TÜRKİYE CUMHURİYETİ
CUMHURBAŞKANLIĞI
SİBER GÜVENLİK
BAŞKANLIĞI

SİBER OLAY MÜDAHALE SÜREÇLERİNDE TESPİT EDİLEN YAYGIN EKSİKLİKLER

MAYIS 2026

BELGE ADI: Siber Olay Müdahale Süreçlerinde Tespit Edilen Yaygın Eksiklikler

SÜRÜM NO: 1.0

SÜRÜM TARİHİ: 20.05.2026

GİZLİLİK DERECESİ: Tasnif Dışı

Değişiklik No	Değişiklik Tarihi	Değişiklik Nedeni
1.0	Mayıs 2026	İlk Yayın

İçindekiler Tablosu

1. POLİTİKA VE PROSEDÜRLER

Bu bölüm, Başkanlığın siber olay müdahalesi esnasında politika ve/veya prosedür eksikliği ile bunlara karşılık yapılması gereken işlemleri ve alınabilecek tedbirleri içermektedir. Genel olarak aşağıda belirtilen maddelerde; standartların belirlenmemesi sonucu personelin kendi yetenekleriyle veya yöneticilerin sözlü talimatlarıyla sistemi yönetmesi neticesinde ve ilerleyen zamanlarda bu personelin iş akdinin sonlanması durumunda iş sürekliliğinin aksadığı veya kurumsal hafızanın yok olduğu görülmektedir.

No.	Detay
1.1	**Sistem yönetimine dair politikaların hazırlanmaması** **Değerlendirme Soruları** **1.** Sistem güvenlik dokümanı hazırlanmış mı? **2.** Sistem güvenlik dokümanı, sistem yönetiminde sistem yöneticisinin inisiyatifine yer bırakmayacak şekilde detaylandırılmış mı? **3.** Hesap oluşturma, parola sıfırlama, erişim izni verilmesi gibi tüm sistem ayar değişiklikleri onay mekanizmasına tabi tutuluyor mu? **4.** Sistemde yapılan tüm değişiklikler kayıt altına alınıyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi esnasında sistem yönetimine dair herhangi bir doküman hazırlanmadığı, yönetimin tamamen sözlü olarak yapıldığı görülmüştür. Başka bir siber olay müdahalesinde ortak kullanılan hesapların mevcut olduğu görülmüştür. Hesap ile gerçekleştirilen şüpheli aktivitelerin hangi personel tarafından uygulandığını tespit etmek süreci uzatmıştır. **Tedbirler:** Sistem işleyiş ve yönetim standartları belirlenerek "Sistem Güvenlik Dokümanı"nda yazı altına alınmalı, ilgili personele tebliğ edilmelidir. Örneğin "Ortak Hesap" kullanılmayacağı prensip olarak belirlenerek yazı altına alınmalıdır. Diğer bir örnek ise oluşturulacak kullanıcı hesap adlarında notasyon belirlenmeli ve standart hâle getirilmelidir. Ayrıca "Kabul Edilir Kullanıcı Politikası" oluşturulmalı ve kullanıcılara, kendilerine teslim edilen bilişim cihazları-yazılımları ile neler yapabilecekleri ve neler yapamayacakları bildirilmelidir.

No.	Detay
1.2	**Sistem yönetimine dair prosedürlerin hazırlanmaması** **Değerlendirme Soruları:** **1.** Bir personelin işten ayrılması veya tayin olması durumunda yapılması gerekenler belirlenip yazılı hâle getirilmiş mi? **2.** Sisteme yeni bileşen eklendiğinde yapılacaklar belirlenerek yazılı hâle getirilmiş mi? **3.** Kullanım ömrü sona eren bilişim cihazlarına uygulanacak işlemler belirlenerek yazılı hâle getirilmiş mi? **Karşılaşılan Durum:** Siber olay müdahalesi esnasında daha önce oluşturulmuş, standart olmayan birtakım kullanıcı hesaplarının ne amaçla oluşturulduğu ve kimlere ait olduğunun bilinmediği görülmüştür. Başka bir siber olay müdahalesinde işten ayrılan personelin hesaplarında aktivite tespit edilmiş, ayrıca ayrılan personel tarafından kullanılan bazı parolaların değiştirilmediği görülmüştür. **Tedbirler:** Sistem güvenliğini sağlama amacıyla öngörülebilir durumlar karşısında alınacak aksiyonlar belirlenmelidir. • Bir personel işyerinden ayrıldığında, • Sisteme yeni bir bileşen eklendiğinde, • Sistemde bir cihaz arızalandığında ve benzeri durumlarda yapılması gerekenler belirlenerek yazılı hâle getirilmelidir.

2. AĞ GÜVENLİĞİ

Bu bölüm, Başkanlığın siber olay müdahaleler esnasında ağ güvenliği tarafında karşılaştığı eksik ve yanlış durumlar ile bunlara karşılık yapılması gereken işlemleri ve alınabilecek tedbirleri içermektedir. Genel olarak aşağıda belirtilen maddelerin ağ cihazlarındaki yapılandırma eksikliklerinden kaynaklandığı görülmektedir.

