ise devre dışı bırakılmalıdır. Eğer bellek paylaşımı özelliği kullanılacak ise sanal makineler arasında gruplandırma gibi gerekli güvenlik önlemleri alınmalıdır.
5.3.2.14	2	Sunucu Yedeklerinin Alınması	Düzenli olarak sunucu sistem yedekleri alınmalıdır. Yedekler yetkisiz erişime karşı güvenli ortamlarda muhafaza edilmelidir. Belirli aralıklarla yedekten geri dönme testleri gerçekleştirilmelidir.
5.3.2.15	3	Disk ve İmajların Şifreli Olarak Saklanması	Sanal makineye ait imajlar ve anlık görüntüler şifreli olarak muhafaza edilmelidir. Ayrıca, sanal makinelerde disk seviyesinde şifreleme yapılmalıdır.

Denetim Maddeleri

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.2.1	Güncel Sanallaştırma Yazılımının Kullanılması	Mülakat, Güvenlik Denetimi	Sanallaştırma sunucusu için kullanılan sanallaştırma yazılımı güncel midir?
5.3.2.2	Konteynerların /Sanal Makinelerin Çalıştığı Ana Makine Üzerinde Sıkılaştırmaların Yapılması	Mülakat, Güvenlik Denetimi	İşletim sistemi sıkılaştırmaları en iyi çözüm önerilerine uygun mudur? Bk. Bölüm 5.1
5.3.2.3	Sanal Makineler Arasında Zaman Senkronizasyonunun Sağlanması	Mülakat, Güvenlik Denetimi	Sanal makineler arasında zaman senkronizasyonunun sağlanması için gerekli yapılandırma sağlanmış mıdır?
5.3.2.4	Sanallaştırma Yazılımı Güvenlik Duvarının Aktif Olması	Mülakat, Güvenlik Denetimi	Sanallaştırma yazılımı güvenlik duvarı aktif midir?
5.3.2.5	Mantıksal Birim Numarası (LUN) Maskelemesi Yapılması	Mülakat, Güvenlik Denetimi	SAN etkinliğini ayırmak için LUN maskeleme yapılmış mıdır?

Tedbir No.	Tedbir Adı	Denetim Yöntem Önerileri	Denetim Soru Önerileri
5.3.2.6	Sanallaştırma Ünitesi Üzerinden Konsol Erişimlerinin Kısıtlanması	Mülakat, Güvenlik Denetimi	Sanallaştırma ünitesi üzerinde konsol kısıtlaması için gerekli yapılandırma var mıdır?
5.3.2.7	Sanallaştırma Ünitesinde Kullanıcı Yetkilendirme	Mülakat, Güvenlik Denetimi	Sanal makinelere ait imajlar ve anlık görüntülere erişim yetkisi kimlere verilmektedir? Erişim yetkileri en az yetki prensibine uygun olarak mı verilmektedir?
5.3.2.8	Gereksiz Hizmetlerin ve Kullanılmayan Donanımların Kaldırılması	Mülakat, Güvenlik Denetimi	Ana makine ile sanal makine arasında dosya paylaşımında gerekli kısıtlamalar uygulanmış mıdır? Sanal makine üzerinde kullanılan/çalışmakta olan gereksiz donanım/hizmet mevcut mudur?
5.3.2.9	Sanal Makineler Üzerindeki Diskler için Disk Küçültme Konfigürasyonuna Erişimin Kısıtlanması	Mülakat, Güvenlik Denetimi	Disk kapasite küçültme işlemi için kullanıcı bazlı izin tanımlaması mevcut mudur?
5.3.2.10	Sanallaştırma Yazılımının Merkezi Olarak Güncellenmesi	Mülakat	Sanallaştırma yazılımı merkezi olarak güncellenmekte midir?
5.3.2.11	Sanal Makineler için İz Kayıtlarının Yönetilmesi	Mülakat, Gözden Geçirme	Sanal makineler için iz kayıtları tutulmakta mıdır? Tutulan bu kayıtlar merkezi bir kayıt sistemine gönderilmekte midir?
5.3.2.12	Sanal Makinelerin Güvenli İmhası	Mülakat, Gözden Geçirme	Sanal makinelerin güvenli imhası için belirli bir politika bulunmakta mıdır?
5.3.2.13	Hipervizörler Tarafından Sunulan Bellek Paylaşımı Özelliklerinin Kullanımı	Mülakat, Güvenlik Denetimi	Hipervizörler tarafından sunulan bellek paylaşımı özellikleri kullanılmakta mıdır? Sanal makineler arasında bellek paylaşımı ile ilgili bir gruplandırma yapılmış mıdır?
5.3.2.14	Sunucu Yedeklerinin Alınması	Mülakat, Gözden Geçirme	Sanallaştırma sisteminin yedeklemesi yapılmakta mıdır?
5.3.2.15	Disk ve İmajların Şifreli Olarak Saklanması	Mülakat, Gözden Geçirme, Güvenlik Denetimi	Sanal makinelere ait diskler şifreli olarak korunmaktadır? Anlık görüntüler şifreli olarak korunmakta mıdır?

