T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Haberleşme Genel Müdürlüğü

Sektörel SOME Kurulum ve Yönetim Rehberi

Sürüm 1

Kasım 2014

İÇİNDEKİLER

EKLER LİSTESİ

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

YÖNETİCİ ÖZETİ

Ülkeler siber güvenliklerini sağlamak amacıyla idari yapılanmalar gerçekleştirmekte, teknik önlemler almakta ve hukuki altyapılar hazırlamaktadır. Konunun önemi dikkate alınarak ülkemizde de "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar", 20 Ekim 2012 tarihli Resmi Gazete'de Bakanlar Kurulu Kararı olarak yayınlanmıştır. Bu önemli adımla ülkemizin siber güvenliğinin sağlanması konusunda idari, teknik ve hukuki yapıların oluşturulması hız kazanmış olup, bu Karar ile siber güvenliğe ilişkin program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla "Siber Güvenlik Kurulu" oluşturulmuştur. Kamu kurum ve kuruluşlarının, ulusal siber güvenliğin sağlanması amacıyla Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yayımlanan plan, program, usul, esas ve standartlara uyması esas alınmıştır. Bu bağlamda ilgili tüm kurum ve kuruluşların Siber Güvenlik Kurulu kararları çerçevesinde işbirliği ve eşgüdüm içerisinde çalışmalara katılım ve katkı sağlaması, alınan kararları titizlikle uygulaması siber güvenlik çalışmalarının başarı ile sonuçlanması ve ulusal siber güvenliğimizin arttırılması bakımlarından büyük önem arz etmektedir.

Siber Güvenlik Kurulu'nun ilk toplantısında "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiş ve 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak yayımlanmıştır. Söz konusu eylem planı kapsamında temel görevi koordinasyon ve işbirliği olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) 27 Mayıs 2013 tarihinde kurularak, faaliyetlerine başlamıştır. Yine söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür.

USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 4. Eylem Maddesi "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması" başlığını taşımaktadır. Bu madde bağlamında Resmi Gazete'de 11 Kasım 2013 Tarihli ve 28818 Sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" yayımlanmıştır. Tebliğin 6. maddesinde Siber Güvenlik Kurulu tarafından belirlenen kritik sektörlerde, sektörün düzenleyici ve denetleyici kurumu veya sektörün ilgili olduğu bakanlık bünyesinde "Sektörel SOME" kurulmasının zorunlu olduğu belirtilmektedir. Bahse konu Tebliğde SOME'lerin yapısı, görevleri ve USOM'la ilişkileri de açıklanmıştır.

Kalkınma Bakanlığı 2012 Yatırım Programı içerisinde yer alan "Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi" kapsamında kritik altyapıların ve kritik altyapıları barındıran kritik sektörlerin belirlenmesi için ilk çalışmalar yapılmış, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 5 numaralı eylem maddesi kapsamında, Siber Güvenlik Kurulu'nca ilk etapta "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" ülkemizin kritik sektörleri olarak belirlenmiştir.

Bu kritik sektörlerin düzenleyicisi konumunda bulunan ve Sektörel SOME kurma yükümlülüğüne sahip olan kurum ve bakanlıkların faydalanması, Tebliğ'de yer alan hükümlerin açıklanması ve kurumlara yardımcı olması amacıyla "Sektörel SOME Kurulum ve Yönetim Rehberi" dokümanı hazırlanmıştır.

Siber güvenliğe ilişkin oluşturulan organizasyon yapısında hiyerarşik bir yapı oluşturulmuştur. Bu yapıda USOM, Sektörel SOME ve Kurumsal SOMEler bulunmaktadır. Sektörel SOME ve Kurumsal SOME ler USOM koordinasyonunda çalışacaktır. Kritik alt yapı olarak belirlenen sektörlerde yer alan Kurumsal SOME ler bağlı bulunduğu Sektörel SOME lerle çalışacaklardır. Organizasyonun tamamı göz önünde bulundurulduğunda, Kurumsal SOME'lerin kendi kurumları kapsamında olaylara müdahale, Sektörel SOME'lerin sektörleri kapsamında idari düzenleme ve

koordinasyon, USOM'un ise ulusal kapsamda teknik destek ve koordinasyon görevi bulunmaktadır. Buna ilaveten Sektörel SOME'lerin başlıca görevi, gerçekleşen siber olayları yakından izlemek, alınması gereken önlemleri belirlemek ve sektöre yönelik düzenlemeler yapmaktır.

Sektörel SOME Kurulum ve Yönetim Rehberi, Sektörel SOME'lerin kurum organizasyonu içerisindeki yerini, Kurumsal SOME'ler ve USOM'la ilişkilerini, kapasite planlamasını, personelin niteliklerini (eğitim düzeyi ve tecrübe), alması gereken eğitimleri, bu personelin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları, kurum içi/kurum dışı paydaşlarla iletişim esaslarını, Sektörel SOME'lerin kurulması için gereken kuruluş süreleri ve esasları ile bu süreçte kullanılacak olan ekler, şekiller ve tablolar listesini içermektedir.

1 Giriş

1.1 Amaç

Bu rehber, 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında Sektörel SOME kurma yükümlülüğü olan kurumların faydalanması için hazırlanmıştır.

1.2 Kapsam

Bu rehberde özellikleri ve sorumlulukları verilen; Sektörel SOME'ler, kritik sektörleri düzenlemek ve denetlemekten sorumlu kurumlar bünyesinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan kritik sektörlerde ise ilgili olduğu Bakanlık bünyesinde kurulacaktır.

Rehber, Sektörel SOME'lerin kurum organizasyonu içerisindeki yerini, Kurumsal SOME'ler ve USOM'la ilişkisi, kapasite planlamasını, personelin niteliklerini (eğitim düzeyi ve tecrübe), alması gereken eğitimleri, bu personelin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları, kurum içi/kurum dışı paydaşlarla iletişim esaslarını, Sektörel SOME'lerin kurulması için gereken kuruluş süreleri ve esasları ile bu süreçte kullanılacak olan ekler, şekiller ve tablolar listesini içermektedir. Ancak kurumlar büyüklük, görev, teknik yeterlilik, personel ve benzeri hususlardaki farklılıklardan dolayı rehberin içeriğini imkân ve kabiliyetleri ile orantılı olarak uygulayacaklardır.

