

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURULU
KARARI

Karar Tarihi : 24.12.2024
Karar Sayısı : 2024/İK-BTD/497
Gündem Konusu : Ulusal Siber Güvenliğin Sağlanmasına ve Siber Caydırıcılığın Artırılmasına Yönelik Yönetmelik Taslağı
KARAR : Bilgi Teknolojileri Dairesi Başkanlığının hazırladığı
takrir ve ekleri incelenmiştir.

Ulusal siber güvenlik faaliyetlerin daha etkin bir şekilde yürütülebilmesi adına kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması, bu saldırılara karşı caydırıcılığın sağlanması ve yüksek düzeyde siber güvenlik seviyesine ulaşılması amacıyla yürütülecek faaliyetlere ilişkin usul ve esasların belirlenmesi amacıyla Ek'te yer alan "*Ulusal Siber Güvenliğin Sağlanmasına ve Siber Caydırıcılığın Artırılmasına Yönelik Yönetmelik Taslağı*"nın, kamuoyunun görüşleri alınmak üzere Kurumumuz İnternet sitesinde on beş (15) gün süreyle yayımlanması, ilgili kamu kurum ve kuruluşlarına görüş alınması için gönderilmesi ve bu kapsamda usule ilişkin gerekli tüm işlemlerin yapılması için icraya yetki verilmesi

hususlarına karar verilmiştir.

Bilgi Teknolojileri ve İletişim Kurumundan:**ULUSAL SİBER GÜVENLİĞİN SAĞLANMASINA VE SİBER CAYDIRICILIĞIN
ARTIRILMASINA YÖNELİK YÖNETMELİK TASLAĞI****BİRİNCİ BÖLÜM
Başlangıç Hükümleri****Amaç**

MADDE 1- (1) Bu Yönetmeliğin amacı, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması, bu saldırılara karşı caydırıcılığın sağlanması ve yüksek düzeyde siber güvenlik seviyesine ulaşılması amacıyla yürütülecek faaliyetlere ilişkin usul ve esasların belirlenmesidir.

Kapsam

MADDE 2- (1) Bu Yönetmelik, kamu kurum ve kuruluşları ile gerçek ve tüzel kişileri kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 6 ncı maddesinin birinci fıkrasının (v) ve (y) bentleri, 60 ıncı maddesinin iki, on bir, on iki ve on üçüncü fıkralarına ve 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 10 uncu maddesinin altıncı fıkrasına ve 1 Nolu Cumhurbaşkanlığı Kararnamesine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) BİT: Bilgi ve iletişim teknolojilerini,
- b) Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran altyapıları,
- c) Kritik sektörler: Kritik altyapıları bünyesinde barındıran sektörleri,
- ç) Kurum: Bilgi Teknolojileri ve İletişim Kurumunu,
- d) Kurul: Bilgi Teknolojileri ve İletişim Kurulu'nu,
- e) Risk: Bir olayın neden olduğu kayıp veya aksaklık potansiyeli ile bu kayıp veya aksaklığın büyüklüğü ile olayın meydana gelme olasılığının bir kombinasyonunu,
- f) Siber olay: Depolanan, iletilen veya işlenen verilerin veya şebeke ve bilgi sistemleri tarafından sunulan veya bunlar aracılığıyla erişilebilen hizmetlerin kullanılabilirliğini, gerçekliğini, bütünlüğünü veya gizliliğini tehlikeye atan bir siber olayı,
- g) Siber tehdit: Şebeke ve bilgi ve bilgi sistemlerine, bu sistemlerin kullanıcılarına ve diğer kişilere zarar verebilecek, bunları kesintiye uğratabilecek veya başka bir şekilde olumsuz etkileyebilecek her türlü potansiyel durum, olay veya eylemi,
- ğ) SOME: 20/6/2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı'nın ekinde yer alan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 üncü maddesi gereğince oluşturulan siber olaylara müdahale ekiplerini,

h) SOME İletişim Platformu (SİP): USOM ile kurumsal ve sektörel SOME'ler arasındaki güvenli iletişimi sağlayan platformunu,

ı) USOM: 20/6/2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanan 2013/4890 sayılı Bakanlar Kurulu Kararı'nın ekinde yer alan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 üncü maddesi gereğince kurulan ve Kurum bünyesinde faaliyetlerini yürüten Ulusal Siber Olaylara Müdahale Merkezini,

i) Zararlı yazılım: Sahibinin bilgisi ve isteği dışında bilgisayarlara bulaşan, kullanıcı bilgisayarını, sunucuları veya bilişim ağlarını hedef alan virüs ve benzeri yazılımları,

ifade eder.