No.	Detay
2.1	**VLAN'lar arası erişim kısıtlamalarının yapılmaması** **Değerlendirme Soruları:** **1.** Kurumsal ağda VLAN yapısı mevcut mu? **2.** Birimler arası VLAN'lar için servis (RDP, SMB, VNC vb.) bazında erişim kısıtlaması yapıldı mı? **Karşılaşılan Durum:** Siber olay müdahalesi esnasında kurum ağında VLAN yapısının varlığı görülmüş, ancak yapılandırma kontrolü sonucunda tüm VLAN'ların birbirleriyle kontrolsüz olarak haberleştiği tespit edilmiştir. **Tedbirler:** Kurum ağında VLAN yapısı yoksa oluşturulması ve VLAN'lar arası erişim ihtiyacı varsa kontrollü bir şekilde sağlanması gerekmektedir.
2.2	**Misafir, VOIP gibi güvensiz kablosuz ağlardan iç ağlara erişim yapılabilmesi** **Değerlendirme Soruları:** **1**. Kuruma gelen misafirler için ayrı oluşturulan bir ağ var mı? **2**. Misafirlerin internete erişimi için oluşturulan ağdan kullanıcı ve sunucu ağlarına erişim kısıtlandı mı? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında kurumun misafir kablosuz ağından iç ağına (kullanıcı ve sunucu ağı) erişilebildiği tespit edilmiştir. **Tedbirler:** Misafir ağından kurumun iç ağına hiçbir şekilde erişilmemesi gerekmektedir. Mümkünse misafir ağının ayrı bir hat üzerinden internete erişiminin sağlanması gerekmektedir.

No.	Detay
2.3	**Sunucu ağlarının internete kontrolsüz erişimi** **Değerlendirme Soruları:** **1.** İç ağda bulunan sunucuların internete çıkış yönündeki trafiği güvenlik duvarı üzerinde kısıtlandı mı? **2.** Kurumsal ağda 3 katmanlı mimari modeli uygulanıyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında web ve veritabanı sunucularının herhangi bir kontrol olmaksızın internete erişebildiği görülmüştür. **Tedbirler:** DMZ ağında bulunan sunucuların çıkış yönündeki internet trafiğinin güvenlik cihazları üzerinde engellenmesi gerekmektedir. Ayrıca 3 katmanlı mimarinin uygulanması önerilmektedir. Bu mimaride, ilk katman DMZ ağı, ikinci katman uygulama sunucuları, üçüncü katman ise veritabanı sunucuları olarak düşünülebilir. Bu tanıma göre 2. ve 3. katmanda bulunan sunucuların internete erişiminin olmaması gerekmektedir. Sunucuların güncelleme ihtiyaçlarına karşılık iç ağda "WSUS" sunucu uygulaması kurularak gerekli güncellemeler temin edilebilir.
2.4	**İstemcilerin internete kontrolsüz erişimi** **Değerlendirme Soruları:** **1.** İstemcilerin internet erişimi sınırlandırılmış mı? **2.** İstemcileri zararlı olduğu bilinen sitelere erişimi engellenmiş mi? **3.** İstemcilerin indirdikleri dosyalar ağ veya istemci tabanlı olarak güvenlik taramasına tabi tutuluyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında istemcilerin internet trafiğinin filtrelenmediği, dosya indirmelerinde istemci üzerinde ya da ağ tabanlı herhangi bir inceleme yapılmadığı tespit edilmiştir. Böylelikle kullanıcı tarafından yanlış bir linke tıklanması ve güvenilir olmayan kaynaktan dosya indirilerek açılması sonucunda istemci bilgisayara erişim sağlayan siber saldırgan, diğer ağ cihazlarına saldırı yapma imkânı bulmuştur. **Tedbirler:** İstemci cihazların internet trafiği güvenlik filtrelemesine tabi tutulmalıdır. Başkanlık tarafından yayımlanan zararlı adreslere erişim engellenmelidir.

No.	Detay
2.5	**Kurum iç ağına uzaktan erişimlerin uzun süreli / süresiz tanımlanması** **Değerlendirme Soruları:** **1.** İnternetten kurum iç ağına güvenli erişim için kullanılan bir protokol (SSLVPN, 3. parti yazılım vb.) var mı? **2.** Kurumsal ağa erişim sağlayan kişilere tanımlanan oturum süresi iş ihtiyacına göre mi belirleniyor? **3.** Kurumsal ağa SSLVPN ile yapılan erişimlerde 2 faktörlü doğrulama kullanılıyor mu? **4.** Kurumsal ağa erişim sağlayan kişilere tanımlanan oturum süresinin azami sınırı nedir? Sınırsız oturum süresine sahip bir kullanıcı var mı? **Karşılaşılan Durumlar:** **1.** Siber olay müdahalesi sırasında SSLVPN ile kurum iç ağına sağlanan erişimin kullanıcılara süresiz olarak tanımlandığı görülmüştür. **2.** Siber olay müdahalesi sırasında kullanıcı erişim bilgilerini ele geçiren siber saldırganın yurt dışı IP adresinden SSLVPN bağlantısı kurduğu görülmüştür. **3.** Siber olay müdahalesi sırasında SSLVPN sunucusu üzerinde zayıf ve sabit parola ile statik SSLVPN hesabı oluşturulduğu görülmüştür. **Tedbirler:** Kurumun iç ağına uzaktan erişim için tanımlanan SSLVPN bağlantılarının kontrolü için oturum süre sınırı tanımlanması, iki faktörlü doğrulama uygulanması ve gerekmiyorsa yurt dışı bağlantıların engellenmesi gerekmektedir.
2.6	**Yalıtılması gereken yerel ağların diğer ağlara bağlanması** **Değerlendirme Soruları:** **1.** "Çok Gizli" derecesine sahip bilgilerin işlendiği cihazlar mevcut mudur? **2.** Yazılım geliştirme ağı gibi izole edilmesi gereken ağlar için yeterli önlemler alınmış mı? **Karşılaşılan Durum:** Siber olay müdahalesi esnasında işlenen verinin hassasiyeti itibariyle fiziksel olarak izole edilmesi gereken ağların, farklı gerekçelerle internet ağına bağlandığı görülmüştür. Başka bir siber olay müdahalesinde yazılım geliştirme ağının, istemciler tarafından erişilebilir olduğu tespit edilmiştir. **Tedbirler:** Yerel ağlar, oluşturulma amacı ve işlenen verinin hassasiyeti gibi kriterlere göre dereğerlendirilmeli ve gereken şartlarda izolasyonu sağlanmalıdır. Bu ağlara bağlantı kurmanın zorunlu olduğu durumlarda yerli teknoloji "Sanal Hava Boşluğu" veya "Veri Diyotu" ve benzeri önlemler entegre edilerek iletişimin sınırlandırılması güvenliği artıracaktır.