1.3 Tanımlar ve Kısaltmalar

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nda yapılan tanımlara ilave olarak, bu rehberde geçen;

a. BDDK: Bankacılık Düzenleme ve Denetleme Kurumunu,
b. BTK: Bilgi Teknolojileri ve İletişim Kurumunu,
c. EPDK: Enerji Piyasası Düzenleme Kurumunu,
ç. İz kaydı: Bilişim sistemlerinin işletilmesi esnasında veya siber olaya maruz kalması durumunda ürettiği kayıtlar,
d. 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 sistemlerini barındıran altyapıları,

e. Kurumsal SOME: Temel görevleri, Tebliğ'de yer alan Kurumsal Siber Olaylara Müdahale Ekibini,

f. Sektörel Çalışma Grubu: Sektörel SOME, sektördeki Kurumsal SOME ve USOM temsilcilerinin yer alacağı, kurumlar arası iletişim ile sektör içi mevzuat ve teknik çalışmalarda bulunacak çalışma grubunu,

g. Sektörel SOME: Temel görevleri, Tebliğ'de yer alan Sektörel Siber Olaylara Müdahale Ekibini,

ğ. Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

h. SPK: Sermaye Piyasası Kurumunu,

ı. Tebliğ: 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği,

i. UDHB: Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,

j. Ulusal Siber Ortam: Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı,

k. USOM: Temel görevleri, Usul ve Esaslar'da yer alan Ulusal Siber Olaylara Müdahale Merkezini,

l. Usul ve Esaslar: Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esasları,

ifade eder.

1.4 Dayanak

Bu doküman, 5809 sayılı Elektronik Haberleşme Kanununun 5 inci Maddesi 1 inci fıkrasının (h) bendi ile "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", "11.06.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ve "Tebliğ" e dayanılarak hazırlanmıştır.

1.5 İlgili Mevzuat ve Dokümanlar

USOM, Sektörel SOME ve Kurumsal SOME ile ilgili mevzuat ve dokümanlar Tablo 1'de yer almaktadır.

Organizasyon	İlgili Mevzuat	İlgili Doküman
USOM	22 Mayıs 2013 Tarihli 2013/278 Sayılı Usul ve Esaslar (BTK Kurul Kararı)[1]	–
Sektörel SOME	Tebliğ[2]	Sektörel SOME Kurulum ve Yönetim Rehberi
Kurumsal SOME		Kurumsal SOME Kurulum ve Yönetim Rehberi

Tablo 1 - İlgili Mevzuat ve Dokümanlar

1.6 Güncelleme

Bu doküman gelişen teknoloji, değişen şartlar, ihtiyaçlar ve sektörel gelişmeler göz önünde bulundurularak güncellenecektir. Güncelleme talepleri USOM tarafından alınacak, değerlendirme ve güncellemeler UDHB koordinasyonunda BTK/USOM aracılığı ile yapılacak ve ilgili taraflara bildirilecektir.

1.7 Gizlilik

Sektörel SOME birimlerinde görev yapan personel, bu rehber kapsamındaki görevleri dolayısıyla elde etmiş oldukları bilgiler bakımından sır saklama yükümlülüğüne tabidir. Bu yükümlülük görev sona erdikten sonra da devam eder. Hizmet alımı sözleşmesine dayalı işlemlerde de bu hususa riayet edilir.

2 Ulusal Siber Olaylara Müdahale Organizasyonu

Ülkemiz kamu kurum ve kuruluşları ile kritik altyapı işleten özel sektör kuruluşlarını içine alan siber olaylara müdahale organizasyonu Şekil 1'de gösterilmiştir. Siber olaylara müdahale organizasyonundaki üç temel bileşen USOM, Sektörel SOME'ler ve Kurumsal SOME'lerdir.

[1] BTK Kurul Kararına USOM web sayfasından erişilebilir. (www.usom.gov.tr)

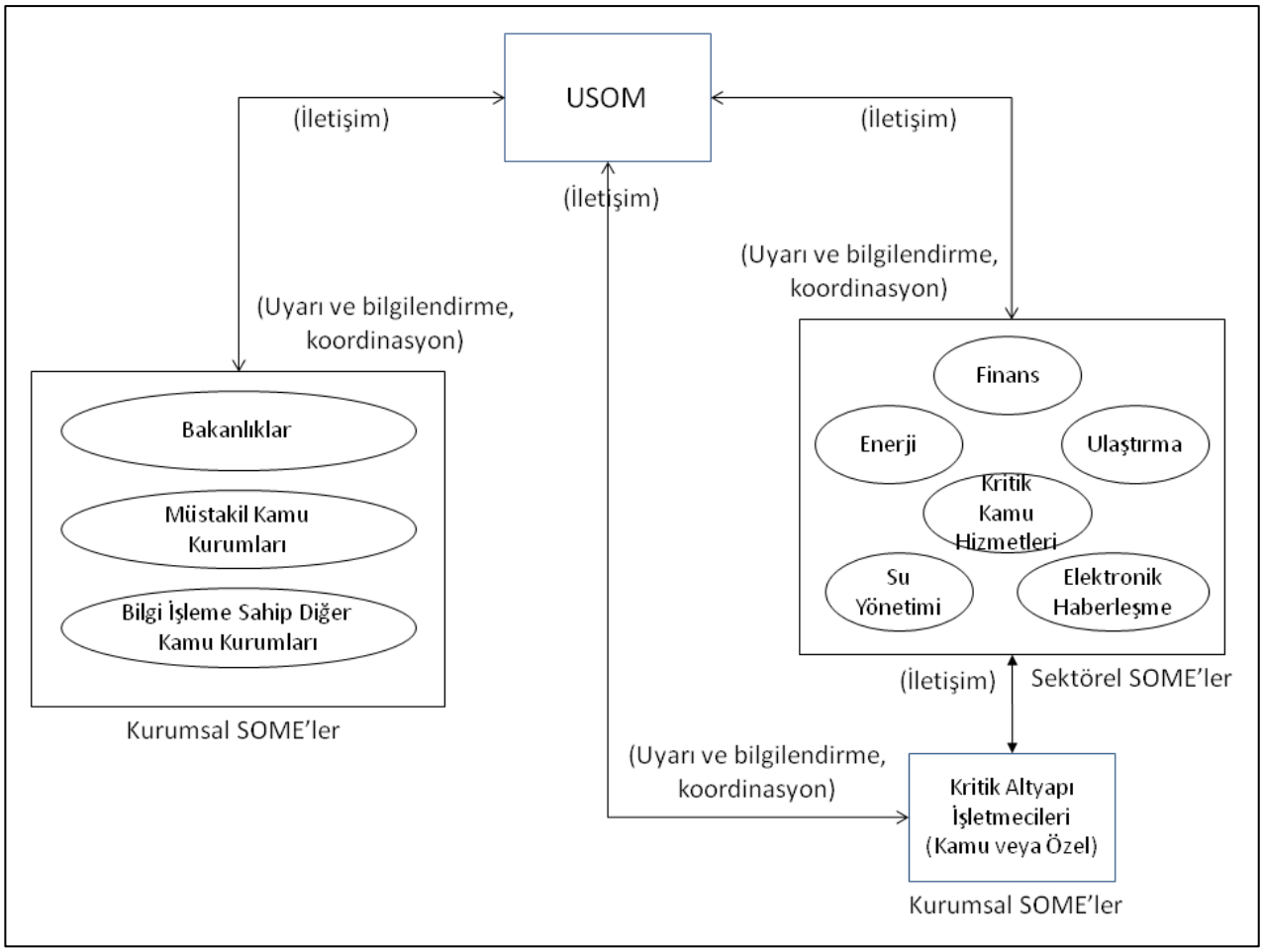
[2] Tebliğe Resmi Gazete web sayfasından erişilebilir. (http://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm)

USOM, Sektörel SOME ve Kurumsal SOME'nin hizmet alanları Tablo 2'de verilmiştir.