KAYNAKÇA

1. Bilişim Terimleri Sözlüğü, TSE (2006)
2. CIS (Center for Internet Security) Controls v7.1 (2019)
3. Cloud Controls Matrix 3.0.1 (2016)
4. NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity (2018)
5. NIST IR (National Institute of Standards and Technology Internal Report) 8228 (2019)
6. OWASP (Open Web Application Security Project) Application Security Verification Standard 4.0 (2019)
7. OWASP (Open Web Application Security Project) IoT (Internet of Things) Security Guidance (2018)
8. OWASP (Open Web Application Security Project) Mobile Application Security Verification 1.1.4 (2019)
9. PCI DSS (Payment Card Industry Data Security Standard) Requirements and Security Assessment Procedures 3.2.1 (2018)
10. TS ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler Standardı (2017)
11. 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu
12. 28.10.2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
13. 30.12.2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik
14. 10.03.2018 tarihli Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ
15. 10.03.2018 tarihli Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ
16. 04.05.2017 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
17. TÜBİTAK BİLGEM Güvenli Yazılım Geliştirme Kılavuzu 1.1 (2018)
18. Kurumsal SOME Kurulum ve Yönetim Rehberi (2014)

EKLER

EK-A: GENELGE MADDELERİ EŞLEŞTİRME TABLOSU

06.07.2019 Tarihli ve 30823 Sayılı Resmi Gazete'de yayımlanan 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi'nde yer alan 21 adet tedbirin ilgili rehber başlıklarıyla eşleşmesi aşağıdaki tabloda yer almaktadır. Söz konusu maddelerin tabloya ilaveten farklı başlıklarla da ilişkilendirilmesi mümkündür. Genelge Maddesi doğrudan Rehber başlığıyla ilişkiliyse tablodaki ilgili hücreye A (Asıl) yazılmıştır. Genelge Maddesi ile Rehber başlığı arasında dolaylı bir ilişki varsa tablodaki ilgili hücreye D (Dolaylı / Destekleyici) yazılmıştır.

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
1	Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.	A	A	D			D	A		A	A		
2	Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.	A	D				A					A	
3	Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.	A	A				D			A			
4	Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.		A						A		D		

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
5	Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.					A							
6	Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.								A				
7	Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.						A						
8	Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.				D		A						
9	Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.	D		A	D	D							
10	Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla kullanılan cihazlar kayıt altına alınacaktır.	A		D							D		
11	Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.										A		

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
12	Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.		A			D							D
13	Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.	D	A						D				D
14	Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.	A										A	
15	Üst düzey yöneticiler de dâhil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.	A	A			A	A	A					
16	Endüstriyel kontrol sistemlerinin, internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.	D	D									A	
17	Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması veya arşiv araştırması yaptırılacaktır.					A							

Madde No	Genelge Maddesi	Varlık Gruplarına Yönelik Güvenlik Tedbirleri						Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri					
		Ağ ve Sistem Güvenliği	Uygulama ve Veri Güvenliği	Taşınabilir Cihaz ve Ortam Güvenliği	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	Personel Güvenliği	Fiziksel Mekânların Güvenliği	Kişisel Verilerin Güvenliği	Anlık Mesajlaşma Güvenliği	Bulut Bilişim Güvenliği	Kripto Uygulamaları Güvenliği	Kritik Altyapılar Güvenliği	Yeni Geliştirmeler ve Tedarik
18	Kamu e-posta sistemlerinin ayarları güvenli olacak biçimde yapılandırılacak, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.	A							A	D			
19	Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.					A			D				
20	Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye'de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.											A	
21	İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişiminde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kripto sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.										A	A	