No.	Detay
2.7	**Firma-Kurum yerleşkesinde firma-kurum tarafından yönetilmeyen ağ(lar) bulunması** **Değerlendirme Soruları:** **1.** Yerleşke içerisinde kurum-kuruluş tarafından yönetilmeyen ağ bulunmakta mıdır? (Kurum-kuruluş sadece kendisine ait bir yerleşkede bulunuyorsa) **2.** Kablosuz ağ saldırılarına karşı önlem alınmış mı? (Kurum-kuruluş sadece kendisine ait bir yerleşkede bulunmuyorsa) **Karşılaşılan Durumlar:** **1.** Siber olay müdahalesi sırasında kendisine tahsisli yerleşkede konuşlu kurumun sınırları içerisinde çalışanların bağlı bulunduğu sendikaya ait kablosuz yayın yapan bir ağ olduğu görülmüştür. **2.** Siber olay müdahalesi sırasında kritik sektörde alt yüklenici olarak faaliyet gösteren bir firmanın alt katında halka açık kafeterya bulunduğu, ayrıca firma içerisinde tüm bilişim altyapısının kablosuz ağ teknolojisiyle oluşturulduğu görülmüştür. **Tedbirler:** Yerleşke içerisinde kurum-kuruluş tarafından yönetilmeyen ağlar bulunmaması gerekmektedir. Eğer kurum-kuruluş dışından kablosuz ağ erişim mesafesinde dış birim var ise kablosuz iletişim teknolojileri tercih edilmemeli ya da katı sıkılaştırmalar uygulanmalı ve kablosuz ağ saldırılarına karşı direnç oluşturulmalıdır.
2.8	**Güvenlik cihazlarının ve uygulamalarının varsayılan ayarlarda kullanılması** **Değerlendirme Soruları:** **1.** Sistemde kullanılan istemci veya ağ tabalı tüm güvenlik yazılımları ve cihazları sadece gereken izinler verilerek ve sadece iş süreçlerinin yürütülmesini sağlayacak kadar sıkılaştırılmış mı? **2.** Güvenlik ürünlerinde mevcut varsayılan hesaplar mümkünse devre dışı bırakıldı mı? Mümkün değilse parolaları değiştirildi mi? **Karşılaşılan Durumlar** **1.** Siber olay müdahalesi esnasında güvenlik cihazları üzerinde mevcut varsayılan hesapların aktif ve varsayılan parola ile bırakıldığı görülmüştür. **2.** Siber olay müdahalesi esnasında kuruluş tarafından büyük meblağlar karşılığı satın alınan güvenlik duvarının varsayılan ayarlarda bırakıldığı ve filtreleme yapmadığı tespit edilmiştir. **Tedbirler:** Temin edilen güvenlik cihazlarında varsayılan hesaplar mümkünse devre dışı bırakılmalı, mümkün değilse parolaları değiştirilmelidir. Yönetim sanal ağı oluşturulmalı ve güvenlik cihazlarının yönetim arayüzlerine sadece bu ağdan erişim sağlanmalıdır. Temin edilen güvenlik cihazlarında kullanılmayan tüm servisler devre dışı bırakılmalı, kullanılan servisler ise sıkılaştırılmalı ve ayrıntılı olarak amacına uygun konfigüre edilmelidir.

3. SİSTEM GÜVENLİĞİ

Bu bölüm, Başkanlığın siber olay müdahaleler esnasında sistem güvenliği tarafında karşılaştığı eksik ve yanlış durumlar ile bunlara karşılık yapılması gereken işlemleri ve alınabilecek tedbirleri içermektedir. Genel olarak aşağıda belirtilen maddelerin son kullanıcı ve sunucu sistemleri üzerindeki yapılandırma eksikliklerinden kaynaklandığı görülmektedir.

