Cumhurbaşkanlığı (Siber Güvenlik Başkanlığı)'ndan:

SİBER DAYANIKLILIK YÖNETMELİĞİ TASLAĞI

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1– (1) Bu Yönetmeliğin amacı, kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların siber saldırılara karşı korunmasına ilişkin kriterleri, sorumlulukları ve yükümlülükleri belirlemek ile siber güvenlik risk yönetimi tedbirlerinin uygulanması ve ulusal siber dayanıklılığın güçlendirilmesi amacıyla yürütülecek faaliyetlere ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2– (1) Bu Yönetmelik, siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşları kapsar.

(2) 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ve 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu uyarınca yürütülen istihbari faaliyetler ile 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu uyarınca yürütülen faaliyetler bu Yönetmeliğin kapsamı dışındadır.

Dayanak

MADDE 3– (1) Bu Yönetmelik, 177 sayılı Cumhurbaşkanlığı Kararnamesinin 4 üncü ve 9 uncu maddelerine, 7545 sayılı Siber Güvenlik Kanununun 5 inci, 6 ncı, 7 nci, 8 inci, 16 ncı ve 17 nci maddelerine dayanılarak hazırlanmıştır.

Tanımlar ve Kısaltmalar

MADDE 4– (1) Bu Yönetmelikte geçen;

a) Ayrıcalıklı hesap: Standart kullanıcı yetkilerinin ötesinde, sistemlerin yönetilmesi, yapılandırılması veya denetlenmesi amacıyla üst düzey erişim haklarına sahip hesapları,

b) Başkan: Siber Güvenlik Başkanını,

c) Başkanlık: Siber Güvenlik Başkanlığını,

ç) Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sistemli, kurallı, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetim tarafından taahhüt edilmiş, ulusal ve uluslararası standartlarla uyumlu şekilde güvence altına alan yönetim sistemini,

d) Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda kullanılan donanım, yazılım, sistem ve aktif veya pasif durumda bulunan tüm diğer bileşenleri,

e) Dijital Delil: Bilişim sistemleri aracılığıyla oluşturulan, saklanan, iletilen veya işlenen, bütünlüğü korunarak elde edilmiş, doğrulanabilen ve hukuki süreçte ispata katkı sağlayabilecek elektronik veriyi,

TASLAK

f) FKM: Felaket kurtarma merkezini,

g) Kanun: 12/3/2025 tarihli ve 7545 sayılı Siber Güvenlik Kanununu,

ğ) Kritik altyapı: İşlediği bilginin ya daverinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara ve güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,

h) Kritik hizmet: Kesintiye uğraması veya zarar görmesi halinde ulusal güvenlik, ülkenin sosyal veya ekonomik refahı, kamu düzeni veya sağlığı ya da diğer hizmetlerin sunumu üzerinde önemli bir etki oluşturabilecek hizmeti,

ı) Log kaydı: Bilişim sistemlerinde gerçekleşen kullanıcı ve sistem hareketlerine ilişkin, hangi işlemlerin kimin tarafından gerçekleştirildiğini veya gerçekleştirilmeye çalışıldığını gösteren ve operasyonel bir işlemin başlangıcından bitişine kadar adım adım takip edilmesini sağlayacak şekilde eksiksiz, tutarlı ve kronolojik olarak üretilen kayıtları,

i) Mikro segmentasyon: Ağ altyapısının kendi içinde fonksiyon, süreç ve kritiklik derecelerine göre alt bölümlere ayrılarak katmanlar arasındaki veri akışlarının sıkı kurallarla sınırlandırılmasını,

j) Risk iştahı: Kuruluşun stratejik hedeflerine ve misyonuna ulaşma doğrultusunda göze almayı veya kabul etmeyi tercih ettiği toplam risk miktarını,

k) Risk toleransı: Kabul edilebilir risk iştahı sınırlarının aşılması durumunda kuruluşun hedeflerinden sapma olarak katlanabileceği veya geçici olarak kabul edebileceği maksimum zarar eşiğini veya sapma miktarını,

l) SİP: SOME iletişim platformunu,

m) SOME: Siber olaylara müdahale ekibini,

n) Taraflar: Siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşları,

o) Tek hata noktası: Arızalanması, kesintiye uğraması veya çalışamaz hale gelmesi durumunda bilişim sisteminin veya hizmetin durmasına veya kabul edilemez bir kesintiye uğramasına sebep olan varlığı,

ö) UVET: Ulusal varlık envanteri veri tabanını,

p) Varlık: Elektronik veya fiziksel ortamlarda yer alan ve iletişim yoluyla aktarılabilen veriyi içeren tüm bilgi ve bilgi işleme olanaklarını, veriyi kullanan veya taşıyan personeli ve veriyi barındıran fiziksel mekânları,

r) Zafiyet: Siber uzayda yer alan varlıkların herhangi bir siber tehdit tarafından istismar edilebilecek zayıflık ve güvenlik açıklarını,

s) Zararlı yazılım: Bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini bozmayı hedefleyen yazılım veya sistemi
ifade eder.

(2) Bu Yönetmelikte geçen ve birinci fıkrada yer almayan tanımlar için Kanunda ve ilgili mevzuatta yer alan tanım ve kısaltmalar geçerlidir.

İKİNCİ BÖLÜM
Başkanlığın Görev ve Yetkilerine İlişkin Hususlar

Sınıflandırma yetkisi

MADDE 5– (1) Başkanlık risk temelli yaklaşımı esas alarak, siber güvenlik yükümlülüklerinin kapsamını belirlemek ve ulusal siber dayanıklılık seviyesini artırmak amacıyla bu Yönetmelik kapsamında yer alan tarafları; faaliyet alanı, sunduğu hizmet, kritiklik

seviyesi, sunulan hizmetin sosyal ve ekonomik etkileri, siber risk düzeyi ve benzeri kriterler bakımından sektörel veya faaliyet bazlı sınıflandırabilir.

(2) Başkanlık, sınıflandırma doğrultusunda taraflara risk yönetimi, olay yönetimi, tatbikat, eğitim ve raporlama gibi hususlarda farklı siber güvenlik yükümlülükleri getirebilir.

(3) Başkanlık, sınıflandırmaları, değişen siber tehdit ortamı, teknolojik gelişmeler, sektörel riskler, hizmet kapsamındaki değişiklikler, organizasyon yapısındaki farklılaşmalar veya ulusal güvenlik ihtiyaçları doğrultusunda re'sen ya da talep halinde gözden geçirir ve gerekli gördüğü hâllerde günceller.

(4) Başkanlık, Yönetmelik kapsamında yer alan taraflara sahip oldukları bilişim altyapısının veya sunduğu hizmetin niteliğine ve kritikliğine göre ek yükümlülükler getirebilir, taraflardan ilave tedbirler almasını isteyebilir.

Kritik altyapıya sahip kuruluşların belirlenmesine ilişkin kriterler

MADDE 6– (1) Başkanlık, siber olayların, ulusal güvenlik, kamu düzeni, kamu sağlığı, ekonomik ve sosyal hayatın devamlılığı gibi toplumsal etkilerini en aza indirmek amacıyla Siber Güvenlik Kurulu tarafından belirlenen kritik altyapı sektörlerinde faaliyet gösteren tarafların belirlenmesinde esas alınacak teknik, idari, sektörel ve operasyonel kriterleri belirler.

(2) Kritik altyapıya sahip kuruluşların belirlenmesinde aşağıdaki kriterler esas alınır:

a) Sunulan hizmetin sekteye uğraması halinde ulusal güvenlik, kamu düzeni, kamu güvenliği, kamu sağlığı veya toplum üzerindeki etkisi.

b) Sunulan hizmetin sekteye uğraması halinde bu hizmetin benzer kalitede veya sürede başka bir kaynaktan sağlanmasının mümkün olup olmaması.

c) Sunulan hizmet veya altyapının diğer hizmetlere olan bağımlılığı, tedarik zincirindeki konumu ile altyapının diğer kritik sektörlerin işleyişi üzerindeki doğrudan veya dolaylı etkisi.

ç) Sunulan hizmetin sekteye uğraması halinde etkilenecek kişi sayısı ve niteliği.

d) Olası bir siber olayın can kaybına, büyük ölçekli ekonomik zarara veya çevresel felakete yol açma potansiyeli.

e) Olası bir siber olayın etkilerinin ulusal sınırları aşarak bölgesel veya uluslararası güvenliği tehdit etme riski.

(3) İkinci fıkrada belirtilen kriterlere ilave olarak; kuruluşun faaliyet hacmi, pazar payı, hizmet kapasitesi ve yıllık brüt satış hasılatı gibi diğer teknik, idari, sektörel ve operasyonel kriterler de dikkate alınabilir.

(4) Başkanlık, bu maddede belirtilen kriterler çerçevesinde, gerekli gördüğü hâllerde kritik altyapıya sahip kuruluşları belirleyebilir.

Ulusal varlık envanteri veri tabanı

MADDE 7– (1) Başkanlık, kamu kurum ve kuruluşları ile kritik altyapıların veri envanteri de dahil olmak üzere tüm varlıklarının envanterini tutulmasını sağlamak üzere UVET'i kurar ve işletir.

(2) UVET'te asgari olarak; kuruluşların künye bilgileri, bilişim sistemleri ve operasyonel teknolojiler ile veri envanteri, ağ ve sistem mimarisine ilişkin bilgiler, kritik hizmetler ve bunlara ilişkin bağımlılıklar, kritik varlık sahipliği ve sorumluluk bilgileri, varlıkların kritiklik seviyeleri, risk durumları ve sınıflandırmaları ile Başkanlıkça gerekli görülen bilgi ve kayıtlar yer alır.

(3) UVET'te tutulacak bilgiler Başkanlıkça belirlenen usul, esas, format ve sürelerde elektronik ortamda Başkanlığa bildirilir. Bu bilgilerde meydana gelen değişiklikler aksi Başkanlıkça belirtilmedikçe en geç bir ay içerisinde aynı yöntemle Başkanlığa bildirilir.

(4) Başkanlık, UVET'te yer alan bilgilerin doğruluğunu ve güncelliğini sağlamak amacıyla ilave bilgi ve belge talep edebilir, elektronik doğrulama yöntemlerini kullanabilir, ilgili kurum ve kuruluşlardan açıklama isteyebilir ve gerektiğinde yerinde inceleme yapabilir.

(5) UVET'te yer alan bilgiler, Kanun ve ilgili mevzuatta öngörülen hâller dışında üçüncü kişilerle paylaşılmaz.

(6) Başkanlık, UVET'in kurulması, işletilmesi, güvenliği, veri standartları, veri modeli, elektronik veri paylaşım yöntemleri, entegrasyon esasları, erişim yetkileri, kayıtların saklanma yöntemleri ve süreleri ile güncellenmesine ilişkin usul ve esasları belirleyebilir.

(7) Başkanlık, kullanılan bilişim sistemlerinin üretici bağımlılığını belirlemeye yönelik analiz çalışması yapabilir. Analiz kapsamında, bilişim sistemlerinin kritikliğini esas alarak sınıflandırma yapabilir, her ürün sınıfında kabul edilebilir bağımlılık seviyelerini, riskleri ve tedbirleri belirleyebilir.

Zafiyet tespiti, yönetimi ve bildirimi

MADDE 8– (1) Başkanlık, ağ ve bilişim sistemlerini tarayarak siber tehditleri ve güvenlik zafiyetlerini tespit edip, gerekli analizleri yaparak alarm, uyarı, duyuru ve bilgi paylaşımı yapabilir.

(2) Başkanlık, taraflara ait bilişim sistemlerinde siber güvenlik zafiyetlerinin tespiti, değerlendirilmesi, önceliklendirilmesi ve önlemlerin alınmasına yönelik zafiyet taraması veya sızma testi yapar veya yaptırır.

(3) Başkanlık, açık kaynaklar, ulusal ve uluslararası siber tehdit istihbaratı ve zafiyet bildirim sistemleri, teknik analizler, siber olaylardan elde edilen bulgular, otomatik izleme sistemleri, zafiyet taramaları, sızma testleri ile diğer teknik ve idari yöntemler vasıtasıyla tespit ettiği bulguları veya kendisine bildirilen ihbarları analiz ederek zafiyetlerin risk seviyelerini belirler.

(4) Başkanlık, ulusal güvenlik, kamu düzeni, kritik hizmetlerin sürekliliği veya siber uzayın güvenliği bakımından risk oluşturduğu değerlendirilen zafiyetleri ilgili taraflara bildirir.

(5) Başkanlık, bildirilen zafiyetlerin giderilmesine ve doğrulanmasına ilişkin bilgi, belge, teknik veri, kayıt, log kaydı, test sonucu, yapılandırma bilgisi ve diğer gerekli verileri ilgili kurum ve kuruluşlardan talep edebilir, zafiyet giderme sürecini izleyebilir, bu kapsamda doğrulama çalışmaları gerçekleştirebilir ve gerekli gördüğü hâllerde ilave teknik veya idari tedbirlerin uygulanmasını talep edebilir.

(6) Zafiyet bildirimi yapılan taraflar, kendisine bildirilen zafiyetler hakkında gerekli işlemleri derhal başlatmak, yapılan ve yapılacak işlemleri Başkanlıkça belirlenecek süre içerisinde bildirmek, belirtilen zafiyetlerin süresi içerisinde giderilememesi durumunda, gecikmenin gerekçesi, mevcut risk ve zafiyetin giderilmesine yönelik yapılacak çalışmalar ile çalışma takvimini Başkanlığa bildirmekle yükümlüdür.

(7) Başkanlık, yaygın olarak kullanılan ürün, hizmet veya sistemlerde tespit edilen ve birden fazla kurum veya kuruluşu etkileyebilecek zafiyetlere ilişkin ulusal güvenlik uyarıları, güvenlik bildirimleri, zafiyet duyuruları ve rehberler yayımlayabilir.

(8) Başkanlık, taraflardan zafiyetlerin izlenmesi ve analiz edilmesi amacıyla düzenli raporlama talep edebilir, bu kapsamda Başkanlık sistemleriyle entegre çalışacak şekilde gerçek zamanlı izleme ve takip sistemleri kurdurabilir.

Siber risk yönetimi

MADDE 9– (1) Başkanlık, siber dayanıklılığın sağlanması ve kritik altyapıların korunması amacıyla sektörel siber risk yönetimi sürecini işletir veya işlettirir. Başkanlık, siber risk yönetimi sonucunda belirlenen kritiklik seviyelerine uygun tedbirleri alır veya aldırır.

(2) Başkanlık, taraflardan siber risk yönetimine esas bilgi, belge, kayıt, teknik veri ve raporları talep edebilir; gerekli hâllerde yerinde inceleme yapabilir veya yaptırabilir.

(3) Başkanlık, taraflardan bu Yönetmelikte belirlenmiş olan usullere uygun şekilde siber risk yönetim sürecini işletmelerini, belirlenen aralıklarla güncellemelerini ve sonuçlarını Başkanlığa sunmalarını isteyebilir.

(4) Başkanlık, kritik zafiyetlerin ortaya çıkması, yeni saldırı yöntemlerinin tespit edilmesi veya ulusal güvenliği etkileyebilecek durumların oluşması hâlinde taraflardan ilave siber risk yönetimi sürecini işletmesini isteyebilir.

Siber risk yönetim süreci esasları

MADDE 10– (1) Siber risk yönetimi; kuruluşun kritik hizmetlerinin, bilgi varlıklarının, ağ ve bilişim sistemlerinin, operasyonel teknoloji sistemlerinin, fiziksel tesislerinin ve destekleyici süreçlerinin gizlilik, bütünlük, erişilebilirlik ve sürekliliğini etkileyebilecek siber risklerinin sistematik olarak belirlenmesi, analiz edilmesi, değerlendirilmesi, önceliklendirilmesi, işlenmesi ve izlenmesi amacıyla yürütülür.

(2) Siber risk yönetimi sürecinden önce, kuruluş tarafından siber risk yönetiminin kapsamı, organizasyonel ve teknolojik sınırları, kritik hizmetleri, varlıklar, bağımlılıklar, siber risk yönetimi, değerlendirme kriterleri, varsayımları, risk iştahı ve risk toleransı esasları belirlenir ve kuruluşun yetkili yönetim organı tarafından onaylanır.

(3) Siber risk yönetim süreci kuruluş genelinde tutarlı, tekrarlanabilir, ölçülebilir ve dokümante edilmiş bir metodoloji kullanılarak gerçekleştirilir. Kullanılan metodoloji ve önemli varsayımlar kayıt altına alınır.

(4) Siber risk yönetim sürecinde bunlarla sınırlı olmamak kaydıyla, aşağıdaki hususlar dikkate alınır:

a) Kuruluşun kritik hizmetlerinin, kritik iş süreçlerinin, bilgi varlıklarının, ağ ve bilişim sistemlerinin, operasyonel teknoloji varlıklarının, fiziksel tesislerinin ve destekleyici sistemlerinin ve diğer ilgili varlıklarının envanteri oluşturularak bunların yaşam döngüsü boyunca kritiklik seviyelerinin belirlenmesi.

b) Kritik hizmetlerin kesintiye uğraması ile varlıkların gizlilik, bütünlük ve erişilebilirliğinin ihlal edilmesine yönelik kabul edilebilir risk seviyelerinin belirlenmesi.

c) İnsan, süreç, teknoloji, fiziksel çevre, doğal afetler, tedarik zinciri, üçüncü taraf hizmet sağlayıcıları, mevzuat değişiklikleri ve diğer iç veya dış faktörlerden kaynaklanabilecek risk kaynaklarının belirlenmesi.

ç) İç ve dış tehditler, tehdit aktörleri, saldırı yöntemleri, tehdit senaryoları, güncel tehdit istihbaratı ve teknolojik gelişmelerin değerlendirilmesi.

d) Kuruluşun tabi olduğu mevzuattan, tarafı olduğu sözleşmelerden ve tabi olduğu uluslararası yükümlülüklerden kaynaklanabilecek uyum risklerinin değerlendirilmesi.

e) Bilişim sistemleri, operasyonel teknoloji sistemleri, ağ altyapıları, bulut hizmetleri, tedarik zinciri, üçüncü taraf hizmet sağlayıcıları ve diğer bağımlılıklardan kaynaklanabilecek zafiyetler ve tek hata noktalarının belirlenmesi.

f) Her bir risk senaryosunun gerçekleşme olasılığı ile kritik hizmetler, iş sürekliliği, hizmet sunumu, bilgi varlıkları, kamu hizmetleri, kamu düzeni ve sağlığı, ekonomik faaliyetler, sosyal hayatın devamlılığı, ulusal güvenlik, operasyonel faaliyetler, finansal durum, itibar, kişisel veriler ve kritik altyapılar üzerindeki muhtemel etkilerinin değerlendirilmesi.

g) Bilişim sistemleri, operasyonel teknoloji sistemleri, kritik altyapılar, sektörler ve üçüncü taraflar arasındaki karşılıklı bağımlılıklar ile bir riskin diğer riskleri tetikleyebileceği zincirleme etkilerin değerlendirilmesi.

