T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Haberleşme Genel Müdürlüğü

Kurumsal SOME Kurulum ve Yönetim Rehberi

Sürüm 1

Temmuz 2014

İÇİNDEKİLER

EKLER LİSTESİ

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

YÖNETİCİ ÖZETİ

Bilgi ve iletişim teknolojileri yaşantımızın ayrılmaz bir parçası haline gelmiş, tüm dünyada olduğu gibi ülkemizde de bu teknolojilerin kullanımı coğrafi, sosyal ve ekonomik açıdan yaygınlaşmıştır. İnternete bağlanmak, internet ortamında sunulan birçok hizmetten yararlanmak, cep telefonu ve diğer birçok akıllı cihazı kullanmak, ülkemizin her köşesinde, her yaştan ve ekonomik düzeydeki vatandaşımız için mümkün hale gelmiştir. Birçok vatandaşımız bireysel ve ekonomik faaliyetlerini internet ortamında yürütmektedir. Bu gelişmeler bilgi toplumu olma yolunda önemli kilometre taşları olarak değerlendirilmektedir. Bununla birlikte bilgi ve iletişim teknolojilerinin kullanımının çeşitli siber tehditleri de beraberinde getirdiği ve bunun toplumda güvenlik kaygılarına yol açtığı da bir gerçektir.

Bilgi ve iletişim teknolojilerinin yaygın kullanımı ile siber ortam tehditlerinin niteliğinde ve niceliğinde muazzam gelişmeler yaşanmaktadır. Siber tehditler bireyleri, kurum ve kuruluşları hatta devletleri hedef almaktadır. Ülkeler siber güvenliklerini sağlamak amacıyla idari yapılanmalar gerçekleştirmekte, teknik önemler 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 Gazetede Bakanlar Kurulu Kararı olarak yayınlanmıştır. Bu önemli adımla ülkemizin siber güvenliğinin sağlanması konusunda idari, teknik ve hukuki yapıların oluşturulması süreçleri hız kazanmıştır. 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. 29 ana eylem ve 95 alt eylem maddesinden oluşan eylem planında, her eylem kapsamındaki çalışmaları sorumlu ve ilgili kuruluş olarak yürütecek kurum ve kuruluşlar belirlenmiştir. 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. Bu bağlamda kurum ya da kuruluşların bünyesinde

etkin ve verimli bir Kurumsal SOME'nin kurulması, bu Kurumsal SOME'nin USOM ve varsa bağlı olduğu Sektörel SOME ile diğer Kurumsal SOME'lerle koordineli çalışması ve işbirliği halinde olması ulusal siber güvenliğimize katkı sağlayacaktır.

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" kapsamında 11 Kasım 2013 Tarihli ve 28818 Sayılı "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" Resmi Gazete'de yayımlanmış olup, ayrıca Kurumsal SOME kurmak yükümlülüğünde olan kurumların faydalanması için "Kurumsal SOME Kurulum ve Yönetim Rehberi" dokümanı hazırlanmıştır.

Bu rehberde yer alan yapının, müstakil bir bilgi işlem birimi barındıran tüm kamu kurum ve kuruluşları ile kritik altyapı işleten özel sektör kuruluşlarında oluşturulması beklenmektedir. Rehber, Kurumsal SOME'lerin kurum organizasyonu içerisindeki yerini, 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, Kurumsal SOME'lerin kurulması için gereken kuruluş süreleri ve esasları ile bu süreçte kullanılacak olan ekleri, şekilleri ve tabloları içermektedir.

Bu rehber gelişen teknoloji, değişen şartlar ve ihtiyaçlar göz önünde bulundurularak güncellenecektir.

Söz konusu Kurumsal SOME yapısının etkin bir şekilde oluşturulmasında ve işletilmesinde ilgili kurum ve kuruluşun üst düzey yöneticileri tarafından desteklenmesi büyük önem arz etmektedir.

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 Kurumsal SOME kurma yükümlülüğü olan kurumların faydalanması amacıyla hazırlanmıştır.

1.2 Kapsam

Bu rehberde yer alan yapı, müstakil bir bilgi işlem birimi barındıran tüm kamu kurum ve kuruluşları ile kritik altyapı işleten özel sektör kuruluşlarını kapsamaktadır. Müstakil bir bilgi işlem birimi barındırmayan kurum ve kuruluşlar bu kapsamın dışındadır. Bilgi işlem hizmetlerinin bir kısmını veya tamamını sözleşmeler çerçevesinde firmalardan alan kurum ve kuruluşlar için de bu dokümanda yazılan hususlar geçerlidir.
Rehber, Kurumsal SOME'lerin kurum organizasyonu içerisindeki yerini, 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, Kurumsal SOME'lerin kurulması için gereken kuruluş süreleri ve esasları ile bu süreçte kullanılacak olan ekleri, şekilleri ve tabloları içermektedir. Ancak kurumlar büyüklük, görev, teknik yeterlilik, personel ve benzeri hususlardaki farklılıklardan dolayı rehberin içeriğini imkân ve kabiliyetleri ile orantılı olarak uygulayabileceklerdir.