EK-B: ULUSLARARASI STANDARTLAR VE YAYIMLI KILAVUZLAR EŞLEŞTİRME TABLOSU

Rehber Ana Başlıkları	Standart/Yayımlı Doküman																		
	CMMC v1.0	ISO 27001:2017	CIS Controls v7.1	Cloud Controls Matrix 3.0.1	NIST 800-53	OWASP Application Security Verification Standard 4.0	OWASP Mobile Application Security Verification 1.1.4	TÜBİTAK BİLGEM Güvenli Yazılım Geliştirme Kılavuzu 1.1	Mobile Application Security Checklist 1.1	OWASP IoT Security Guidance	NIST 800-82	CIS Benchmark	ENISA Security Aspects of Virtualization	NIST 800-125	Ubuntu Server Guide - Security	Oracle Linux 7 Security Guide	DISA STIG - Canonical Ubuntu 16.04 LTS Security Technical Implementation Guide	DISA STIG - Red Hat Enterprise Linux 7 Security Technical Implementation Guide	Red Hat Enterprise Linux 8 Security Hardening
3.1 Ağ ve Sistem Güvenliği	+	+	+	+	+														
3.2 Uygulama ve Veri Güvenliği		+				+	+	+											
3.3 Taşınabilir Cihaz ve Ortam Güvenliği	+	+	+	+	+				+										
3.4 Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği		+							+	+									
3.5 Personel Güvenliği	+	+	+	+															
3.6 Fiziksel Mekânların Güvenliği	+	+		+															
4.1 Kişisel Verilerin Güvenliği		+																	
4.2 Anlık Mesajlaşma Güvenliği		+		+															

Standart/Yayımlı Doküman \ Rehber Ana Başlıkları	4.3 Bulut Bilişim Güvenliği	4.4 Kripto Uygulamaları Güvenliği	4.5 Kritik Altyapılar Güvenliği	4.6 Yeni Geliştirmeler ve Tedarik	5.1 İşletim Sistemi Sıkılaştırma	5.2 Veri Tabanı Sıkılaştırma	5.3 Sunucu Sıkılaştırma
CMMC v1.0		+	+	+			
ISO 27001:2017	+	+	+	+			
CIS Controls v7.1		+	+	+			
Cloud Controls Matrix 3.0.1	+		+	+			
NIST 800-53			+				
OWASP Application Security Verification Standard 4.0			+				
OWASP Mobile Application Security Verification 1.1.4			+				
TÜBİTAK BİLGEM Güvenli Yazılım Geliştirme Kılavuzu 1.1			+				
Mobile Application Security Checklist 1.1			+				
OWASP IoT Security Guidance			+				
NIST 800-82			+				
CIS Benchmark					+	+	+
ENISA Security Aspects of Virtualization							+
NIST 800-125							+
Ubuntu Server Guide - Security					+		
Oracle Linux 7 Security Guide					+		
DISA STIG - Canonical Ubuntu 16.04 LTS Security Technical Implementation Guide					+		
DISA STIG - Red Hat Enterprise Linux 7 Security Technical Implementation Guide					+		
Red Hat Enterprise Linux 8 Security Hardening					+		

EK-C: BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ KAPSAMINDA KULLANILACAK FORMLAR, ŞABLONLAR VE ÖRNEK DOKÜMANLAR

EK-C.1: VARLIK GRUBU KRİTİKLİK DERECELENDİRME ANKETİ

Bu anket, Rehber'de yer alan varlık grubu ana başlıkları altında yer alan ve Kurum tarafından belirlenen tüm varlık grupları için tek tek doldurulmalıdır.

Varlık Grupları Tanımlanırken Dikkat Edilecek Hususlar:

Kurum bilgi güvenliği yönetim sistemi kapsamında yer alan varlıkların, aşağıda listelenen altı varlık grubu ana başlığı altında gruplandırılması gerekmektedir.

1. Ağ ve Sistemler
2. Uygulamalar
3. Taşınabilir Cihaz ve Ortamlar
4. IoT Cihazları
5. Personel
6. Fiziksel Mekânlar

Aşağıda varlık grubu ana başlıkları altında bulunabilecek varlıklara örnekler verilmektedir. Varlık grubu ana başlıkları altında yer alan varlıklar gruplandırılarak bir veya daha fazla sayıda varlık grupları tanımlanmalıdır. Bu kapsamda varlık grubunda yer alan varlıkların envanteri yönetilmelidir. Tüm varlıkların en az bir varlık grubunda yer alması sağlanmalıdır.