Organizasyon	Kurulduğu Kurum / Kuruluş	Hizmet Alanı
USOM	BTK / Telekomünikasyon İletişim Başkanlığı (TİB)	Ulusal siber ortam
Sektörel SOME	• Kritik sektörü düzenleyici ve denetleyici kurumlar • Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

Tablo 2 - Hizmet Alanları

USOM, Sektörel SOME ve Kurumsal SOME'ler Tablo 2'deki hizmet alanlarında siber güvenlik yönetimini gerçekleştirirler.



Şekil 1: Ulusal Siber Olaylara Müdahale Organizasyonu

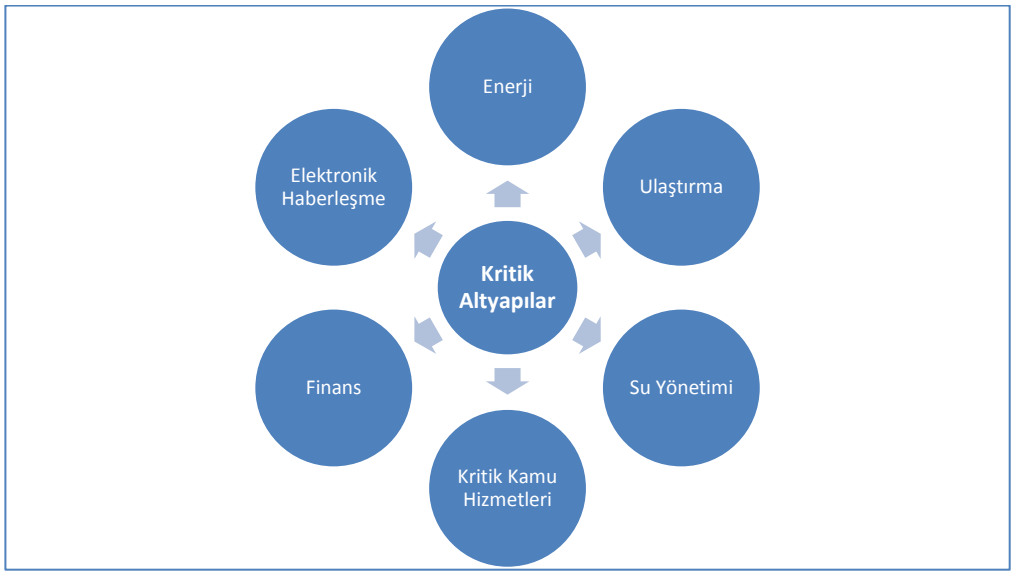
Şekil 1'de yer alan;

a) Uyarı ve bilgilendirme: Siber olay öncesinde USOM tarafından hazırlanan bülten, duyuru gibi bilgileri,
b) Koordinasyon: Siber olay esnasında USOM, Kurumsal SOME ve bağlı olduğu Sektörel SOME arasında yapılan koordinasyonu,
c) İletişim: Siber olay öncesi, esnası ve sonrasında USOM ve/veya Kurumsal SOME'nin bağlı olduğu Sektörel SOME tarafından talep edilen rapor, form ve bilgilendirmeyi,

ifade etmektedir. Sektörel SOME kendisine bağlı Kurumsal SOME'lerin USOM ile olan iletişim faaliyetlerini düzenleyecek olup, sektör dahilinde kullanılacak iletişim yöntemi ile ilgili usul ve esasları belirleyecektir. USOM'un belirlediği yöntemi de kullanabilecektir.

2.1 Kritik Altyapılar ve Sektörel SOME'ler

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın 5 numaralı eylem maddesi kapsamında, Siber Güvenlik Kurulu'nca ülkemizin kritik altyapı sektörleri "Ulaştırma, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi, Kritik Kamu Hizmetleri" olarak belirlenmiştir.



Şekil 2: Türkiye'nin kritik altyapı sektörleri

Her kritik altyapı sektörü için, Sektörel SOME'nin kurulacağı kurum Tablo 3'te gösterilmiştir. Düzenleyici ve denetleyici kurumların yetki alanı dışında kalan, ulaştırma, su yönetimi ve kritik kamu hizmetleri (Ek-3) için ilgili bakanlık bünyesinde Sektörel SOME'ler kurulur. Kritik sektörler Siber Güvenlik Kurulu tarafından ihtiyaç halinde güncellenir.

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum
Enerji	EPDK
Elektronik Haberleşme	BTK
Finans	SPK, BDDK
Su yönetimi	Orman ve Su İşleri Bakanlığı
Kritik Kamu Hizmetleri	Ek 3'te belirtilmiştir
Ulaştırma	Ek 4'te belirtilmiştir

Tablo 3: Sektörel SOME'leri Kurulacağı Kurumlar

Sektörel SOME, sorumluluk alanındaki kritik sektördeki siber güvenliğin koordinasyonundan, düzenlenmesinden ve yetki alanı varsa denetlenmesinden sorumludur.

Sektörel SOME'ler görev ve sorumluluklarını yerine getirirken, USOM ve sektöründeki Kurumsal SOME'ler ile koordinasyon ve iletişim içerisinde bulunurlar.

Sektörel SOME, sektör içi siber güvenlik politikalarını, ihtiyaç duyulması halinde, USOM ile işbirliği içerisinde belirlemekte ve bu politikaların uygulandığını kontrol etmektedir. Siber Güvenlik Kurulunun aldığı stratejik kararın sektörel seviyedeki karşılığı Sektörel SOME'ler tarafından yerine getirilir. Sektörel SOME'ler, sorumluluk alanındaki sektörde faaliyet gösteren kurum ve kuruluşları bilgilendirme ve başlıca siber güvenlik çözümleri hakkında bilgi sağlama hizmeti vermektedir. Sorumluluk alanını oluşturan kritik sektörü kapsayacak şekilde siber saldırı uyarısı ve güvenlik açığı duyurusu yayınlar.