ğ) Mevcut idari, teknik ve fiziksel güvenlik kontrollerinin varlığı, etkinliği ve uygulanma olgunluğu değerlendirilerek artık risk seviyesinin belirlenmesi.

h) Risk iştahı ve risk toleransı esasları doğrultusunda kabul edilebilir seviyeyi aşan riskler için riskin azaltılması, paylaşılması, kaçınılması veya kabul edilmesine yönelik uygun risk işleme yönteminin belirlenmesi.

ı) Her bir risk için risk sahibinin belirlenerek, risklerin giderilmesi veya kabul edilebilir seviyeye indirilmesine yönelik uygulanacak teknik ve idari tedbirleri, sorumluları, öncelikleri, ihtiyaç duyulan kaynakları, telafi edici kontrolleri, uygulama sürelerini ve izleme ile doğrulama faaliyetlerini içeren risk işleme planının hazırlanması ve uygulanması.

Zararlı yazılım inceleme

MADDE 11– (1) Başkanlık, zararlı yazılımların tespiti, analizi, sınıflandırılması, teknik olarak incelenmesi, etkilerinin değerlendirilmesi ve bunlara karşı alınacak tedbirlerin belirlenmesine yönelik faaliyetleri yürütür.

(2) Başkanlık, zararlı yazılım incelemesi veya siber olayların analizi kapsamında gerekli görülmesi hâlinde ilgili taraflardan zararlı yazılım örneği, kaynak kodları, ağ kayıtları, log kayıtları, yapılandırma bilgisi, dijital delil ve diğer teknik verileri talep edebilir.

(3) Başkanlık, zararlı yazılım analizlerinin yürütülmesi amacıyla analiz laboratuvarları kurabilir veya kurdurabilir, otomatik analiz sistemleri ve siber tehdit istihbaratı platformları işletebilir.

(4) Başkanlık, zararlı yazılım analizleri sonucunda elde edilen teknik bulguları siber tehdit istihbaratının oluşturulması, siber olaylara müdahale kapasitesinin geliştirilmesi, zafiyet yönetimi, erken uyarı mekanizmalarının işletilmesi, ilgili tarafların uyarılması ve ulusal siber güvenlik kapasitesinin artırılması amacıyla kullanabilir.

İhbarların alınması, değerlendirilmesi ve sonuçlandırılması

MADDE 12– (1) Başkanlık, siber tehditler, zafiyetler, zararlı yazılımlar, gerçekleşmesi muhtemel veya gerçekleşmesi engellenmiş olanlar da dâhil olmak üzere siber olaylar, kritik altyapıları etkileyebilecek riskler ile mevzuata aykırılıklar ve ulusal siber güvenliği ilgilendiren diğer hususlara ilişkin ihbarları almaya, değerlendirmeye ve sonuçlandırmaya yetkilidir.

(2) İhbarlar Başkanlıkça belirlenen sistemler üzerinden elektronik ortamda, yazılı olarak veya Başkanlıkça belirlenen diğer yöntemlerle yapılabilir.

(3) Başkanlık kendisine bildirilen ihbarların incelenerek doğrulanması halinde, yapılan ihbarın kritiklik, önem ve etki derecesine göre;

a) Teknik inceleme başlatabilir.

b) İlgili kurum veya kuruluştan açıklama isteyebilir.

c) Denetim veya yerinde inceleme yapılmasına karar verebilir.

ç) Zafiyet yönetimi veya olay müdahale süreçlerini başlatabilir.

d) İlgili tarafları bilgilendirebilir ve gerekli koordinasyonu sağlayabilir.

(4) Başkanlık, ihbarların değerlendirilmesi sonucunda elde edilen bulguları ulusal siber risk yönetim süreçlerinde, denetim ve gözetim faaliyetlerinde, tehdit analizlerinde, güvenlik duyurularının hazırlanmasında, rehber ve teknik kriterlerin geliştirilmesinde kullanabilir.

(5) Başkanlık, ihbarların etkin şekilde değerlendirilmesini sağlamak amacıyla kamu kurum ve kuruluşları, kolluk birimleri, sektörel ve kurumsal SOME'ler ile koordinasyon mekanizmaları oluşturabilir ve güvenli elektronik bilgi paylaşım sistemleri kurabilir.

(6) Başkanlık, ihbarda bulunan taraflar ve ihbara konu olaydaki taraflar arasındaki koordinasyonu sağlamak üzere gerekli faaliyetleri yürütür. Başkanlık, ihbarın başka ülkelerde önemli bir etkiye sahip olabileceğini değerlendirdiği durumlarda ilgili ülkenin eş değer kurum ve kuruluşu ve uluslararası siber güvenlik organizasyonları ile irtibata geçebilir, iş birliği yapabilir.

(7) İhbarda bulunan tarafların kişisel verileri ile ihbar kapsamında elde edilen bilgi, belge ve kayıtlar gizlidir. Bu bilgiler kanunlarda açıkça öngörülen hâller saklı kalmak kaydıyla üçüncü kişilerle paylaşılmaz. Başkanlık, ihbarda bulunan tarafın, kimlik bilgilerinin korunmasına yönelik gerekli teknik ve idari tedbirleri alır.

(8) Kötü niyetle, bilerek ve isteyerek gerçeğe aykırı veya yanıltıcı bilgi verilerek yapılan ihbarlar hakkında ilgili mevzuat hükümleri uygulanır.

Siber tehdit istihbaratı

MADDE 13– (1) Başkanlık, ulusal siber güvenliğin sağlanması amacıyla siber tehdit istihbaratı faaliyetlerini yürütür, koordine eder.

(2) Siber tehdit istihbaratı faaliyeti; siber tehditlere, tehdit aktörlerine, saldırı yöntemlerine, güvenlik zafiyetlerine, siber olaylara, tehdit göstergelerine, etkilenen varlıklara, muhtemel etkilere ve alınması gereken tedbirlere ilişkin verilerin toplanması, doğrulanması, işlenmesi, analiz edilmesi, ilişkilendirilmesi, yorumlanması, sınıflandırılması, paylaşılması ve sonuçların izlenmesi aşamalarını kapsar.

(3) Başkanlık, ulusal veya sektörel düzeyde siber tehditlerin tespit edilmesi, erken uyarı mekanizmalarının işletilmesi, olaylara proaktif müdahale edilmesi ve siber dayanıklılığın artırılması amacıyla kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde faaliyet gösteren taraflar için siber tehdit istihbaratı paylaşımı ve kullanımına ilişkin usul ve esasları belirleyebilir.

(4) Başkanlık, siber tehdit istihbaratı edinimi ve üretimi amacıyla açık kaynaklar, teknik araştırmalar, ulusal ve uluslararası bildirim ve paylaşım sistemleri, sektörel ve kurumsal SOME'ler, kamu kurum ve kuruluşları, kritik altyapıya sahip kuruluşlar, üreticiler, hizmet sağlayıcılar, akademik kuruluşlar, güvenlik araştırmacıları ve benzeri güvenilir kaynaklardan yararlanabilir, koordinasyon mekanizmaları, güvenli iletişim altyapıları ve iş birliği modelleri tesis edebilir.

Siber olay sınıflandırması

MADDE 14– (1) Siber olaylar; türü, niteliği, etkilenen bilişim sistemleri ve varlıkları, hizmet kesintisinin süresi ve kapsamı, etkilenen kullanıcı sayısı, ekonomik ve toplumsal etkisi, kurumsal, sektörel düzeydeki etkisi, diğer kritik altyapı sektörlerine etkisi, sınır ötesi etkisi ile

ulusal güvenlik bakımından taşıdığı önem gibi ölçütler dikkate alınarak aşağıdaki şekilde sınıflandırılır:

a) Seviye 1 - Düşük Etkili Olay: Yalnızca sınırlı sayıdaki bilişim sistemi, kullanıcı veya hizmeti etkileyen, veri sızıntısı bulunmayan, kuruluşun temel hizmetlerinin sunumunu kesintiye uğratmayan veya ihmal edilebilir düzeyde etkileyen, kuruluşun olağan operasyonel imkân ve kabiliyetleriyle giderilebilen siber olaylardır.

b) Seviye 2 - Orta Etkili Olay: Kuruluşun belirli hizmetlerinde geçici aksamalara neden olan, sınırlı ölçüde veri kaybı veya veri ihlaline yol açabilen, ancak temel faaliyetlerini tamamen durdurmayan ve kuruluşun olay müdahale kapasitesi kullanılarak kontrol altına alınabilen siber olaylardır.

c) Seviye 3 - Yüksek Etkili Olay: Kuruluşun kritik bilişim sistemlerini veya temel hizmetlerini önemli ölçüde etkileyen, kritik veri veya sistemlerin gizliliği, bütünlüğü ya da erişilebilirliği üzerinde ciddi sonuçlar doğuran, hizmet sürekliliğini önemli ölçüde aksatan veya kamu hizmetlerinin sunumunu etkileyen siber olaylardır.

ç) Seviye 4 - Çok Yüksek Etkili Olay: Birden fazla kuruluşu önemli düzeyde etkileyen, sektörler arası yayılım gösteren veya yayılma potansiyeli bulunan, ekonomik faaliyetler, toplumsal yaşam veya kritik hizmetlerin sürekliliği üzerinde ciddi sonuçlar doğuran siber olaylardır.

d) Seviye 5 - Ulusal Siber Kriz: Bir veya birden fazla kritik altyapıyı veya kritik kamu hizmetini ciddi şekilde kesintiye uğratan ya da uğratma riski taşıyan, milli güvenlik, kamu düzeni, kamu sağlığı, ekonomik istikrar veya devletin temel fonksiyonları üzerinde ağır sonuçlar doğuran, ulusal siber kriz yönetimi mekanizmalarının devreye alınmasını gerektiren yaygın veya koordineli siber olaylardır.

(2) Taraflar, tespit ettikleri siber olayları Başkanlıkça belirlenen sınıflandırma kriterlerine uygun olarak değerlendirir ve Başkanlığa bildirir. Başkanlık, gerekli görmesi hâlinde yapılan sınıflandırmayı yeniden değerlendirebilir ve değiştirebilir.

(3) Siber olayın gelişimi veya etkilerinin değişmesi hâlinde olay seviyesi yeniden değerlendirilir ve gerekli görülmesi durumunda güncellenir.

(4) Başkanlık, siber olaylara ilişkin kayıtları tutar; bu kayıtları ulusal siber tehdit değerlendirmesi, erken uyarı faaliyetleri, istatistik üretimi, risk analizleri, denetim faaliyetleri ve ulusal siber güvenlik politikalarının oluşturulmasında kullanabilir.

(5) Başkanlık, siber olayın niteliği ve etkisini dikkate alarak her seviyedeki olaya müdahale edebilir veya ilgili kuruluşlar ya da sektörel SOME'ler tarafından olayın öncelikli olarak ele alınmasını sağlayabilir.

Siber olaylara müdahale ve koordinasyon

MADDE 15– (1) Başkanlık; siber olaylara ilişkin hazırlık, izleme, koordinasyon, uzaktan veya yerinde müdahale, teknik destek, iyileştirme ve olay sonrası değerlendirme faaliyetlerini yürütür veya yürütülmesini sağlar, gerek görmesi halinde SOME'lerden olay müdahale süreçlerini yürütmesini ister.

(2) Başkanlık, siber uzayda bulunan veya elde ettiği veri, imaj veya log kayıtları üzerinden saldırılara ait izleri takip edebilir, bunları inceleyerek delillendirebilir, suç teşkil ettiği değerlendirilen bulguları adli makamlar ve diğer ilgililer ile paylaşır.

(3) Başkanlık, olayın niteliği ve etkisi dikkate alınarak taraflardan; olayın teknik analizine ilişkin bilgi ve raporları, olay kayıtlarını, sistem ve güvenlik kayıtlarını, olayın etkileri

ve alınan tedbirler hakkında bilgi ve belgeyi, olayın giderilmesine yönelik hazırlanan eylem planlarını talep edebilir.

(4) Başkanlık, bir siber olayın sınır ötesi etkisi olduğu durumlarda, gerekli görmesi hâlinde etkilenen ülkedeki eşdeğer kurum veya kuruluşu bilgilendirebilir. Başkanlık, bildirilen önemli olaylar, vakalar ve siber tehditler hakkında anonimleştirilmiş ve birleştirilmiş verileri karşılıklılık ilkesi uyarınca bölgesel veya uluslararası kuruluşlarla paylaşabilir.

(5) Taraflar, Başkanlık tarafından; 14 üncü maddede yer alan seviye 4 ve seviye 5 siber olayların ulusal düzeyde eşgüdüm içerisinde yürütülmesini sağlamak üzere hazırlanan Ulusal Siber Güvenlik Acil Durum ve Kriz Yönetimi Planında kendilerine verilen görev, sorumluluk ve operasyonel süreçlere uymak, kriz anında talep edilen tedbirleri gecikmeksizin uygulamakla yükümlüdür.

SOME'lerin Kurulması ve Faaliyetlerinin Düzenlenmesi

MADDE 16– (1) Başkanlık, ulusal siber güvenliğin sağlanması, siber olaylara hazırlık seviyesinin artırılması, siber olayların tespiti, önlenmesi, analizi ve müdahalesinin etkin şekilde yürütülmesi amacıyla bünyesinde SOME kurulacak kuruluşları belirler, faaliyetlerini denetler.

(2) Başkanlık, SOME'lerin kuruluşuna, görev ve sorumluluklarına, çalışma usul ve esaslarına, idari yapılanmasına, personel yetkinliklerine ve teknik kapasitesine ilişkin hususları belirleyebilir.

SİP kullanımına ilişkin hususlar

MADDE 17– (1) Başkanlık tarafından, ulusal siber güvenlik ekosisteminde görev yapan SOME'ler ve Başkanlık arasında güvenli elektronik haberleşmenin ve koordinasyonun sağlanması, siber olaylara ilişkin bilgi ve belge paylaşımının gerçekleştirilmesi, koordinasyonun güçlendirilmesi ve siber olay müdahale süreçlerinin etkin şekilde yürütülmesi amacıyla SİP kurulur.

(2) SİP, Başkanlık ile SOME'ler arasındaki siber güvenlik faaliyetlerine ilişkin resmî elektronik iletişim ve koordinasyon platformudur. Başkanlık tarafından dördüncü fıkra kapsamında yer alan ve SİP üzerinden oluşturulan ve gönderilen elektronik bildirimler, bu Yönetmelikte belirtilen usul ve esaslara uygun olmak kaydıyla resmî elektronik bildirim niteliğindedir.

(3) Bu Yönetmelik kapsamında SOME'ler, Başkanlıkla ve SOME'lerle olan iletişimi SİP üzerinden yürütmekle, Başkanlık tarafından SİP üzerinden yayımlanan bildirimleri takip etmekle ve bu kapsamda gerekli önlemleri almakla, Başkanlık tarafından talep edilen bilgi, belge ve teknik kayıtları belirlenen sürelerde sistem üzerinden iletmekle yükümlüdür.

(4) Aşağıda belirtilen faaliyetlerin Başkanlık ile SOME'ler arasında SİP aracılığıyla yürütülmesi esastır:

a) Siber olay bildirimlerinin iletilmesi ve alınması.

b) Zafiyet, siber tehdit istihbaratı, zararlı yazılım göstergeleri, saldırı teknikleri ve diğer teknik siber güvenlik bilgilerinin güvenli şekilde paylaşılması.

c) Erken uyarı, alarm, duyuru, tavsiye ve teknik yönlendirmelerin ilgili taraflara ulaştırılması.

ç) Başkanlık tarafından yayımlanan politika, rehber, teknik doküman, talimat ve duyuruların paylaşılması.

d) Siber olay koordinasyonu kapsamında kurumlar arasında ortak çalışma yürütülmesi.

e) Ulusal ve sektörel siber güvenlik faaliyetlerinin koordinasyonu.

f) Başkanlıkça gerekli görülen diğer koordinasyon ve bilgi paylaşımı faaliyetlerinin yürütülmesi.

(5) SİP üzerinden gerçekleştirilecek tüm bilgi paylaşımı; gizlilik derecesi, bilgi güvenliği sınıflandırması ve yetki matrisi esas alınarak yürütülür.

Siber güvenlik olgunluk modeli

MADDE 18– (1) Başkanlık, kuruluşların siber güvenlik kapasitelerinin ve siber dayanıklılık düzeylerinin ölçülmesi, hedeflenen siber güvenlik olgunluk seviyesine ulaşmalarının sağlanması amacıyla Siber Güvenlik Olgunluk Modelini belirler ve yayımlar.

(2) Başkanlık, kuruluşun faaliyet alanı, büyüklüğü, sunduğu hizmetin ve sahip olduğu altyapının kritikliği gibi hususları dikkate alarak, kuruluşlara ya da sektöre özgü farklı olgunluk seviyeleri belirleyebilir.

(3) Kuruluşlar, Siber Güvenlik Olgunluk Modelinin yayımlanmasını müteakip altı ay içerisinde olgunluk değerlendirmesini gerçekleştirir. Periyodik olarak yılda bir defa olgunluk değerlendirmesi yaparak sonuçları takip eden yılın ocak ayı sonuna kadar Başkanlığa ve sektörel SOME'ye bildirir.

(4) Başkanlık, risk seviyesi, sektörün kritiklik derecesi, geçmiş olay kayıtları veya ulusal siber güvenlik ihtiyaçlarını dikkate alarak kuruluşlardan yeniden değerlendirme yapılmasını isteyebilir.

(5) Yapılan değerlendirmeler sonucunda, belirlenen asgari siber güvenlik olgunluk seviyesinin altında kaldığı veya model kapsamında değerlendirilen bileşenlerden herhangi birinde eksiklik bulunduğu tespit edilen kuruluşlar, eksikliklerin giderilmesine yönelik faaliyetleri, sorumlu birimleri, ihtiyaç duyulan insan kaynağını, teknolojik yatırımları, tahmini mali kaynakları ve uygulama takvimini içeren siber güvenlik iyileştirme planını tespit tarihinden itibaren en geç üç ay içinde hazırlar ve Başkanlığa sunar.

Bilgi ve belge talep etme

MADDE 19– (1) Başkanlık, bu Yönetmelik kapsamındaki yükümlülüklerin yerine getirilip getirilmediğinin tespiti, siber risklerin değerlendirilmesi, siber olayların incelenmesi, denetim, gözetim, izleme, uygunluk değerlendirmesi, sertifikasyon, yetkilendirme gibi görevlerin yerine getirilmesi amacıyla, taraflardan her türlü bilgi, belge, veri, kayıt, log kaydı, rapor, teknik doküman, varlık envanteri, yapılandırma bilgisi ve gerekli görülen diğer bilgi ve belgeleri yazılı veya elektronik ortamda talep edebilir, elektronik sistemler üzerinden yerinde veya uzaktan erişim sağlanmasını isteyebilir.