1.3 Tanımlar ve Kısaltmalar

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

a) İz kaydı: Bilişim sistemlerinin işletilmesi esnasında veya siber olaya maruz kalması durumunda ürettiği kayıtları,
b) Kurumsal SOME: Temel görevleri Tebliğ'de yer alan, kurumunda bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibini,
c) Sektörel SOME: Temel görevleri Tebliğ'de yer alan ve düzenlemekle yükümlü olduğu sektörde bulunan kritik altyapı veya kamu sistemlerini siber olaylardan korumak için çeşitli çalışmalar yapan Sektörel Siber Olaylara Müdahale Ekibini,
d) Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya ihlal teşebbüsünde bulunulmasını,
e) Siber Ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,
f) Tebliğ: 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği,
g) UDHB: Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,

h) USOM: Temel görevleri, "Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esasların "da yer alan Ulusal Siber Olaylara Müdahale Merkezini,
i) Ulusal Siber Ortam: Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı,
j) BTK: Bilgi Teknolojileri ve İletişim Kurumunu,
k) TSE: Türk Standardları Enstitüsünü,
l) ISO: International Organization for Standardization (Uluslararası Standartlar Organizasyonunu)
m) IEC: International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonunu) ifade eder.

1.4 Dayanak

Bu doküman, "5809 sayılı Elektronik Haberleşme Kanununun 5 inci Maddesi 1 inci fıkrasının (h) bendi", "11.06.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı" ,"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 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 Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esasları (BTK Kurul Kararı)[1]	–
Sektörel SOME	Tebliğ[2]	Sektörel SOME Kurulum ve Yönetim Rehberi
Kurumsal SOME		Kurumsal SOME Kurulum ve Yönetim Rehberi (Bu doküman)

Tablo 1 - İlgili Mevzuat ve Dokümanlar

[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)

1.6 Güncelleme

Bu rehber gelişen teknoloji, değişen şartlar ve ihtiyaçlar göz önünde bulundurularak güncellenecektir. Güncelleme talepleri USOM tarafından alınacak, değerlendirme ve güncellemeler UDHB/USOM aracılığı ile yapılacak ve yayınlanacaktır.

1.7 Gizlilik

Kurumsal 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

Siber olaylara müdahale organizasyonundaki üç temel bileşen USOM, Sektörel SOME'ler ve Kurumsal SOME'lerdir.