3 Sektörel SOME Kurulum Aşamaları

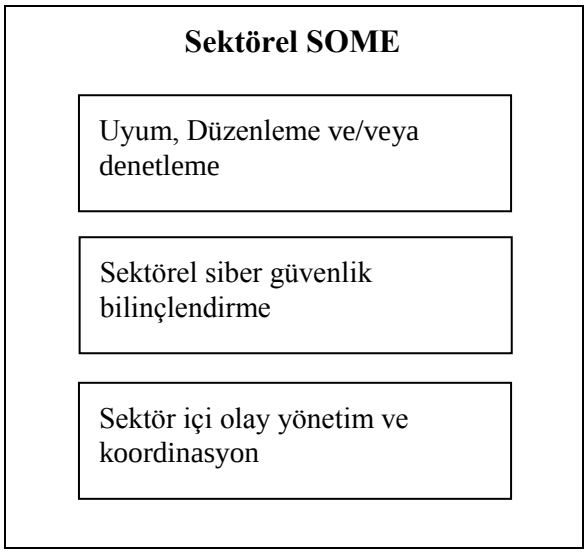
3.1 Kurum İçerisindeki Yeri ve Kapasite Planlaması

Sektörel SOME'lerin, kurum içinde düzenleme ve/veya denetleme fonksiyonlarını doğrudan icra eden birim altında oluşturulması esastır. Kurumun ifa etmekte olduğu denetleme ve/veya düzenleme fonksiyonları birden fazla birim altında ise; Sektörel SOME bu birimlerde çalışanların temsilcilerinin oluşturduğu bir yapılanma şeklinde kurulabilir.

Sektörel SOME amirinin en az lisans derecesine ve sektör tecrübesine sahip olması ve bilgi güvenliği/siber güvenlik konusunda tecrübeli personel arasından seçilmiş olması tavsiye edilir.

Kurulacak olan Sektörel SOME, sektörde faaliyet gösteren kuruluşların Kurumsal SOME'leri yanında, kurum bünyesindeki Kurumsal SOME ile de aynı şekilde koordinasyon içerisinde olacaktır.

Sektörel SOME'lerin yerine getireceği fonksiyonlar Şekil 3'de gösterilmiştir. Kurumun imkânları çerçevesinde Şekil 3'deki fonksiyonların tamamını yerine getirmesi için hâlihazırda görev yapan personelin görevlendirilebileceği; nihai hedef olarak ayrı bir uzmanlık gerektiren her bir fonksiyon için en az bir sözleşmeli/kadrolu personel istihdamı yapılması tavsiye edilmektedir.



Şekil 3: Sektörel SOME Fonksiyonları

Sektörel SOME'nin görev ve sorumlulukları göz önünde bulundurularak istihdam edilecek personelin sadece bu fonksiyonları ifa etmek için istihdam edilmesi tavsiye edilmektedir. Sektörel SOME'lerin görev ve sorumluluklarını gerçekleştirmesi için, burada çalışacak personelin en az ön lisans programından mezun olması, sektör tecrübesine sahip olması veya bilgi güvenliği/siber güvenlik uzmanlığına sahip olması önerilmektedir. Kurumlar personel ihtiyacını firmalardan hizmet alımı yolu ile de temin edebilirler. Firmadan temin edilen personelin kurumun gereksinimleri çerçevesinde güvenlik soruşturmasının (adli sicil kaydı, şahıs güvenlik belgesi vb.) yaptırılması ve firma personeline gizlilik sözleşmesi imzalatılması tavsiye edilir ve bu şekilde çalıştırılacak personel için hazırlanacak olan sözleşmelerde kurumda personel istihdamını düzenleyen kanun maddeleri gözetilir.

3.2 Kurum İçi Paydaşlarla İletişim Esasları

Sektörel SOME, sektöründeki siber güvenliği yönetirken varsa hukuk ve basın / halkla ilişkiler müşavirlikleri ile birlikte çalışır.

Sektörel SOME ilgili sektöründeki siber güvenlik ile ilgili çalışmaları düzenler ve yetkisi varsa denetler. Sektör ile ilgili siber güvenlik organizasyonları düzenler, gerekli mevzuatları hazırlar, uyarı ve bilgilendirme yapar ve sektörü ilgilendiren siber olaylarda koordinasyon görevini üstlenir. İhtiyaç durumunda yetkili makamlarla iletişime geçer.

Sektörel SOME'ler, yıllık olarak hazırlayacakları "Sektörel Siber Güvenlik Faaliyet Raporu" nu bağlı bulundukları kurum veya kuruluşun üst yönetimine sunar.

Sektörel Siber Güvenlik Faaliyet Raporu'nun aşağıdaki ana başlıklardan oluşması tavsiye edilmektedir:

1. İnsan Kaynağı
    a. Sektörel SOME'nin insan kaynağı durumu
    b. Sektör içi farkındalık çalışmaları
    c. Alınan eğitimler, gidilen konferanslar, verilen eğitimler
2. Sektörde yer alan kurumların denetlenmesi ile ilgili faaliyetler
3. Müdahale ve koordine edilen siber olaylar
    a. Olayların dökümü
    b. Edinilen tecrübeler ve uygulanan düzeltici faaliyetler
4. Sektör içi ve dışı paydaşlarla yapılan çalışmalar
5. Diğer faaliyetler

3.3 Kurum Dışı Paydaşlarla İletişim Esasları

Bu bölümde, Sektörel SOME'lerin kurum dışı paydaşlar (USOM ve Sektör İçerisindeki Kurumsal SOME'ler) ile olan iletişim esasları yer almaktadır.

Sektörel SOME'ler, 7x24 ulaşılabilir durumda olan personelin iletişim bilgilerini USOM'a EK-1'de yer alan Sektörel SOME İletişim Formu ile iletirler.

Kritik Sektörlerdeki Kurumsal SOME'ler, 7x24 ulaşılabilir durumda olan personelin iletişim bilgilerini bağlı olduğu Sektörel SOME'ye ve USOM'a EK-1'de yer alan Sektörel SOME İletişim Formu ile iletirler. Sektörel SOME İletişim Formunda yer alan bilgiler Sektörel SOME tarafından belirlenir.

Formun güvenli iletişim sistemi üzerinden USOM'a gönderilmesi gerekmektedir. Sektörel SOME'ler gerekli gördükleri durumlarda USOM'un yanı sıra diğer Sektörel SOME'lere de bilgi verebilir.

Sektörel SOME'ler bünyesinde faaliyet gösteren Kurumsal SOME'lerden gelen "Siber Olay Müdahale Raporu" nu USOM'a ileteceklerdir.

Yurt dışı bağlantılı siber olaylar için USOM'la iletişime geçilmesi, siber olayların USOM üzerinden çözüme kavuşturulması tavsiye edilir.