No.	Detay
3.1	**Domain admin gibi yüksek yetkili kullanıcıların sunucu ve kullanıcı bilgisayarlarında kullanılması** **Değerlendirme Soruları:** **1.** Domain Admin grubundaki kullanıcılar ile kullanıcı ve sunucu sistemlerine uzak masaüstü bağlantısı (RDP) yapılıyor mu? **2.** Yönetimsel ihtiyaçlar için Domain Admin grubundaki kullanıcılar haricinde farklı kullanıcılar mevcut mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında domain admin grubunda bulunan kullanıcı hesaplarından birçok sunucuya giriş yapıldığı tespit edilmiştir. Bu durumdan yararlanan saldırganların, sunucu üzerinden domain admin kullanıcısının yetkileri yardımıyla iç ağda yayıldığı gözlemlenmiştir. **Tedbirler:** Domain Admin grubunda bulunan kullanıcılar ile herhangi bir kullanıcı veya sunucu sistemine bağlantı (SMB, RDP) yapılmaması gerekmektedir. Bağlantıların, domain admin kullanıcı grubunda olmayan bir kullanıcı üzerinden sağlanması ve yönetimsel ihtiyaçlar Domain Admin grubundaki kullanıcılar haricinde eklenecek yeni bir kullanıcıya iş ihtiyacına göre (Diğer sistemlere uzak bağlantı için RDP ve SMB gibi) yetki verilmesi gerekmektedir.
3.2	**DMZ'teki sunucuların etki alanında bulunması** **Değerlendirme Soruları:** **1.** DMZ ve benzeri dışa açık ağlarda kullanılan sunucularda domain yapısı var mı? **2.** DMZ ağında bulunan sunucular yerel ağda bulunan sunucular ile aynı etki alanı içerisinde mi? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında saldırgan, DMZ ağında bulunan bir sunucudaki kod çalıştırma zafiyetinden faydalanıp, kullanıcı ve diğer sunucuların da içinde bulunduğu domain içerisinde sızdığı gözlemlenmiştir. Bu durumdan yararlanan saldırgan domainde bulunan diğer sistemlere bağlantı sağlayabilmiştir. **Tedbirler:** DMZ ağında bulunan sunucuların iç ağda kullanıcı ve yerel sunucuların yönetimi için kullanılan domainden ayrı bir yapıda (lokal olarak veya DMZ ağında bulunan sunucular için oluşturulan ayrı bir domain içerisinde) kullanılması gerekmektedir.

No.	Detay
3.3	**Yedeklerin aynı sunucu üzerinde saklanması** **Değerlendirme Soruları:** **1.** Sunucuların yedekleri düzenli olarak alınıyor mu? **2.** Sunucuların yedekleri aynı sunucu üzerinde mi saklanıyor? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında sunucu üzerinden alınan veritabanı yedeklerinin yine aynı sunucu üzerinde saklandığı görülmüş dolayısıyla saldırganın mevcut yedekleri sildiği tespit edilmiştir. **Tedbirler:** Sunucu üzerinden alınan yedeklerin farklı bir sunucu üzerinde saklanması gerekmektedir. Verilerin en az iki kopyası olmalı.
3.4	**Windows kullanıcı ve sunucu sistemleri üzerinde varsayılan olarak gelen "administrator" kullanıcısının aktif olması** **Değerlendirme Soruları:** **1.** Varsayılan Administrator hesabı aktif mi? **2.** Sunucular üzerindeki Lokal Admin yetkisine sahip kullanıcıların parolaları birbirinden farklı mı? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında saldırganların komut çalıştırabildiği Windows sunucu üzerinde varsayılan "Administrator" kullanıcısının aktif olduğu görülmüştür. Ayrıca bu kullanıcının diğer sunucu sistemleri üzerinde de aktif olduğu ve aynı parolaya sahip olduğu tespit edilmiştir. **Tedbirler:** Varsayılan "Administrator" kullanıcısının pasif hale getirilmesi ve sistemler üzerinde yeni bir lokal admin kullanıcısının tanımlanması gerekmektedir. Ayrıca her sistem üzerindeki lokal admin kullanıcılarının farklı parolaya sahip olması gerekmektedir. Lokal admin yetkisine sahip kullanıcıların her sistemde farklı bir parola ile kullanılması için Microsoft LAPS (Local Admin Password Solution) uygulaması kullanılabilir.
3.5	**Veritabanı servisinin yönetici grubunda bulunan kullanıcı ile çalıştırılması** **Değerlendirme Soruları:** **1.** Veritabanı servisi yönetici grubundaki bir kullanıcı yetkisi ile mi çalışıyor? **2.** Yönetici yetkisi gerekmeyen fakat yönetici yetkisi ile çalışan servisler mevcut mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında saldırganın uygulamadaki SQL enjeksiyonu zafiyetini tetikleyip MSSQL xp_cmdshell özelliğini kullanarak ve MSSQL veritabanı kullanıcısının sistem yetkisi ile çalışmasından faydalanarak sisteme yeni bir kullanıcı eklemiş ve bu kullanıcıyı admin haklarına yükseltmiştir. **Tedbirler:** Servisleri çalıştıran kullanıcılar iş ihtiyaçlarına göre minimum yetki ilkesine göre belirlenmelidir. Örnek olarak MYSQL servisinin root, MSSQL servisinin NT AUTHORITY\SYSTEM kullanıcıları ile çalıştırılmaması gerekir.