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

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

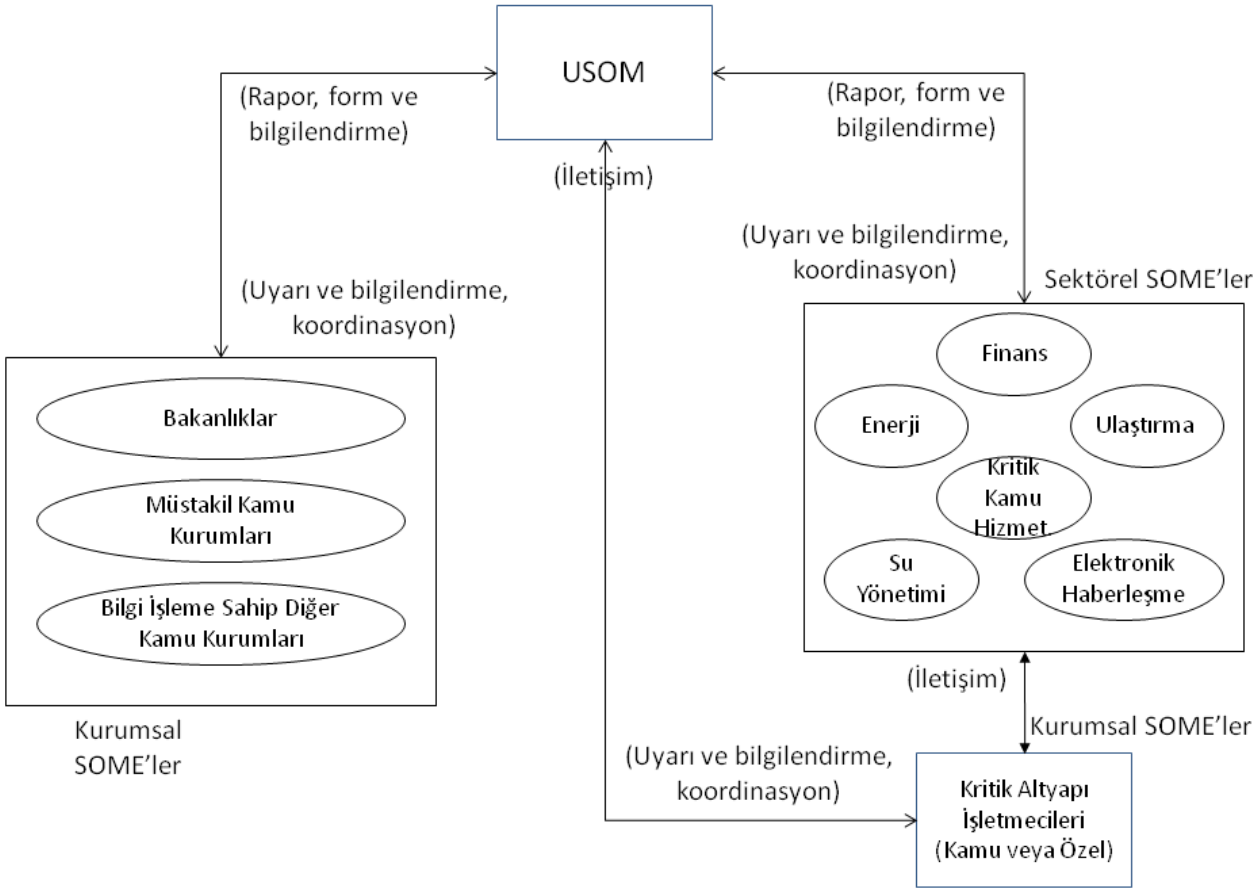
Tablo 2 - Hizmet Alanları

Her bir kritik altyapı sektörü için, Sektörel SOME'nin kurulacağı kurum Tablo 3'te gösterilmiştir. Kritik sektörler Siber Güvenlik Kurulu tarafından ihtiyaç halinde güncellenir. Sektörel SOME'lerin görev ve sorumlulukları "Sektörel SOME Kurulum ve Yönetim Rehberi"nde detaylı olarak yer almaktadır.

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum
Enerji	İlgili düzenleyici ve denetleyici kurum
Elektronik Haberleşme	
Finans	
Su yönetimi	Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık
Kritik Kamu Hizmetleri	
Ulaştırma	

Tablo 3 - Sektörel SOME

Ülkemiz kamu kurumlarını ve kritik altyapıları içine alan siber olaylara müdahale organizasyonu Şekil 1'de gösterilmiştir.



Şekil 1: Ulusal Siber Olaylara Müdahale Organizasyonu

Kurumsal SOME'ler Şekil 1'de görüldüğü gibi kamu kurumları bünyesinde veya kritik altyapı işletmecileri bünyesinde oluşturulur. Kritik altyapı işletmecileri, kamu veya özel sektör kurum/kuruluşu olabilir.

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

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 ve varsa bağlı olduğu Sektörel SOME tarafından yapılan koordinasyonu,
c) Rapor, form ve bilgilendirme: Siber olay öncesi, esnası ve sonrasında USOM ve varsa bağlı olduğu Sektörel SOME tarafından talep edilen ve Kurumsal SOME'ler tarafından iletilen bilgileri,

ifade etmektedir.

3 Kurumsal SOME Kurulum Aşamaları

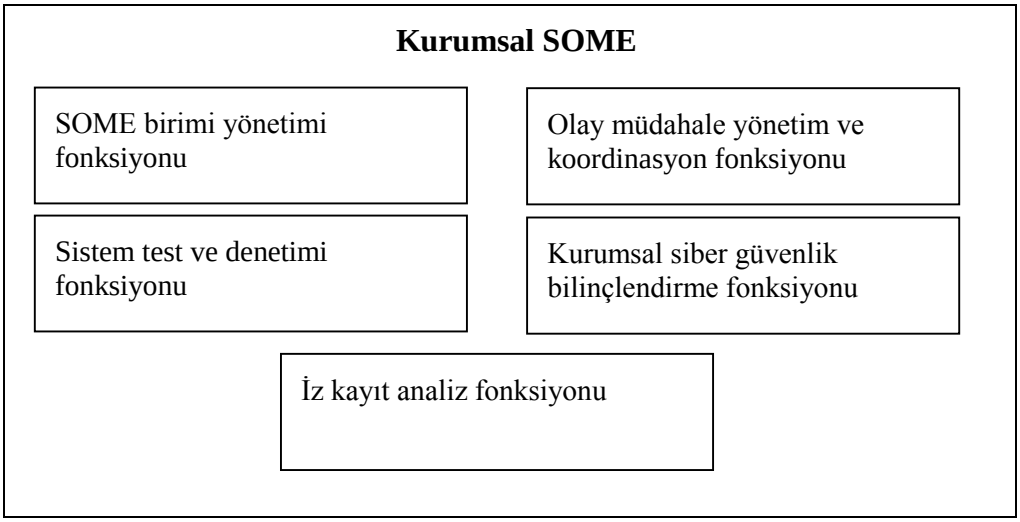
3.1 Kurum İçerisindeki Yeri ve Kapasite Planlaması

Kurumsal SOME, bilgi işlem birimi (şube müdürlükleri, daire başkanlıklar, başkanlık vb.) bünyesinde veya bilgi işlem birimi dışında kurulabilir.

Kurumda hâlihazırda bilgi güvenliği veya siber güvenlikten sorumlu birim (şube müdürlükleri, daire başkanlıkları, başkanlık vb.) kurulmuş ise Kurumsal SOME'nin görevlerini bu birim yerine getirebilir veya Kurumsal SOME bu birim altında kurulabilir.

Kurumsal SOME'nin, temel sorumluluğu siber güvenlik olan bir amir yönetiminde, bir birim olarak kurulması tavsiye edilir. Kurumsal SOME amirinin en az lisans derecesine sahip olan ve bilgi güvenliği/siber güvenlik konusunda uzmanlaşmış personel arasından seçilmiş olması tavsiye edilir.