- Ağ ve Sistemler:
    - Ağ: Yönlendirici, modem, gateway, kablosuz erişim noktası, ağ erişim kontrol cihazı, 3G haberleşme cihazları, sanal ağ, iç ağ, internet ağı vb.
    - BT Sistemleri: Kullanıcı bilgisayarları, sunucular, güvenlik duvarları, saldırı tespit/önleme sistemleri vb.
    - OT Sistemleri: SCADA sistemleri, RTU (Uzak Terminal Birimi) ve PLC (Programlanabilir Mantıksal Kontrolör) vb.
- Uygulamalar: Personel yazılımı, EBYS, kurum içi portal, e-Devlet uygulaması, ana hizmet uygulaması vb.
- Taşınabilir Cihaz ve Ortamlar: Kurum bilgisine erişebilen akıllı telefon, tablet, dizüstü bilgisayar, USB bellek, taşınabilir sabit disk, CD/DVD vb.
- Nesnelerin İnterneti (IoT) Cihazları: Kamera, sensör (nem, gaz, sıcaklık) vb.
- Personel: Üst yöneticiler, idari yöneticiler, sistem yöneticileri, yazılım geliştiriciler, son kullanıcılar, altyüklenici personeli vb.
- Fiziksel Mekânlar: Merkez veri merkezi, felaket kurtarma merkezi, taşra veri merkezi, personel odası, yönetici odası, kat anahtarlarının (switch) bulunduğu odalar vb.

Anket Doldurulurken Dikkat Edilecek Hususlar

Anket, ilgili varlık grubuyla alakalı paydaşların, Kurumun sahip olduğu en yetkin personelin ve yöneticilerin katılımı ile doldurulur. Anket doldurma çalışmasında delfi metodunun kullanılması önerilir.

Ankette her bir soru için sadece bir şık işaretlenebilir. Sorular, varlık grubu içerisinde yer alan en kritik ve en etkili varlık dikkate alınarak yanıtlanmalıdır. Soruların Kurumunuzla ilişkili birden fazla doğru cevabı varsa en yüksek puanlı olan şık seçilmelidir. Cevaplandırdığınız her seçeneğin gerekçesi de ayrıntılı olarak yazılmalıdır.

Varlık Grubu No / Adı:

Varlık Grubu için Anket Soruları

A) Varlık Grubunun İşlediği Veri Açısından Değerlendirilmesi

Gizlilik Boyutu:

1. Varlık grubunuzun işlediği en kritik bilginin açığa çıkması veya yetkisiz kişiler tarafından ele geçirilmesi durumunda;
    a. Herhangi bir zarar oluşmaz, Kurum ve kişiler işlerine devam edebilir.
    b. Kurumun ya da ilgili kişilerin işlerini ve çıkarlarını etkileyecek zararlar gelir.
    c. Milli güvenlik ve ulusal çıkarlara saygınlık anlamında zararlar gelir. Söz konusu zararın telafisi mümkündür.
    d. Milli güvenlik ve ulusal çıkarlara yaşamsal zararlar gelir. Söz konusu zararın telafisi mümkün olamaz.

Bütünlük Boyutu:

2. Varlık grubunuzun işlediği en kritik bilginin içeriğinin yetkisiz kişiler tarafından değiştirilmesi durumunda;
    a. Herhangi bir zarar oluşmaz. Kurum ve kişiler işlerine devam edebilir.
    b. Kurumun ya da ilgili kişilerin işlerini ve çıkarlarını etkileyecek zararlar gelir.
    c. Milli güvenlik ve ulusal çıkarlara saygınlık anlamında zararlar gelir. Söz konusu zararın telafisi mümkündür.
    d. Milli güvenlik ve ulusal çıkarlara yaşamsal zararlar gelir. Söz konusu zararın telafisi mümkün olamaz.

Erişilebilirlik Boyutu:

3. Varlık grubunuzdaki varlıklara bağımlılığı bulunan hizmetlerde, hizmetin en yoğun olarak kullanıldığı periyodu göz önünde bulundurduğunuzda en fazla tolere edebildiğiniz devre dışı kalma süresi nedir?
    a. 24 (yirmi dört) saatten fazla
    b. 8 (sekiz) – 24 (yirmi dört) saat arası
    c. 1 (bir) – 8 (sekiz) saat arası
    d. 1 (bir) saatten az

B) Varlık Grubunun Etki Alanı Açısından Değerlendirilmesi

Etkilenen Kişi Sayısı:

4. Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı;
    a. Binden azdır.
    b. Binden fazla, 10 binden azdır.
    c. 10 binden fazla, 100 binden azdır.
    d. 100 binden fazla, 1 milyondan azdır.
    e. 1 milyondan fazladır.