(2) Başkanlık, talebinde bilgi ve belgelerin kapsamını, sunulma usulünü, formatını ve süresini belirler. Talep edilen bilgi ve belgeler eksiksiz, doğru, güncel ve istenilen formatta, belirlenen süre içerisinde Başkanlığa sunulur. Başkanlık, gerekli görmesi hâlinde ilave bilgi ve belge talep edebilir.

(3) Kendisinden bilgi ve belge talep edilen taraflar, Başkanlıkça belirlenen süre içerisinde ve belirlenen formatta bu talebi karşılamakla yükümlüdür. Taraflara, talep etmeleri ve Başkanlık tarafından da uygun görülmesi durumunda ek süre verilebilir.

(4) Taraflar, kendi mevzuatındaki hükümleri gerekçe göstermek suretiyle talebin yerine getirilmesinden kaçınamazlar.

(5) Talep edilen bilgi ve belgelerin süresi içerisinde sunulmaması, eksik veya gerçeğe aykırı olarak sunulması hâlinde Kanun ve ilgili mevzuat hükümleri uygulanır.

Başkanlığın diğer görev ve yetkileri

MADDE 20– (1) Başkanlık, taraflara ait arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilir ve bunlarla irtibat kurabilir, yürüttüğü faaliyetlerle sınırlı olmak üzere bilgi, belge, veri, imaj ve kayıtları elde edebilir, inceleme ve değerlendirmede bulunabilir.

(2) Başkanlık, ulusal veya uluslararası siber güvenlik tatbikatlarını planlar, koordine eder, gerekli hâllerde uluslararası siber güvenlik tatbikatlarına katılım veya ülke adına koordinasyonu sağlar. Tatbikat sonuçlarını değerlendirir, tespit edilen eksikliklerin giderilmesine yönelik faaliyetleri takip eder.

(3) Başkanlık, siber güvenlik ile ilgili yurtiçinde veya yurtdışında etkinlik, fuar ve benzeri faaliyetler düzenleyebilir veya düzenlenenlere katılım sağlayabilir.

(4) Başkanlık, SOME'ler, ulusal ve uluslararası paydaşlar, sektörler, kamu, özel sektör ve üniversiteler arasında iş birliği ve koordinasyonu sağlar, gerekli görmesi durumunda çalışma grupları ve teknik komisyonlar oluşturabilir.

(5) Başkanlık, stratejik iş birliği, bilgi paylaşımı ve ortak politikalar geliştirme gibi amaçlarla bölgesel ve uluslararası iş birliği gruplarına katılım sağlayabilir.

(6) Başkanlık, siber güvenlik ile ilgili hususlarda, ulusal ve uluslararası düzeyde iş birliği yapılması, koordinasyonun sağlanması, iş birliği ağlarına katılım sağlanmasına ilişkin irtibat noktası olarak faaliyet yürütür.

(7) Başkanlık, siber güvenlik konusunda ulusal ve uluslararası düzeyde eğitim, sertifikasyon, kapasite inşası, farkındalık çalışmaları yürütür veya yürütülmesini sağlar.

(8) Başkanlık, yürüttüğü faaliyetler kapsamında elde edilen bilgiler doğrultusunda güvenlik uyarıları, raporlar, istatistikler, teknik ve idari tavsiyeler, rehberler, bültenler ve iyi uygulama önerileri yayımlar.

(9) Başkanlık, ulusal güvenlik ihtiyaçları, teknolojik gelişmeler ve uluslararası yükümlülükler doğrultusunda ulusal veya uluslararası standartları, teknik gereksinimleri, iyi uygulama rehberlerini ve sektörel güvenlik kriterlerini uyumlaştırabilir ve bunların uygulanmasına ilişkin yükümlülük getirebilir.

ÜÇÜNCÜ BÖLÜM
SOME'lere İlişkin Hususlar

Sektörel SOME'lerin kurulması

MADDE 21– (1) Siber Güvenlik Kurulunca belirlenen kritik altyapı sektörlerinde düzenleyici ve denetleyici faaliyet yürüten kamu kurumları bünyesinde faaliyet alanları ile sınırlı olmak üzere sektörel SOME kurulur.

(2) Sektörel SOME kurulacak kamu kurumları ve faaliyet alanları Başkanlık tarafından belirlenerek ilgili kurumlara bildirilir.

(3) Sektörel SOME'ler, kurumun ana faaliyet alanından ya da bilişim altyapılarından sorumlu biri en az daire başkanı olmak üzere faaliyet gösterilen sektörün büyüklüğü, kritiklik derecesi dikkate alınarak yeterli sayıda ve yetkinlikte personelden oluşur. Sektörel SOME'de görev alan tüm personelin yetkinlik ve yeterliliğine ilişkin bilgi ve belgeler Başkanlığa iletilir. Kurumun ana faaliyet alanının ve bilişim altyapılarının farklı birimler tarafından yürütülüyor olması halinde ilgili tüm birimlerden temsilcilerin sektörel SOME bünyesinde yer alması sağlanır.

TASLAK

(4) Sektörel SOME'ler, bünyesinde görev alacak personel için 7315 sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu kapsamında güvenlik soruşturması ve arşiv araştırması yaptırır.

(5) Sektörel SOME'nin yedi gün yirmi dört saat ulaşılabilir iletişim bilgileri Başkanlık ve kurumsal SOME'ler ile paylaşılır. İletişim bilgilerinde değişiklik olması halinde üç işgünü içinde SİP üzerinden gerekli değişiklik yapılır.

(6) Sektörel SOME'ler bu Yönetmelik kapsamındaki faaliyetlerini Başkanlık koordinasyonunda yürütür.

Sektörel SOME'lerin görev ve sorumlulukları

MADDE 22– (1) Sektörel SOME'ler, bu Yönetmeliğin sektör bazlı uygulanmasına, takibine ilişkin faaliyetleri Başkanlık koordinasyonunda yürütür.

(2) Sektörel SOME'ler, 5 inci ve 6 ncı maddeler uyarınca belirlenen kritik altyapı kriterlerini kendi sektörleri bakımından dikkate alarak kritik altyapıya sahip kuruluşları ve kritik altyapıya sahip olmamakla birlikte, sektördeki önemi nedeniyle kurumsal SOME kurma yükümlülüğü getirilecek kuruluşları tespit ederek Başkanlık onayına sunar ve onaylanmasını müteakip bu kuruluşlara bildirimde bulunulur.

(3) Sektörel SOME'ler tarafından kuruluşların adı, vergi numarası, resmi iletişim bilgileri, kayıtlı elektronik posta adresi, konumları, yıllık brüt satış hasılatı, kritik altyapı değerlendirme kriterine konu olan bilgiler Başkanlık ile paylaşılır. Kuruluşların kayıtlı elektronik posta adresi dâhil resmi iletişim bilgileri veya konumlarında gerçekleşen değişiklik beş iş günü içinde Başkanlığa bildirilir.

(4) Faaliyete yeni başlamış olan kuruluşlara ilişkin değerlendirme, kuruluşun faaliyete başlamasından itibaren bir ay içinde yapılarak Başkanlığa bildirilir.

(5) Sektörel SOME'ler tarafından her yıl mayıs ayı sonuna kadar sektöründeki kuruluşların kritik altyapıya sahip olup olmadığına ilişkin değerlendirme yapılarak güncel bilgiler Başkanlığa bildirilir.

(6) Sektörel SOME'ler, sektörlerinde faaliyet gösteren tarafların sağlaması gereken siber güvenlik gereksinimlerine yönelik düzenlemeleri, bu Yönetmelikte yer alan yükümlülüklerle uyumlu olacak şekilde yapar veya mevcut düzenlemelerini bu doğrultuda günceller. Sektörel SOME'ler bu doğrultuda yapacakları düzenlemelerde aşağıdaki hususları dikkate alır:

a) Kurumsal SOME'lerde görev yapan personelin niteliği, görev ve sorumlulukları.

b) Sektöründe faaliyet gösteren kuruluşlara ilişkin siber güvenlik, iş sürekliliği ve hizmet kalitesine ilişkin sektöre özgü gereksinimler.

c) Sektöründe faaliyet gösteren kritik altyapı kuruluşlarının kritik altyapı kapsamında değerlendirilecek bilişim sistemleri ve hizmetleri.

(7) Sektörel SOME'ler, 31 inci madde kapsamında yapılan kurumsal siber riskleri dikkate alarak iki yılda bir sektörel siber risk yönetim sürecini işletir ve hazırlayacağı sektörel siber risk raporunu ilgili yılın mayıs ayı sonuna kadar Başkanlık ile paylaşır. Sektörel siber risk yönetiminde, 10 uncu maddede düzenlenen hususlar gözetilir.

(8) Sektörel SOME'ler, 14 üncü maddede belirlenen siber olay sınıflandırması doğrultusunda sektöründe faaliyet gösteren kuruluşların etkilendiği siber olaylara uzaktan veya yerinde müdahale, teknik destek, iyileştirme ve olay sonrası değerlendirme faaliyetleri yürütebilir.

(9) Sektörel SOME'ler, faaliyet alanı kapsamında acil durum, iş sürekliliği ve kriz yönetim planlarını hazırlar ve gerekli durumlarda Başkanlık ile koordineli bir şekilde bu planları uygulamaya alır.

(10) Sektörel SOME'ler, siber saldırılara karşı hazırlık seviyesini, tespit ve müdahale yeteneklerini, organizasyon ve karar alma süreçlerini test etmek amacıyla sektöründe faaliyet gösteren kuruluşların katılımıyla yılda en az bir kez sektörel tatbikat gerçekleştirir. Tatbikatlar, canlı sistem senaryolarını içerebileceği gibi simülasyon veya süreçlerin tatbik edildiği masabaşı senaryolarını da içerebilir. Sektörel tatbikat sonuçları analiz edilerek kurumsal ve sektörel düzeyde iyileştirilmesi gereken hususlar belirlenerek ilgili kuruluşlar ile paylaşılır.

(11) Sektörel SOME'ler, siber olgunluk seviyelerinin artırılması amacıyla periyodik olarak eğitim ve farkındalık faaliyetleri düzenler.

(12) Sektörel SOME'ler, her yıl mayıs ayı sonuna kadar bir önceki yıl siber güvenlik alanında gerçekleştirilen faaliyetleri bir rapor halinde Başkanlığa iletir. Raporda asgari aşağıdaki hususlar yer alır:

a) Üçüncü fıkra kapsamında tespit edilen kuruluşların güncel bilgileri.

b) Yaşanan siber olaylara, etkilerine ve sonuçlarına ilişkin istatistikler.

c) Siber olay müdahale faaliyetleri.

ç) Sektörün genelini etkileyen siber zafiyetlerin giderilmesine yönelik yapılan faaliyetler.

d) Sektörde ürün ve hizmet bağımlılığından kaynaklı risklerin azaltılmasına yönelik yürütülen faaliyetler ile alınması gereken tedbirler.

e) Sektörel tatbikatların katılım ve sonuçlarına ilişkin bilgiler ile olgunluğun artırılmasına yönelik atılacak adımlar.

f) Siber olgunluğun artırılmasına yönelik yürütülmüş olan eğitim ve farkındalık faaliyetleri.

Kurumsal SOME'lerin kurulması

MADDE 23– (1) 28 inci madde kapsamında yer alanlar, siber tehditlerin önlenmesi, siber dayanıklılığın, kurumsal olgunluğun ve olay müdahale kapasitesinin artırılması amacıyla bünyelerinde Başkanlık tarafından bildirilmesinden itibaren bir ay içerisinde kurumsal SOME kurar, Başkanlık ve sektörel SOME'ye bildirir.

(2) Kurumsal SOME, büyüklük, kritiklik derecesi, bilişim sistemlerinin yaygınlığı ve risk profili göz önünde bulundurularak, görevlerini eksiksiz yerine getirebilecek idari ve operasyonel yetkiye sahip, bilgi güvenliği veya siber güvenlik alanında uzmanlaşmış, en az biri yönetici seviyesinde ve üç kişiden az olmamak üzere yeterli sayıda ve yetkinlikte personelden oluşur. Aynı kişi, birden fazla kurumsal SOME'de görev alabilir.

Kurumsal SOME'lerin görev ve sorumlulukları

MADDE 24– (1) Kurumsal SOME'lerin görev ve sorumlulukları şunlardır:

a) Siber dayanıklılığın artırılması amacıyla ihtiyaç duyulan teknik ve idari kaynaklar ile bütçenin belirlenmesine yönelik üst yönetime öneriler sunmak.

b) Başkanlık veya sektörel SOME tarafından yapılan alarmları, uyarıları, duyuruları ve zafiyet bildirimlerini yedi gün yirmi dört saat takip etmek, kuruluş bünyesinde gerekli aksiyonların alınmasını koordine etmek.

c) Kendisine doğrudan veya dolaylı olarak yapılan ya da yapılması muhtemel siber saldırılara karşı gerekli koruma, engelleme ve sıkılaştırma tedbirlerini almak veya alınmasını

sağlamak; siber olayların tespiti, analizi, kök neden tespiti ve bertaraf edilmesine yönelik müdahale mekanizmalarını işletmek.

ç) Siber olayların önlenmesi ve siber tehditlerin bertaraf edilmesine yönelik faaliyetleri sektörel SOME ve Başkanlık ile koordinasyon içerisinde yürütmek; meydana gelen siber olayları ve tehditleri 33 üncü maddede öngörülen usul ve esaslar çerçevesinde bildirmek ve raporlamak.

d) Bir siber olayla karşılaşılması hâlinde, olaya öncelikle kurumsal imkân ve kabiliyetler çerçevesinde müdahale etmek; müdahale kapasitesinin yetersiz kalması hâlinde bağlı olunan sektörel SOME'den veya Başkanlıktan teknik destek talebinde bulunmak.

e) Siber olaya müdahale esnasında veya yürütülen incelemelerde suç teşkil eden bir durumla karşılaşılması hâlinde dijital delillerin bütünlüğünün korunmasını teminen, durumu gecikmeksizin yetkili adli makamlara, kolluk kuvvetlerine, sektörel SOME'ye ve Başkanlığa bildirmek.

f) Yedi gün yirmi dört saat esasına göre erişilebilir güncel iletişim ve sorumlu personel bilgilerini sektörel SOME ve Başkanlık ile paylaşmak, değişiklikleri derhal bildirmek.

g) Başkanlık veya sektörel SOME koordinasyonunda gerçekleştirilen siber güvenlik tatbikatlarına ve bilgi paylaşım platformlarına katılım sağlamak, bu süreçlere yönelik teknik, idari ve insan kaynağı altyapısını hazır bulundurmak.

(2) Kurumsal SOME personeli, yürüttükleri görevler dolayısıyla elde ettikleri her türlü bilgi ve belge bakımından sır saklama yükümlülüğüne tabidir. Bu yükümlülük, görevin sona ermesi hâlinde de süresiz olarak devam eder.

(3) Kurumsal SOME'ler, Başkanlık tarafından yayımlanan politika, standart, rehber, teknik kriter, talimat ve diğer ulusal düzenlemelere uymakla yükümlüdür.

SİP kullanıcılarının görev ve sorumlulukları

MADDE 25– (1) SİP kullanıcılarına yalnızca görev alanları kapsamındaki bilgi ve içeriklere erişim yetkisi tanımlanır.

(2) SİP kullanıcılarının görev ve sorumlulukları şunlardır:

a) SİP'in kullanımına ilişkin Başkanlıkça belirlenen usul ve esasları, SİP üzerinden kendilerine iletilen bildirim, yazı ve belgeleri ve bu kapsamda doğan yükümlülükleri kabul ettiklerine ilişkin elektronik onay vermek.

b) Başkanlık tarafından belirlenen kimlik doğrulama ve erişim güvenliği tedbirlerine uymak.

c) Hesap bilgilerini ve kimlik doğrulama araçlarını üçüncü kişilerle paylaşmamak.

ç) Platform üzerinden edinilen bilgi ve belgeleri yetkisiz kişi veya sistemlerle paylaşmamak.

d) Siber olaylara ilişkin doğru, güncel ve teyit edilmiş bilgileri gecikmeksizin paylaşmak.

e) Başkanlık tarafından belirlenen usullere uymak.

DÖRDÜNCÜ BÖLÜM
Genel Yükümlülükler

Temel siber hijyen yükümlülükleri

MADDE 26– (1) Taraflar, sahip oldukları veya kullandıkları bilişim sistemleri, cihazlar ve dijital varlıklar nezdinde asgari düzeyde aşağıdaki tedbirleri almakla ve uygulamakla yükümlüdür:

a) Bilişim sistemlerine, kablosuz ağlara, dijital hesaplara ve servislere erişimde tahmin edilmesi zor ve güçlü parolalar belirlenir. Parolalar, tek kullanımlık doğrulama kodları ve erişim bilgileri üçüncü kişilerle paylaşılmaz.

b) Kişisel ve kurumsal kullanıma yönelik bilgisayarlarda zararlı yazılımlara karşı koruma sağlayan uygun güvenlik önlemleri bulundurulur. Bu cihazlarda kullanılan uygulamalar, resmi üretici veya uygulama mağazaları aracılığı ile yüklenir.

c) Kullanıcılar tarafından işletim sistemleri, yazılımlar ve uygulamalar, üreticileri tarafından yayımlanan güncel ve kararlı sürümleri kullanılır. Üretici desteği veya güvenlik güncellemesi sona ermiş bireysel kullanıma yönelik cihaz ve yazılımların kullanımında, olası siber riskler göz önünde bulundurularak gerekli dikkat ve özen gösterilir.

ç) Kaynağı doğrulanmamış veya şüpheli e-posta, mesaj, bağlantı ve dosya eklentileri açılmaz, çalıştırılmaz veya bunlar üzerinden işlem yapılmaz, sosyal mühendislik faaliyetleri ve oltalama saldırılarına karşı azami hassasiyet gösterilir.

d) Veri kaybını önlemek veya zararlı yazılımların etkilerini azaltmak amacıyla, kritik kişisel veya kurumsal veriler imkân dâhilinde düzenli aralıklarla yedeklenir.

e) Kamuya açık internet sitesi, e-ticaret platformu veya dijital uygulama üzerinden hizmet sunan taraflar; kullanıcı kayıt ve üyelik işlemlerinde e-posta veya kısa mesaj servisi gibi doğrulama yöntemlerini uygular; kullanıcı oturumlarının belirli bir hareketsizlik süresi sonunda otomatik olarak kapatılmasını sağlar.

f) Dijital hizmet sunumunda kullanılan internet sayfaları ve uygulamalarda; veri giriş alanlarında yetkisiz komut veya veritabanı sorgusu çalıştırılmasını engelleyecek temel güvenlik tedbirleri ile parola, kimlik ve hesap bilgileri gibi hassas verilerin internet adresi üzerinden açık metin haliyle iletilmesini önleyici tedbirler alınır.

g) Başkanlık veya yetkili merciler tarafından kitlesel bildirim araçları, kısa mesaj servisi veya genel iletişim kanalları üzerinden yapılan resmi siber güvenlik uyarıları ve acil tedbirler takip edilir ve uygulanır.