İKİNCİ BÖLÜM

Ulusal Siber Güvenlik Organizasyonu

Bilgi Teknolojileri ve İletişim Kurumu

MADDE 5- (1) Kurum, bu Yönetmeliğin ülke genelinde uygulanmasından, takibinden ve gerekli koordinasyonun sağlanmasından sorumludur.

(2) Kurum, siber güvenlik ile ilgili hususlarda, ulusal ve uluslararası düzeyde eşdeğer kurum ve kuruluşlarla iş birliği yapılması, koordinasyonun sağlanması, iş birliği ağlarına katılım sağlanmasına ilişkin olarak tek irtibat noktasıdır.

(3) Kurum, bu Yönetmelikte yer alan hükümleri USOM aracılığıyla yürütür. USOM'a yapılan atıflar aynı zamanda Kuruma yapılmış sayılır.

Ulusal Siber Olaylara Müdahale Merkezi

MADDE 6- (1) Kurum bünyesinde yer alan Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) görev, yetki ve sorumlulukları şunlardır:

a) Ulusal düzeyde siber tehditleri, güvenlik zafiyetlerini, siber olayları, şebeke ve bilgi sistemlerini gerçek zamanlı olarak taramak, izlemek ve analiz etmek.

b) Siber tehditler, güvenlik zafiyetleri ve siber olaylar hakkında temel ve önemli kuruluşlar, SOME'ler ve diğer paydaşlara alarm, uyarı, duyuru ve bilgi paylaşımı yapmak.

c) Siber olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemleri almak veya alınmasını sağlamak.

ç) Siber olaylara müdahale etmek ve uygun olduğu durumlarda temel ve önemli kuruluşlara yardım sağlamak, koruyucu tedbirlerin alınması konusunda koordinasyon sağlamak.

d) Potansiyel olarak önemli bir etkiye sahip güvenlik zafiyetini tespit etmek için ilgili kuruluşun şebeke ve bilgi sistemlerine uzaktan veya yerinde müdahale desteği sağlamak.

e) Güvenlik zafiyeti bildirimi süreçlerinde koordinasyonu sağlamak.

f) SOME'ler, ulusal ve uluslararası paydaşlar ve sektörler arasında iş birliği ve koordinasyonu sağlamak.

g) Bilgi paylaşımı sağlamaya yönelik uygun, güvenli ve esnek bir iletişim ve bilgi altyapısını kurmak ve yönetmek.

ğ) Ulusal ve uluslararası düzeyde siber tatbikat, eğitim, kapasite inşası, farkındalık çalışmaları gerçekleştirmek.

h) Siber tehdit istihbaratı edinimi, zararlı yazılım analizi, olay müdahale ve ulusal siber güvenliğin sağlanması amacıyla bilgi, belge, veri ve kayıtlara erişmek ve incelemek, ihtiyaç halinde ilgili kurum ve kuruluşlarla edindiği bilgileri paylaşmak,

ı) Çalışmaları esnasında, konusu suç teşkil eden veriler ile karşılaşması halinde adli makamlar ve kolluk kuvvetlerine bildirimde bulunmak.

i) Ulusal siber güvenliğin sağlanması ile ilgili konularda ülkemizde yapılması gereken iş ve işlemlere ilişkin hukuki, teknik ve idari konularda öneriler geliştirmek.

j) Güvenli iletişim kanalı aracılığıyla kurumsal ve sektörel SOME'lerin önemli siber olay ve tehditlere ilişkin bildirimler almalarını veya göndermelerini sağlamak, sektörel ve kurumsal SOME'lere güvenlik bildirimleri, alarm, duyuru, mesaj ve ihbarlar göndermek ve acil olarak alınması gereken tedbirleri bu iletişim kanalı vasıtasıyla çevrim içi olarak paylaşmak.

k) İnternet aktörleri, özel sektör kuruluşları, kamu kurum ve kuruluşları, uluslararası kuruluşlar ile iş birliği yapmak.

l) Görevleri kapsamında adli bilişim analizi, zararlı yazılım analizi, nesnelerin interneti güvenliği analizi gibi faaliyetleri yürütmek için laboratuvar kurmak ve işletmek.

Sektörel SOME'ler

MADDE 7- (1) Kritik sektörlerle ilişkin olarak, ilgili kamu kurum ve kuruluşları tarafından kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde sektörel SOME kurulur.

(2) Sektörel SOME'lere yönelik koordinasyon USOM tarafından yürütülür.