Kurumsal SOME'lerin yerine getireceği fonksiyonlar Şekil 2'de gösterilmiştir. Kurumun imkânları çerçevesinde Şekil 2'deki fonksiyonların tamamını yerine getirmesi için hâlihazırda bilgi işlem bünyesinde görev yapan personelin Kurumsal SOME kurulumunun ilk aşamasında ikiz görevli olarak görevlendirilebileceği; nihai hedef olarak ayrı uzmanlık gerektiren her bir fonksiyon için en az bir sözleşmeli/kadrolu personel istihdamı yapılması tavsiye edilmektedir.



Şekil 2: Kurumsal SOME Fonksiyonları

Rehberin dördüncü bölümünde yer alan, Kurumsal SOME'lerin görev ve sorumluluklarının gerçekleştirilmesi için, burada çalışacak personelin ön lisans veya lisans programlarından mezun olması ve en az iki yıl bilgi işlem tecrübesine sahip olması veya bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip olması önerilmektedir.

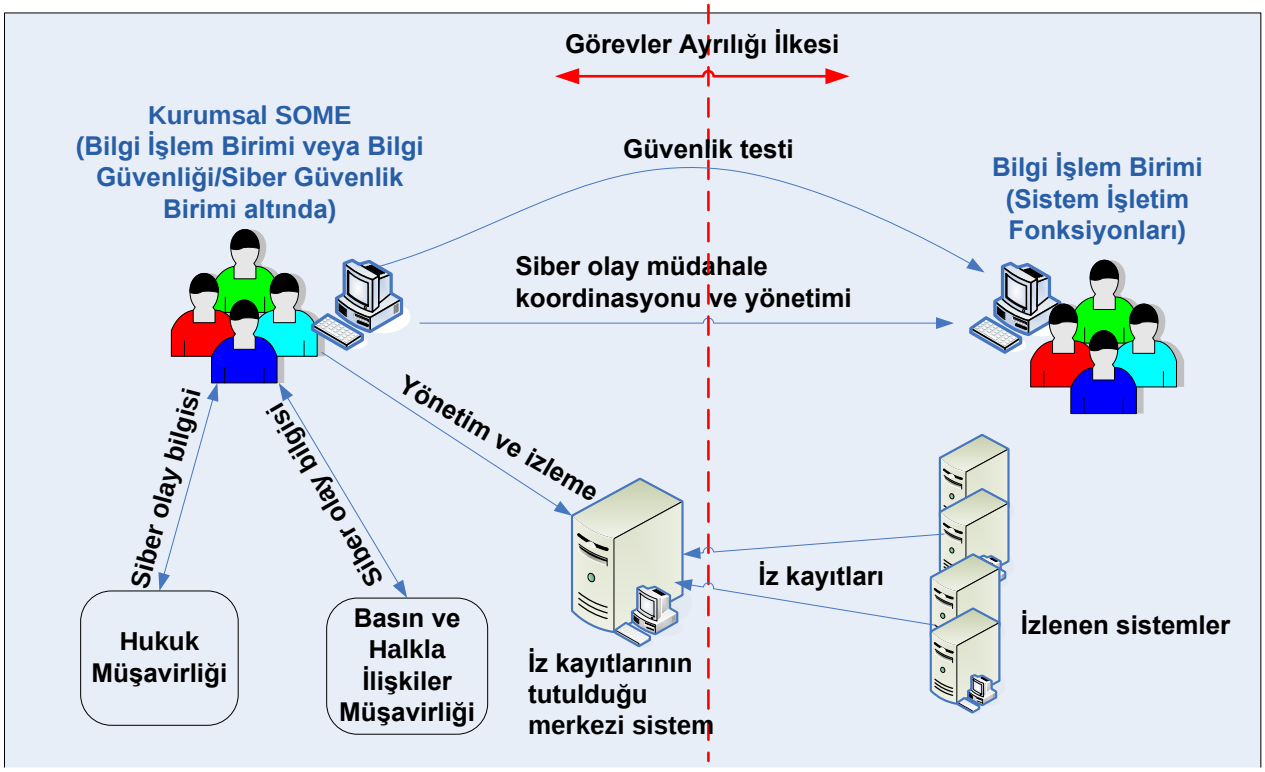
Kurumlar personel ihtiyacını firmalardan hizmet alımı yolu ile de temin edebilirler. Firmadan temin edilen personel için kurumun gereksinimleri çerçevesinde güvenlik soruşturması (adli sicil kaydı, şahıs güvenlik belgesi v.b.) yaptırılır, firma personeline gizlilik sözleşmesi imzalatılır ve bu şekilde çalıştırılacak personel için hazırlanacak olan sözleşmelerde kurumda personel istihdamını düzenleyen kanun maddeleri gözetilir.

3.2 Kurum İçi Paydaşlarla İletişim Esasları

Kurumsal SOME'nin kurum içi paydaşları Şekil 3'de gösterilmiştir. Kurumsal SOME siber olay öncesi, esnası ve sonrasında, siber güvenliği yönetmek amacıyla kurumdaki bilgi işlem birimi ve varsa hukuk ve basın / halkla ilişkiler müşavirlikleri ile birlikte çalışır.