3.4 Sektörel SOME'lerin Kuruluş Süreleri ve Esasları

Ulusal Siber Güvenlik Strateji ve 2013-2014 Eylem Planında, Sektörel SOME'lerin Aralık 2013'e kadar kurulması öngörülmüştür. Sektörel SOME'lerin, bu Rehber göz önünde bulundurularak kurulması esastır. Bu kapsamda, Sektörel SOME, Ek 1'de yer alan SOME İletişim Bilgileri Formunu doldurarak güvenli iletişim sistemi üzerinden USOM'a iletir. USOM, kurulan Sektörel SOME'lerin listesini UDHB'ye iletir.

3.5 Eğitimler

Sektörel SOME'lerde istihdam edilecek personelin, kurum ve/veya kuruluşların hizmet içi eğitimlerine ilave olarak Tablo 4'deki eğitimleri de alması tavsiye edilir. İhtiyaç duyulan asgari eğitimlerden bazıları USOM tarafından verilebilecektir[3].

Tablo 4'te yer alan eğitimlerin içerikleri Ek 2'de verilmiştir. Ek 2'deki eğitim içeriklerinde, her bir eğitim için gerekli olan ön şartlar belirtilmiştir.

Temel Yetenek	Eğitimler	Eğitimden Beklenen Faydalar
Kayıt Yönetimi	- Saldırı Tespit ve Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi	Sektörel SOME personelinin sistemler ve tehditler ile ilgili farkındalık kazanabilmesi
Siber Olay Yönetimi	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilişim Hukuku Eğitimi	Bir siber olay gerçekleşmesi durumunda gerekli olacak olay yönetimi ve koordinasyonu yeteneklerinin kazanılmasıdır.
Bilgi Güvenliği Yönetimi	- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi	Bilgi güvenliği/siber güvenlik sürecinin kavratılması ve Bilgi Güvenliği Yönetim Sistemi ile ilgili farkındalık oluşması

Tablo 4: Sektörel SOME'lerin Alması Tavsiye Edilen Eğitimler

[3] Bu konudaki gelişmeler USOM'un internet sayfasından (www.usom.gov.tr) takip edilebilir.

4 Sektörel SOME'lerin Görev ve Sorumlulukları

Sektörel SOME'lerin siber olay öncesi, siber olay esnası ve siber olay sonrasındaki temel görev ve sorumluluklarına bu bölümde yer verilmiştir.

4.1 Siber Olay Öncesi

Sektörel SOME ilk aşamada sektördeki firmaların, kamu kurum/kuruluş temsilcilerinin ve USOM'un yer alacağı sektör içi mevzuat ve teknik çalışmalarda bulunmak üzere bir sektörel çalışma grubu oluşturacaktır.

Sektörel SOME'ler düzenli olarak aşağıdaki çalışmaları gerçekleştirirler:

4.1.1 Düzenleme Çalışmaları

a. Sektörel SOME, Sektörel çalışma grubuyla beraber sektör içi siber güvenlik mevzuatının kapsamını belirler.
   i. Sektörde bulunan kritik bilgi sistemlerinin belirlenmesi için kullanılacak kriter belirlenir. Aşağıda görülen Tablo 5, kritik sektörlerin her birinde hangi parametrelerin göz önünde bulundurularak kritik sistemlerin belirlenebileceğine ilişkin fikir vermektedir:

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum	Kritik sistemlerin belirlenmesi için kullanılabilecek parametreler
Enerji	EPDK	Sistemlerin ürettiği, depoladığı, ilettiği, dağıttığı veya satışına aracılık ettiği enerji miktarı
Elektronik Haberleşme	BTK	Sistemlerin depoladığı veya taşıdığı veri miktarı, yapılmasına aracılık ettiği konuşma sürelerinin toplam uzunluğu
Finans	SPK, BDDK	Sistemlerin sakladığı mevduat hacmi veya transferine aracılık ettiği mevduat miktarı
Su yönetimi	Orman ve Su İşleri Bakanlığı	Sistemlerin ürettiği, ilettiği, arıttığı veya dağıttığı su miktarı
Kritik Kamu Hizmetleri	Ek 3'te belirtilmiştir	Sistemlerin yapılmasına eşlik ettiği işlem sayısı, iç kullanıcı veya dış kullanıcı sayıları kullanılabilir.
Ulaştırma	Ek 4'te belirtilmiştir	Sistemlerin taşıdığı yük ve/veya yolcu sayısı

Tablo 5: Kritik sistemlerin belirlenmesi için kullanılabilecek parametreler

ii. Yukarıdaki parametreler kullanılarak sektörde bulunan sistemlerden hangilerinin kritik olduğunu belirlemek için kullanılacak eşik değerleri tanımlanır.

iii. Belirlenen eşik değeri göz önünde bulundurularak sektörde yer alan kritik sistemler ve bunları işleten kurum ve kuruluşlar belirlenir. Bu kurumların Kurumsal SOME'lerini kurma yükümlülüğüne mevzuatta yer verilir, çalışmaları öncelikli olarak takip edilir.

iv. Sektörde yer alan kritik sistemlerin belirlenmesine dönük çalışma en geç iki yılda bir tekrar edilmelidir.

b. Sektörel SOME, Sektörel çalışma grubuyla beraber sektör içi siber güvenlik mevzuatını (yönetmelik, tebliğ) hazırlar veya gözden geçirir.

c. Sektörel SOME, Sektörel çalışma grubuyla beraber sektör içi asgari siber güvenlik kriterlerini belirler.

ç. Sektörel SOME, Sektörel çalışma grubuyla beraber bilgi güvenliği ve siber güvenliğe ilişkin çerçeve sözleşme hükümleri[4] üretir ve yayınlar. (Sözleşme hükümlerinin ilave edilmesi firmalardan alınacak hizmetlerin çerçevesini belirleme açısından büyük önem arz etmektedir.)

d. Sektörel SOME Sektörel çalışma grubuyla beraber, Kurumsal SOME'lerden yapmasını talep ettiği risk analizlerinin metodunu, kapsamını, hazırlama periyodunu ve rapor formatını belirler.

e. Sektörel SOME, Sektörel çalışma grubuyla beraber sektörel siber olay müdahale prosedürü oluşturur ve tatbikatlarda test ederler.

f. Sektördeki kurumsal SOME'lerin Ulusal Siber Güvenlik Tatbikatı başta olmak üzere test ve tatbikatlara katılmalarını teşvik ederler.

g. NATO Siber Savunma Mükemmeliyet Merkezi tarafından düzenlenen eğitim programları ve tatbikatlara katılımda bulunmayı teşvik ederler.