(3) Sektörel SOME'lerin görev, yetki ve sorumlulukları şunlardır:

a) Bu Yönetmeliğin sektör bazlı uygulanmasına, takibine, denetimine ve yaptırımına ilişkin faaliyetleri yürütmek ve gerekli koordinasyonu sağlamak.

b) Siber tehdit veya siber olay durumunda, hangi tedbirlerin alınacağı veya olayın çözümü, olumsuz etkisinin azaltılması veya ortadan kaldırılması için yapılması gerekenler hususunda temel ve önemli kuruluşları yönlendirmek, ilgili kuruluşlarla iş birliği içerisinde çalışmak ve 7/24 erişilebilir iletişim bilgilerini belirleyerek kurumsal SOME'ler ve USOM ile paylaşmak.

c) Sektörel risk analizi ve sektörel siber olay acil durum iş sürekliliği planlarını yapmak ve bu planları asgari iki yılda bir gözden geçirerek gerekli güncellemeleri yapmak.

ç) Siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütmek.

d) Kendisine bildirilen siber olayları ve siber tehditleri gecikmeksizin USOM'a bildirmek.

e) Siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları kurumsal SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütmek.

f) Sektörlerine ilişkin kurumsal SOME'lerin yapılanması konusunda düzenleyici faaliyetleri yürütmek ve kurumsal SOME'ler arasındaki iş birliğini koordine etmek.

g) Sektörlerine ilişkin bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri bu Yönetmelik ile uyumlu olacak şekilde oluşturmak ve yürütmek.

ğ) Birlikte çalıştıkları kurumsal SOME'lerde yaşanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlamak ve gerekli görülmesi durumunda USOM'dan destek almak.

h) Çalışmaları esnasında, konusu suç teşkil eden veriler ile karşılaşması halinde durumu gecikmeksizin adli makamlar, kolluk kuvvetleri ve USOM'a bildirmek.

ı) Sorumlu oldukları sektörlerde faaliyet gösteren kuruluşları bu Yönetmeliğin 8 inci Maddesinde belirtilen kriterler kapsamında temel veya önemli kuruluş olarak belirlemek.

i) Sorumlu oldukları sektörlerde faaliyet gösteren kurum ve kuruluşların SOME olgunluk seviyelerinin tespitinde ve geliştirilmesinde USOM ile koordineli çalışmak.

Temel ve önemli kuruluşlar

MADDE 8- (1) Sektörel SOME'ler, sorumlu oldukları sektörlerde faaliyet gösteren kuruluşları, aşağıdaki kriterler kapsamında temel veya önemli kuruluş olarak belirler ve gecikmeksizin USOM'a iletir:

a) Kritik toplumsal veya ekonomik faaliyetlerin sürdürülmesi için gerekli olan bir hizmetin ülke genelinde tek veya önemli sağlayıcısı olması,

b) Sağladığı hizmetin kesintiye uğramasının kamu güvenliği, ulusal ekonomi veya kamu sağlığı üzerinde önemli bir etki yaratabilecek olması,

c) Belirli bir sektör veya hizmet türü ya da diğer sektörlerle arasındaki bağ nedeniyle ulusal veya uluslararası düzeyde taşıdığı özel ve kritik öneme sahip olması,

ç) Ulusal politika veya sektörel SOME'ler tarafından sektör özelinde belirlenen diğer kriterleri sağlaması.

(2) Sektörel SOME'ler, sektörleriyle ilişkili kuruluşların listesini tutar, yılda en az bir defa tüm kuruluşların bu maddede yer alan kriterler nezdinde kontrolünü sağlar. Sektörel SOME'ler, sektörleriyle ilişkili kuruluşlar listesinde herhangi bir değişikliği on beş (15) gün içerisinde USOM'a bildirir. Bu bildiride asgari olarak kuruluşun adı, iletişim bilgisi, e-posta adresi, telefon numarası ve irtibat kişi bilgisi yer alır.

(3) Temel ve önemli kuruluşlara ilişkin yükümlülükler ve bunlara ilişkin kriterler bağlı oldukları sektörel SOME tarafından belirlenir. Temel kuruluşlar bu Yönetmelik kapsamında önemli kuruluşlara göre daha fazla görev ve yükümlülüğe tabiidir.

Kurumsal SOME'ler

MADDE 9- (1) Bu Yönetmeliğin kapsamına dahil olan tüm kamu kurum ve kuruluşları ile temel ve önemli kuruluşlar kendi bünyelerinde kurumsal SOME kurar.