Toplumsal Sonuçlar:

5. Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde karşılaşılan durum aşağıdaki sonuçlardan hangisine yol açar?
    a. Toplumsal kargaşa olmaz, yazılı görsel basına intikal etmez.
    b. Toplumsal kargaşa olmaz, fakat olay yazılı görsel basına intikal eder.
    c. Toplumsal kargaşa meydana gelir.
    d. Can kaybı meydana gelir.
    e. Diğer (a, b, c, d seçeneklerinden daha yüksek etkili bir sonuç doğurması durumu)

Kurumsal Sonuçlar:

6. Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip herhangi bir bilgi güvenliği ihlal olayı olduğunda söz konusu olayın Kuruma etkisi ne olur?
    a. Kuruma etkisi olmaz, Kurum mevcut organizasyonu ve itibarını devam ettirir.
    b. Kurumun itibarı olumsuz etkilemez, fakat bilgi güvenliği organizasyon yapısını etkiler ya da personel değişikliğine gidilir.
    c. Kurumun itibarı olumsuz etkilenir.

Sektörel Etki:

7. Varlık grubunun hizmet verdiği sektöre etkisi nedir?
    a. Varlık grubu kurumun ana fonksiyonuna/sektöre doğrudan hizmet vermemektedir.
    b. Kamu kurum ve kuruluşları ana fonksiyonlarını yerine getirir ve sektöre doğrudan hizmet eder.
    c. Düzenleyici ve denetleyici kurum ve kuruluşlar, büyük ölçekli sanayi ve ticari kurumlar, AR-GE kurumlarının ana fonksiyonlarını yerine getirir ve sektöre doğrudan hizmet eder.
    d. Enerji, su yönetimi, bankacılık ve finans, ulaştırma, elektronik haberleşme, sağlık ve milli güvenlik/savunma sektörlerindeki ana fonksiyonlardan birini yerine getirir ve sektöre doğrudan hizmet eder.

Bağımlı Varlıklar:

8. Diğer varlıkların (entegre olan diğer yazılımlar, sunucular vb.) yönetiminizdeki varlığa olan bağımlılığı göz önünde bulundurulduğunda, varlığınızın işlediği verinin (uygulanabilir durumlarda) gizlilik, bütünlük veya erişilebilirliğine zarar gelmesi durumunda;
    a. Bağımlılığı olan varlıkların çalışması etkilenmez.
    b. Bağımlı varlıkların çalışmasını etkileyecek zararlar oluşur ancak ana faaliyet devam eder.
    c. Bağımlı varlıkların çalışmasını etkileyecek zararlar oluşur ve ana faaliyette aksamalar meydana gelir.
    d. Bağımlı varlıkların çalışmasını etkileyecek zararlar oluşur ve ana faaliyet durur.
    e. Diğer (a, b, c, d seçeneklerinden daha yüksek etkili bir sonuç doğurması durumu)

Anket Özeti

Varlık Grubu No / Adı:

a) Anket çalışmasına katılan ve anketi dolduran kişilerle ilgili bilgiyi aşağıdaki tabloya yazınız.

No.	Anket Katılımcısı	Görevi / Unvanı	Birimi / Kurumu	İrtibat	Tarih
1					
2					
3					
4					
5					
6					
7					
8					
9					

b) Her soru için anket cevaplarını aşağıdaki tabloya işaretleyerek anket puanını hesaplayınız.

Boyut	Soru No.	Şıkların Puanları					Soru Puanı
		a	b	c	d	e	
İşlenen Veri Açısından							
Gizlilik	1	1 puan	2 puan	3 puan	5 puan		
Bütünlük	2	1 puan	2 puan	3 puan	5 puan		
Erişilebilirlik	3	1 puan	2 puan	3 puan	5 puan		
Etki Alanı Açısından							
Etkilenen Kişi Sayısı	4	1 puan	2 puan	3 puan	4 puan	5 puan	
Toplumsal Sonuçlar	5	1 puan	2 puan	3 puan	5 puan	6 puan	
Kurumsal Sonuçlar	6	1 puan	2 puan	3 puan			
Sektörel Etki	7	1 puan	2 puan	3 puan	5 puan		
Bağımlı Varlıklar	8	1 puan	2 puan	3 puan	5 puan	6 puan	
Anket Puanı (Tüm soruların puanlarının toplamı)							

c) Her soru için işaretlediğiniz cevap şıkkını, olası senaryoyu da belirterek, gerekçelendiriniz.