No.	Detay
3.6	**Domain istemcilerinde yerel admin hesabının sabit parola ile bırakılması** **Değerlendirme Soruları:** **1.** Windows domain'ine dahil edilen cihazlarda bulunan "Yerel Admin" hesabının parolasının sürekli değişmesi için önlem alındı mı? **2.** Linux cihazlarda "root" hesabı ile oturum açılması engellendi mi? Parola değiştirme politikası uygulandı mı? **3.** Servislerin zorunlu olmadıkça yönetici yetkisini kullanmaması prensip olarak uygulanıyor mu? Yönetici yetkisi gerekli servislere ayrı birer hesap tahsis edilmiş mi? **Karşılaşılan Durum:** Siber olay müdahalesinde Windows domainde bulunan tüm istemci ve sunucuların (DC hariç) yerel admin hesaplarının aynı ve sabit olacak şekilde ayarlandığı görülmüştür. Başka bir siber olay müdahalesinde yönetici yetkileri ile çalışması gereken servise "root" hesap bilgileri tanımlandığı tespit edilmiştir. **Tedbirler:** Windows domainlerde sysinternals araçlarından LAPS (Local Admin Password Solution) kullanılarak yerel admin parolalarının belirli periyotlarla değişmesi sağlanmalıdır. Linux cihazlarda "root" hesabı ile oturum açılabilmesi ve SSH bağlantısı kurulabilmesi engellenmelidir. Gerekli durumlarda sadece belirli kullanıcıların "su" yetkisi ile işlem yapabilmesine izin verilmelidir. Çalışabilmesi için yönetici yetkisi verilmesi zorunlu olans servisler için ayrı birer servis hesabı tanımlanmalıdır. Bu hesap ile yapılan işlemler ayrıca takip edilmelidir.
3.7	**Sistem kullanıcılarının siber güvenlik farkındalıklarının eksik olması** **Değerlendirme Soruları:** **1.** Kullanıcıların-personelin farkındalık seviyelerini tespit edici ve artırmaya yönelik faaliyetler yürütülmekte midir? **2.** Kuruluşun kurum-şirket e-posta hesabı ile kişisel işlemler için sitelere kayıt olan kullanıcı var mı? **Karşılaşılan Durum:** Kullanıcıların farklı platformlara şirket hesabı ile kayıt olması sonucu ilgili platformlarda yaşanan veri sızıntısı durumunda şirkete ait e-posta hesapları ifşa olmaktadır. Kullanıcıların aynı parolayı birden fazla platformda kullanması sonucu ifşa olan kullanıcı adları ile şirket platformunda saldırganlar oturum açabilmek için gerekli tüm bilgiye erişmiş olmaktadırlar. **Tedbirler**: Personele belirli periyotlarla farkındalık eğitimi verilmelidir. Periyodik olmayan zamanlarda oltalama e-posta ve SMS'leri gönderilerek personelin farkındalık derecesi ölçülmelidir. Kurumsal e-posta adreslerine sosyal medya veya alışveriş siteleri benzeri platformlardan gelen e-postalar filtrelenmeli ve iletilmemelidir.

4. UYGULAMA GÜVENLİĞİ

Bu bölüm, Başkanlığın siber olay müdahalesi esnasında uygulama güvenliği tarafında karşılaştığı eksik ve yanlış durumlar ile bunlara karşılık yapılması gereken işlemleri ve alınabilecek tedbirleri içermektedir. Genel olarak aşağıda belirtilen maddelerin uygulama geliştirilirken güvenli yazılım geliştirme yaşam döngüsüne uyulmadığından kaynaklandığı görülmektedir.

No.	Detay
4.1	**Versiyon kontrol sistemi bulunmaması** **Değerlendirme Soruları:** **1.** Yazılım geliştirme sürecinde kaynak kodları herhangi bir versiyon kontrol sisteminde tutuluyor mu? **2.** Yazılımın herhangi bir kısmında yapılan değişiklikten sonra versiyon kontrol sistemindeki kaynak kodu güncelleniyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında yazılım geliştirilirken herhangi bir versiyon kontrol sisteminin (SVN, Git vb.) kullanılmaması, meydana gelen problemin kaynak koddaki hangi değişiklik sebebiyle olduğunun tespit edilememesine neden olmuştur. **Tedbirler:** Yazılım geliştirme yaşam döngüsü süreçleri işletilerek tüm uygulamaların kaynak kodlarının iç ağda bir sunucu üzerindeki versiyon kontrol sisteminde tutulması gerekmektedir.
4.2	**Uygulamanın onay mekanizmasından geçirilmeden canlı ortama çıkarılması** **Değerlendirme Soruları:** **1.** Yazılım geliştirme sürecinde ortamların (geliştirme, test, canlı) birbirinden ayrı olduğu bir yapı var mı? **2.** Ortamlar arasında kontrol ve onay mekanizması var mı? Geliştirme ortamındaki bir uygulama kodu test edilmeden direkt olarak canlı ortama yükleniyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında dış kaynak veya kurum çalışanının, yazılım geliştiricilerinin herhangi bir onay süreci olmadan canlı ortama kod yüklemesi yapabildiği görülmüştür. **Tedbirler:** Ortamların geliştirme, test, canlı şeklinde ayrıştırılması ve geliştirilen kodların ancak onay sonrasında canlı ortama aktarılması gerekmektedir. Aynı zamanda her kullanıcıya canlı ortama kod yükleme yetkisi verilmemelidir.