(2) Kurumsal SOME'lerin görev, yetki ve sorumlulukları şunlardır:

a) Kendilerine doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri almak veya aldırarak, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olayların tespiti için gerekli iz kayıt sistemlerini kurmak veya kurdurmak ve bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmak.

b) Siber olayların önlenmesi veya zararlarının azaltılmasına yönelik, bilişim sistemlerini kurmak, işletmek veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirleri almak veya aldırarak.

c) Siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini sektörel SOME ile koordineli olarak yürütmek, siber olayları ve siber tehditleri raporlamak ve durumdan gecikmeksizin USOM’u haberdar etmek.

ç) Siber olayla karşılaşması durumunda, sektörel SOME’ye ve USOM’a bilgi vererek olaya kendi imkân ve kabiliyetleri çerçevesinde müdahale etmek ve ihtiyaç halinde sektörel SOME’den ve/veya USOM’dan yardım talebinde bulunmak.

d) Çalışmaları esnasında, konusu suç teşkil eden veriler ile karşılaşması halinde durumu gecikmeksizin adli makamlar, kolluk kuvvetleri, sektörel SOME ve USOM’a bildirmek.

e) USOM ve/veya sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak gerekli tedbirleri almak.

f) 7/24 erişilebilir iletişim bilgilerini belirleyerek sektörel SOME ve USOM ile paylaşmak.

Uyumlaştırma

MADDE 10- (1) Bu Yönetmelik, sektörel SOME’ler tarafından sorumlu oldukları sektöre uyumlaştırılacaktır.

(2) Sektörel SOME’ler, bu Yönetmeliğin ilgili sektörde uygulanmasına yönelik ulusal ve uluslararası bilgi güvenliği standartlarını da dikkate alarak düzenleme yapar veya mevcut düzenlemelerini bu kapsamda günceller.

(3) Bu Yönetmelikte belirlenen yükümlülükler asgari yükümlülükler olup sektörel SOME’ler tarafından gerçekleştirilen uyumlaştırma çalışmalarında ek yükümlülükler getirilebilir. Sektörel SOME’ler, sektöre özel ek yükümlülüklerin uygunluğuna yönelik USOM ile iş birliği yapar.

(4) Sektörel SOME’ler bu Yönetmeliğe olan uyumluluğunu Kurum tarafından belirlenen yöntem ile Kuruma sunarlar.

SOME olgunluk modeli

MADDE 11- (1) SOME’lerin olgunluk modeline ilişkin usul ve esaslar USOM tarafından belirlenir.

(2) SOME’ler USOM tarafından belirlenen olgunluk seviyesinin artırılması amacıyla gerekli çalışmaları yapar.

(3) SOME’lerin olgunluk modeli ölçümü yılda en az bir defa USOM tarafından yapılır. USOM tarafından belirlenen SOME’lerin olgunluk modeline ilişkin usul ve esaslar kapsamında, SOME’ler olgunluk modeli ile ilgili ilerleme ve faaliyet raporlarını USOM ile paylaşır.

(4) SOME’ler USOM tarafından oluşturulan olgunluk modeli kapsamında talep edilen bilgileri USOM’a sağlamakla yükümlüdür.

ÜÇÜNCÜ BÖLÜM

Siber Güvenlik Risk Yönetimi Tedbirleri ve Raporlama Yükümlülükleri

Siber güvenlik risk yönetimi tedbirleri

MADDE 12- (1) Kurumsal SOME’ler, kullandıkları şebeke ve bilgi sistemlerinin güvenliğine yönelik riskleri belirlemek, risklerin etkisini önlemek veya en aza indirmek için faaliyet gösterilen sektör ve hizmetin kritikliği dikkate alınarak teknik, operasyonel ve organizasyonel tedbirleri alır.

(2) Kurumsal SOME'ler, yeni ve güvenilir teknolojiyi kullanmakla ve yeterli bilgi ve deneyimi haiz personel istihdam etmekle yükümlüdür.

(3) Kurumsal SOME'ler, risklere maruz kalma derecesi, kuruluşun büyüklüğü ve toplumsal ve ekonomik etkileri de dahil olmak üzere, olayların meydana gelme olasılığını ve muhtemel etkilerini dikkate alarak gerekli tedbirleri alır.