Bilgi işlem ekibi tarafından gerçekleştirilen faaliyetlerin temel hedefi bilişim sistemlerinin yönetimini yapmak ve sürekliliğini sağlamaktır. Kurumsal SOME'nin görevi ise siber güvenliğe ilişkin belirlenen politikalara uygun şekilde faaliyet göstermek, ihtiyaç durumunda yetkili makamlarla iletişime geçmek, kayıt vb. veriyi yetkili makamlara aktarmak ve müdahalenin yapılmasına yardımcı olmaktır. Bu iki görev birbirinden farklı görevler olup bu görevleri yapan ekipler arasında "görevler ayrılığı" ilkesinin uygulanması, mevcut personel kapasitesi de dikkate alınarak farklı personel tarafından yapılması tavsiye edilir. Bu ilkenin tam anlamıyla uygulanabilmesi amacıyla bilgi işlem biriminin sistem işletimi fonksiyonları ile Kurumsal SOME fonksiyonlarının farklı personel tarafından yapılması önem arz etmektedir. Bu alandaki personel kapasitesinin artırılması ve iyileştirilmesi için kurumlar gerekli tedbirleri alırlar.

Şekil 3'de de gösterildiği üzere Kurumsal SOME siber olay öncesi, bilgi işlem varlıkları üzerinde rutin güvenlik testi çalışması yapar veya yaptırır. Kayıt yönetimi sistemi ara yüzünden rutin olarak iz kayıtlarını takip eder. Siber olay esnasında ise, bilgi işlem biriminin yapacağı müdahaleyi yönetir ve bilgi işlem birimindeki ilgili personeli koordine eder.



Şekil 3: Kurumsal SOME'nin Kurum İçindeki Paydaşları ve Temel Fonksiyonları

3.3 Kurum Dışı Paydaşlarla İletişim Esasları

Bu bölümde, Kurumsal SOME'lerin kurum dışı paydaşlar ile olan iletişim esasları yer almaktadır.

Kurumsal SOME - Sektörel SOME ve USOM - Sektörel SOME ilişkilerinin detaylarına Sektörel SOME Kurulum ve Yönetim Rehberi'nde yer verilmiştir.

Kurumsal SOME'ler, 7x24 ulaşılabilir durumda olan personelin iletişim bilgilerini USOM ve varsa bağlı olduğu Sektörel SOME'ye EK-1'de yer alan SOME İletişim Formunu doldurarak, USOM tarafından oluşturulan güvenli iletişim sistemi üzerinden iletirler. Söz konusu formda yer alan bilgilerde değişiklik olması durumunda Kurumsal SOME'ler bu değişikliği gecikmeksizin USOM ve varsa bağlı olduğu Sektörel SOME'ye bildirirler.

İletişimin USOM üzerinden gerçekleştirilmesi esas olmakla birlikte, Kurumsal SOME'ler gerekli gördükleri durumlarda USOM'un yanısıra diğer Kurumsal SOME'lere bilgi verebilir.

USOM tarafından güvenli bir iletişim kanalı oluşturuluncaya kadar, yapılacak iletişimde mevcut iletişim kanalları kullanılabilir. SOME'lerin e-posta yoluyla yapacağı iletişimin şifreli olması önerilir.

Kurumsal SOME'lerin oluşturacağı dokümanlar, bu dokümanları hangi paydaşlarla paylaşabileceği ve oluşturma periyodları Tablo 4'te yer almaktadır. Tablo 4 tavsiye niteliğinde olup Kurumsal SOME'lerden talep edilen dokümanların sayısına, tipine, içeriğine, detay seviyesine ve gönderim periyoduna USOM ve varsa bağlı olduğu Sektörel SOME karar verecektir. Ayrıca kurum üst yönetimi de Kurumsal SOME'den farklı tiplerde dokümanlar (örn. risk analizi raporu) talep edebilir. Yurt dışı

bağlantılı siber olaylar için USOM'la iletişime geçilmesi, siber olayların USOM üzerinden çözüme kavuşturulması tavsiye edilir. Ayrıca yurt dışı temsilciliği olan kurumlarda yaşanacak siber olaylarda da aynı şekilde USOM'la iletişime geçilmesi tavsiye edilir.

Kurumsal SOME'lerin oluşturması beklenen dokümanlardan biri olan Faaliyet Raporu'nun aşağıdaki ana başlıklardan oluşması tavsiye edilmektedir.

1. İnsan Kaynağı
    a. Personel durumu
    b. Kurum içi farkındalık çalışmaları
    c. Alınan eğitimler, gidilen konferanslar
2. Risk Analizi Süreci
    a. Bilişim sistemleri test faaliyetleri
    b. İz kayıtları inceleme faaliyetleri
    c. Müdahale ve koordine edilen siber olaylar
3. Edinilen tecrübeler ve uygulanan düzeltici faaliyetler
4. Kurum içi ve dışı paydaşlarla yapılan çalışmalar
5. Diğer faaliyetler

Doküman Adı	USOM	Varsa Sektörel SOME	Oluşturma Periyodu
Faaliyet Raporu	-	Evet	Yıllık
Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi Raporu	-	-	Yıllık
Siber Olay Müdahale Raporu	Evet	Evet	Siber olaya müdahale sonrası

Tablo 4 - Kurumsal SOME'lerin Oluşturması Tavsiye Edilen Dokümanlar, Paylaşım Durumu ve Oluşturma Periyodu

Ayrıca Kurumsal SOME'lerin siber olay öncesi, siber olay esnası ve siber olay sonrasında kullanması tavsiye edilen formlarla ilgili bilgi Tablo 5'te yer almaktadır.