ğ) Temel siber hijyen gereksinimlerine yönelik Başkanlık tarafından yayımlanacak yazılı veya görsel rehber, kılavuz, tavsiye ve duyurular ile belirtilen önlemler alınır.

(2) Bu Yönetmelik kapsamında yer alan gerçek kişiler ile kurumsal SOME kurma yükümlülüğü bulunmayan tarafların birinci fıkrada belirtilen yükümlülüklere aykırı hareket etmesi ve bu aykırılığın kritik altyapılara yönelik siber saldırı veya siber olaylarda kullanılmasına imkân sağladığının tespit edilmesi hâlinde, fiilin niteliği ve doğurduğu riskler dikkate alınarak Kanunda ve ilgili mevzuatta öngörülen yaptırımlar uygulanır.

Olay bildirimi

MADDE 27– (1) Taraflar, etkilendiği veya haberdar olduğu siber olayları, olası ihlalleri ve şüpheli durumları gecikmeksizin Yönetmeliğin 12 nci maddesi çerçevesinde Başkanlıkça belirlenen usul ve formata uygun olarak Başkanlığa bildirmekle yükümlüdür.

(2) Bu madde kapsamında yapılan bildirimlerde paylaşılan ticari, kişisel veya teknik veriler gizli tutulur ve amacı dışında kullanılamaz. Siber olaya maruz kalan tarafların bildirimde bulunmuş olması, bu Yönetmelik ve ilgili mevzuat kapsamındaki idari veya hukuki sorumluluklarını ortadan kaldıran veya azaltan bir husus olarak ileri sürülemez.

BEŞİNCİ BÖLÜM

Kurumsal SOME Kurma Yükümlülüğü Bulunan Kuruluşlara İlişkin Hususlar

Kurumsal SOME Kurma Yükümlülüğü Bulunan Kuruluşlar

MADDE 28– (1) Kurumsal SOME kurma yükümlülüğü getirilenler, dördüncü bölümde yer alan yükümlülüklere ek olarak, bu bölümde düzenlenen hususlara ilişkin gerekli tedbirleri alır.

(2) Başkanlık, kritik altyapı sektörlerinde faaliyet göstermeyenlere de kurumsal SOME kurma yükümlülüğü getirebilir. Bu kapsamda yer alanlar, dördüncü ve beşinci bölümde yer alan yükümlülüklere tabidir.

(3) Siber güvenliğin sağlanmasına yönelik bilişim sistemlerinde öncelikli olarak yerli ve milli ürün ve hizmetler kullanılır.

Bilgi güvenliği yönetim sistemi

MADDE 29– (1) Kurumsal bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması amacıyla, ulusal ve uluslararası standartlarla ve iyi uygulama örnekleriyle uyumlu, üst yönetimin taahhüdünü içeren yazılı bir bilgi güvenliği politikası belirlenir ve tüm kritik sistemleri ve hizmetleri kapsayacak şekilde BGYS kurulur, yürütülür ve sürekli iyileştirilir.

(2) BGYS faaliyetlerinin yürütülmesi ve bu faaliyetler kapsamında gerçekleştirilen işlemlerin takibi amacıyla, doğrudan üst yönetim tarafından yetkilendirilmiş en az bir kişi BGYS sorumlusu olarak görevlendirilir veya BGYS ekibi oluşturulur.

Varlık envanteri

MADDE 30– (1) BGYS kapsamındaki tüm bilişim sistemi ve varlıkların, aralarındaki karşılıklı bağımlılıklarını, yaşam döngüsü durumlarını ve üstlendikleri kritik iş fonksiyonlarını gösterecek şekilde dokümante edilerek merkezi bir varlık envanteri oluşturulur. Birçok alt varlığın belirli bir kritik hizmeti veya fonksiyonu yerine getirmek üzere birlikte kullanıldığı karmaşık sistem mimarileri, bütüncül siber risk yönetimi faaliyetine imkân tanımak şartıyla tek bir ana varlık grubu olarak kabul edilebilir.

(2) Varlık envanterinde asgari olarak aşağıdaki bilgiler tutulur;

a) Varlığın adı, benzersiz tanımlayıcısı, varlık türü, amacı, hizmet veya iş fonksiyonu ve ilişkilendirildiği kritik hizmet.

b) Varlığın fiziksel, mantıksal, sanal, bulut veya coğrafi konumu, ağ bölgesi, dışa açıklığı bilgisi.

c) Üretici, ürün, model, sürüm, seri numarası, lisans, destek ve bakım durumu ile üretici desteğinin sona erme tarihi.

ç) Varlığın sahibi, işletmecisi, teknik sorumlusu, bilgi güvenliği sorumlusu, hizmet sağlayıcısı ve gerektiğinde yedi gün yirmi dört saat ulaşılabilir iletişim bilgisi.

d) Varlığın iş sürekliliği ve felaket kurtarma ilişkisi; yedekleme sıklığı, yedek konumu, kurtarma süresi hedefi, kurtarma noktası hedefi bilgisi ve bağımlı olduğu varlıklar.

e) Varlığın kullandığı veya ürettiği verilerin sınıfı, veri sahibi, veri işleme amacı, saklama süresi, veri akışları ve sınır ötesi aktarım durumu.

f) Varlığın zafiyet, yama, güvenlik testi, sertifika, anahtar, olay ve değişiklik geçmişine ilişkin ilgili kayıtlarla bağlantısı.

g) Varlığın, planlanan, tedarik edilen, geliştirilmekte olan, test sürecinde, uygulamada, askıda olan, kullanım dışı kalan, devredilen veya imha edilen gibi yaşam döngüsü durumu.

ğ) Varlığın üçüncü taraf, tedarik zinciri, bulut, uzaktan erişim ve diğer teknik veya operasyonel bağımlılıkları.

h) Başkanlıkça veya yetkili mercilerce belirlenen diğer bilgiler.

(3) Varlıklarda meydana gelebilecek zafiyetlerin gizlilik, bütünlük ve erişilebilirlik seviyeleri; yasal gereksinimler, varlığın kritikliği ve olası bir ihlalin doğuracağı etki kriterlerine göre belirlenerek, varlıklar uygun biçimde sınıflandırılır ve etiketlenir.

TASLAK

(4) Belirlenen her bir sınıf için asgari olarak, erişim, yetkilendirme, kullanım, depolama, sınır ötesi de dâhil olmak üzere iletim, üçüncü taraflarla paylaşım ve ömrünü tamamlayanların güvenli imha süreçlerine ilişkin kurallar ve güvenlik kriterleri yazılı olarak tanımlanır ve uygulanır.

(5) Varlıklarda meydana gelen her türlü değişiklik, ekleme veya devreden çıkarma işleminde envanter eş zamanlı olarak güncellenir.

(6) Varlığın kullanım ömrünü tamamlaması, devreden çıkarılması, devredilmesi veya imha edilmesi hâlinde; varlıkta bulunan veriler, yedekler, kimlik doğrulama bilgileri, sertifikalar, anahtarlar ve yapılandırma kayıtları güvenli şekilde ayrıştırılır, geri döndürülemez biçimde silinir veya ilgili mevzuata uygun olarak imha edilir. Bu varlıklara ait sistem erişim izinleri, dijital sertifikalar ve envanter kayıtları derhal iptal edilir.

(7) Kullanılan yazılımların üretici, ürün adı, sürüm ve lisans doğrulama bilgilerini içeren güncel bir yazılım ve lisans envanteri merkezi olarak tutulur ve Başkanlığın talebi hâlinde gecikmeksizin sunulur.

(8) Varlık envanteri en az yılda bir kez; önemli bir siber olay, mimari değişiklik, yeni kritik hizmet, tedarikçi değişikliği, birleşme veya kuruluş yapısında değişiklik olması durumunda ise yeniden gözden geçirilir. Gözden geçirme sonucunda eksik, hatalı veya mükerrer kayıtlar düzeltilir.

(9) Varlık envanteri kayıtlarına erişim, görev ve yetki esasına göre sınırlandırılır. Ekleme, değiştirme, silme, dışa aktarma ve sorgulama işlemleri kullanıcı, tarih, saat, kaynak ve işlem türü bilgileriyle kaydedilir, kayıtların bütünlüğü ve geriye dönük izlenebilirliği korunur.

(10) Başkanlık, varlık envanterinin kapsamının belirlenmesi, tutulması, güncellenmesi ve diğer süreçlere ilişkin usul ve esasları belirleyebilir.

Kurumsal siber risk yönetimi

MADDE 31– (1) 10 uncu maddeye uygun olarak yılda en az bir kez risk yönetimi yapılır.

(2) Risk yönetimi sonuçları üst yönetime raporlanır ve risk işleme kararları yönetim tarafından onaylanır.

(3) Risk yönetimine esas tüm iş ve işlemler kayıt altına alınarak asgari beş yıl süreyle güvenli ortamlarda muhafaza edilir.

(4) Risk yönetimi süreci; değişen tehdit ortamı, önemli değişiklikler, siber olaylar ve denetim sonuçları doğrultusunda yönetim periyodu beklenmeksizin gözden geçirilir.

(5) Risk işleme planında yer alan tedbirlerin uygulanma durumu belirlenen aralıklarla izlenir. Süresi içinde tamamlanmayan tedbirler için gecikme gerekçesi, geçici kontrol ve yeni hedef tarih kayıt altına alınır.

Siber olay müdahale planı

MADDE 32– (1) Bilişim sistemlerine ve varlıklara yönelik gerçekleştirilen veya gerçekleştirilmesi muhtemel olan her türlü siber tehdit ve olay, sızma girişimi, veri ihlali ve zararlı faaliyetlerin zamanında tespit edilmesi, analiz edilmesi, kontrol altına alınması ve ortadan kaldırılması amacıyla siber olay müdahale planı hazırlanır, uygulanır ve gözden geçirilir.

(2) Siber olay müdahale planı asgari olarak; olayların tespit edilmesi, doğrulanması, analiz edilmesi ve önceliklendirilmesi, müdahaleden sorumlu rol ve görevlerin belirlenmesi, olayın yayılmasının ve etkilerinin sınırlandırılması, tehdidin ve olayın nedenlerinin ortadan

kaldırılması, olayla ilgili delil ve kayıtların güvenliğinin ve bütünlüğünün korunması, etkilenen sistem ve varlıkların güvenli şekilde kurtarılması ve normal işleyişe döndürülmesi ile olay sonrasında değerlendirme ve iyileştirme faaliyetlerini içerir.

(3) Meydana gelen siber olayların kök nedenlerinin tespit edilmesi, benzer olayların tekrarlanmasını engelleyecek kalıcı çözümlerin geliştirilmesi ve sistem zafiyetlerinin ortadan kaldırılması amacıyla kurumsal düzeyde problem yönetimi süreci işletilir. Siber olay müdahale ve problem yönetimi süreçlerinden elde edilen bulgular; risk yönetimi, politika yönetimi ve farkındalık faaliyetlerinde dikkate alınır.

(4) Personelin görevleri esnasında karşılaştıkları, fark ettikleri veya şüphelendikleri her türlü siber güvenlik olayını, zafiyeti ve siber tehdidi, kurumsal cihaz ve taşınabilir medyaların kaybı veya çalınması gibi siber risk teşkil eden olayları hızlı, kolay ve güvenli bir şekilde kurumsal SOME'ye veya yetkilendirilmiş bilgi güvenliği sorumlularına bildirebilecek iç bildirim kanalları oluşturulur ve işler durumda tutulur.

Siber olay yönetimi

MADDE 33– (1) 14 üncü madde kapsamında düzenlenen birinci ve ikinci seviye siber olaylar bağlı bulunulan sektörel SOME'ye, üçüncü, dördüncü, beşinci seviye siber olaylar ise bağlı bulunulan sektörel SOME'ye ve Başkanlığa, siber olayın tespit edilmesinden itibaren en geç on iki saat içinde mevcut bilgiler ve teknik verilerle birlikte bildirilir. Sektörel SOME, Başkanlığa bildirim yapılmadığını tespit ederse gelen bildirimi gecikmeksizin Başkanlığa iletir. Sektörel SOME'nin bulunmaması durumunda, doğrudan Başkanlığa bildirim yapılır.

(2) Siber olayın tespit edilmesinden itibaren en geç yetmiş iki saat içinde olayın güncel durumu, ilk değerlendirme sonuçları, tespit edilen tehdit göstergeleri ve alınan önlemleri içeren güncel durum bilgisi, birinci fıkrada belirtilen olay seviyelerine göre bildirilir. Olayın seyrini veya etkisini değiştiren önemli bir gelişmenin meydana gelmesi hâlinde bu süre beklenmeksizin bildirim güncellemesi yapılır.

(3) Başkanlık, birinci fıkrada yer alan bildirimi aldıktan sonra bildirimde bulunan tarafa olayla ilgili teknik destek sağlayabilir, olay bildirimi ve güncellemeler ile ilgili ek bilgi, belge ve açıklama talep edebilir.

(4) Başkanlık, siber olaydan olumsuz etkilenenlerin veya etkilenme ihtimali bulunanların bilgilendirilmesini ve alabilecekleri her türlü tedbir veya çözümü gecikmeksizin duyurmasını talep edebilir.

(5) Birinci fıkrada belirtilen olay bildiriminden itibaren en geç bir ay içinde aşağıdaki hususları içeren detaylı olay raporu sunulur:

a) Olayın ciddiyeti ve etkisi de dâhil olmak üzere ayrıntılı açıklaması.

b) Olayı tetiklemiş olması muhtemel tehdit türü veya kök neden.

c) Uygulanan ve devam eden etki ve risk azaltma önlemleri.

ç) Varsa olayın sınır ötesi etkileri.

d) Saldırının başlangıcından olayın tespit edilmesine kadar geçen süre içerisinde saldırganların davranışlarına ilişkin zaman çizelgesi.

(6) Siber olaya ilişkin her türlü bilgi, belge, işlem ve log kaydı, olay inceleme ve kök neden analizi süreçleri boyunca güvenli ortamlarda bütünlüğü korunarak muhafaza edilir.

(7) Siber olaylardan elde edilen teknik tecrübelerin, alınan tedbirlerin ve iyi uygulamaların kurumsal hafızaya kazandırılmasını, ilgili personelle kontrollü şekilde paylaşılmasını ve kullanılmasını sağlayacak kayıt ve değerlendirme mekanizmaları oluşturulur.

Zafiyet yönetimi

MADDE 34– (1) Başkanlık tarafından yetkilendirilmiş bağımsız kuruluşlara yılda en az bir kez sızma testi yaptırılır.

(2) Düzenlenen sızma testi sonuç raporları, sızma testini gerçekleştiren bağımsız kuruluşlar tarafından Başkanlığa ve kuruluşa sunulur. Tespit edilen bulgular, önem derecelerine göre önceliklendirilerek makul süre içerisinde teknik sıkılaştırma tedbirleri uygulanır ve doğrulaması yapılır. Söz konusu rapor ve kayıtlar, asgari beş yıl süreyle güvenli ortamlarda muhafaza edilir.

(3) Bilişim sistemlerinde düzenli olarak zafiyet taraması yapılır veya yaptırılır; tarama sonuçları, tespit edilen zafiyetler ve uygulanan düzeltici işlemlere ilişkin bilgiler, Başkanlığın talebi halinde belirlenen yöntem çerçevesinde Başkanlığa iletilir.

Kurumsal iş sürekliliği

MADDE 35– (1) Sektörel faaliyet alanı kapsamında yer alan hizmetler ile bilişim sistemleri ve varlıkların fiziksel tehditler, salgın hastalıklar, doğal afetler, kazalar, donanım arızaları, ağ ve enerji kesintileri, insan hataları, siber tehditler ile siber saldırılar neticesinde zarar görmesini ve kesintiye uğramasını önlemek, hizmet kesinti sürelerini kabul edilebilir seviyede tutmak ve kurumsal iş sürekliliğini sağlamak amacıyla kurumsal iş sürekliliği planı hazırlanır ve yürütülür.

(2) Kurumsal iş sürekliliği planı asgari olarak; iş etki analizini, kritik iş süreçlerini kesintiye uğratabilecek siber ve siber olmayan riskleri, kritik hizmet ve bilişim sistemlerindeki tek hata noktalarının tespitini ve bunların etkisinin azaltılmasına yönelik tedbirleri, riskler karşısında uygulanacak adımları, acil durum iş gücü ve görev tanımlarını, planın devreye alınması için gerekli koşulları, yedekli altyapıların kullanım senaryolarını, paydaş ve kamuoyu iletişim stratejilerini içerir.

(3) Hazırlanan planların işlerliğini, güncelliğini ve varlıkların hazırlık seviyesini ölçmek amacıyla; siber ve siber olmayan senaryoları içeren masaüstü, simülasyon veya canlı sistem tatbikatları gerçekleştirilir ve sonuçlarını kayıt altına alınır. Tatbikat sonuçları, elde edilen bulgular, varlık envanterindeki önemli değişiklikler, siber risk yönetimi ve işleme faaliyetleri ile siber ve siber olmayan tehdit ortamındaki güncel değişimler doğrultusunda iş sürekliliği planları güncellenir.

Güvenli kimlik doğrulama

MADDE 36– (1) Kritik hizmetlerin sunumunda kullanılan sunucular, kritik uygulama ve internet arayüzleri, ağ altyapısı yönetimi, veri tabanı yönetimi gibi bilişim sistemlerine ayrıcalıklı yetkiye sahip erişimler ile uzaktan erişim noktası vasıtasıyla yapılan tüm erişimlerde, statik parolalara ek olarak en az bir bağımsız katman içeren çok faktörlü kimlik doğrulama mekanizmalarının kurulması ve kullanılması zorunludur.

(2) Bilişim sistemlerinde kullanılan parolaların oluşturulması ve değiştirilmesi süreçlerinde asgari olarak aşağıdaki kurallara uyulur:

a) Parolalar tahmin edilmesi zor, belirli bir asgari uzunluk ve karmaşıklık standardına sahip olacak şekilde sistem tarafından zorunlu kılınır.

b) Geçici parolalar ilk girişte zorunlu olarak değiştirilir.

c) Kullanıcıların eski parolalarını belirli bir süre boyunca yeniden kullanmaları sistem tarafından engellenir, parolaların fiziksel veya elektronik ortamlarda açık metin olarak saklanmasını önleyici tedbirler alınır.

ç) Sistem, donanım, veri tabanı ve yazılımların üreticisi tarafından atanmış varsayılan hesap ve parolalar, kurulum ve devreye alma aşamasında derhal değiştirilir.