Soru No.	Açıklama/Gerekçe
1	
2	
3	
4	
5	
6	
7	
8	

d) Anket puanına göre varlık grubunun kritiklik derecesini aşağıdaki tablodan faydalanarak belirleyiniz.

Anket Puanı	Varlık Grubu Kritiklik Derecesi
Anket puanı 18'den küçük ise	Derece 1
Anket puanı 18 (dâhil) ile 28 arasında ise	Derece 2
Anket puanı 28 ve daha yüksek ise	Derece 3

e) Varlık Grubu için Kritiklik Derecelendirme Anketi sonuçlarını aşağıdaki tabloda özetleyiniz.

Varlık Grubu No/Adı			
Anket Tamamlanma Tarihi			
Anket Çalışması Koordinatörü			
Anket Puanı (Tüm soruların puanlarının toplamı)			
Varlık Grubu Kritiklik Derecesi	Derece 1	Derece 2	Derece 3

f) Anket sonuçlarını onaylayan yetkililerin bilgilerini yazınız.

Anket Sonucu Onay Tarihi	
Anket Sonuçlarını Onaylayan Yetkili	
Anket Sonuçlarını Onaylayan Yetkilinin İmzası	

EK-C.2: VARLIK GRUBU VE KRİTİKLİK DERECESİ TANIMLAMA FORMU

Varlık grubunda yer alan tüm varlıklar göz önünde bulundurularak, varlık grubu ile ilişkili uygulama ve teknoloji alanlarına yönelik uygulanması gereken güvenlik tedbirleri ile ilgili sıkılaştırma tedbirleri, varlık grubu kritiklik derecesi ile birlikte aşağıdaki tabloda kayıt altına alınmalıdır.

Varlık Grubu Ana Başlığı	**Varlık Grubu No**	**Varlık Grubu Adı**	**Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların Uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)						**Sıkılaştırma Tedbirleri** (Her varlık grubu için aşağıdaki başlıkların Uygulanabilir (U) / Uygulanabilir Değil (UD) olduğunu belirtiniz.)			**Kritiklik Derecesi (Derece 1/ Derece 2/ Derece 3)**
			Kişisel Verilerin Güvenliği	**Anlık Mesajlaşma Güvenliği**	**Bulut Bilişim Güvenliği**	**Kripto Uygulamaları Güvenliği**	**Kritik Altyapılar Güvenliği**	**Yeni Geliştirmeler ve Tedarik**	**İşletim Sistemi Sıkılaştırma Tedbirleri**	**Veri Tabanı Sıkılaştırma Tedbirleri**	**Sunucu Sıkılaştırma Tedbirleri**	
Ağ ve Sistemler												
Uygulamalar												
Taşınabilir Cihaz ve Ortamlar												
Nesnelerin İnterneti (IoT) Cihazları												
Fiziksel Mekânlar												
Personel												

EK-C.3: MEVCUT DURUM VE BOŞLUK ANALİZ FORMU

Her bir varlık grubu için tedbir maddelerinin uygulanıp uygulanmadığı Uygulama Durumu açıklamaları dikkate alınarak belirlenmelidir. Mevcut duruma yönelik açıklamalar detaylı olarak belirtilmelidir. Ayrıca ilgili varlık grubu için hedeflenen duruma ulaşılması amacıyla yapılması gereken çalışmalar aşağıdaki tabloda kayıt altına alınmalıdır.

- Tedbir varlık grubunda yer alan tüm varlıklara uygulanmakta ise “tamamen”(T)
- Tedbir varlık grubunda yer alan varlıkların çoğuna uygulanmakta fakat bazı varlıklara kısmen uygulanmakta veya henüz uygulanmamakta ise “çoğunlukla” (Ç)
- Tedbir varlık grubunda yer alan bir kısım varlığa uygulanmakta veya tedbir kısmen uygulanmakta ise “kısmen”(K)
- Tedbir hiç uygulanmamakta ise “hiç” (H)
- Tedbirin teknik olarak uygulanma ihtimali bulunmuyorsa “uygulanamaz”(UD)

Varlık Grubu Adı / Kodu:	

Tedbir No	Uygulanma Durumu * (T/Ç/K/H/UD)	Mevcut Duruma Yönelik Açıklama	Hedeflenen Durum (T/Ç/K/H/UD)	Telafi Edici Kontrol ** (Tedbirin Birebir Uygulanamadığı Durumda)	Hedeflenen Durum İçin Yapılması Gereken Çalışmalar

* Varlık gruplarının mevcut durum ve boşluk analizi kapsamında belirlenen çalışmalar yazılmalıdır.