Form Adı	Siber Olay Öncesi	Siber Olay Esnası	Siber Olay Sonrası
SOME iletişim bilgileri formu (Ek 1)	Evet		
Siber olay bildirim formu (Ek 2)		Evet	
Siber olay değerlendirme formu (Ek 3)			Evet

Tablo 5 - Kurumsal SOME'lerin Kullanması Tavsiye Edilen Formlar

3.4 Eğitimlerin Alınması

Kurumsal SOME'lerde istihdam edilecek personelin alması tavsiye edilen eğitimler Tablo 6'da verilmiştir. Eğitimler, Kurumsal SOME personelinin sistemli bir şekilde kayıt analizi ve yönetimi yapabilmesi, kurumun bilişim sistemlerindeki önemli güvenlik zafiyetlerini tespit edebilmesi ve siber olay müdahale koordinasyonu yapabilmesi için gerekli olan temel yetkinlikleri vermeyi hedeflemektedir. İhtiyaç duyulan asgari eğitimlerden bazıları USOM tarafından da verilebilecektir[3].

Tablo 6'da yer alan eğitimlerin içerikleri Ek 4'te verilmiştir. Ek 4'teki eğitim içeriklerinde, her bir eğitim için gerekli olan ön şartlar belirtilmiştir.

Temel Yetenek	Eğitimler	Eğitimden Beklenen Faydalar
Zafiyet Analizi	- Güvenli Yapılandırma Denetimi Eğitimi - Sızma Testleri Eğitimi - Saldırı Teknikleri Eğitimi	Kurumsal SOME personelinin bir siber olay gerçekleşmeden önce sistemlerindeki önemli zafiyetleri tespit etmesi ve karşı önlem uygulamasını koordine etmesi için gerekli yetenekleri kazanması
Kayıt Yönetimi	- Saldırı Tespit ve Kayıt Yönetimi Eğitimi - Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi	Kurumsal SOME personelinin sistemdeki kayıtları takip edebilmesi, sistemler ve tehditler ile ilgili farkındalık kazanabilmesi
Siber Olay Müdahale	- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi - Bilişim sistemleri Adli Analizi Eğitimi	Bir siber olay gerçekleşmesi durumunda gerekli olacak olay yönetimi ve koordinasyonu yeteneklerinin kazanılması, dijital

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

Temel Yetenek	Eğitimler	Eğitimden Beklenen Faydalar
	- Bilgisayar Adli Analizi - Derinlemesine Windows Eğitimi - Ağ Adli Analizi Eğitimi - Zararlı Yazılım Analiz Yöntemleri Eğitimi - DDoS Saldırıları ve Korunma Yolları Eğitimi - Bilişim Hukuku Eğitimi	delillerin geçerliliğinin bozulmaması için alınacak tedbirlerin öğrenilmesi. Adli analiz esasen kolluk makamının görevi olmakla birlikte, kurumların "sistem izleme" ve "kayıt yönetimi" kapsamında giriş seviyesinde adli analiz bilgisine sahip olması gerekmesi.
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 6 - Kurumsal SOME'lerin Alması Tavsiye Edilen Eğitimler

3.5 Kurumsal SOME'lerin Kuruluş Süreleri

Ulusal Siber Güvenlik Strateji ve 2013-2014 Eylem Planında, Kurumsal SOME'lerin Eylül 2014'e kadar kurulması öngörülmüştür.

3.6 Kurumsal SOME'ler için Kuruluş Esasları

Kurumsal SOME'lerin, Ek 5'de yer alan "Kurumsal SOME'ler için Gereksinim Listesi" göz önünde bulundurularak kurulması esastır. Bu kapsamda, Kurumsal SOME, Ek 1'de yer alan SOME İletişim Bilgileri Formunu doldurarak güvenli iletişim sistemi üzerinden USOM'a ve varsa bağlı olduğu Sektörel SOME'sine iletir. Kurumsal SOME, ihtiyaç duyması halinde karşılıklı mutabakat ile USOM'dan kuruluş şartlarının yeterliliği ile ilgili yerinde inceleme talep edebilir. USOM, kurulan Kurumsal SOME'lerin listesini UDHB'ye iletir.

4 Kurumsal SOME'lerin Görev ve Sorumlulukları

Kurumsal 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

Kurumda bir siber olayın yaşanmadığı veya gerçekleşmediği durumda Kurumsal SOME'ler, kurum içi farkındalık çalışmalarının gerçekleştirilmesi, kurumsal bilişim sistemleri sızma testlerinin yapılması / yaptırılması ve kayıtların düzenli olarak incelenmesi çalışmalarını yaparlar. Yapılacak çalışmaların detaylarına bu bölümde yer verilmiştir.