ğ. Sektörel SOME, USOM ile birlikte kendi sektörüne özgü siber güvenlik tatbikatı veya çalıştay düzenleyebilir ya da düzenlenen tatbikatlara ve çalıştaylara katılım sağlarlar.

h. USOM tarafından yayınlanan duyuru ve bildirilerin sektöre aktarılmasını sağlarlar.

ı. Siber Güvenlik Kurulu tarafından alınan ve kritik sektörleri ilgilendiren bir kararın sektörde faaliyet gösteren Kurumsal SOME'lere duyurulmasını ve koordinasyonunu sağlarlar.

[4] Çerçeve sözleşme hükümleri EK 5'de açıklanmaktadır.

4.1.2 İletişim

a. Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini EK-1'e göre belirleyerek birlikte çalıştıkları Kurumsal SOME'lere ve USOM'a bildirirler, aynı zamanda birlikte çalıştıkları Kurumsal SOME'ler ve USOM'a ait iletişim bilgilerini alırlar.

4.1.3 Bilgilendirme

a. Sorumluluk alanındaki sektörde faaliyet gösteren kurum ve kuruluşlara faydalı siber güvenlik pratikleri[5] hakkında bilgi sağlama hizmeti verir.
b. Sektördeki kurumlara siber güvenlikle ilgili ve özellikle kendi sektörüne ilişkin bilgiler içeren bülten gönderir.
c. Sorumluluk alanını oluşturan kritik sektörü kapsayacak şekilde genel siber saldırı uyarısı ve güvenlik açığı duyurusu yayınlar.
ç. USOM'dan aldığı sektöre özel siber güvenlik önlemlerini Kurumsal SOME'lere aktarır.
d. Sektördeki kurumlara siber güvenlik eğitim ve konferanslarını önerir.
e. Kurumsal SOME'lere verilecek eğitimler ile ilgili ihtiyaç tespit çalışmalarını ve eğitimlerin verilmesini koordine eder.
f. Sektörde yer alan kurumların sistemleri göz önünde bulundurularak tedarikçi kurumlar tarafından yayınlanan açıklıklar ve bu açıklıklarla ilgili olarak alınması gereken önlemler konusunda koordinasyonu sağlar.

4.1.4 Teknolojik Önlemler

a. Sektöre özel siber tehditleri tespit etmek için Sektörel Çalışma Grubu ile koordinasyon içinde sektöre özgü bilgi sistemlerini kapsayan bal küpü sistemlerinin Kurumsal SOME'lere kurulmasını tavsiye edebilir.
b. Kurumsal SOME'lerin kendi bünyelerinde gerçekleştirecekleri sızma testleri için kapsam, rapor formatı ve minimum ihtiyaçların belirlenmesi hususunda Kurumsal SOME ve USOM ile koordinasyonu sağlar.
c. Sektöre özgü bilgi sistemlerinde (SCADA vb.) ve geniş alanlara yayılmış kurumsal bilişim sistemlerinde geniş alan ağı iletişiminin güvenliğinin sağlanması için internet

[5] Faydalı siber güvenlik pratikleri: ABD, Avrupa vb. yerlerde aynı sektörde alınan güvenlik önlemlerinin ve yapılan çalışmaların izlenmesi en çok kullanılan standartların gözden geçirilmesi, uluslar arası konferansların takip edilmesi ve tüm bu kaynaklardan alınan bilgilerin Türkiye'ye uyarlanmasını kapsar.

servis sağlayıcıları, uydu operatörleri vb. iletişim hizmeti sağlayan taraflarla kurumsal SOME'ler arasında çalışmaların yapılmasını koordine eder.

ç. Sektöre özgü bilgi sistemlerinin (SCADA, vb.) üreticileri/geliştiricileri ile kurumsal SOME'leri bir araya getirerek sistemlerde yapılabilecek iyileştirmelerin ve alınabilecek önlemlerin belirlenmesi hususunda çalışmaların yapılmasını koordine eder.

d. Dünya'da benzer sektörlerde gerçekleşen olayları izler ve kurumları bilgilendirir.

e. Kurumsal SOME rehberinde yer alan iz kayıt mekanizmalarının, Kurumsal SOME'ler tarafından belirlenen asgari niteliklerde kurulup kurulmadığının denetler.

4.2 Siber Olay Esnasında

Sektörde yer alan bir kurumda veya sektörde bir siber olayın yaşanması durumunda Sektörel SOME'ler aşağıdaki çalışmaları gerçekleştirirler:

a. Siber olay esnasında, Kurumsal SOME'de gözlemci bulundurabilir, imkanları ölçüsünde gerekli desteği sağlarlar.

b. Kendisine bağlı olan Kurumsal SOME'lere ve USOM'a siber olayla ilgili bilgilendirme mesajı gönderir.

c. Siber olaya müdahale aşamasında suç işlendiği izlenimi veren bir durumla karşılaşıldığında durumu gecikmeksizin Kurumsal SOME'lerin yetkili makamlara (savcılık veya kolluk kuvvetlerine) bildirmesini ve siber olay raporunun USOM'a iletilmesini sağlarlar.

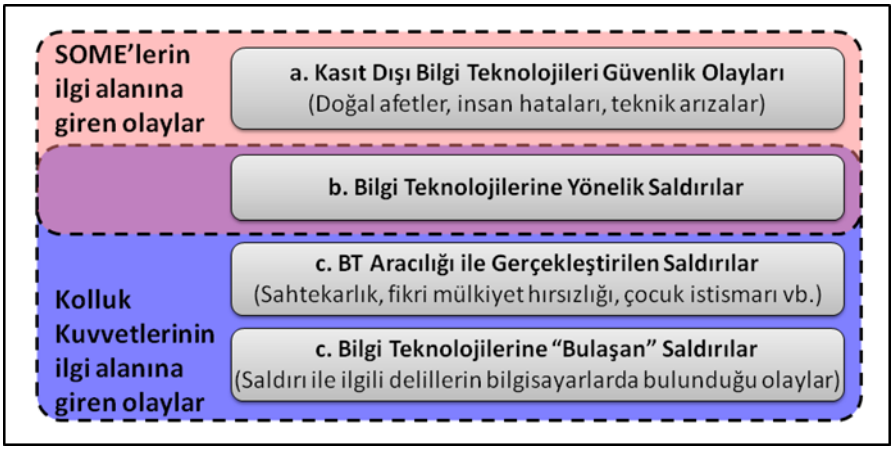
   Gerçekleşen siber olaylar kolluk kuvvetleri ile işbirliği gerekliliği açısından değerlendirildiğinde üç bölüme ayrılmıştır.

   i. Olayların bir bölümü sadece Kurumsal SOME'lerle ilgili olup, kolluk kuvvetlerine haber verilmesi gerekli değildir. Bu olaylara örnek olarak teknik arızalar, doğal afetlerle bilgi sistemlerinin durması ve kullanıcı hataları ile ortaya çıkan istenmeyen durumlar sayılabilir.

   ii. Kurumsal bilgi sistemlerine içeriden veya dışarıdan yapılan saldırıların Kurumsal SOME'ler ve kolluk kuvvetlerinin işbirliği ile çözümlenmesi gerekmektedir.

   iii. Kurumsal bilgi sistemleri kullanılarak işlenen sahtekârlık, fikri mülkiyet hırsızlığı vb. suçlarla, delillerin bilgisayar ortamında bulunduğu işgal, hırsızlık, fiziksel

saldırı vb. eylemlerde görev ağırlıklı olarak kolluk kuvvetlerine düşmekte, kurumsal SOME'lerden delillerin yetkili makamlara aktarılması beklenmektedir.