(4) Kurumsal SOME'lerin alacağı siber güvenlik risk yönetimi tedbirleri asgari düzeyde aşağıdaki hususları içermelidir;

- a) Bilgi güvenliği yönetim sistemi ve politikaları,
- b) Varlık envanteri ve yönetimi,
- c) Risk analizi, değerlendirmesi ve işlenmesi faaliyetleri,
- ç) Siber olay müdahale ve yönetim prosedürleri,
- d) Donanımsal ve yazılımsal yedekleme,
- e) İşlem kayıtlarının kaydedilmesi ve kayıt bilgilerinin korunması,
- f) Felaket kurtarma ve kriz yönetimi senaryolarını da içeren iş sürekliliği,
- g) Tedarikçi ve üçüncü taraflarla olan ilişkilerde bilgi güvenliği,
- ğ) Şebeke ve bilgi sisteminin temini, geliştirilmesi ve bakımı süreçlerine ilişkin güvenlik zafiyetinin ele alınması ve ifşa edilmesini de dikkate alan güvenlik tedbirleri,
- h) Siber güvenlik risk yönetimi tedbirlerinin etkinliğini değerlendirmek için politika ve prosedürler,
- ı) Temel siber hijyen uygulamaları ve siber güvenlik eğitimi,
- i) Şifreleme, çok faktörlü kimlik doğrulama ve güvenli iletişim sistemlerinin kullanımına ilişkin politika ve prosedürler,
- j) İnsan kaynakları güvenliği, erişim kontrol politikaları,
- k) Fiziksel ve çevresel güvenliğine ilişkin tedbirler,
- l) İç denetim ve sürekli iyileştirme faaliyetleri.

(5) USOM, dördüncü fıkarda yer alan tedbirlerin uygulanmasına yönelik açıklayıcı kılavuz yayımlayabilir, rehberlik sağlayabilir ve yeni tedbirler belirleyebilir.

(6) Sektörel SOME'ler, sorumlu oldukları sektör özelinde USOM ile iş birliği yaparak sektöre özgü ek tedbirler belirleyebilir.

Kritik tedarik zincirlerinde koordineli güvenlik risk değerlendirmeleri

MADDE 13- (1) USOM, bölgesel ve uluslararası değerlendirmeleri ve risk faktörlerini dikkate alarak belirli kritik BİT ürün, hizmet ve sistemlerinin tedarik zincirlerine yönelik koordineli güvenlik riski değerlendirmeleri gerçekleştirebilir ve BİT ürün, hizmet ve sistemlerini belirleyebilir.

(2) Kurumsal SOME'ler, tedarikçi ve üçüncü taraflarla olan ilişkilerinde birinci fıkarda belirlenen koordineli güvenlik risk değerlendirmelerini dikkate alır.

Önemli olay ve raporlama yükümlülükleri

MADDE 14- (1) Kurumsal SOME'ler önemli bir olayın tespit edilmesinden itibaren, en geç 12 saat içinde bağlı oldukları sektörel SOME'ye ve USOM'a gecikmeksizin olayı teknik detaylarıyla birlikte bildirir. Sektörel SOME, USOM'a bildirim yapılmadığını tespit ederse gelen bildirimi gecikmeksizin USOM'a iletir.

(2) USOM gelen olay bildirimi ile ilgili ek bilgi ve açıklama talep edebilir.

(3) USOM hizmetten faydalananların olumsuz yönde etkilenmemesi veya etkinin en aza indirilmesi için, kurumsal SOME'nin hizmetten faydalananları bilgilendirmesini ve alabilecekleri her türlü tedbiri veya çözümü gecikmeksizin bildirmelerini talep edebilir.

(4) Önemli olayı tanımlamak için kullanılacak ölçütler, USOM ve sektörel SOME tarafından, ilgili sektörün kendine özgü nitelikleri ve ihtiyaçları dikkate alınarak belirlenir. Bir olayın önemli kabul edilebilmesi için aşağıdaki ölçütler dikkate alınır:

- a) Hizmetlerde ciddi operasyonel aksamaya veya ilgili kuruluş için mali kayba veya can kaybına neden olması veya olması ihtimali,
- b) Gerçek veya tüzel kişileri önemli ölçüde maddi veya manevi zarara uğratmak suretiyle etkilemiş olması veya olması ihtimali,
- c) İlgili kritik hizmetten doğrudan veya dolaylı yararlanan kişi sayısı veya kişi sayısı oranı,
- ç) Gizlilik, erişilebilirlik ve bütünlüğe karşı ciddi düzeyde risk içermesi,
- d) Ele geçirilen verilerin gizli, çok gizli veya ticari sır niteliğinde olması,
- e) Siber olayın kamu düzeni, kamu güvenliği, milli güvenlik, toplum sağlığı, ekonomik veya toplumsal faaliyetler üzerinde etkisi,
- f) Siber olaydan etkilenebilecek coğrafi alan genişliği.