4.1.1 Kurum içi farkındalık çalışmalarının gerçekleştirilmesi

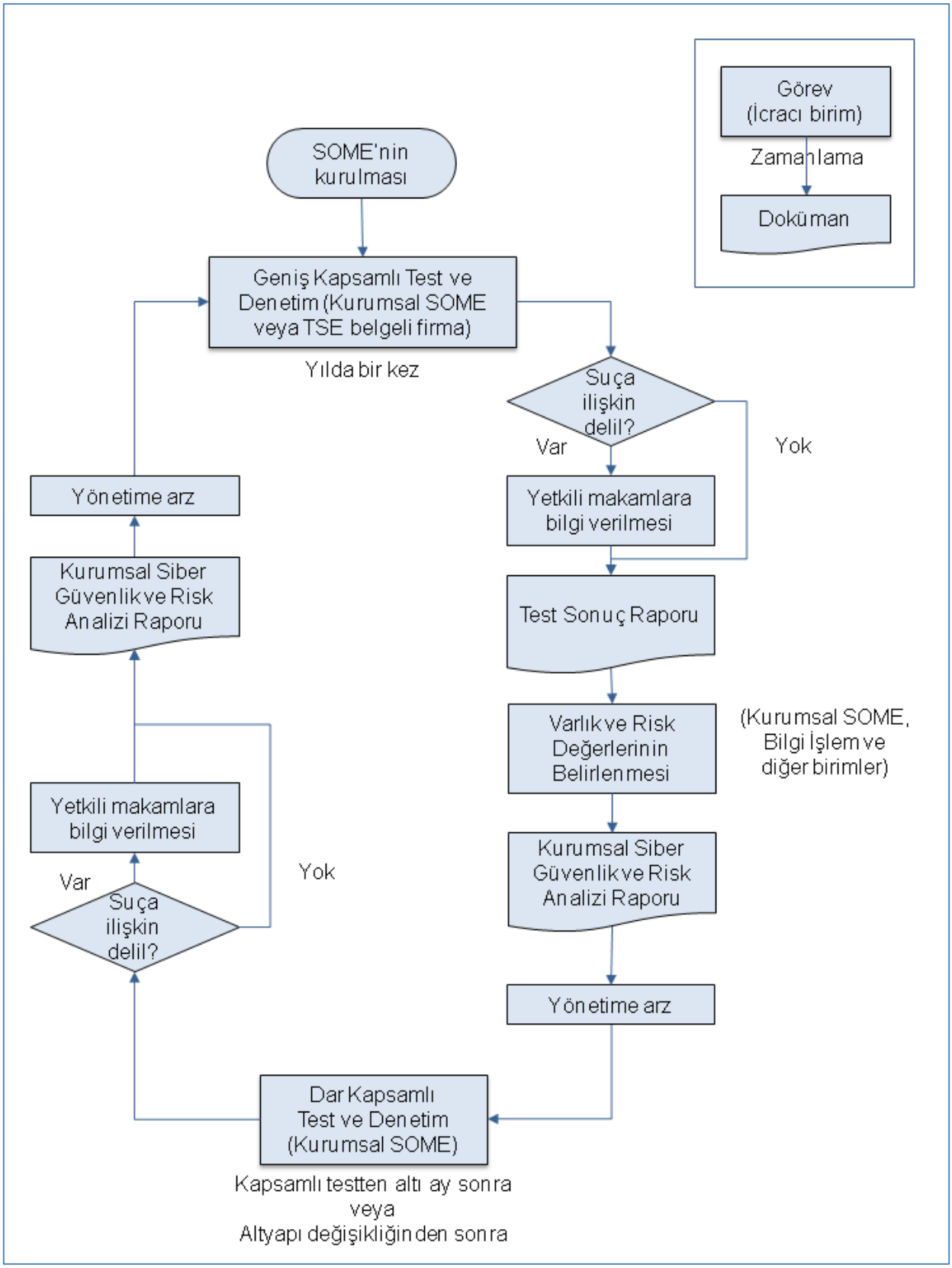
Kurumsal SOME'lerin, farkındalık çalışmaları kapsamında;

a. Kurum personeline periyodik olarak bilinçlendirme sunumu yapılması,
b. Kurumun yemekhane, toplantı odaları gibi ortak kullanılan bölgelerine bilgi güvenliğiyle ilgili posterler asılması,
c. Siber güvenlik ile ilgili periyodik olarak kurum içi bülten hazırlanması,
d. Kurum çalışanlarına periyodik olarak bilgi güvenliğiyle ilgili hatırlatma e-postaları gönderilmesi,
e. Varsa kurumun iç portalında siber güvenlik ile ilgili bir bölüm oluşturulması,
f. Siber güvenlikle ilgili ekran koruyucuların ve arka plan resimlerinin hazırlanması,
g. Kurumun bilgi güvenliği farkındalığını ölçecek anketlerin düzenli olarak yapılması

faaliyetlerini yapması veya yaptırması tavsiye edilir.