** Tedbir için telafi edici kontrol tanımlanması gerekiyorsa EK-C.5 formu doldurulur ve kontrol formunun numarası bu bölüme girilir.

EK-C.4: REHBER UYGULAMA YOL HARİTASI BELİRLEME FORMU

Mevcut durum ve boşluk analizi kapsamında yapılan çalışmalar göz önünde bulundurarak yapılması gereken iş paketleri ve bu kapsamda yapılacak 3 - 24 aylık çalışmalar aşağıdaki tabloda kayıt altına alınmalıdır.

İş Paketi No	İş Paketi Adı	İş Paketinin Kapsadığı Faaliyetler	İş Paketi Hedefleri	
			3.Ay	
			6.Ay	
			9.Ay	
			12.Ay	
			15.Ay	
			18.Ay	
			21.Ay	
			24.Ay	

EK-C.5: TELAFİ EDİCİ KONTROL KAYIT FORMU

Kurum, boşluk analizi sonucunda uygulanması gereken ilave tedbirler kapsamındaki herhangi bir gereksinimi; üst yönetim tarafından onaylanmış teknik kısıtlamalar ve iş gereksinimlerinden dolayı rehberde tanımlandığı şekli ile karşılayamaması durumunda telafi edici kontroller uygulamalıdır. Telafi edici kontroller, yerine uygulandıkları tedbir maddeleri ile aynı amaç ve etkiye sahip olmaları durumunda kullanılabilir olarak kabul edilecektir. Tedbir maddesi ile ilgili gereklilikleri karşılamak amacıyla kullanılan her bir telafi edici kontrolü tanımlamak için aşağıdaki form kullanılmalıdır.

TELAFİ EDİCİ KONTROLE YÖNELİK BİLGİ		AÇIKLAMA
Telafi Edici Kontrolün Numarası	Telafi edici kontrole ait numara bilgisi	
Telafi Edici Kontrolün Tanımı	Güvenlik tedbir maddesi yerine uygulanan telafi edici kontrolün tanımının yapıldığı alan	
Telafi Edici Kontrolün Niteliği (Geçici / Kalıcı)	Telafi edici kontrolün geçici ya da kalıcı nitelikte olduğunun tanımlandığı alan	
Telafi Edici Kontrolün Geçici Olması Durumunda Planlanan Uygulama Zaman Aralığı	Telafi edici kontrolün geçici nitelikte olması durumunda, kontrolün planlanan uygulama zaman aralığı	
İlişkili Güvenlik Tedbiri Madde Numarası	Telafi edici kontrolün hangi güvenlik tedbiri yerine uygulanacağının tanımlandığı alan	
İlişkili Güvenlik Tedbiri Gereklilikleri	Telafi edici kontrolün ilişkili olduğu güvenlik tedbir maddesinin gerekliliklerinin tanımlandığı alan	
İlişkili Güvenlik Tedbirinin Uygulanamamasından Kaynaklanan Riskler	Güvenlik tedbir maddesinin uygulanmaması durumunda ortaya çıkacak risklere yönelik açıklamaların yapıldığı alan	
İlişkili Güvenlik Tedbirinin Uygulanamamasının Gerekçeleri	Güvenlik tedbir maddesinin mevcut durumda uygulanamamasının nedenlerinin, uygulama kısıtlarının ve gerekçelerinin tanımlandığı alan	
Telafi Edici Kontrolün Doğrulama Yöntemi	Telafi edici kontrolün etkinliği ve yeterliliğine yönelik yapılan doğrulama ve test faaliyetlerinin açıklandığı alan	

EK-C.6: TAAHHÜTNAME ÖRNEĞİ

İşbu taahhütname, 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi'nin 12. maddesinde yer alan hükme dayanılarak hazırlanmıştır.