No.	Detay
4.3	**Uygulamanın veritabanına erişiminin tam yetkili kullanıcı ile olması** **Değerlendirme Sorusu:** Uygulamanın veritabanına erişim sağlayan kullanıcı düşük yetkili bir kullanıcı mı? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında SQL sunucusu üzerinde sistem yetkisine sahip "sa" kullanıcısının aktif olduğu görülmüştür. Bir zafiyetten yararlanan saldırganın "sa" kullanıcısı üzerinden sistem yetkisi ile komut çalıştırdığı tespit edilmiştir. **Tedbirler:** Veritabanına erişimin sistem yetkisine sahip olmayan bir kullanıcı üzerinden sağlanması gerekmektedir.
4.4	**Güncel olmayan yazılım ve/veya bileşen kullanması** **Değerlendirme Soruları:** **1.** Sistemde kullanılan tüm yazılım ve bileşenlerinin güncel olduğu sürekli kontrol ediliyor mu? **2.** Sunucular üzerinde hizmet veren yazılımlar sanal çevre içerisinde mi çalışmaktadır? **Karşılaşılan Durum:** Siber olay müdahalesinde Başkanlık tarafından sürekli yapılan kontrollerde tespit edilen ve kuruluşa daha önce bildirilen zafiyeti istismar eden bir siber saldırganın, sistem üzerinde komut çalıştırarak diğer sunuculara da erişim sağladığı tespit edilmiştir. Başka bir siber olay müdahalesinde zafiyetli olduğu bilinen bileşenin, başka bir yazılımın uyum sağlayamayacağı için güncellenemediği görülmüştür. **Tedbirler:** Başkanlık tüm sistem yöneticilerine *8 saat içerisinde güncellenemeyecek hiçbir yazılım veya bileşenin internet erişimine açılmaması* prensibine uymalarını tavsiye etmektedir. Bu durum tüm sistem için geçerli, ancak sunucular özelinde daha kritik olan; güncel uygulama ve bileşen kullanma prensibi uygulanmalı ve sürekli kontrol edilmelidir. İnternete açık uygulamaları barındıran sunucular, amaçlarına göre gruplandırılarak birbirinden yalıtılmalıdır.

No.	Detay
4.5	**Statik kod analizinin yapılmaması** **Değerlendirme Soruları:** **1.** Yazılım geliştirme sürecinde güvenli yazılım geliştirme yaşam döngüsü süreçleri işletiliyor mu? **2.** Geliştirilen veya güncellenen yazılımlar statik kod analizine tabi tutuluyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında güvenli yazılım geliştirme yaşam döngüsü süreçlerinin işletilmediği, geliştirilen kodların statik kod analizinin yapılmadan canlı ortama yüklendiği, bunun sonucunda da temel web uygulama zafiyetlerine sebebiyet verdiği görülmüştür. **Tedbirler:** Yazılım geliştirilirken güvenli yazılım geliştirme yaşam döngüsü süreçlerinin işletilmesi, geliştirilen yazılımın statik kod analizine tabi tutulması ve en azından temel web uygulama zafiyetlerinin olmadığı kodların canlı ortama yüklenmesi gerekmektedir.
4.6	**Uygulama kodlarında statik kullanıcı adı ve parola/API anahtarı bulunması (Hardcoded-Key)** **Değerlendirme Soruları:** **1.** Geliştirilen uygulamalar zafiyet taramasına tabi tutuluyor mu? **2.** Geliştirilen uygulamalar statik kod analizine tabi tutuluyor mu? **Karşılaşılan Durum:** Başkanlık tarafından yapılan incelemelerde, uygulama içerisinde açık metin olarak kullanıcı adı ve parola yer aldığı tespit edilmiştir. **Tedbirler:** Geliştirilen uygulamalar canlı sistemlere entegre edilmeden önce test ortamında test posedürlerine tabi tutulmalıdır. Bu test süreçleri içerisinde statik kod analizi adımı da yer almalıdır. Geliştiriciler tarafından "Sunucuya gelen trafiğin uygulamadan geldiğini test etmek amacı" açıklamasıyla kullanıcı adı ve parola eklendiği görülse de bu yöntem son derece zafiyetli bir yöntemdir. Bunun yerine sürekli değişen çıktılar veren algoritmalar kullanılarak veya farklı tekniklerle trafik kaynağı sınırlandırılmalıdır. Ayrıca bu yöntem sadece "Tanıma" amacıyla kullanılmalıdır, "Tanımlama" ve "Yetkilendirme" için ayrıca kullanıcı etkileşimi dâhilinde prosedürler uygulanmalıdır.

5. İZLEME VE İZ KAYIT YÖNETİMİ

Bu bölüm, Başkanlığın siber olay müdahaleler esnasında izleme-iz kayıt yönetimi tarafında karşılaştığı eksik ve yanlış durumlar ile bunlara karşılık yapılması gereken işlemleri ve alınabilecek tedbirleri içermektedir. Genel olarak aşağıda belirtilen maddelerin iz kayıtlarının toplanmasından ve alarm üretilmesindeki eksikliklerden kaynaklandığı görülmektedir.