(3) Parola yenileme periyotları, sistemlerin ve hesapların kritiklik derecesine göre kuruluşlar tarafından belirlenir. Güvenlik ihlali şüphesi veya siber olay meydana gelmesi durumunda ilgili tüm kullanıcı ve sistem parolaları derhal yenilenir.

(4) Çok faktörlü kimlik doğrulamayı teknik olarak desteklemeyen eski sistemler ve operasyonel teknoloji bileşenleri bakımından; erişim ağ geçidi, atlama sunucusu veya eşdeğer telafi edici kontroller üzerinden çok faktörlü kimlik doğrulamanın sağlanması yeterli kabul edilir. Bu istisnadan yararlanan sistemler gerekçesiyle birlikte kayıt altına alınır.

Yetki ve rol yönetimi

MADDE 37– (1) Kullanıcıların kendileri ile ilişkilendirilebilecek ve yaptıkları işlemlerden hukuken sorumlu olmalarını sağlayacak nitelikte, ayırt edilebilir ve eşsiz kullanıcı adı tanımlanması sağlanır, ortak veya paylaşımlı hesap kullanımı sınırlandırılır. Üretici tarafından atanmış varsayılan hesapların teknik olarak kapalı duruma getirilmesi ve kullanılmaması esas olup, zorunlu kullanımlarda varsayılan hesapların zimmetlendiği gerçek kişi bilgileri kayıt altına alınır.

(2) Kullanıcı hesaplarının erişim yetkileri ve görev tanımları, bilmesi gereken ve en az yetki ilkeleri doğrultusunda ve ilgili işin gerektirdiği kapsamı aşmayacak şekilde belirlenir. Rol ve yetkiler, kurumsal değişiklikler gözetilerek en az yılda bir kez düzenli aralıklarla gözden geçirilir, kullanılmayan yetkiler iptal edilir ve gözden geçirme sonuçları kayıt altına alınır ve gerektiğinde güncellenir.

(3) Görev yeri değişen veya ayrılan personelin rol, yetki ve erişim hakları gecikmeksizin güncellenir veya derhal iptal edilir, bu işlemlere ait log kayıtları tutulur.

(4) Üçüncü taraf tedarikçiler ve dış kaynak hizmeti kapsamında görev yapan personelin erişimleri de bu madde kapsamında değerlendirilir.

(5) Yetkiler, birim bazlı rol tanımları üzerinden verilir, bireysel istisnalar onaylı ve süreli tutulur.

(6) Ayrıcalıklı yetkiye sahip hesaplara kalıcı veya sürekli yetki tanımlanmaz ve yetkilendirmeler sadece ilgili işin gerektirdiği süreyle sınırlı ve hiyerarşik onay mekanizmalarına bağlı olarak yapılır. Ayrıcalıklı yetkiye sahip hesaplar ile günlük rutin işlemler yapılmaması sağlanır. Bu hesapların kullanımında çok faktörlü kimlik doğrulama kullanılır.

Temel ağ güvenliği

MADDE 38– (1) Kurumsal iç ağlar ile bilişim sistemlerini dış ağlardan ve genel internet ortamından izole etmek üzere, merkezi ağ trafiği filtreleme, sınır güvenliği ve erişim kontrolü sağlayan ağ güvenliği sistemleri kurulur ve işletilir. Dış ağlardan kurumsal iç ağlara veya bilişim sistemlerine yönlendirilen tüm veri trafiğinin istisnasız olarak bu sistemler üzerinden geçirilmesi zorunludur.

(2) Kurulan ağ güvenlik sistemleri üzerindeki erişim kontrol kuralları, sadece izin verilmiş güvenli servis ve protokolleri kapsayacak şekilde ve en az yetki prensibi çerçevesinde tanımlanır. Kaynağı ve hedefi belirsiz, geniş kapsamlı erişim kuralları tanımlanamaz, mevcut kurallar yılda en az bir kez gözden geçirilerek güncellenir.

(3) Dış ağlar üzerinden kurumsal sistemlerin yönetim arayüzlerine yapılacak uzaktan erişimlerde kimlik ve cihaz doğrulaması içeren güvenli, şifreli ve izole bağlantı mekanizmaları kullanılır ve doğrudan internet ortamına açık yönetim arayüzü barındırılamaz.

(4) Kritik bilişim sistemleri, sunucu ortamları ve veri tabanları ile genel kullanıcı ve misafir ağları birbirinden bağımsız ağlara bölünür. Misafir ağı, kurumsal kaynaklara erişim sağlayamaz.

(5) Ağ ve güvenlik sistemleri hizmet sürekliliğini sağlayacak şekilde fiziksel veya mantıksal yedeklilikle yapılandırılır.

(6) Operasyonel teknoloji ve endüstriyel kontrol sistemleri bulunması durumunda bu sistemler ile bilişim sistemleri ağları birbirinden ayrılır.

(7) Sanallaştırma katmanını oluşturan ana yazılımlar ile yönetim arayüzleri uygulama ağından ve kullanıcı ağından izole edilir. Sanal ortam yönetimi, ayrı bir yönetim ağı üzerinden ve ayrıcalıklı erişim yönetimi ile yapılır.

Uygulama Güvenliği

MADDE 39– (1) Geliştirilen, tedarik edilen veya kullanılan uygulamaların güvenliğinin sağlanması amacıyla uygulama geliştirme yaşam döngüsünün tüm aşamalarında uygulamanın kapsamı ve kritiklik düzeyi dikkate alınarak güvenlik gereksinimleri belirlenir, uygulanır ve doğrulanır. Bu gereksinimler asgari olarak aşağıdaki hususları içerir:

a) Kimlik doğrulama ve kimlik doğrulama bilgilerinin güvenli yönetimi.

b) Yetki ve rol yönetimi.

c) Oturum belirteçlerinin güvenli şekilde oluşturulması, iletilmesi, saklanması ve oturumun sona ermesi, kullanıcının güvenli çıkış yapması veya güvenlik olayı tespit edilmesi halinde geçersiz kılınması.

ç) Azami oturum ve hareketsizlik zaman aşımı sürelerinin belirlenerek belirlenen süre boyunca işlem yapılmaması halinde oturumun sonlandırılması.

d) Kimlik doğrulama sonrasında oluşturulan oturumun yetkisiz şekilde başka bir kullanıcı, cihaz veya işlem tarafından kullanılmasını önleyici tedbirlerin uygulanması.

e) Uygulama ve kullanıcı oturumlarına ilişkin log kayıtlarının kayıt altına alınması ve izlenmesi.

f) Risk düzeyi yüksek işlemler öncesinde yeniden kimlik doğrulama veya ilave kimlik doğrulama mekanizmalarının uygulanması.

g) Kritik iş süreçlerinde üst seviye yetkiye sahip kullanıcının onayını gerektirecek süreç tanımlanması.

ğ) Hata ve istisna mesajlarının uygulamadaki yazılım ve veritabanı mimarisine yönelik ifadeler içermeyecek ve güvenlik zafiyeti oluşturmayacak şekilde yönetilmesi.

h) Parola ve kritik verilerin işlenmesi, aktarılması ve saklanması sırasında uygun kriptografik mekanizmaların kullanılması.

ı) Güvenli yazılım geliştirme süreçlerine ilişkin ilkelerin uygulanması.

i) Uygulamaların güvenlik testlerinden geçirildikten sonra canlı ortama alınması.

j) Uygulamalarda tespit edilen güvenlik zafiyetlerinin önem derecesine göre giderilmesi.

k) Uygulama ara birimlerinin (API) güvenli erişim, yetkilendirme ve log kaydı tutma ilkelerine göre geliştirimesi.

(2) Uygulamalarda canlı ortam, geliştirme ve test ortamlarından ayrılır.

Değişim yönetimi

MADDE 40– (1) Kritik sistemlerin ağ, donanım, yazılım, mimari, tesis ve prosedürlerinde yapılacak tüm değişikliklerin kontrollü bir şekilde yürütülmesini sağlamak üzere değişim yönetimi süreci kurulur ve işletilir

(2) Yapılan değişiklikler uygulama sürecine alınmadan önce belirlenmiş onay sürecinden geçirilir.

(3) Değişim yönetimi süreci asgari aşağıdaki aşamaları kapsar:

a) Değişiklik talebinin gerekçesi ve kapsamıyla birlikte kayıt altına alınması.

b) Değişikliğin bilgi güvenliği ve hizmet sürekliliği üzerindeki risklerinin analiz edilmesi.

c) Değişikliğin canlı ortama alınmadan önce test ortamlarında doğrulanması.

ç) Değişikliğin yetkili merci veya güvenlik sorumlularınca onaylanması.

d) Değişim yönetimi sürecindeki tüm adımların yalnızca yetkilendirilmiş personelce gerçekleştirilmesi ve log kayıtlarının tutulması.

e) Etkilenecek iç ve dış paydaşlara önceden bilgilendirme yapılması.

f) Değişikliğin başarısız olması veya beklenmeyen bir kesintiye yol açması halinde, sistemlerin çalışan son kararlı durumuna ivedilikle döndürülmesini sağlayacak en az bir geri dönüş planının hazır bulundurulması.

g) Değişikliklerin acil durumlar haricinde, hizmetin en az etkilenecek zaman diliminde ve önceden planlanarak yapılması.

Yedekleme

MADDE 41– (1) Yedekleme sıklığı, yöntemi, saklama süresi ve kaynak ortam detaylarını içeren kurumsal bir yedekleme matrisi oluşturulur. Kritik veriler, veritabanları sistem, ağ ve güvenlik yapılandırma dosyaları, kaynak kodlar ve sistem imajları bu matris doğrultusunda; uygulama ortamlarından ve asıl sistemlerden fiziksel veya mantıksal olarak ayrıştırılmış farklı ortamlarda, veri kaybını önleyecek ve iş sürekliliğini sağlayacak şekilde yedeklenir.

(2) Yedekler asıl kopyalarının bulunduğu ortamlara uygulanan güvenlik önlemleriyle eşdeğer güvenlik önlemlerinin uygulandığı ortamlarda saklanır.

(3) Alınan yedeklerin güvenliği yetkisiz erişim, değiştirilme ve silme girişimlerine karşı teknik mekanizmalarla korunur.

(4) Yedeklerin bütünlüğü ile yedeklerden geri dönüş kabiliyeti kurumsal risk yönetimi ve varlıkların kritiklik dereceleri dikkate alınarak, canlı ortamın işlerliğini aksatmayacak şekilde yılda en az bir kez test edilir, doğrulanır ve raporlanır.

Log kaydı yönetimi

MADDE 42– (1) Bilişim sistemlerinde gerçekleşen kullanıcı, sistem ve erişim hareketlerine ilişkin log kayıtları eksiksiz, tutarlı ve kronolojik olarak oluşturulur.

(2) Log kayıtları asgari olarak başarılı veya başarısız tüm erişim girişimleri, yetki ve ayrıcalık kullanımları, yapılandırma ve sistem durum değişiklikleri ile hatalar dâhil olmak üzere uygulama, veritabanı, ağ ve sunucu donanımları üzerinden gerçekleştirilen her türlü işlemin; içeriği, kim tarafından, hangi bilişim sisteminde, hangi bileşen veya arayüz üzerinden, ne zaman, hangi yöntemle ve ne şekilde yürütüldüğünü inkar edilemezlik koşulunu sağlayacak ve geriye dönük tespit edilmesine imkan tanıyacak şekilde tutulur.

(3) Log kayıtları, değiştirilmesini, silinmesini veya yetkisiz erişilmesini engelleyecek şekilde kriptografik yöntemler veya zaman damgası kullanılarak korunur, en az iki yıl süreyle güvenli ortamlarda saklanır ve yedeklenir. Yönetici yetkilerine sahip hesaplara ilişkin log kayıtları ile bu kayıtların yönetildiği sistemlere ait log kayıtları da ek güvenlik tedbirleriyle korunur.

Üçüncü taraf ve tedarikçi güvenliği

MADDE 43– (1) Ürün, yazılım, donanım veya hizmet alınan üçüncü taraflarla imzalanacak sözleşme ve şartnamelerde; asgari siber güvenlik şartları, gizlilik ve ifşa etmeme hükümleri, hizmet seviyesi gereklilikleri ve siber olay ve zafiyet bildirimi ile alt yüklenicinin yükümlülüklerine yer verilir.

(2) Tedarikçilerin kurumsal ağ ve sistemlere yerinden veya uzaktan erişimleri yalnızca ilgili işin gerektirdiği süreyle ve bu kapsamla sınırlı yetkiyle sınırlı olacak şekilde, çok faktörlü kimlik doğrulama ve güvenli bağlantı yöntemleri kullanılarak sağlanır. İşin tamamlanması, askıya alınması veya sözleşmenin feshi halinde tedarikçinin tüm erişim hakları derhal iptal edilir. Sözleşme ilişkisinin veya hizmet sunumunun sona ermesi halinde üçüncü tarafların uhdesinde bulunan kurumsal bilişim varlıkları ve veriler eksiksiz olarak geri alınır veya tüm ortamlardan geri döndürülemez şekilde güvenli imha edildiği belgelendirilir.

(3) Bilişim sistemlerinin bakım, onarım veya idamesinin bir kısmının veya tamamının üçüncü taraflardan temin edilmesi, bu Yönetmelikte düzenlenen yükümlülük ve sorumlulukları ortadan kaldırmaz.

(4) Tedarikçilerin kullandığı kurumsal bilişim varlıkları, hesaplar, sertifikalar, anahtarlar, yapılandırmalar ve veriler envantere kaydedilir. Tedarikçi sözleşmesi sona erdiğinde bu kayıtlar gözden geçirilir.

Zaman senkronizasyonu

MADDE 44– (1) Tüm bilişim sistemlerinin güvenilir ve aynı zaman kaynağına göre ayarlanması ve senkronize şekilde çalışmaları sağlanır.

(2) Zaman kaynağına erişilememesi, senkronizasyon hatası veya kabul edilebilir sapmanın aşılması hâlinde olay tespit edilir, sorumlu birime bildirilir, alternatif zaman kaynağı devreye alınır ve kayıtların güvenilirliğini koruyacak tedbirler uygulanır.

İnsan kaynakları güvenliği

MADDE 45– (1) Personelin işe alımı, istihdamı, görev değişikliği ve istihdamının sonlandırılması süreçlerine yönelik gerekli prosedürler tanımlanır ve uygulanır. Personelin, siber güvenliğe ve bilgi gizliliğine yönelik yükümlülüklerinin yazılı bir gizlilik taahhütnamesi ile imza altına alması sağlanır. Taahhütname görevin sona ermesinden sonra devam eden yükümlülükleri de kapsar.

(2) Personelin siber güvenlik farkındalığını ve yetkinliğini sağlamak amacıyla işe başlama aşamasında ve devamında düzenli aralıklarla eğitimler verilir, eğitimlerin etkinliği değerlendirilerek kayıt altına alınır.

(3) Kurumsal politika ve kuralların ihlali hâlinde uygulanmak üzere etkin, orantılı ve caydırıcı bir kurumsal disiplin süreci oluşturulur ve işletilir.

(4) Personelin görev değişikliği veya istihdamının sonlandırılması hâlinde kurumsal varlıkların güvenli şekilde teslim alınması ve ilişik kesme işlemleri, önceden belirlenmiş yazılı usuller doğrultusunda kontrollü ve güvenli bir şekilde yürütülür.

(5) Personelin kurumsal bilişim kaynakları, e-posta sistemleri ve internet kullanımına yönelik politika belirlenir.

Fiziksel ve çevresel güvenlik

MADDE 46– (1) Bilişim sistemleri, sunucular, ağ cihazları ve veri depolama ortamlarının barındırıldığı bina, tesis, sistem odası ve çalışma alanlarının, yetkisiz fiziksel erişim, kasıtlı zarar verme eylemleri ve saldırılar ile doğal afetler ve diğer çevresel tehditlere karşı korunması amacıyla gerekli idari ve teknik tedbirler alınır.

(2) Bilişim sistemleri ile kritik donanımların bulunduğu alanlara fiziksel erişim yalnızca yetkilendirilmiş personelle sınırlandırılır. Erişim yetkileri düzenli aralıklarla gözden geçirilir ve görev değişikliği veya işten ayrılma hâlinde derhal iptal edilir. Sistem odaları ile kritik donanımların barındırıldığı güvenlikli alanlara girişlerde çift faktörlü doğrulama mekanizmaları kullanılır. Bu alanlara yapılan tüm giriş ve çıkış hareketleri elektronik geçiş kontrol sistemleri ve güvenlik kameraları vasıtasıyla kayıt altına alınır, görüntü kayıtları en az bir yıl, geçiş log kayıtları ise 42 inci maddede yer alan şartları sağlayacak şekilde muhafaza edilir.

(3) Ziyaretçiler ile üçüncü taraf hizmet sağlayıcıların bina ve tesislere girişlerinde kimlik tespiti ve kayıt işlemleri yürütülür, ziyaretçilere yalnızca onaylanmış alanlarla sınırlı geçici erişim izni verilir.

(4) Sistem odaları ve kritik donanım barındırma alanlarında asgari düzeyde yangın algılama ve söndürme sistemleri, su baskını algılama sensörleri, sıcaklık ve nem takip mekanizmaları, iklimlendirme sistemleri ile iş sürekliliği planı ile uyumlu ve asgari altı saat süreyle enerji sağlayabilecek kesintisiz güç kaynakları ve jeneratör altyapısı tesis edilir. Bu altyapıların periyodik bakım ve işlerlik testleri düzenli olarak yapılır ve kayıt altına alınır.

(5) Bilişim sistemlerini besleyen enerji, veri ve haberleşme iletim hatları; fiziksel hasar, tahribat ve yetkisiz müdahalelere karşı koruma altına alınacak şekilde kablo şaftları, kapalı kablo kanalları, korumalı güzergâhlar veya uygun muhafazalar içerisinden geçirilir, enerji iletim hatları ile veri iletim hatları arasında gerekli fiziksel ayrım sağlanır.

(6) Bilişim sistemleri, sunucu, ağ cihazları ve veri depolama ortamlarının barındırıldığı bina, tesis, sistem odası ve çalışma alanlarının kendi bünyelerinde bulunmaması halinde, ancak bu madde kapsamında belirtilen şartları sağlayan üçüncü taraflardan hizmet alımı yoluna gidilebilir.

Uç nokta ve cihaz güvenliği

MADDE 47– (1) Kurumsal ağlara bağlanan tüm sunucu, istemci ve uç nokta cihazların siber güvenliğini sağlamak amacıyla gerekli tedbirler alınır.

(2) Personelin kurumsal sistemler üzerinden dış ağlara ve genel internet ortamına erişimlerinde, zararlı yazılım barındıran veya oltalama amacıyla kullanılan adreslere erişimi teknik olarak sınırlandıracak merkezi filtreleme mekanizmaları işletilir.