Şekil 4: Kurumsal SOME'lerin ve Kolluk Kuvvetlerinin İlgi Alanına Giren Olaylar.

4.3 Siber Olay Sonrası

Sektörde yer alan bir kurumda bir siber olay gerçekleştikten ve olaya müdahale edildikten sonra Sektörel SOME'ler aşağıdaki görevleri icra ederler:

a. Kurumsal SOME Rehberi'nin Ek -2'sinde yer alan Siber Olay Bildirim Formu'nun Kurumsal SOME tarafından doldurulmasını, USOM'a iletilmesini sağlar ve kayıt altına alır.
b. Kurumsal SOME'nin yaşadığı siber olay tecrübesinden hareketle yapacağı düzenlemelere esas teşkil edebilecek bilgileri (türü, miktarı ve yaklaşık maliyeti) ister ve kayıt altına alır.
c. Siber olaydan elde edilen, olayın önlenmesine yönelik bilgi ve tecrübeleri, rekabet şartları ve ticari sırları gözeterek, sektördeki diğer Kurumsal SOME'ler ile paylaşır.
ç. Gerekli durumlarda Kurumsal SOME ile koordinasyon içinde medya ile iletişime geçip son durum hakkında bilgilendirme yapar.

Ek 1: Sektörel SOME İletişim Bilgileri Formu

SEKTÖREL SOME İLETİŞİM BİLGİLERİ FORMU					
Kurum Adı					Tarih:
SOME Takımı 7/24 İletişim Bilgileri		Telefon	Cep telefonu	Faks	Kurumsal e-posta
SOME Personelinin	**Adı Soyadı**	**Ünvanı**	**Telefonu**	**Cep telefonu**	**Kurumsal e-posta adresi**

Ek 2: Eğitim İçerikleri

Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi

Ön Şartlar

- Temel işletim ve bilişim sistemleri bilgisi
- TCP/ IP Temel Ağ ve Güvenlik bilgisi
- Kayıt Yönetimi ve Saldırı Tespit temelleri bilgisi

Ana Konular

- Merkezi Kayıt Yönetimi sistemleri
- Olay ilişkilendirme sistemleri (SIM)
- SIM çözümlerine örnekler
- Envanter analizi ile yüksek riske sahip varlıkların belirlenmesi
- Açık Kaynak Kodlu Merkezi Güvenlik İzleme Yazılımı (OSSIM)
    - OSSIM Mimarisi ve entegre araçlar
    - OSSIM Kurulumu
    - OSSIM Konfigürasyonu
    - OSSIM Web Konsolu
    - Güvenlik politikalarının ve raporlarının düzenlenmesi
    - OSSIM ajanı ile bilgi toplama
    - SYSLOG ile bilgi toplama
- Güvenlik Olaylarının Korelasyonu (Saldırı ilişkilendirme)
- Güvenlik istihbaratı için olay analitik iş akışlarının optimize edilmesi
- Olay analizi ve müdahale
- Sistem bakımı ve güncelleme

Siber Olaylara Müdahale Ekibi Kurulum ve Yönetimi Eğitimi

Ön Şartlar

Hem idari süreçler, hem bilişim sistemleri altyapısı konularında orta derecede tecrübe sahibi olmak.

Ana Konular

- Giriş (Tarihçe, örnek bilgisayar olayları, örnek SOME'ler ve organizasyonlar)
- SOME temel konuları (SOME nedir, SOME çerçevesi, SOME servis çerçevesi)
- Siber olay müdahale süreci (olay müdahale servis tanımı ve servis işlevleri)
- SOME operasyonel elemanları (yazılım, donanım, politika ve prosedürler)
- SOME proje planı

Bilişim Hukuku Eğitimi[6]

[6] Eğitim içeriği Ankara Barosu İnternet Sitesinden alınmıştır.

Ön Şartlar

- Belirli bir ön şart yoktur.

Ana Konular

- Bilgisayar teknolojisi
- Sayısal veri teknolojisi
- İşletim sistemi ve yazılımlar
- İnternet teknolojisi
- İstemciler için ağ güvenliği
- Kablosuz internet erişimi ve güvenliği
- Bilişim kültürü
- İnternet arama motorları
- İnteraktif bankacılık-ceza
- Bilişim suçları-kanun maddeleri
- Elektronik imza
- Bilişim suçları-örnek olaylar
- Hakaret-sövme suçları (internet-SMS vb.)
- Bilirkişi raporları
- Alan adları hukuku
- Delil tespiti-hukuk
- Delil tespiti-ceza
- İnternet servis sağlayıcılar
- Spam-yığın e-posta-SMS
- İnternet sitelerinin filtrelenmesi
- E-tüketici
- Av.tr- e-baro
- Sanal kumar
- E-devlet uygulamaları
- Uluslararası mevzuat
- İnteraktif bankacılık-hukuk
- Yüksek mahkeme kararları

- UYAP
- Kişisel verilerin korunması
- Fikri haklar-ilgili hükümler
- Telekomünikasyon hukuku
- Çocuk pornografisi

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi

Ön Şartlar

- Belirli bir ön şart yoktur. Kalite sistemleri ile tanışıklık avantaj olmaktadır.