No.	Detay
5.1	**Envanter yönetimi eksiklikleri** **Değerlendirme Soruları:** **1.** Kullanıcı, sunucu, ağ cihazı ve benzeri sistemleri içeren topoloji (ağ ve sistem kaynakları) mevcut mu? **2.** Kurumsal yapıya yeni bir ağ, sunucu ve benzeri bir sistem eklendiğinde topoloji güncelleniyor mu? **Karşılaşılan Durum:** Siber olay müdahale sırasında ağ topoloji bilgisine ulaşılamaması, IP adreslerinin hangi sunucuya ait olduğu hakkında net bilgi verilememesi ve kurumun kritik varlıkları sorulduğunda kesin yanıtların alınamaması gibi durumlar gözlemlenmiştir. **Tedbirler:** Siber olay müdahalesi esnasında (ve benzeri diğer çalışmalarda; sızma testi zafiyet kapatma süreci vb.) olay müdahale ekibine hızlı bir şekilde verilebilmesi adına ağ topoloji bilgisi, kurum IP-sunucu eşleşme bilgisi, yüksek riske sahip varlıkların bilgisi gibi envanter bilgilerinin önceden hazır hâlde bulunması gerekmektedir.
5.2	**Sunucu ve istemcilerin ayrıntılı kayıt üretecek şekilde ayarlanmaması.** **Değerlendirme Soruları:** **1.** Sistemlerin kayıt tutma ayarları ayrıntılı konfigüre edilmiş mi? **2.** Sistemler, kaynaklara erişimleri kayıt altına alacak şekilde ayarlanmış mı? **Karşılaşılan Durum:** Siber olay müdahalesi esnasında, sistemlerin varsayılan ayarlarda kayıt tuttuğu, mümkün olmasına rağmen olay kayıtlarının ayrıntılı hâle getirilmediği görülmüştür. **Tedbirler:** Sunucuların ve istemcilerin işletim sistemi özelinde tutulan kayıtları, politikaların güncellenmesi suretiyle ayrıntılı hâle getirilmelidir. Aynı işlem, yüklenen diğer yazılımlara da uygulanmalıdır. Windows sistemlerde sysinternals araçlarından “Sysmon” aracı kurularak işletim sisteminin yeteneklerinden daha fazla kayıt tutulması sağlanabilmektedir.

No.	Detay
5.3	**İz kayıtlarının merkezi bir sistem üzerinde tutulmaması** **Değerlendirme Soruları:** **1.** Sitemdeki cihazlar üzerindeki işletim sistemi iz kayıtları cihazdan silindiğinde, bu kayıtlara erişmek için alternatif bir yol var mı? **2.** Kurumda tüm sistemler merkezi iz kayıt alma yapısına dâhil edildi mi? **3.** Adli bilişim incelemeleri için gerekli olan, geriye dönük iz kayıtları silinmeden muhafaza ediliyor mu? **4.** Kurumsal yapıda, iz kayıtlarının merkezi yönetiminin sağlanması için herhangi bir SIEM sistemi kullanılıyor mu? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında saldırganların ele geçirdiği sunucularda oluşan iz kayıtlarını sildiği, buna karşın kurumların iz kayıtlarını ayrı merkezî bir sistemde toplamadığı görülmüştür. Ayrıca iz kayıtları tutulsa dahi test sunucuları gibi bazı sunucuların iz kayıtlarının bu merkezi sisteme dâhil edilmediği, ek olarak diski dolan sunucudaki iz kayıtlarının geriye dönük olarak yetkililer tarafından silindiği tespit edilmiştir. Başka bir siber olay müdahalesinde kayıtların sadece sistem üzerinde ve varsayılan boyut büyüklüğünde tutulduğu tespit edilmiştir. Varsayılan kayıt dosyası büyüklğünde erişildiğinde yeni kayıtlar, sistem tarafından mevcut kayıtların eski tarihten başlayarak üzerine yazılmaktadır. **Tedbirler:** Sunucularda oluşan iz kayıtlarının silinme ihtimali göz önünde bulundurularak tüm iz kayıtlarının merkezî bir sistemde sınıflandırma yapılarak (anti virüs, firewall, sistem vb.) tutulması ve istenildiği zaman sorgulanabilmesi gerekmektedir. Geriye dönük iz kayıtlarının adli bir süreç göz önünde bulundurularak silinmemesi, yasal süreler dikkate alınarak saklanması gerekmektedir. Sistemlerin en az hangi olayları kayıt altına alacağı ve bu kayıtların nerede muhafaza edileceği en iyi uygulama yöntemlerine göre belirlenmeli ve bu kayıtlar “Sistem İşletme Politikası”nda yer almalıdır. İz kayıt yönetimi belirlenen bu kaidelere göre yürütülmelidir.

No.	Detay
5.4	**Kritik iz kayıtlarından alarm üretilmemesi** **Değerlendirme Soruları:** **1.** Merkezî iz kayıt alma sistemine gelen kritik öneme sahip iz kayıtları (Örnek olarak: yeni bir Domain Admin kullanıcısının eklenmesi, varolan yönetici grubundaki kullanıcıların parolalarının değiştirilmesi veya SIEM kullanıcısının pasif hâle gelmesi vb.) için alarm mekanizması mevcut mu? **2.** Üretilen alarmlar için ilgili kurum personeli analiz çalışmaları yapıyor mu? **Karşılaşılan Durumlar:** **1.** Siber olay müdahalesi sırasında iz kayıtlarının merkezi bir sistemde tutulmasına rağmen bu iz kayıtlarına uygun alarmlar üretilmediği ve analizinin yapılamadığı görülmüştür. **2.** Siber olay müdahalesi sırasında, kullanıcı adı siber saldırgan tarafından ele geçirilen hesaba kaba kuvvet saldırısı (brute force) yapıldığı, ancak bu saldırının sistem yöneticileri tarafından fark edilmediği, dolayısıyla saldırıya karşı herhangi bir savunma faaliyeti icra edilmediği görülmüştür. **Tedbirler:** Kritik olabilecek iz kayıtlarının ilgili çalışanlara analiz edebilmeleri için e-posta benzeri bir mekanizma ile alarm olarak iletilmesi gerekmektedir. İz kayıt alma işleminde bir aksaklık olduğu durumlarda (SIEM kullanıcısının pasif hâle gelmesi gibi) bir alarm üretilerek ilgili çalışanlar uyarılmalıdır.