(5) Kurumsal SOME tarafından önemli olay ile ilgili olarak aşağıda yer verilen yükümlülükler çerçevesinde sektörel SOME ve USOM'a raporlama yapılır:

- a) Önemli olay ile ilgili teknik detaylar ve mevcut tüm bilgiler belirtilir,
- b) Birinci fıkrada belirtilen olay bildiriminden en geç bir ay içinde aşağıdaki bilgileri içeren rapor sunulur:
 - 1) Olayın ciddiyeti ve etkisi de dahil olmak üzere ayrıntılı açıklaması,
 - 2) Olayı tetiklemiş olması muhtemel tehdit türü veya kök neden,
 - 3) Uygulanan ve devam eden etki ve risk azaltma önlemleri,
 - 4) Varsa olayın sınır ötesi etkisi,
 - 5) Saldırının başlangıcından olayın tespit edilmesine kadar geçen süre boyunca saldırganların davranışlarına ilişkin zaman çizelgesi.

(6) USOM, birinci fıkrada yer alan bildirimi aldıktan sonra 24 saat içerisinde, bildirimde bulunan kuruluşa önemli olayla ilgili teknik destek sağlayabilir.

(7) USOM, önemli olayın sınır ötesi etkisi olduğu durumlarda, gerekli görmesi halinde etkilenen ülkedeki eşdeğer kurum veya kuruluşu önemli olay hakkında bilgilendirebilir. Bu bilgilendirmede, kuruluşun ticari ve yasal bilgilerinin gizliliği sağlanır. USOM, bu madde ve 17'inci madde uyarınca bildirilen önemli olaylar, vakalar ve siber tehditler hakkında

anonimleştirilmiş ve birleştirilmiş verileri karşılıklılık ilkesi uyarınca bölgesel veya uluslararası kuruluşlarla paylaşabilir.

(8) Önemli bir olayın önlenmesi veya devam etmekte olan önemli bir olayın çözülmesi veya etkisinin azaltılması için kamuoyunun bilinçlendirilmesinin gerekli olduğu veya önemli olayın duyurulmasının kamu yararına olduğu durumlarda, USOM önemli olay hakkında kamuoyunu bilgilendirebilir veya kuruluştan bunu yapmasını talep edebilir.

DÖRDÜNCÜ BÖLÜM

İş Birliği ve Bilgi Paylaşımı

Güvenlik zafiyeti bildirimi

MADDE 15- (1) Ulusal ve uluslararası düzeyde güvenlik zafiyeti bildirimleri USOM tarafından yapılır. Zafiyet bildirimlerinde USOM'un belirlemiş olduğu yöntemler esas alınır. USOM'un belirlediği yöntem dışında iletilen bildirimler dikkate alınmaz.

(2) USOM, güvenlik zafiyeti bildirimlerini aşağıda belirtildiği şekilde yerine getirir:

- a) Bildirilen zafiyetler ile ilgili iletilen kanıtları doğrulamak ve gerek görülmesi halinde test ortamında zafiyeti test etmek.
- b) Zafiyet ile ilgili kuruluşları tespit etmek ve bu kuruluşlarla irtibata geçmek.
- c) Güvenlik zafiyetini bildiren gerçek veya tüzel kişilerin talebi halinde anonim olarak bildirim yapabilmelerini sağlamak.
- ç) Bildirim zaman çizelgelerini müzakere etmek ve birden fazla kuruluşu etkileyen güvenlik zafiyetlerinin giderilmesinde gerekli koordinasyonu sağlamak.
- d) Bildirilen güvenlik zafiyetinin başka ülkelerde önemli bir etkiye sahip olabileceği durumlarda ilgili ülkenin eş değer kurum ve kuruluşu ile irtibata geçmek ve iş birliği yapmak.
- e) Gerekli görülmesi halinde bölgesel ve uluslararası kuruluşlarla güvenlik zafiyeti paylaşımı yapmak.
- f) Zafiyetin birden fazla yazılımda kullanılan ortak bir bileşende bulunması durumunda ve gerekli hallerde güvenlik bildirimi yayınlamak.

(3) USOM talep edilmesi halinde güvenlik zafiyetini bildiren gerçek veya tüzel kişi ile, güvenlik zafiyeti bulunduğu değerlendirilen BİT ürün veya hizmetlerinin üreticisi veya tedarikçisi arasındaki etkileşimi kolaylaştırmak üzere gereken faaliyetleri yürütür.

