SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ

BİRİNCİ BÖLÜM
Amaç ve Kapsam, Dayanak, Tanımlar

Amaç ve kapsam

MADDE 1 − (1) Bu Tebliğin amacı ve kapsamı, Siber Olaylara Müdahale Ekiplerinin kuruluş, görev ve çalışmalarına ilişkin usul ve esaslarını belirleyerek, hizmetlerin etkin ve verimli bir şekilde yürütülmesini sağlamaktır.

Dayanak

MADDE 2 − (1) Bu Tebliğ, 20/10/2012 tarihli ve 28447 sayılı Resmî Gazete'de yayımlanan 2012/3842 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın 5 inci maddesinin birinci fıkrasının (ç) bendi ile üçüncü fıkrası ve 25/3/2013 tarihli ve 2013/4890 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 üncü maddesi ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 29 uncu maddesinin yedinci fıkrası ile 30 uncu maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 − (1) Bu Tebliğde geçen;

a) Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, veri ve bunların sunumunda yer alan sistemleri,

b) Endüstriyel Kontrol Sistemi: Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan bilgi sistemleridir. Bu sistemler Veri Tabanlı Merkezi Kontrol ve Gözetleme Sistemi (SCADA) ile coğrafi olarak Dağınık Kontrol Sistemleri (DKS) şeklinde gruplanmaktadır.

c) 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,

ç) Kritik sektörler: Kritik altyapıları bünyesinde barındıran sektörleri,

d) Kurul: Siber Güvenlik Kurulunu,

e) Siber olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

f) Siber olaya müdahale: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemlerde tutulan veya işlenen verilerin gizlilik, bütünlük ve erişilebilirliğinde meydana gelme riski bulunan veya meydana getiren siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmaları,

g) SOME: Siber Olaylara Müdahale Ekibini,

ğ) USOM: Ulusal Siber Olaylara Müdahale Merkezini,

ifade eder.

İKİNCİ BÖLÜM
SOME'lerin Kuruluşu, Yapısı, Görev ve Yükümlülükleri, USOM'la İlişkileri

Kurumsal SOME'lerin kuruluşu

MADDE 4− (1) Kurumsal SOME'ler Bakanlıkların bünyesinde, hizmet gereklerine göre, Bakanlık birimlerini, bağlı, ilgili ve ilişkili kurumlarını kapsayacak şekilde kurulur. Ancak Bakanlık koordinesinde Bakanlık birimleri, bağlı, ilgili ve ilişkili kurum ve kuruluşları altyapılarının önem ve büyüklüğüne göre kendi bünyelerinde bir kurumsal SOME kurabilirler.

(2) Diğer tüm kamu kurum ve kuruluşları kendi bünyelerinde kurumsal SOME kurabilirler.

(3) Bakanlıkların merkez birimleri, bağlı, ilgili ve ilişkili kurum ve kuruluşlarının yanı sıra 10/12/2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli I, II, III ve IV sayılı cetvellerde yer alan kurum ve kuruluşlar da kendi bünyelerinde kurumsal SOME kurabilirler.

(4) Kurumsal SOME'lerin kuruluşunun eşgüdümü Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yürütülür.

(5) Sektörel SOME'lerin bulunduğu sektörlerdeki özel kurumlar ve diğer kuruluşlar kendi bünyelerinde kurumsal SOME kurabilirler.

Kurumsal SOME'lerin görev ve sorumlulukları

MADDE 5 − (1) Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler.

(2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar.

(3) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütürler. Durumdan gecikmeksizin USOM'u haberdar ederler.

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle sö konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar. Bunun mümkün olmaması halinde varsa birlikte çalıştığı sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunabilirler.

(5) Kurumsal SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

(6) Kurumsal SOME'ler kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığı sektörel SOME'ye bildirirler.

(7) Kurumsal SOME'ler USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alırlar.

(8) Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler.

Sektörel SOME'lerin kuruluşu

MADDE 6 − (1) Sektörel SOME'ler düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulur.

(2) İhtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan diğer sektörlerde ilgili olduğu Bakanlık bünyesinde sektörel SOME kurulabilir.

(3) Kritik sektörlerde, sektörel SOME kurulması zorunludur. Kritik sektörlerin listesi Kurul tarafından belirlenir, ilgililere duyurulur ve güncellenir.