1. Tanımlar ve Kısaltmalar

İşbu taahhütnamede geçen;

1.1. "Arka kapı", Uygulama yazılımı, donanım ve işletim sistemleri veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistemlerde mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıklarını,

1.2. "Dağıtıcı", Bir üreticiye ait olan ürünlerin belirli bölgelerde tanıtımı ve satışını sağlamakla yetkili tüzel kişiyi,

1.3. "Kurum", …… adresinde faaliyet göstermekte olan …….. Kurumu'nu,

1.4. "Tedarikçi", tedarik zincirinde yer alan, üretici ve dağıtıcı dışındaki tüzel kişiyi,

1.5. "Üretici", ürünü üreten, imal eden veya ürüne adını, ticari markasını veya ayırt edici işaretini koyan tüzel kişiyi,

1.6. "Ürün", Kurum tarafından tedarik edilmesi planlanan uygulama yazılımı, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistemi,

1.7. "Şirket", işbu taahhütnamede yer alan yükümlülüklerden sorumlu üretici, dağıtıcı veya tedarikçiyi

ifade etmektedir.

2. Ürün Özellikleri

Üretici	
Ürünün Markası	
Ürünün Adı	
Ürünün Modeli	
Ürün Üzerindeki Yazılımlara Ait Versiyon Bilgisi	
Ürünü Kapsayan Ulusal/Uluslararası Standartlar	

3. Yükümlülükler

3.1. İşbu taahhütnamenin 2. maddesinde özellikleri belirtilen ürünün, Kurum yetkililerinin bilgisi ve izni olmadan; ürünü veya ürün içerisindeki herhangi bir bileşeni devre dışı bırakmak, yetkisiz kod çalıştırmak, ürün içerisindeki verilere erişim sağlamak, verileri silmek ya da bütünlüğünü bozmak amacıyla tasarlanmış herhangi bir arka kapı bulunmadığını,

3.2. Ürüne bakım, onarım ve garanti süreci dâhil olmak üzere tüm yaşam döngüsü süresince şirket tarafından sunulan yama ve güncellemeler ile yeni versiyonların kurulum ve yönetim süreçlerinde işbu taahhütnamenin 3.1. maddesinde yer alan hükümlere herhangi bir uygunsuzluk olmayacağını,

3.3. Yukarıda beyan ve taahhüt edilen yükümlülüklere uyulmadığı ve/veya Kurum tarafından, verdiğimiz bilgilerde gerçeğe aykırı durumların saptanması halinde, Kurum tarafından bu konuda alınacak kararlara uyacağımızı ve uygulanacak yaptırımların tarafımıza doğrudan uygulanma kabiliyeti bulunduğunu kabul ve taahhüt ederiz.

4. Muhtelif Hükümler

4.1. İşbu taahhütnamede yer almayan hususlarda Türkiye Cumhuriyeti mevzuat hükümleri uygulanacaktır.

4.2. İşbu taahhütnameden kaynaklanan uyuşmazlıklarda yalnız …….. Mahkemeleri yetkili olacaktır.

4.3. İşbu taahhütnamenin hükümlerinden biri ya da birkaçının kısmen veya tamamen geçersiz addedilmesi, taahhütnamenin kalan hükümlerinin geçerliliğine etki etmeyecektir.

4.4. İşbu taahhütname kapsamında şirkete yapılacak bildirim, tebligat ve diğer haberleşme yöntemlerinde aşağıda şirket yetkilileri tarafından beyan edilen adres(ler) ve diğer iletişim bilgileri geçerlidir. Şirket adres değişikliklerini derhal noter yolu ile Kurum'a bildirmek zorundadır. Aksi halde taahhütnamede belirtilen adreslere yapılan tebligatlar geçerli olacaktır.

4.5. İşbu taahhütname şirketi temsil ve ilzama yetkili kişiler tarafından imzalanmış olup imza tarihi itibarıyla ……. (süresince) yürürlükte kalacaktır.

Taahhütte Bulunan Şirketin

Unvanı:

Adresi:

Telefon / Faks:

Vergi Dairesi:

Vergi Numarası:

Ticaret Sicil Numarası:

Tedarik Zincirindeki Rolü: ☐ Üretici ☐ Dağıtıcı ☐ Tedarikçi

Taahhütte Bulunan Şirketi Temsil ve İlzama Yetkili Kişi(ler)

İmza Tarihi:

Yetkili Kişi Ad – Soyad	Yetkili Kişi Ad – Soyad	Yetkili Kişi Ad – Soyad
Kaşe/İmza	Kaşe/İmza	Kaşe/İmza

BİLGİ ve İLETİŞİM GÜVENLİĞİ REHBERİ