Bölgesel ve uluslararası siber güvenlik tehdit istihbaratı ağlarına ve iş birliği gruplarına katılım

MADDE 16- (1) USOM, teknik kabiliyetlerin geliştirilmesi, teknoloji ve bilgi transferi, en iyi uygulama paylaşımı, siber olaylar, siber tehditler, riskler ve güvenlik zafiyetleri hakkında bilgi paylaşımında bulunmak, başka bir ülkenin yargı yetkisi dahilinde tespit edilen bir siber olaya yönelik koordineli bir müdahaleyi görüşmek, sınır ötesi olaylar ele almak, karşılıklı yardım sağlamak gibi amaçlarla bölgesel ve uluslararası iş birliği ağlarına katılım sağlar.

(2) USOM stratejik iş birliği, bilgi paylaşımı ve ortak politikalar geliştirme gibi amaçlarla bölgesel ve uluslararası iş birliği gruplarına katılım sağlar.

Gönüllü bildirim

MADDE 17- (1) SOME'ler dışında kalan diğer gerçek ve tüzel kişiler de, gönüllülük esasına dayalı olarak USOM'a, siber olay, siber tehdit ve zafiyet bildirimlerini yapabilir. USOM tarafından bildirimde bulunanlara ödül verilebilir. Bu bildirimler bu Yönetmeliğin 14 üncü maddesinde yer alan hükümler çerçevesinde gerçekleştirilir.

BEŞİNCİ BÖLÜM

Denetim ve Yaptırım

Denetim ve idari yaptırıma ilişkin hususlar

MADDE 18- (1) Sektörel SOME'ler, bu Yönetmeliğin etkin bir şekilde uygulanması için gerçekleştirilecek faaliyetlere ilişkin denetim ve idari yaptırım tedbirlerini bu Yönetmelik ve ilgili mevzuatları dahilinde yerine getirir.

(2) Sektörel SOME'ler belirli bir konuyla sınırlı veya genel amaçlı, ihbar üzerine ya da re'sen, planlı veya plansız denetimler yapar veya yaptırır ve gerekli durumlarda idari yaptırım uygular.

(3) Sektörel SOME'ler önemli bir siber olay, ihlal veya siber güvenlik taraması gibi durumlarda da denetim yapabilir.

(4) Sektörel SOME'ler görev ve yetkileri kapsamında denetim görevlerini yerine getirmek için her türlü bilgi, belge ve veriye ulaşabilir erişebilir veya talep edebilir.

(5) Sektöre özgü denetim ve yaptırım yetkisinin farklı kurum ve kuruluşlar nezdinde bulunması halinde, sektörel SOME'ler ilgili kurum ve kuruluşlarla iş birliği içerisinde denetim ve idari yaptırım faaliyetlerini yerine getirir.

(6) Sektörel SOME'ler, tespit edilen ihlalin kişisel veri ihlali içermesi halinde, kişisel verilerin korunmasından sorumlu makamı konuyla ilgili bilgilendirir ve iş birliği içerisinde çalışır.

(7) Bu Yönetmelik kapsamında siber güvenliğin sağlanmasına ilişkin uygulanacak denetim faaliyetlerinin ve idari yaptırım tedbirlerinin etkili, orantılı ve caydırıcı olması esastır.

ALTINCI BÖLÜM

Çeşitli ve Son Hükümler

Bölgesel ve uluslararası siber güvenlik sertifikasyonları

MADDE 19- (1) USOM, belirli BİT ürün, hizmet ve süreçlerine yönelik bölgesel ve uluslararası siber güvenlik sertifikasyonlarının, kurumsal SOME'ler tarafından uygulanmasını zorunlu tutabilir.

Standardizasyon

MADDE 20- (1) USOM veya sektörel SOME'ler tarafından 12 nci maddenin uygulanması amacıyla, şebeke ve bilgi sistemlerinin güvenliğiyle ilgili bölgesel veya uluslararası standartlara ve teknik şartnamelere uyum şartı ve belgelendirme yükümlülüğü getirilebilir.

Yürürlükten kaldırma

MADDE 21- (1) Bu Yönetmeliğin yayımı ile 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği yürürlükten kalkmıştır.

Yürürlük

MADDE 22- (1) Bu Yönetmelik yayımlandığı tarihte yürürlüğe girer.

(2) Bu Yönetmeliğin 8 inci maddesinin birinci fıkrası ve 10 uncu maddesi yönetmeliğin yayımlandığı tarihten itibaren 12 ay sonra yürürlüğe girer.

Yürütme

MADDE 23- (1) Bu Yönetmelik hükümlerini Bilgi Teknolojileri ve İletişim Kurulu Başkanı yürütür.