6. TEST VE TATBİKAT SÜREÇLERİ

Bu bölüm, Başkanlığın siber olay müdahalesi esnasında sırasında test ve tatbikat süreçleri tarafında karşılaştığı eksik ve yanlış durumlar ile bunlara karşılık yapılması gereken işlemleri ve alınabilecek tedbirleri içermektedir. Genel olarak aşağıda belirtilen maddelerin olay müdahalesi öncesinde, sırasında ve sonrasında yapılmayan veya eksik yapılan durumlardan kaynaklandığı görülmektedir.

No.	Detay
6.1	**Olay müdahale ekibinin belli olmaması** **Değerlendirme Sorusu:** Kurumda siber olay öncesi, sırası ve sonrasında ilgili personel(ler) ve bu personellerin görevleri iyi tanımlanmış mı? **Karşılaşılan Durum:** Kurum bilgi sistemlerine gerçekleştirilen siber saldırı esnasında ve/veya sonucunda siber olay müdahale ekibinin ve görevlerin tanımlanmaması, aynı zamanda bilgi eksikliğinden kaynaklı koordinasyon eksikliği sonucunda olaya ilk müdahale sağlıklı bir şekilde gerçekleştirilememiştir. **Tedbirler:** Kuruma yapılacak siber saldırılara karşı olay müdahale ekibinin belirlenmesi ve siber olay müdahalesi öncesinde, siber olay müdahalesi sırasında ve sonrasında yapılması gerekenlerin personel tarafından bilinmesi gerekmektedir.
6.2	**Olay müdahale sırasında delillere zarar verilmesi** **Değerlendirme Sorusu:** Kurumda daha önce bir siber saldırı yaşandı mı? Siber olay müdahale sırasında saldırıya maruz kalan sistemler üzerinde yapılan ilk işlem (ağ izolasyonu, imaj alma, formatlama, cihazı yeniden başlatma) neydi? **Karşılaşılan Durum:** Kurum bilgi sistemlerine gerçekleştirilen siber saldırı esnasında ve/veya sonucunda saldırganlar tarafından erişim sağlandığı tespit edilen kullanıcı ve sunucu sistemlerinin kapatıldığı tespit edilmiştir. **Tedbirler:** Siber saldırıdan etkilendiği tespit edilen sistemlerin iç ağ ile bağlantısı kesilmelidir. RAM üzerindeki bilgilerin kaybolmasını önlemek açısından sistemin kapatılmaması ve cihaza ağ izolasyonu gibi yöntemlerle müdahale edilmesi gerekmektedir.
6.3	**İlişkili kurum kuruluşların (üst kurul veya müşteri) belli olmaması** **Değerlendirme Sorusu**: Kuruma yapılabilecek bir siber saldırının etki alanını iyi analiz edebilmek için ilişkili olunan kuruluşlar (Üst Kurul veya Müşteri) ve bu kuruluşlarla olan bağlantılar (side-to-side VPN, ortak domain yapısı, barındırılan sunucu vb.) belli mi? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında bazı kurum çalışanlarının e-posta hesaplarının ele geçirildiği ve ele geçirilen bu e-posta hesapları üzerinden kurumun ilişkili olduğu diğer bir kuruma oltalama saldırısı yapıldığı tespit edilmiştir. **Tedbirler:** Saldırı yüzeyinin iyi analiz edilebilmesi ve siber olay müdahale yöntemlerinin isabetli olabilmesi için kurum kaynaklarının ve kurum ile ilişkili diğer kurumların da tanımlanması gerekmektedir.

No.	Detay
6.4	**Sızma testi süreçlerindeki eksiklikler** **Değerlendirme Soruları:** **1.** Belirli aralıklarla yapılması gereken sızma testleri gerçekleştiriliyor mu? **2.** Sızma testleri sonucunda tespit edilen bulgular için doğrulama testleri ve yama çalışmaları yapıldı mı? **Karşılaşılan Durum:** Kurumlarda yaşanan siber olaylarla ilgili olarak saldırganların, kuruma yapılan sızma testleri sonucunda tespit edilmiş hususların doğru olarak giderilmemesi sebebiyle kuruma sızmayı başarabildiği gözlemlenmektedir. **Tedbirler:** Sızma testlerinin yetkin kurumlar tarafından yapılmasının sağlanması ve test sonucunda tespit edilen zafiyetlerin kapatıldıktan sonra kontrollerinin yapılması gerekmektedir.
6.5	**Gerçekleşen siber olayın Başkanlık ve ilişkili kurumlara bildirilmemesi** **Değerlendirme Sorusu:** Kurumda daha önce bir siber saldırı yaşandı mı? Konu ile ilgili ve/veya ilişkili kurumlara ilgili platformlardan bilgi verildi mi? **Karşılaşılan Durum:** Siber olay müdahalesi sırasında kurumun daha önce benzer bir siber saldırıya uğradığı; bu süreç hakkında yetkililere bilgi verilmeden ve herhangi bir düzeltme çalışması yapılmadan sadece yedekten dönüldüğü görülmüş, böylece saldırganın aynı zafiyeti kullanarak sisteme tekrar sızdığı tespit edilmiştir. **Tedbirler:** Kurumda siber saldırının yaşandığına dair bir bulgu tespit edildikten sonra bu olayın benzerinin diğer kurumlarda da yaşanmaması ve ulusal çapta önlem alınabilmesi için Başkanlık ve Sektörel SOME'nin konu ile ilgili bilgilendirilmesi gerekmektedir.