Ana Konular

- Bilgi güvenliği yönetim sistemi nedir? Neden gereklidir?
- ISO 27001'de "Planla-Uygula-Kontrol Et-Önlem al" döngüsü
- Bilişim sistemi risk analizi ve tedavisi
- ISO 27001 temel kontrol alanları
    - Güvenlik politikası
    - Bilgi güvenliği organizasyonu
    - Varlık yönetimi
    - İnsan kaynakları güvenliği
    - Fiziksel ve çevresel güvenlik
    - İletişim ve işletim yönetimi
    - Erişim kontrolü
    - Bilişim sistemi edinim, geliştirme ve bakımı
    - Bilgi güvenliği olay yönetimi
    - İş sürekliliği yönetimi
    - Uyum
- ISO 27001'e uygunluk denetimi
    - Denetim planlama
    - Denetim kontrol listeleri
    - Uygunsuzluklar ve raporlama
- Çeşitli uygulamalar

Ek 3: Kritik Kamu Hizmetleri Sektöründe Sektörel SOME'lerin Kurulacağı Kurumlar

Kritik Kamu hizmetleri; vatandaşın gündelik hayatında sıklıkla etkileşimde bulunduğu nüfus, tapu, vergi, ticaret, sosyal güvenlik, sağlık (acil servis, tıbbı hizmetler, kan ve organ bankacılığı ve halk sağlığı), gıda, güvenlik (polis, jandarma, sahil güvenlik), yollar ve köprüler, barajlar, maaş ve adli işlemlerin yapıldığı ve kayıtlarının bulunduğu kritik sistemlerden sunulan servislerdir. Bu doğrultuda düzenleyici ve denetleyici kurumlar kuruluncaya kadar aşağıdaki Bakanlıklarda Sektörel SOME'ler kurulacaktır.

1. İçişleri Bakanlığı
2. Adalet Bakanlığı
3. Maliye Bakanlığı
4. Çevre ve Şehircilik Bakanlığı
5. Çalışma ve Sosyal Güvenlik Bakanlığı
6. Gıda, Tarım ve Hayvancılık Bakanlığı
7. Sağlık Bakanlığı,

Ek 4: Ulaştırma Sektöründe Sektörel SOME'lerinin Kurulacağı Kurumlar

Ulaştırma sektörü için Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ilgili Bakanlık olarak belirlenmiştir. Bu kapsamda aşağıdaki birimlerde Sektörel SOME'ler kurulması öngörülmüştür.

1. Karayolu Düzenleme Genel Müdürlüğü
2. Demiryolu Düzenleme Genel Müdürlüğü
3. Deniz ve İç sular Düzenleme Genel Müdürlüğü
4. Sivil Havacılık Genel Müdürlüğü
5. Tehlikeli Mal ve Kombine Taşımacılık Düzenleme Genel Müdürlüğü

Ek 5: Çerçeve Sözleşme Hükümleri

Bilgi sistemlerinin güvenliği kapsamında tedarikçi firmalarla tam işbirliği ve yapılacak işbirliğinin şartlarının sözleşme ile güvence altına alınması önem arz etmektedir.

Kurumların yazılım ve donanım sistemlerini, ağ bileşenlerini ve iletişim hizmetlerini sağlayan firmalarla yaptıkları sözleşmelerde

a. Bakım,
b. Sistemin uzaktan izlenmesi,
c. Olaylara müdahale
ç. Yazılım güvenliği ve güvenli yapılandırma

konularında firmalardan beklentilerini güvence altına alan hükümlerin yer almasının son derece faydalı olacağı değerlendirilmektedir.

Yukarıdaki başlıkların her biri tedarikçi firmalarla müzakere edilmeli, kurum beklentilerini firmanın tam olarak anlaması sağlanmalı ve nihayet beklentiler sözleşmeye aktarılmalıdır.

Yukarıdaki başlıklardan "d. Yazılım güvenliği ve güvenli yapılandırma" kapsamında kurumların firmalarla müzakere etmesi gereken alt başlıklar şu şekilde açıklanabilir (a., b. ve c. Başlıkları için de benzer hükümlerin geliştirilmesi faydalı olacaktır):

1. Sunucu sistemlerinde çalışan uygulama yazılımlarının ve bu sunucuların işletim sistemlerinin güvenliğinin sağlanması kapsamında,
    a. Geliştirici tarafından, yapılan uygulama yazılımı güvenliği testleri ile ilgili bilgi verilecektir.
    b. Kurum tarafından veya farklı kullanıcılar tarafından belirlenen uygulama yazılımı açıklıklarının giderilmesi ile ilgili yöntem belirlenecektir.
    c. Uygulama yazılımının ve çalıştığı sunucuda kullanılan işletim sisteminin güvenli yapılandırılması gerçekleştirilecektir.
    ç. Uygulama yazılımının ve çalıştığı sunucuda kullanılan işletim sisteminin yama yönetiminin nasıl yapılacağı kararlaştırılacaktır.
    d. Uygulama yazılımının ve çalıştığı sunucuda kullanılan işletim sisteminin kötücül yazılımlardan korunması için alınabilecek önlemler kararlaştırılacaktır.

e. Uygulama yazılımının kayıt üretme kabiliyeti değerlendirilecek, yeterli bulunmaması halinde kurumun gereksinimleri göz önünde bulundurularak uygulama yazılımının güncellenmesi sağlanacaktır.
f. Uygulama yazılımına ağ üstünden erişimle ilgili olarak sınır güvenliği sistemlerinde alınması gereken önlemler belirlenecektir.

2. Ağ bileşenlerini tedarik eden firmalarla bu bileşenlerin güvenliğinin sağlanması kapsamında:
   a. Ağ bileşenlerinde kullanılan işletim sisteminin güvenli yapılandırılması sağlanacaktır.
   b. Ağ bileşenlerinde kullanılan işletim sisteminin yama yönetiminin nasıl yapılacağı kararlaştırılacaktır.
   c. Ağ bileşenlerinde bulunan kayıt üretme kabiliyeti değerlendirilecek, yeterli bulunmaması halinde kurumun gereksinimleri göz önünde bulundurularak işletim sisteminin güncellenmesi sağlanacaktır.
   ç. Ağ bileşenlerine ağ üstünden erişimle ilgili olarak alınması gereken önlemler belirlenecektir.
3. SCADA sistemlerinde ve geniş alanlara yayılmış kurumsal bilişim sistemlerinde geniş alan ağı iletişiminin güvenliğinin sağlanması için servis sağlayıcıları ve iletişim servisini sağlayan taraflarla yapılacak işbirliği kapsamında:
   a. Devrelere bağlanan cihazların kimlik kontrolü ile ilgili uygulamalar ve mevcut önlemler değerlendirilecektir.
   b. Devrelerde taşınan verinin bütünlüğünün ve gizliliğinin sağlanması ile ilgili uygulamalar ve mevcut önlemler değerlendirilecektir.
   c. Devrelerin sürekliliği ve süreklilik, gecikme, hata oranı ve benzeri performans parametreleri değerlendirilecektir.
   ç. Yapılan değerlendirmeler göz önünde bulundurularak devrelerin kurumun güvenlik gereksinimini karşılayıp karşılamadığı, karşılamıyorsa servis sağlayıcının sunduğu alternatif devrelerden hangisinin tercih edilmesi gerektiği veya hangi ilave önlemlerin alınması gerektiği belirlenir.