(4) Düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin eşgüdümü Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülür.

Sektörel SOME'lerin görev ve sorumlulukları

MADDE 7 − (1) Sektörel SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler.

(2) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olayları gecikmeksizin USOM'a bildirirler.

(3) Sektörel SOME'ler siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütürler.

(4) Sektörel SOME'ler birlikte çalıştıkları SOME'lerin yapılanması konusunda düzenleyici faaliyetleri yürütürler.

(5) Sektörel SOME'ler ilgili oldukları sektörde, bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri yürütürler.

(6) Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştıkları SOME'lere ve USOM'a bildirirler.

(7) SOME'ler 7/24 erişilebilir olan iletişim bilgilerini Sektörel SOME'lere ve USOM'a bildirirler.

(8) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlarlar. Sektörel SOME'ler, imkânlarının yetersiz olması durumunda USOM'dan destek alırlar.

(9) Sektörel SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

(10) Sektörel SOME'ler gerekmesi durumunda birlikte çalıştıkları SOME'ler arasındaki işbirliğini koordine ederler.

Kurumsal ve sektörel SOME'lerin yapısı

MADDE 8 − (1) SOME'lerin Bakanlık ve diğer kurumlar içinde nasıl yapılandırılacağı, hangi birim içinde çalışacağı, Bakanlığın veya kurumun diğer birimleri ile ilişkileri, bilişim ve endüstriyel kontrol sistemlerinin yapısı da dikkate alınarak ilgili Bakanlık veya kurum tarafından belirlenir ve kurum içerisinde uygun yöntem ile duyurulur.

(2) SOME'ler kurumların bilişim ve endüstriyel kontrol sistemlerinin büyüklük ve kritikliği dikkate alınarak meydana gelebilecek siber olaya müdahale edebilecek yeterlilikte personel ve teçhizatla desteklenirler.

(3) SOME'ler; bilgi güvenliği, bilişim ağları, yazılım ve sistem uzmanlığı gibi alanlarda bilgili ve tecrübeli personel öncelikli olmak üzere ilgili bakanlık ve kurumların belirleyeceği personelden teşkil edilir.

(4) Mevcut ve olası siber olayların niteliği ve yoğunluğuna göre USOM tarafından bu yapıların geliştirilmesi önerilebilir.

(5) SOME'ler iletişim kanallarını 7/24 açık tutarlar.

(6) SOME'ler siber olaylara imkânları dâhilinde 7/24 esasına göre müdahale ederler.

(7) SOME'ler, ilgili kurumların teşkilat yapılarına ve hizmet gereklerine göre farklı birim personelinden oluşturulabilir.

SOME'lerin USOM'la ilişkisi

MADDE 9 − (1) SOME'lerin USOM ile ilişkilerini varsa birlikte çalıştıkları sektörel SOME'ler üzerinden yürütmesi esastır.

(2) Birlikte çalıştıkları bir sektörel SOME olmayan kurumsal SOME'ler, faaliyetlerini doğrudan USOM ile koordineli yürütürler.

(3) Siber olaylar ile ilgili olarak diğer ülkelerin eşdeğer makamları ve uluslararası kuruluşlarla işbirliği USOM tarafından yerine getirilir.

(4) USOM gerekli gördüğü durumlarda kurumsal SOME'ler ve sektörel SOME'ler ile doğrudan çalışma yürütebilir.

(5) Kurumsal/Sektörel SOME'ler siber olayların tespiti, önlenmesi, zararlarının en aza indirilmesi gibi konularda USOM tarafından geliştirilen veya yürütülen projelerin gerçekleştirilmesinde USOM ile işbirliği içerisinde hareket ederler.

Eğitim

MADDE 10 − (1) Kurumsal SOME'ler, USOM ve/veya birlikte çalıştıkları sektörel SOME'lerin planladığı eğitimlere katılım sağlar.

(2) Sektörel SOME'ler, USOM'un planladığı eğitimlere katılım sağlar.

Siber Güvenlik Kurulu

MADDE 11 − (1) Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığındaDışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur.

Yürürlük

MADDE 12 − (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 13 − (1) Bu Tebliğ hükümlerini Ulaştırma, Denizcilik ve Haberleşme Bakanı yürütür.