(3) Standart yetkiye sahip kullanıcı hesaplarının kurumsal cihazlara yetkisiz uygulama veya yazılım yüklemesi, yetkisiz taşınabilir medya ve harici depolama cihazlarını veri iletimi veya depolama amacıyla kullanması, sistem konfigürasyonlarında değişiklik gerçekleştirmesi ve kritik işletim sistemi parametrelerini değiştirmesi teknik mekanizmalarla engellenir. Uç nokta cihazlarında yönetici veya ayrıcalıklı yetki tanımlamaları en az yetki prensibine uygun olarak sadece yetkilendirilmiş teknik sorumlulara tahsis edilir.

(4) Taşınabilir cihaz ve ortamlarda bulunan bilgi varlıklarının kayıp, hırsızlık, yetkisiz erişim, değiştirme ve aktarım risklerine karşı korunmasını sağlayacak tedbirler alınır.

Veri transferi, veri maskeleme ve güvenli silme

MADDE 48– (1) E-posta veya dosya paylaşım sistemleri üzerinden gerçekleştirilecek kritik bilgi transferi ve veri iletim süreçleri güvenli şifreli protokoller üzerinden yürütülür.

(2) Canlı ortamdan alınan verilerin yazılım geliştirme, test veya simülasyon ortamlarında kullanılması durumunda, söz konusu verilerin içerdiği hassas veya kritik alanların asıl veriye ulaşılamayacak şekilde maskelenmesini veya anonimleştirilmesini sağlayacak teknikler uygulanır.

(3) Kurumsal politikalar veya ilgili mevzuat gereği saklama süresi tamamlanan kritik veriler ve bilgi varlıkları, kurumsal sistemlerden ve depolama ortamlarından geri döndürülemez şekilde güvenli silme ve veri arındırma işlemlerine tabi tutularak imha edilir.

(4) Kritik hizmetlerin geliştirilmesinde kullanılan yazılım kaynak kodlarının depolandığı ortamlar, yetkisiz kod değişiklikleri, manipülasyonlar ve veri sızıntılarını önleyecek şekilde izole edilir.

Bulut ve sanallaştırma güvenliği

MADDE 49– (1) Bulut bilişim hizmetleri ve sanallaştırma altyapılarında sanal makineler, sanal ağlar ve depolama katmanları birbirinden izole edilir, sanal makine imajlarının bütünlüğü korunur ve yönetim arayüzleri dış ağlardan ayrılır.

(2) Sanallaştırma altyapılarında işlevini yitiren veya kullanılmayan sanal sistemler ağdan izole edilerek kapatılır, güvenli imha prosedürleri uygulanır, imaj ve anlık görüntüler güvenli bir şekilde kayıt altında tutulur.

(3) Bulut bilişim hizmetlerinin üçüncü taraflardan paylaşımlı olarak temin edilmesi hâlinde hizmet sözleşmesinde asgari olarak;

a) Diğer paylaşımcılardan mantıksal ve mimari izolasyonun sağlanması,

b) Şifreleme anahtarlarının kuruluşun kontrol ve denetiminde bulundurulması,

c) Erişim yetkilerinin kurumsal politikalara uygun olarak yönetilmesi,

ç) Hizmetin sonlandırılması durumunda kurumsal verilerin eksiksiz olarak iade edilmesi ve güvenli imhaya ilişkin usullerin belirlenmesi
hususlarına ilişkin yükümlülükler yer alır.

(4) Bulut ve sanallaştırma altyapılarında tedarikçi bağımlılığını önlemek, verilerin ve uygulamaların taşınabilirliğini sağlamak amacıyla açık standartlara ve veri formatlarına uyumlu mimariler tercih edilir, tek bir üreticiye bağımlı kapalı sistemlere bağımlılık yaratacak tasarımlardan kaçınılır ve alternatif platformlara geçiş planları oluşturulur.

İç tetkik ve sürekli iyileştirme

MADDE 50– (1) Bu Yönetmelik kapsamında yürütülen siber güvenlik faaliyetlerinin, kurumsal politika ve prosedürlerin, risk işleme planlarının ve BGYS'nin uygunluğunu, yeterliliğini ve etkinliğini değerlendirmek amacıyla yılda en az bir kez iç tetkik gerçekleştirilir.

(2) İç tetkikler nesnellik ve tarafsızlık ilkeleri doğrultusunda, tetkik edilen faaliyetlerin yürütülmesinde doğrudan görev almayan personel tarafından gerçekleştirilir.

(3) Her yılın mart ayı sonuna kadar kurumsal siber güvenlik risk durumu, meydana gelen siber olaylara ilişkin bilgiler, iç tetkik bulguları ile bunlara yönelik düzeltici ve önleyici faaliyetlerin güncel takip durumunu ve belirlenen kurumsal siber güvenlik performans

göstergelerine ilişkin değerlendirmeleri içeren ve üst yönetim tarafından onaylanan siber güvenlik faaliyet raporu hazırlanır.

(4) Üst yönetim tarafından üçüncü fıkra kapsamında sunulan rapor ve iç tetkik çıktıları doğrultusunda kurumsal siber güvenlik performansı en az yılda bir kez gözden geçirilir, düzeltici ve önleyici faaliyetler, siber güvenlik bütçesi ve kaynak tahsisi ile kurumsal politika güncellemelerine ilişkin stratejik kararlar yazılı olarak kayıt altına alınır.

(5) İç tetkik planları, raporlar, üst yönetim gözden geçirme tutanakları, siber güvenlik faaliyet raporları, düzeltici ve önleyici faaliyet kayıtları asgari beş yıl süreyle güvenli ortamlarda muhafaza edilir.

ALTINCI BÖLÜM
Kritik Altyapıya Sahip Kuruluşların Yükümlülükleri

Kritik altyapıya sahip kuruluşlar

MADDE 51– (1) Kritik altyapıya sahip kuruluşlar, dördüncü ve beşinci bölümde yer alan yükümlülüklere ek olarak bu bölümde düzenlenen siber güvenlik tedbirlerini almak, uygulamak ve sürekli iyileştirmekle yükümlüdür.

(2) Kritik altyapıya sahip kuruluşlar, doğrudan üst yönetime bağlı siber güvenlik komisyonu kurar ve kurumsal karar mekanizmaları ile hesap verebilirlik sınırlarını belirleyen sorumluluk modellerini bu komisyon üzerinden işletir. Siber güvenlik komisyonu, üst yönetim temsilcisi, bilgi güvenliği yöneticisi, kritik altyapı kapsamındaki hizmet ve bilişim sistemi sorumlusu, risk yönetimi, uyum, hukuk, insan kaynakları ve iş sürekliliği temsilcilerinden oluşur.

(3) Kritik altyapıya sahip kuruluşlar, kurumsal risk profili ile sundukları hizmetin ve sahip oldukları altyapının niteliği ve kapsamını dikkate alarak siber güvenlik yatırımları ve harcamaları ile insan kaynağı ihtiyaçlarını karşılamaya yönelik ayrı bir yıllık siber güvenlik bütçesi hazırlar. Bütçe hazırlanırken, 18 inci madde kapsamında hazırlanan siber güvenlik iyileştirme planında belirlenen faaliyetlerin gerçekleştirilmesi, teknolojik yatırımların yapılması, altyapıların güvenli hâle getirilmesi ve gerekli uzman personelin istihdam edilmesi için ihtiyaç duyulan mali kaynakları dikkate alır.

(4) Kritik altyapıya sahip kuruluşlar, siber güvenliğin sağlanmasına yönelik faaliyetler, bütçe tahsisleri ve kabul edilen risklere yönelik tüm yönetsel kararları gerekçeleriyle birlikte kayıt altına alır ve kayıtları asgari beş yıl süreyle güvenli ortamlarda muhafaza eder.

(5) Kritik altyapıya sahip kuruluşlar, siber güvenlik risk yönetimi süreçlerini kurumsal risk yönetiminin bir parçası olarak değerlendirir ve faaliyetlerini bütüncül bakış açısıyla yürütür.

(6) Kritik altyapıya sahip kuruluşlar, 41 inci madde kapsamında alınan yedeklerin ana ağdan tamamen izole edilmiş mimaride ve donanımsal düzeyde değiştirilemez nitelikte saklanmasını sağlar, risk temelli planlar doğrultusunda yüksek riskli sistemlere yönelik yedekten geri dönüş testlerini en az altı ayda bir gerçekleştirir ve doğrulama kanıtlarını kayıt altına alır. Geri dönüş testleri, kritik hizmetin kabul edilebilir süre ve veri kaybı hedefleri içinde çalışır hâle getirilmesini kapsar.

(7) Kritik altyapıya sahip kuruluşlar, 49 uncu maddede düzenlenen bulut ve sanallaştırma altyapılarının; güvenlik yapılandırma hatalarını, zafiyetlerini, yetkisiz değişiklikleri ve uyumluluk sapmalarını merkezi olarak anlık izleyen ve otomatik alarm mekanizmalarına sahip, dinamik güvenlik durumu yönetimi sistemlerini işletir.

(8) Kritik altyapıya sahip kuruluşlar, siber risk yönetimi sonuçlarını dikkate alarak gerekli hallerde kritik veri işleyen bulut ve sanallaştırma kaynaklarının, kuruluş dışı başka varlıklarla aynı fiziksel donanım üzerinde barındırılmamasını sağlar. Başkanlık, ulusal siber güvenliğin ve kritik hizmetlerin güvenliğinin sağlanması amacıyla, bu fıkrada belirtilen tedbirlerin uygulanmasını zorunlu tutabilir veya uygulanma biçimine ilişkin farklı usul ve esaslar belirleyebilir.

(9) Kritik altyapıya sahip kuruluşlar yılda en az bir kez, bulut ve sanallaştırma altyapılarında olası bir hizmet değiştirme veya sonlandırma durumunda sistemlerin kesintisiz devrini sağlayacak teknik ve idari planlarını ve taşınabilirlik testlerini gerçekleştirir ve sonuçlarını kayıt altına alır.

(10) Kritik altyapıya sahip kuruluşlar bulut bilişim hizmetlerini, açık standartlara ve veri formatlarına uyumlu hizmet sunan, veri taşınabilirliğini ve platformlar arası geçişi kısıtlayıcı kapalı mimariye sahip olmayan sağlayıcılardan hizmet temin eder.

(11) Kritik altyapıya sahip kuruluşlar standart bilgi teknolojileri hizmet talepleri ile siber güvenlik operasyonlarını; rol, yetki, iş akışı ve sistem arayüzleri düzeyinde yapılandırılmış kurumsal bir hizmet masası ve talep yönetim mekanizması üzerinden birbirinden ayrıştırarak yürütür.

(12) Kritik altyapıya sahip kuruluşlar 44 üncü maddede belirtilen zaman senkronizasyonunu, atomik saat standardına dayalı güvenli, kesintisiz ve doğrulanabilir ulusal zaman kaynaklarını kullanarak sağlar.

(13) Kritik altyapıya sahip kuruluşlar 50 nci madde kapsamında gerçekleştirilen iç tetkik faaliyetlerine ilaveten, iç denetim faaliyetlerinin yürütülmesine ilişkin hususları Başkanlıkça belirlenecek denetim usul ve esasları çerçevesinde yapar.

BGYS ekibi ve belgelendirme

MADDE 52– (1) Kritik altyapıya sahip kuruluşlar, doğrudan üst yönetime bağlı, Başkanlık, sektörel SOME ve kurumsal BGYS politikaları çerçevesinde belirlenen performans hedefleri ile güvenlik metriklerini sistemli olarak izleyen, idari ve teknik yetkinliği haiz en az üç kişiden oluşan bir BGYS ekibi kurar.

(2) Kritik altyapıya sahip kuruluşlar, ulusal veya uluslararası düzeyde yetkilendirilmiş kuruluşlardan BGYS kurumsal uygunluk belgesi temin etmek ve bu belgenin güncelliğini kesintisiz olarak sağlamakla yükümlüdür. Belgenin askıya alınması, geçerliliğinin sona ermesi veya kapsam değişikliği derhâl sektörel SOME'ye ve Başkanlığa bildirilir.

(3) BGYS belgesinin kapsamı, kuruluşun sunduğu tüm asli ve kritik hizmetleri, bu hizmetlerin yürütüldüğü asıl ve yedek bilişim altyapılarını, birincil ve ikincil veri merkezleri ile felaket kurtarma merkezini eksiksiz olarak içerir.

Değişim yönetimi sürecinde uygulanacak ek hususlar

MADDE 53– (1) Kritik altyapıya sahip kuruluşlar 40 ıncı maddede düzenlenen değişim yönetimi sürecinin tüm aşamalarını dijital olarak izlenebilir, değiştirilemez ve denetlenebilir nitelikte olan merkezi bir kurumsal süreç yönetim sistemi üzerinden yürütür.

(2) Değişikliğin birden fazla birimi veya kritik hizmeti etkilemesi hâlinde etki alanı içindeki tüm sorumlu birimlerin değerlendirmesi, görüşü ve onayı alınmaksızın değişiklik planlanamaz ve uygulanamaz.

(3) Değişiklikler bilgi güvenliği, hizmet sürekliliği, geri dönüş zorluğu, etki alanı ve aciliyet kriterlerine yönelik yapılan siber risk yönetimi sonuçlarına göre risk seviyelerine ayrılır.

TASLAK

Değişikliğin taşıdığı risk seviyesine göre kademeli ve farklılaştırılmış onay mekanizmaları işletilir, yüksek ve kritik risk seviyesini haiz değişiklikler için ilave teknik doğrulamalar ile yönetim veya yetkili siber güvenlik komisyonu onayı zorunlu kılınır.

(4) Değişim yönetim sistemi üzerinde gerçekleştirilen tüm talep, etki analizi, onay, test çıktısı, yetkilendirme ve geri dönüş süreçlerine ilişkin kayıtlar asgari beş yıl süreyle güvenli ortamlarda muhafaza edilir.

Yetkinlik ve uzmanlık yönetimi

MADDE 54– (1) Kritik altyapıya sahip kuruluşlar, kritik altyapıların ve bilişim sistemlerinin güvenliğinden, yönetiminden ve teknik operasyonlarından sorumlu personelin mesleki yetkinliklerini, üstlendikleri rollere göre sınıflandırır ve bu yetkinliklerin sürekliliğini sağlayacak kurumsal uzmanlık yönetim programı yürütür.

(2) Kritik altyapı faaliyetleri kapsamında görevlendirilecek personel, yaptığı görevin niteliği esas alınarak en az aşağıda belirtilen yetkinliklere göre istihdam edilir:

a) Bilişim sistemlerinin kesintisiz izlenmesi, alarm, uyarı ve bildirimlerin temel seviyede analiz edilmesi, rutin güvenlik sıkılaştırmaları ve operasyon faaliyetleri.

b) Siber olay müdahale, zafiyet yönetimi, sızma testleri, adli bilişim analizi, güvenli yazılım ve siber güvenlik mimarisi tasarımı gibi ileri düzey teknik uzmanlık gerektiren alanlar.

c) Siber güvenlik yönetişimi, risk yönetimi, mevzuat uyum, tedarik zinciri güvenliği ve geniş ölçekli kriz yönetim süreçlerinin sevk ve idaresi.

(3) Kurumsal SOME ile bilişim sistemlerinin yönetiminde görevli personelin, ikinci fıkrada belirtilen teknik görev alanlarına uygun mesleki tecrübeye, ulusal veya uluslararası düzeyde teknik geçerliliği olan uzmanlık belgesi veya sertifikalarına sahip olması zorunludur. Sertifikaların geçerliliği ve güncelliği kuruluşlar tarafından kesintisiz olarak takip edilir.

(4) Teknik personelin güncel siber tehdit senaryolarına, karmaşık saldırı vektörlerine ve değişen teknolojik altyapıya uyumunu sağlamak amacıyla her yıl düzenli olarak uygulamalı teknik uzmanlık eğitimleri ve laboratuvar çalışmaları düzenlenir. Personelin aldığı eğitimler, sahip olduğu sertifikalar ve mesleki gelişim faaliyetleri izlenebilir şekilde kayıt altına alınarak muhafaza edilir.

(5) Kritik görevler için yedek personel, vardiya sürekliliği ve çağrı listesi düzeni oluşturulur. Tek kişiye bağımlı kritik süreçler için dokümantasyon hazırlanır.

Gelişmiş erişim ve kimlik yönetimi

MADDE 55– (1) Kritik altyapı kapsamındaki bilişim sistemlerine erişimler ağ içi veya ağ dışı kaynak ayrımı yapılmaksızın kullanıcının, cihazın, konumun ve bağlantının kesintisiz doğrulandığı şekilde ve en az yetki prensibiyle tasarlanır ve işletilir.

(2) Kritik altyapıya sahip kuruluşlar, merkezi bir kullanıcı kimlik doğrulama, yetki ve erişim yönetim sistemi kurar. Bu sistem beşinci bölümde yer alan çok faktörlü kimlik doğrulama mekanizmalarının risk durumuna göre dinamik olarak ayarlanmasını, erişim politikalarının uygulanmasını ve kimlik yaşam döngüsünün uçtan uca otomasyonunu sağlar.

(3) Bilişim sistemlerinin yönetici hesapları ile diğer tüm ayrıcalıklı hesapların erişimleri ve bu sistemler üzerinde gerçekleştireceği tüm işlemler, merkezi bir ayrıcalıklı hesap yönetim sistemi üzerinden yürütülür.

(4) Ayrıcalıklı hesap yönetim sistemi üzerinden gerçekleştirilen tüm oturumlar, ekran kaydı, komut geçmişi ve tuş vuruşları dâhil olmak üzere adli bilişime imkân tanıyacak şekilde eksiksiz olarak kayıt altına alınır ve korunur. Oturumlar esnasında olağan dışı veya yetkisiz bir

işlem tespit edilmesi durumunda, ilgili erişimin sistem tarafından otomatik olarak engellenmesini ve sonlandırılmasını sağlayacak teknik mekanizmalar kurulur.

(5) Kritik altyapı kapsamındaki veri tabanı ve uygulama erişimlerinde kullanıcının rolüne ve yetkisine göre verilerin dinamik olarak maskelenmesine yönelik bir politika oluşturulur ve bu politika doğrultusunda işlem yapılmasını sağlayan teknolojiler kullanılır.

(6) Olağan dışı, yetkisiz veya kural dışı işlem tespitinde oturumun otomatik olarak sonlandırılması, erişimin engellenmesi ve ilgili yetkililere alarm gönderilmesi sağlanır.

(7) Kritik veri tabanı ve uygulama erişimlerinde rol, yetki ve sorumluluklar çerçevesinde veri sahibi ve siber güvenlik komisyonu onayıyla dinamik veri maskeleme mekanizmaları uygulanır.

Güvenli ürün geliştirme, tasarım ve yaşam döngüsü

MADDE 56– (1) Kritik altyapı kapsamındaki bilişim sistemleri için güvenli yapılandırma standartları belirlenir, dokümante edilir ve periyodik olarak doğrulanır. Yetkisiz veya standart dışı yapılandırma değişiklikleri kayıt altına alınır, risk seviyesine uygun sürede giderilir ve düzeltme sonrası yeniden doğrulanır.