GENEL GEREKÇE

Ulusal siber güvenliğin sađlanması milli güvenliğin temel unsurlarından biri olup, kritik altyapıların yer aldığı sektörlerde faaliyet gösteren işletmeler tarafından yürütölen faaliyetlerin etkin ve verimli şekilde yönetilmesi bu anlamda önem arz etmektedir. 6757 sayılı Kanun ile 5809 sayılı Elektronik Haberleşme Kanununda (Kanun) yapılan değışiklik sonrasında Kurumumuza siber saldırıların engellenmesi ve caydırıcılığın sađlanması görevleri verilmiştir. Buna ilave olarak ulusal siber güvenliğin sađlanması amacıyla Kurumumuz ilgili yerlerden bilgi, belge, veri ve kayıtları alabilme ve değıerlendirmesini yapabilme; arşivlerden, elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanabilme, bunlarla irtibat kurabilme ve bu kapsamda diğere gerekli önlemleri alabilme veya aldırabilme yetkisine sahiptir. Ayrıca, Kanun ile kamu kurum ve kuruluşları da dahil olmak üzere ilgili taraflara yaptırım uygulama yetkisi de Kurumumuza verilmiştir.

Kurumumuz bünyesinde kurulmuş olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) yurt içi ve yurt dışı kaynaklı siber tehditleri tespit etme ve önleme faaliyetleri yürütmektedir. USOM; siber tehditleri önlemek amacıyla alarm, uyarı ve duyuru faaliyetleri yürütmek, kritik durumlarda yerinde müdahale ekipleriyle olayın kontrolünü ele almak ve siber olaylara müdahalede ulusal koordinasyonu sađlamak amacıyla faaliyetlerini sürdürmektedir. USOM tarafından kurum, kuruluş, işletmelere siber güvenlik bildiriminde bulunulmakta, söz konusu siber güvenlik bildirimleri ile kurum ve kuruluşlardaki kritik ve acil olarak ele alınması gereken zafiyetler ve internete açık servislerinde tespit edilen açıklıklar; alınması gereken tedbirlerle birlikte ilgililerine iletilmekte, zararlı yazılımlarda ve oltalama amacıyla kullanılan zararlı bağlantılar (URL, IP, domain) tespit edilerek kontrolleri yapılmakta ve altyapı seviyesinde erişim engellenmektedir. Bu sayede ölkede genelinde internet kullanıcıları ve sistemlerine yapılabilecek saldırıların önlenmesi sađlanmaktadır.

Diğere taraftan 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanarak yürürlöğe giren Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ ile USOM'un koordinasyon sađladığı Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) kurulması öngörölmüştür. SOME'ler, kurumların ve kritik altyapı sektörlerinin korunmasına yönelik olarak USOM'un koordinasyonunda 7/24 görev yapmaktadır.

Teknolojik gelişmelerle birlikte, kritik altyapılara yönelik tehditler artmakta ve siber güvenlik önlemleri her geçen gün daha fazla önem kazanmaktadır. Uluslararası kuruluşlar ve devletler sürekli değışen ve gelişen siber tehditlere karşı, siber güvenlik organizasyonlarını günümüz şartlarına uygun hale getirme gayreti içerisinde. Bu doğrultuda hazırlanan, AB Genelinde Yüksek Düzeyde Ortak Siber Güvenliğı Yönelik Tedbirleri içeren NIS2 Direktifi (AB) 2022/2555 sayılı karar ile onaylanarak 16 Ocak 2023 tarihinde yürürlöğe girmiştir.

USOM'u ve SOME'leri kapsayan siber güvenlik organizasyonunun, NIS2 Direktifi de esas alınarak günümüz şartlarına uygun hale getirilmesi, ulusal güvenliğin korunması açısından kritik bir öneme sahiptir. Bu düzenlemenin, etkili bir siber güvenlik altyapısı oluşturarak temel ve önemli kuruluşların siber dayanıklılığını artıracığı ve hızla değışen siber olaylara etkili bir şekilde müdahale edilmesini sađlayacağı değıerlendirilmektedir. Ulusal siber güvenlik faaliyetlerinin daha etkin bir şekilde yürütölebilmesi adına kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması, bu saldırılara karşı caydırıcılığın sađlanması ve yüksek düzeyde siber güvenlik seviyesine ulaşılması amacıyla yürütölecek faaliyetlere ilişkin usul ve esasların belirlenmesi amacıyla Ulusal Siber Güvenliğinin Sađlanmasına ve Siber Caydırıcılığın Artırılmasına Yönelik Yönetmelik Taslağı hazırlanmıştır.