(2) Kritik altyapıya sahip kuruluşlar, kapsamındaki bilişim sistemlerini ve bu sistemleri oluşturan donanım, yazılım, aktif veya pasif durumdaki tüm bileşenleri; tedarik, tasarım, geliştirme, yaygınlaştırma, işletim ve devreden çıkarma aşamalarının tamamını kapsayan güvenli yaşam döngüsü yönetimine tabi tutar. Siber güvenlik gereksinimleri, mimarinin ve tedarik süreçlerinin ilk aşamasından itibaren tasarıma dâhil edilir.

(3) Kritik altyapı kapsamındaki bilişim sistemlerinde kullanılan veya bu altyapılar için özel olarak geliştirilen yazılımlar ve donanımlar için, birbirinden bağımsız en az üç katmanlı geliştirme, test ve canlı ortam altyapısı oluşturulur; bu ortamlar arasında kullanıcı, yetki ve erişim ayrıştırması sağlanır. Yazılımların canlı ortama alınmasından önce; güvenli kodlama standartlarına uygunluğu doğrulanır, kaynak kod analizleri, statik ve dinamik güvenlik testleri ile üçüncü taraf açık kaynaklı bileşenlerin zafiyet taramaları ve gerekli hallerde sızma testleri gerçekleştirilir. Güvenlik doğrulama süreçleri tamamlanmayan hiçbir bileşen kritik altyapı üzerinde devreye alınmaz.

(4) Kullanılan yazılım, donanım ve açık kaynak bileşenlerinin üreticisi, sürümü, lisansı, destek durumu, bağımlılıkları ve zafiyetleri varlık envanterinde izlenir. Kritik sistemlerde yazılım bileşen listesi veya bağımlılık haritası tutulur.

(5) Kritik altyapıya sahip kuruluşların üçüncü taraflardan temin ettikleri, açık kaynak kodlu olmayan tüm bilişim ürün ve yazılımlarının geçerli ve meşru lisanslara sahip olması zorunludur. Telif haklarına aykırı olarak çoğaltılmış, değiştirilmiş veya güvenlik mekanizmaları yetkisiz yöntemlerle devre dışı bırakılmış ürün ve yazılımlar kurumsal sistemlerde kullanılmaz. Kurumsal sistemlerde veya yazılım geliştirme süreçlerinde açık kaynak kodlu yazılım, kütüphane ve bileşenlerin kullanımı, ancak bunların kaynak güvenilirliği doğrulandıktan ve gerekli güvenlik testlerinden geçirildikten sonra gerçekleştirilir.

(6) Kullanım ömrünü tamamlamış, üretici desteği sonlanmış veya güvenlik güncellemesi üretilmeyen hiçbir donanım, yazılım veya sistem bileşeni kritik altyapı bünyesinde kullanılmaz. Bu kapsamdaki bileşenler ancak zorunlu hallerde ve risk işleme, risk kabulü, düzeltici ve önleyici tedbirlerin uygulanması ve bu hususların üst yönetim onayından geçmesi halinde kullanılabilir. Bu kullanım, kuruluşun bu Yönetmelikte düzenlenen diğer yükümlülülerini ortadan kaldırmaz.

(7) Ömrünü tamamlayan veya devreden çıkarılan bilişim sistemlerinin bileşenleri ve depolama ortamları; barındırdıkları verilere ilişkin gerekli yedekleme ve doğrulama işlemlerinin tamamlanmasını müteakip, söz konusu verilerin geriye dönük olarak hiçbir şekilde elde edilemeyeceği güvenli imha yöntemleri ve veri arındırma işlemlerine tabi tutulur.

(8) Kritik altyapıya sahip kuruluşlar, kritik altyapılarda kullanılacak siber güvenlik ürün, sistem ve hizmetleri Başkanlık tarafından yetkilendirilmiş ve belgelendirilmiş siber güvenlik uzmanlarından, üreticilerden veya şirketlerden tedarik eder.

Kriptografik koruma ve anahtar yönetimi

MADDE 57– (1) Bilişim sistemleri arasındaki güvenli iletişimde ve veri şifreleme süreçlerinde kullanılan kriptografik anahtarlar ile dijital sertifikaların saklanması, dağıtılması, değiştirilmesi, arşivlenmesi ve güvenliği ihlal edilenlerin iptal edilerek imha edilmesine yönelik yönetim süreçleri; anahtarların ve sertifikaların gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına alacak, donanımsal güvenlik modülleri veya fiziksel ve mantıksal olarak izole edilmiş güvenli altyapılar üzerinde yürütülür. Anahtarlara ve anahtar yönetim sistemlerine erişim en az yetki, görevler ayrılığı ve çok faktörlü doğrulama ilkelerine göre sınırlandırılır. Anahtar kullanım ve yönetim işlemleri değiştirilemez, zaman damgalı ve inkâr edilemez kayıtlara bağlanır.

(2) Güvenli iletişimde ve veri şifreleme süreçlerinde ulusal veya uluslararası düzeyde güvenilirliği kabul edilmiş güçlü şifreleme algoritmaları ve kriptografik koruma yöntemleri kullanılır.

(3) Anahtar veya sertifikanın güvenliğinin ihlal edildiği, kaybolduğu, yetkisiz kullanıldığı veya geçerlilik süresinin sona erdiği tespit edilirse derhâl iptal edilir ve yeni anahtar ve sertifikalar oluşturularak kullanıma alınır.

(4) Sertifika ve anahtarların geçerlilik süreleri sona ermeden hizmet kesintisi oluşmasını önleyecek tedbirler alınır.

Veri yerelleştirme ve barındırma

MADDE 58– (1) Kritik altyapı kapsamındaki bilişim sistemleri üzerinde üretilen, işlenen veya saklanan tüm veriler ile bu verilere ait yedekler, uygulamalar, kaynak kodları, yapılandırma verileri, log kayıtları ve meta veriler ile kritik altyapılara ait asıl sistemler, ikincil veri merkezi, yedekleme altyapıları, kriz yönetim ve felaket kurtarma merkezi, siber güvenlik operasyon merkezi, ağ operasyon merkezi Türkiye Cumhuriyeti sınırları içinde kurulur ve işletilir.

(2) Birinci fıkra kapsamındaki bilişim sistemleri ve veriler; kanunlarda açıkça düzenlenen veya Başkanlıkça belirlenen istisnalar haricinde, yurt dışına aktarılamaz, sınır ötesi bulut bilişim hizmetleri veya harici altyapılar üzerinde barındırılamaz ya da yurt dışından uzaktan erişime açılamaz. Bu sistemler ve veriler, ülkemizde tesisli ve Başkanlıkça yetkilendirilen hizmet sağlayıcılar bünyesinde barındırılabilir.

(3) Kritik verilerin yetkisiz kişilerce elde edilmesini, sınır ötesine aktarılmasını veya kurum dışına sızdırılmasını engellemek üzere; ağ, uç nokta ve veri depolama katmanlarında veri sızıntısı önleme sistemleri kurulur ve canlı ortamda kesintisiz olarak işletilir. Bu sistemler tarafından üretilen ihlal ve engelleme alarmları, 62 nci madde kapsamında kesintisiz ve anlık olarak izlenir.

İleri düzey ağ güvenliği

MADDE 59– (1) Kritik altyapıya sahip kuruluşlar, kurumsal ağ altyapısı, risk dereceleri ve iş fonksiyonlarına göre mikro segmentasyon ilkelerine uygun olarak alt bölümlere ayrılır, dış ağa açık kurumsal hizmetler için bağımsız arındırılmış bölgeler oluşturulur.

(2) Kritik altyapıya sahip kuruluşlar dış ve iç ağlar ile felaket kurtarma merkezi ve ikincil veri merkezleri arasındaki tüm bağlantı sınırlarında birbirini yedekleyen, fiziksel veya mantıksal olarak bağımsız, çok katmanlı ağ trafiği filtreleme, sınır güvenliği ve erişim kontrolü sağlayan ağ güvenliği mimarilerini kurar ve işletir.

(3) Ağ yedekliliği yalnızca aynı fiziksel güzergâh veya ortak altyapıya dayanmayan, hatta meydana gelecek kesinti veya arızanın aynı anda tüm bağlantıları etkilemesini önleyecek şekilde tasarlanır. Yedek bağlantıların iş sürekliliği gereksinimleri ve kapasitesi asıl bağlantıyla uyumlu tutulur.

(4) Kritik altyapıya sahip kuruluşlar kritik altyapı kapsamındaki bilişim sistemlerine dış veya iç ağdan yapılacak sistem, cihaz ve ağ yönetimi seviyesindeki tüm ayrıcalıklı idari erişimleri sadece bu amaca tahsis edilmiş, uygulama ağından fiziksel veya mantıksal olarak tamamen yalıtılmış ayrı yönetim ağları üzerinden gerçekleştirir.

(5) Birincil veri merkezi, ikincil veri merkezi ve felaket kurtarma merkezi arasındaki veri aktarımları ve veri senkronizasyon hatları, genel internet trafiğinden tamamen yalıtılmış ve ağ katmanında şifrelenmiş güvenli kanallar üzerinden yürütülür.

(6) Ağ bölümleri arasındaki tüm veri trafiği varsayılan olarak engelleme ilkesi uyarınca sıkı erişim kontrol kurallarına tabi tutulur. İzin verilen protokoller dışındaki tüm trafik ağ katmanında otomatik olarak engellenir.

(7) Kritik altyapıya sahip kuruluşlar, kritik hizmetlerin erişilebilirliğini hedefleyen dağıtık hizmet dışı bırakma saldırılarına karşı internet sınır hatlarında ve dış ağ erişim noktalarında, hat kapasitesiyle uyumlu proaktif koruma, anlık trafik filtreleme ve saldırı engelleme mekanizmalarını bulundurur veya kullanır, olası saldırı dalgalarının bertaraf edilmesine yönelik teknik önlemleri kesintisiz olarak uygular.

(8) Ağ ve güvenlik sistemleri için hata, kapasite, gecikme, paket kaybı, bağlantı ve yedeklilik durumu izlenir. Kritik eşiklerin aşılması hâlinde otomatik alarm mekanizması işletilir.

(9) Kritik hizmet veya kurumsal ağa erişim sağlayan kablosuz ağlar, kablolu ve kritik ağ bölümlerinden güvenlik politikalarına uygun şekilde ayrıştırılır; kurumsal, misafir, operasyonel ve yönetim amaçlı kablosuz erişimler birbirinden ayrılır.

(10) Kablosuz erişimlerde güncel ve güvenli kimlik doğrulama ve şifreleme yöntemleri kullanılır. Varsayılan yönetim bilgileri değiştirilir, zayıf, kullanım dışı veya güvenliği yetersiz protokoller kullanılmaz.

(11) Uzaktan erişimlerde, kimlik ve cihaz durumuna dayalı koşullu erişim mekanizmaları devreye alınır, kurumsal verilerin kişisel cihazlarda yerel olarak depolanması engellenir.

Operasyonel teknoloji güvenliği

MADDE 60– (1) Endüstriyel kontrol sistemleri, veri tabanlı kontrol ve gözetleme sistemleri ve operasyonel teknoloji ortamları, kurumsal bilgi teknolojileri ağlarından, üçüncü taraf altyapılarından ve tüm dış ağlardan fiziksel veya mantıksal olarak ayrılır.

(2) Operasyonel teknoloji ağ altyapısı; kendi içinde fonksiyon, süreç ve kritiklik derecelerine göre mikro segmentasyon ilkelerine uygun olarak alt bölümlere ayrılır, bu katmanlar arasındaki tüm veri akışları ve protokol geçişleri sıkı kontrol kurallarıyla sınırlandırılır.

(3) Operasyonel teknoloji varlıklarının fiziksel ve mantıksal topoloji haritaları çıkarılarak güncelliği sağlanır, cihaz ve sistemlerin güvenli yapılandırma kriterleri belirlenerek düzenli aralıklarla gözden geçirilir, tüm yapılandırma değişiklikleri merkezi olarak yönetilir ve kayıt altına alınır.

(4) Operasyonel teknoloji ortamlarına yerinden veya uzaktan yapılacak geçici bağlantılar ile taşınabilir medya, donanım veya harici cihazlar üzerinden gerçekleştirilecek her türlü teknik bakım, onarım ve güncelleme faaliyeti, özel güvenlik doğrulamalarına ve sıkı yetkilendirme prosedürlerine tabi tutulur.

(5) Operasyonel teknoloji sistemlerinin işlevini yitirmesi veya tehlikeli durumların oluşması hâlinde endüstriyel süreçleri güvenli duruma getiren emniyet enstrümantasyon sistemleri, diğer kontrol ve otomasyon sistemlerinden fiziksel ve mantıksal olarak ayrıştırılır ve yalnızca yetkilendirilmiş bileşenlerle bağlantı kurması sağlanır.

(6) Fiziksel süreçleri izlemek ve denetlemek amacıyla kullanılan saha denetleyicilerinin bütünlüğünü, güvenli yapılandırmasını ve anomali tespitini sağlayacak teknik tedbirler alınır ve saha denetleyicilerinin çalışma durumları takip edilerek tespit edilen anomaliler, 62 nci maddede düzenlenen sistemlere anlık olarak bildirilir.

(7) Siber risklerin endüstriyel süreçlerde ve fiziksel bileşenlerde yaratabileceği tehlikeli durumlar ile emniyet ihlallerine yönelik senaryolar siber risk yönetim süreçlerine dâhil edilir.

Gelişen teknolojilerin siber güvenliği

MADDE 61– (1) Sensörler ve yazılımlar aracılığıyla veri toplama, işleme ve iletme yeteneğine sahip olan, makineden makineye iletişim kurabilen ya da internete bağlanarak çevresindeki nesneler ve bilişim sistemleri ile veri alışverişi yapabilen her türlü uç donanım, cihaz ve nesnelerin kurumsal ağlara entegrasyonunda; bağlantının diğer ağ bölümlerinden fiziksel veya mantıksal olarak ayrılması, kullanılmayan erişim ve yönetim protokollerinin kapatılması, uygun kimlik doğrulama ve yetkilendirme yöntemlerinin uygulanması zorunludur.

(2) Algoritmik karar alma ve otonom veri işleme sistemlerinin öğrenme, geliştirme, yaygınlaşma ve kullanım süreçlerinde, kuruluşun korumakla yükümlü olduğu kritik veri ve log kayıtları doğrudan kullanılamaz. Söz konusu veriler, ancak asıl verinin elde edilmesini imkânsız kılacak maskeleme, anonimleştirme veya sentetik veri üretimi işlemlerinden sonra ilgili süreçlere dâhil edilir.

(3) Algoritmik karar alma ve otonom veri işleme sistemleri; manipülasyon, veri zehirlenmesi ve model saptırma tehditlerine karşı girdi çıktı filtreleme mekanizmaları ile donatılır. Modellerin karar alma ve veri işleme süreçlerindeki algoritmik bütünlüğü ve kararlılığı düzenli olarak denetlenir ve doğrulanır.

(4) Kurumsal veriler kullanılarak geliştirilen, eğitilen veya ince ayar uygulanan yapay zekâ modellerinde, gizli veya kritik nitelikte değerlendirilen bilgilerin işlenmesi, erişilmesi, açıklanması veya elde edilmesi risklerine karşı uygun teknik ve idari tedbirler alınmalıdır.

(5) Kritik altyapıya sahip kuruluşlar; kamuya açık yapay zekâ modellerine veri aktaramaz.

(6) Bu maddede belirtilen gelişen teknolojilerden üretilen tüm güvenlik ve anomali verileri, 62 nci maddede yer alan teknik mimari ile entegre şekilde işletilir. Sistemler tarafından üretilen uyarılar, siber olay müdahale planlarını otomatik olarak tetikleyecek teknik mimariyle yönetilir.

(7) Yeni teknolojilerin doğurduğu siber riskler periyodik olarak değerlendirerek kurumsal risk yönetimi süreçlerine dâhil edilir ve bu riskleri karşılayacak gerekli risk yönetimi kontrolleri zamanında devreye alınır.

(8) Algoritmik karar alma ve otonom veri işleme sistemlerinin kritik altyapı karar alma süreçlerinde kullanılması durumunda, modelin karar mekanizmaları denetlenebilir, izlenebilir ve gerekçelendirilebilir nitelikte tasarlanır ve sistem çıktılarının doğrulanmasına imkân tanıyan açıklanabilirlik mekanizmaları işletilir.

Kesintisiz izleme

MADDE 62– (1) Kritik altyapıya sahip kuruluşlar, siber tehditleri gerçek zamanlı tespit etmek, anomali ve zararlı faaliyetlerini analiz etmek üzere asgari düzeyde; merkezi log kaydı toplama ve olay sınıflandırma ve ilişkilendirme, gelişmiş ağ ve uç nokta tehdit tespiti, anomali ve saldırıları izleme, alarm, uyarı ve engelleme mekanizmaları kurar.

(2) Birinci fıkrada belirtilen mekanizmalar, siber tehditlere karşı otomatik müdahale, izolasyon ve teknik orkestrasyon kabiliyetini haiz merkezi mimari üzerinden yönetilmesi esastır.

(3) Otomatik müdahale ve teknik orkestrasyon kabiliyetleri; kurumsal politikalar ile onay süreçleri saklı kalmak kaydıyla, siber olayların yayılımının durdurulması, tehditlerin canlı ortamdan otomatik izolasyonu ve kritik hizmetlerin yedek altyapı ve sistemlere dinamik olarak aktarılması fonksiyonlarını kapsayacak şekilde yapılandırılır ve işletilir.

(4) İkinci ve üçüncü fıkralarda belirtilen otomatik müdahale ve orkestrasyon kabiliyeti, yanlış pozitif kaynaklı kesintileri önlemek amacıyla belgelenmiş bir geri alma mekanizması işletir. Bu sistemlerin karar mantığı, yılda en az bir kez masabaşı tatbikatla test edilir ve sonuçları kayıt altına alınır.

(5) Başkanlık ve sektörel SOME tarafından iletilen siber tehdit istihbaratı verileri dâhil olmak üzere güncel, harici ve dâhili siber tehdit istihbaratı verilerinin, ilgili sistemlerle entegrasyonu sağlanır ve siber olay müdahale süreçlerinde kullanılır.

Düzenli sızma testleri ve sürekli zafiyet yönetimi

MADDE 63– (1) Kritik altyapıya sahip kuruluşlar, bilişim sistemlerindeki güvenlik zafiyetlerinin tespit edilmesi amacıyla, düzenli olarak kurumsal sızma testleri yürütür ve yılda en az bir kez Başkanlık tarafından yetkilendirilmiş bağımsız kuruluşlara sızma testi yaptırır.

(2) Düzenlenen sızma testi sonuç raporları, sızma testini gerçekleştiren bağımsız kuruluşlar tarafından Başkanlığa ve kritik altyapıya sahip kuruluşa sunulur. Tespit edilen bulgular, kurumsal zafiyet yönetim süreci kapsamında önem derecelerine göre önceliklendirilerek makul süre içerisinde teknik sıkılaştırma tedbirleri uygulanır ve doğrulaması yapılarak Başkanlığa bildirilir. Söz konusu rapor ve kayıtlar, asgari beş yıl süreyle güvenli ortamlarda muhafaza edilir.

(3) Kritik altyapıya sahip kuruluşlar, bilişim sistemlerinde düzenli olarak zafiyet taraması yapar veya yaptırır; tarama sonuçları, tespit edilen zafiyetler ve uygulanan düzeltici işlemlere ilişkin bilgileri aylık olarak Başkanlıkça belirlenen yöntem çerçevesinde Başkanlığa iletir. Başkanlık, gerekli durumlarda daha sık periyotlarla raporlama yapılmasını talep edebilir.

(4) Kritik altyapıya sahip kuruluşlar, Başkanlık tarafından yayımlanan zafiyet duyuruları ve acil yama bildirimlerinin kurumsal zafiyet yönetimi süreçlerine entegrasyonunu sağlar.

Adli bilişim ve delil yönetimi

MADDE 64– (1) Siber olaylardan etkilenen bilişim sistemleri üzerinde herhangi bir analiz, kurtarma veya müdahale faaliyeti gerçekleştirilmeden önce, dijital deliller adli kopyalama yöntemleri kullanılarak ham haliyle koruma altına alınır. Dijital delillere yönelik tüm adli kopyalama, erişim ve işlem hareketleri, inkâr edilemezlik niteliğini haiz olacak şekilde, kronolojik delil zinciri bütünlüğünü sağlayacak arşivleme mimarisinde, özel mevzuatta daha uzun bir süre öngörülmemiş olması kaydıyla, verinin elde edilmesinden itibaren en az iki yıl süreyle güvenli ve erişilebilir şekilde saklanır ve sıkı erişim kontrollerine tabi tutulur.

(2) Adli inceleme, adli makam talebi, devam eden soruşturma veya kovuşturma, idari inceleme, denetim, uyuşmazlık veya olay müdahalesi devam ettiği sürece, ilgili kayıtlar saklama süresinin sona ermiş olması gerekçe gösterilerek silinemez veya imha edilemez.

(3) Dijital delillerin elde edilmesi, kopyalanması, incelenmesi ve muhafazasında ilgili mevzuatta öngörülen usul ve esaslar ile adli makamların yetkileri saklıdır. Bu madde kapsamında elde edilen kopyalar, ilgili mevzuatta öngörülen amaçlarla ve hukuki dayanaklara uygun olarak işlenir. 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri saklıdır.

Olay müdahale, hizmet sürekliliği ve siber kriz yönetimi

MADDE 65– (1) Kritik altyapıya sahip kuruluşların bilişim sistemleri; mevcut ve gelecekteki iş yükü ihtiyaçlarını öngören kurumsal kapasite ve performans yönetimi süreçleri doğrultusunda, tek hata noktası barındırmayacak şekilde yedekli ve yüksek erişilebilirlik mimarisine uygun olarak yapılandırılır. Kritik hizmetlerin kesintisiz sürdürülmesi için otomatik yük devretme ve yük dengeleme mekanizmaları canlı ortamda kesintisiz olarak işletilir. Kapasite planlaması sonuçları ile kritik performans göstergeleri periyodik olarak izlenir ve gerekli görülen hâllerde altyapı kapasitesi güncellenir.

(2) Standart siber olay müdahale süreçlerinin kapasitesini aşan veya kritik iş fonksiyonlarının genel olarak durmasına yol açan siber olaylar ve acil durumlar için üst yönetim seviyesinde sevk ve idare edilecek, asgari düzeyde; onay süreçlerini içeren stratejik komuta zinciri, kriz yönetim grubu ile rolleri, karar alma mekanizmaları ve iç paydaş, dış paydaş iletişim bilgilerini eksiksiz olarak içeren ve 15 inci maddede belirtilen Ulusal Siber Güvenlik Kriz Yönetimi Planı ile uyumlu kurumsal siber kriz yönetim planı hazırlanır ve yürütülür.

Felaket kurtarma merkezi

MADDE 66– (1) Geniş ölçekli doğal afetler, genel altyapı kesintileri veya bölgesel düzeyde etki doğuran acil durumlara karşı; asıl veri merkezinin bulunduğu yerde meydana gelebilecek bir felaketten etkilenmeyecek farklı bir coğrafi bölgede FKM tesis edilir.

(2) Tesis edilen FKM altyapısı; iş sürekliliği hedefleri, kurtarma süresi hedefleri, kurtarma noktası hedefleri çerçevesinde kritik hizmetlerin ve ilgili bilişim sistemlerinin asgari işlevlerini, asıl veri merkezi tekrar kararlı hale gelinceye kadar kesintisiz yürütecek teknik kapasitede hazır bulundurulur.

(3) FKM altyapısına geçiş süreçlerine ilişkin tetikleme senaryoları, idari yetki matrisleri ve operasyonel süreçler dokümante edilir ve 67 nci madde kapsamında test edilir.

Siber tatbikat

MADDE 67– (1) Kritik altyapıya sahip kuruluşlar, siber saldırılara karşı hazırlık ve olgunluk seviyesini ölçmek üzere yılda en az bir kez siber tatbikat gerçekleştirir.

(2) Tatbikat senaryoları; siber kriz ve felaket durumlarında rol alacak insan kaynağı, süreç, tedarikçi ilişkileri, teknoloji ve diğer bağımlı taraf bileşenlerini kapsayacak şekilde bütüncül olarak tasarlanır.

(3) Elde edilen tatbikat sonuçlarına göre kriz senaryoları için belirlenen hedef kurtarma süreleri ile veri kayıp toleransları fiilen doğrulanır. Tespit edilen sapmalar, eksiklikler ve siber direnç riskleri doğrultusunda siber kriz yönetimi ve felaket kurtarma planları ile sistem konfigürasyonları güncellenir.

(4) Tatbikat ve siber dayanıklılık testlerinin çıktıları, yürütülen senaryo adımları ve test kanıtlarıyla birlikte resmî sonuç raporları haline getirilerek en az beş yıl süreyle güvenli ortamlarda saklanır.

Tesis güvenliğinde uygulanacak ek hususlar

MADDE 68– (1) Kritik altyapıya sahip kuruluşlarda kritik alanlara, veri merkezine ve FKM'ye fiziksel erişimlerde biyometrik doğrulama içeren çok faktörlü fiziksel erişim kontrol sistemleri kullanılır.

(2) Asıl veri merkezi ile FKM'nin barındırıldığı alanlarda elektriksel, mekanik ve veri iletişim altyapı bileşenleri bakım, onarım veya değişim zamanları dâhil sistemin işleyişinde herhangi bir kesintiye mahal vermeyecek şekilde yedekli mimari ile tesis edilir ve şebeke arızalarında sistemlerin kesintisiz çalışmasını sağlamak üzere tam yedekli kesintisiz güç kaynakları ve jeneratör altyapısı kurulur.

(3) Yükleme ve depo alanları ile kamuya açık alanlar, kritik bilişim sistemlerinin bulunduğu alanlardan güvenli ve kontrollü geçiş noktaları ile fiziki olarak ayrılır. Kritik alanlara üçüncü taraflarca yapılacak zorunlu erişimler yetkili personel refakatinde gerçekleştirilir.

Tedarik zinciri güvenliği

MADDE 69– (1) Kritik altyapıya sahip kuruluşlar, kritik altyapı kapsamında temin edilecek donanım, yazılım ve bilişim sistemi bileşenlerine yönelik olarak tedarikçi seçimi, satın alma ve kabul süreçleri ile bu süreçlerde uygulanacak siber güvenlik gereksinimlerini belirler. Akdedilecek sözleşmelerde, hizmet ve ürünlerin belirlenen siber güvenlik gereksinimlerini karşılayacak üçüncü taraflar ve tedarikçilerden temin edilmesi taahhüt altına alınır.

(2) Tedarikçilerin, ürün yaşam döngüsü boyunca tespit edilen güvenlik zafiyetlerini derhal bildirmesi ve belirlenen süreler içerisinde yama desteği sağlamasına ilişkin hususlar sözleşmede belirtilir.

(3) Kritik altyapı fonksiyonlarını doğrudan etkileyen özelleştirilmiş yazılımlar canlı ortamda devreye alınmadan önce, statik ve dinamik kaynak kod analizleri gerçekleştirilir.

(4) Tedarikçinin teknik desteği taahhüt edilen sürelerde sağlamaması veya tüzel kişiliğinin sona ermesi riskine karşı, ilgili yazılımlara ait kaynak kodların ve yapılandırma mimarisinin, bağımsız bir üçüncü taraf nezdinde kaynak kod emaneti mekanizmasıyla güvence altına alınması zorunludur.

(5) Kritik altyapı sistemlerine mantıksal veya fiziksel erişim yetkisi bulunan ya da kritik bileşen sağlayan tedarikçilerin siber güvenlik uyumlulukları, yılda en az bir kez denetlenir veya bağımsız denetim raporları yoluyla doğrulanır.

Siber güvenlik faaliyet raporu

MADDE 70– (1) Kritik altyapıya sahip kuruluşlar, 50 nci madde çerçevesinde hazırlayacakları siber güvenlik faaliyet raporuna;

a) 51 inci maddenin üçüncü fıkrası kapsamında tahsis edilen siber güvenlik bütçesi ile insan kaynağı yatırımlarının gerçekleşme durumunu,

b) 55 inci madde kapsamındaki gelişmiş erişim ve kimlik yönetimi çıktılarını,

c) 62 nci maddede düzenlenen sistemler ile siber tehdit istihbaratı entegrasyon sonuçlarını,

ç) 63 üncü madde kapsamındaki düzenli sızma testleri ve zafiyet yönetimi sonuçlarını,

d) 67 nci madde uyarınca gerçekleştirilen siber tatbikat çıktıları ile hedef kurtarma süreleri ve veri kayıp toleranslarına ilişkin doğrulama kanıtlarını,

e) 68 inci madde kapsamında tedarikçilerin denetim sonuçlarını

dâhil eder.

(2) Siber güvenlik faaliyet raporu, siber güvenlik performansı, mevcut risk durumu ve birinci fıkrada belirtilen hususlara ilişkin teknik analizleri özetleyen genel bir değerlendirmeyi içerir ve üst yönetim tarafından onaylanır.

(3) Bir önceki takvim yılına ait siber güvenlik faaliyet raporu, izleyen yılın mart ayının sonuna kadar Başkanlığa ve ilgili sektörel SOME'ye sunulur.

YEDİNCİ BÖLÜM
Kamu Kurum ve Kuruluşlarına İlişkin Hususlar

Kamu kurum ve kuruluşlarının yükümlülükleri

MADDE 71– (1) Kamu kurum ve kuruluşları bu Yönetmeliğin dördüncü ve beşinci bölümlerinde yer alan yükümlülük ve sorumluluklara tabidir. Başkanlık tarafından kritik altyapıya sahip olduğu belirlenen kamu kurum ve kuruluşları altıncı bölümde yer alan yükümlülük ve sorumluluklara da tabidir.

(2) Kamu kurum ve kuruluşları, sahip oldukları bilişim sistemleri ve bu sistemler vasıtasıyla sundukları hizmetleri, varsa ikincil sistemlerini ve felaket kurtarma merkezini de kapsayacak şekilde ulusal veya uluslararası düzeyde yetkilendirilmiş kuruluşlardan BGYS kurumsal uygunluk belgesi alır ve bu belgenin güncelliğini kesintisiz olarak sağlar. Belgenin askıya alınması, geçerliliğinin sona ermesi veya kapsam değişikliği derhâl Başkanlığa bildirilir.

(3) Kamu kurum ve kuruluşlarının, diğer kamu kurum ve kuruluşları ile gerçekleştirdikleri veri iletişiminin Başkanlık tarafından belirlenecek usul, esas ve yöntemlere uygun olarak Başkanlık tarafından belirlenecek altyapılar üzerinden gerçekleştirilmesi esastır.

(4) Kamu kurum ve kuruluşlarının kamuya açık internet sitelerinde aşağıdaki güvenlik tedbirleri uygulanır:

a) İnternet sitelerinde yayımlanan içeriklerin yetkisiz olarak değiştirilmesini önlemek amacıyla erişim kontrolü uygulanır.

b) İçeriklerin yayımlanması veya değiştirilmesi için katmanlı yetki mekanizması yürütülür.

c) İçeriklerin yönetildiği arayüzlere erişimde çok faktörlü kimlik doğrulama kullanılır.

ç) Alan adı kayıtlarının kurumsal hesaplar üzerinden yapılması sağlanarak sahip olunan alan adları varlık envanterine eklenir ve alan adlarının yönetimi kuruluş bünyesinde merkezi olarak yürütülür.

d) Kullanılmayan ve artık ihtiyaç bulunmayan alan adlarının ve bu alan adları üzerinden sunulan hizmetlerin sonlandırılması sağlanır.

e) Bu hizmetlerin üçüncü taraflardan tedarik edilmesi halinde de önlemler aynı seviyede uygulanır.

(5) Başkanlık, kamu kurum ve kuruluşlarına sahip oldukları bilişim altyapısının ve sunduğu hizmetin niteliğine ve kritikliğine göre ek yükümlülükler getirebilir, ilave tedbirler almasını isteyebilir.

SEKİZİNCİ BÖLÜM
Çeşitli Hükümler

Türkiye Cumhuriyeti'nin siber uzaydaki millî gücünü meydana getiren unsurlar

MADDE 72- (1) Kanunun 16 ncı maddesinin altıncı fıkrası kapsamında Türkiye Cumhuriyeti'nin siber uzaydaki millî gücünü meydana getiren unsurların tespitinde; millî güvenlik, kamu düzeni, ekonomik güvenlik ve istikrar, kritik kamu hizmetlerinin sürekliliği ve toplumun güvenliği bakımından taşıdığı önem ile siber uzayda kullanılan varlık, sistem, altyapı, veri ve hizmetlerin niteliği, işlevi ve bunlara yönelik bir siber tehdit veya siber saldırının muhtemel etki ve sonuçları dikkate alınır.

(2) Birinci fıkra kapsamında, özellikle aşağıdaki varlık, sistem ve altyapılar dikkate alınır;

a) Kanunun 3 üncü maddesinin birinci fıkrasının (d) bendinde tanımlanan kritik altyapılar ile bunların bilişim sistemleri,

b) Kritik kamu hizmetlerinin sunulmasını sağlayan veya destekleyen bilişim sistemleri, bilgi ve iletişim teknolojileri altyapıları ve diğer bilişim varlıkları,

c) Siber tehditlerin tespiti, izlenmesi, analiz edilmesi ve siber olaylara müdahale edilmesi ile ulusal siber savunma faaliyetlerinin yürütülmesi bakımından ulusal ölçekte stratejik önem taşıyan bilişim sistemleri ve altyapıları,

ç) Devletin temel işlevlerinin yerine getirilmesi, kamu hizmetlerinin kesintisiz yürütülmesi veya millî güvenliğin sağlanması bakımından stratejik nitelik taşıyan veri tabanları ve veri işleme altyapıları da dâhil tüm bilişim sistemleri ile bu sistemlerde işlenen, aktarılan veya muhafaza edilen verileri,

d) Türkiye Cumhuriyeti'nin siber güvenlik ve siber savunma kapasitesi bakımından stratejik veya kritik nitelik taşıyan siber güvenlik ürün, sistem, yazılım, donanım ve teknolojilerinin geliştirilmesi, üretilmesi, test edilmesi veya işletilmesi için kullanılan kritik bilişim varlıkları ve altyapılar.

(3) Birinci ve ikinci fıkralarda belirtilen unsurların tespitinde, somutlaştırılmasında ve kapsamının belirlenmesinde ilgili mevzuat uyarınca belirlenen kritik altyapılar, kritik kamu hizmetleri, kamu kurum ve kuruluşlarının varlıklarına ilişkin envanter, sınıflandırma ve tespitler dikkate alınır.

Gönüllü Bildirim

MADDE 73– (1) Bu Yönetmelik kapsamında zorunlu bildirim yükümlülüğü bulunulmayan siber olaylar, siber tehditler, siber zafiyetler, gerçekleşmesi muhtemel siber olaylar ile siber güvenliğin geliştirilmesine katkı sağlayabilecek diğer teknik bilgi ve bulgular; yükümlüler ile bu Yönetmelik kapsamı dışında kalan gerçek ve tüzel kişiler tarafından Başkanlığa gönüllü olarak bildirilebilir.

(2) Bu madde kapsamında yapılan bildirimler 12 nci maddede yer alan süreçler çerçevesinde yürütülür.

(3) Bildirimde, olayın veya zafiyetin gerçekleştiği ya da öğrenildiği tarih, niteliği ve kapsamı, etkilenen veya etkilenmesi muhtemel varlıklar, alınan ilk tedbirler, mevcut teknik kayıtlar yer almalıdır. Bildirimde bulunan, edindiği bilgi, belge, kayıt ve log kayıtlarını eksiksiz biçimde sunar.

Denetim ve Yaptırım

MADDE 74– (1) Başkanlık, bu Yönetmelik kapsamında yer alan tarafların yükümlülüklerini yerine getirip getirmediğini re'sen veya şikâyet üzerine denetler veya denetlettirir.

(2) Bu Yönetmelikte düzenlenen yükümlülüklere aykırı hareket ettiği tespit edilen taraflar hakkında Kanunun 16 ncı ve 17 nci maddeleri ve sair mevzuat hükümleri uyarınca idari para cezası, diğer yaptırımlar ve tedbirler uygulanır.

DOKUZUNCU BÖLÜM
Son Hükümler

Ek yükümlülükler

GEÇİCİ MADDE 1– Beşinci bölüm kapsamındaki kuruluşlar, altıncı bölüm kapsamına dâhil edilmeleri halinde, bir yıl içinde altıncı bölümde yer alan yükümlülükleri yerine getirirler.

Kamu kurum ve kuruluşlarının belgelendirme yükümlülüğü

GEÇİCİ MADDE 2– Kamu kurum ve kuruluşları, 71 inci maddenin ikinci fıkrası kapsamındaki belgelendirme yükümlülüğünü bir yıl içinde sağlar.

Yürürlük

MADDE 75– (1) Bu Yönetmeliğin;

a) Beşinci bölümü bu Yönetmeliğin yayımından altı ay sonra,

b) Altıncı bölümü bu Yönetmeliğin yayımından bir yıl sonra,

c) Diğer maddeleri yayımlandığı tarihte

yürürlüğe girer.

Yürütme

MADDE 76– (1) Bu Yönetmelik hükümlerini Siber Güvenlik Başkanı yürütür.

TASLAK