4.1.2 Kurumsal bilişim sistemleri güvenlik testlerinin yapılması / yaptırılması süreci

Sürecin a.-g. adımları Şekil 4'te özetlenmiştir:



Şekil 4: Kurumsal Bilişim Sistemleri Güvenlik Testleri Süreci

a. Geniş kapsamlı test ve denetim:
   Kurumsal SOME'ler yılda en az bir kez aşağıdaki kapsamda test ve denetimleri yaparlar veya TSE tarafından belgelendirilmiş firmalara yaptırırlar. Test ve denetim hizmetlerinin sağlaması gereken asgari kriterleri USOM yayınlar.
   i. İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması
   ii. Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması
   iii. Dışa açık web uygulamalarının sızma testleri
   iv. Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri
   v. Veri tabanı yapılandırma testleri
   vi. Kuruma özel geliştirilmiş yazılımlar
   vii. DNS servisi testleri
   viii. E-posta servisi testleri
   ix. Sosyal mühendislik testleri
   x. Sadece kurum içinden erişilen web uygulamaları sızma testleri
   xi. Dağıtık servis dışı bırakma (DDoS) testleri
   xii. Sanallaştırma sistemleri testleri
   xiii. Kablosuz ağ testleri
   xiv. Güvenlik duvarı testleri
   xv. URL ve içerik filtreleme testleri
b. Test sonuç raporlarının içermesi beklenen minimum bilgi aşağıda listelenmiştir:
   i. Zafiyetin önem derecesi (Acil, Kritik, Yüksek, Orta, Düşük)
   ii. Zafiyetin etkisi
   iii. Zafiyetin bulunduğu bileşenler
   iv. Zafiyetin açıklaması ve nasıl tespit edildiği
   v. Alınması gereken önlemler
c. Varlık ve risk değerlerinin belirlenmesi:
   Kurumsal SOME, üstünde zafiyet bulunduğu tespit edilen varlıklar için başta bilgi işlem birimi olmak üzere kurumun ilgili birimleri ile işbirliği içinde varlık değerlerini belirler. Test sonuç raporundan gelen zafiyet değerleri ile varlık değerlerini kullanarak risk değerlerini hesaplar. Böylece, "Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi" raporunu hazırlar ve kurum üst yönetimine sunar.
d. Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi raporunun içermesi beklenen minimum bilgi aşağıda listelenmiştir:
   i. Varlık değeri
   ii. Zafiyetin önem derecesi (Acil, Kritik, Yüksek, Orta, Düşük)
   iii. Zafiyetin etkisi
   iv. Zafiyetin bulunduğu bileşenler
   v. Zafiyetin açıklaması ve nasıl tespit edildiği
   vi. Alınması gereken önlemler
   vii. Risk değeri
e. Dar kapsamlı test ve denetim:
   Kurumsal SOME'nin, a maddesinde tanımlanan testlerden 6 ay sonra, a maddesinin i.'den v.'ye kadar olan adımlarını tekrar gerçekleştirmesi tavsiye edilir. Ayrıca, bilgi

işlem altyapısında değişiklik olması durumunda da 6 aylık süreyi beklemeden aynı test adımları gerçekleştirilir.

f. Yapılan güvenlik testleri sonucunda suç olabilecek iz, delil ve emare (zararlı yazılım, sızma vb.) görülmesi durumunda birim amiri ve kurum hukuk müşavirliği ile görüşülerek gecikmeksizin kanunen soruşturmaya yetkili makamlara (savcılık/kolluk), varsa bağlı olduğu sektörel SOME'ye ve USOM'a bildirirler.
g. Kurumsal SOME, e maddesinde tanımlanan faaliyeti müteakip Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi raporunda gerekli güncellemeleri yapar.
h. Kurum yönetimi ve bilgi işlem birimi ile periyodik toplantılar yaparak, gerçekleşen siber olayları, mevcut riskleri ve düzeltici/önleyici faaliyetlerin durumunu gözden geçirir.
i. Kurumsal SOME'ler, sızma testleri ve denetimler sonucunda bulunan zafiyetlerin ilgili bilgi işlem personeli / firma tarafından kapatılmasını koordine ederler.
j. Testler sonrasında zafiyetler kapatıldıktan sonra doğrulama testlerini yaparlar veya yaptırırlar.
k. Profesyonel saldırganların hedefi durumunda olan kurumların, APT ("Advanced Persistant Threat", Gelişmiş Siber Casusluk Tehditi) analizini de risk işleme yöntemlerinden biri olarak göz önünde bulundurmaları tavsiye edilmektedir. APT analizi, zafiyetlerden faydalanarak kurumun bilişim sistemlerine yerleşen gelişmiş siber casusluk tehditlerinin belirlenmesi için yapılan çalışmalardır.

4.1.3 İz kayıtlarının merkezi olarak yönetilmesi

a. Kurumsal SOME, İçişleri Bakanlığı tarafından hazırlanan "Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri" dokümanına uygun olarak, merkezi bir şekilde tutulmasını ve yönetilmesini sağlar. Görevler ayrılığı prensibi çerçevesinde, merkezi iz kayıt sistemi yönetiminin, iz kayıtlarını üreten bilişim sistemlerinin sorumlularından bağımsız olarak yapılmasını sağlar.
b. Kurumsal SOME, iz kayıtlarının günlük olarak izleme ve incelemesini yapar.
c. Kurumsal SOME, iz kayıtları üzerinde dönemsel (haftalık, aylık vb.) analiz ve ilişkilendirme çalışması yapar; çalışma sonucunda oluşturduğu raporu bilgi işlem birimine ve üst yönetime sunar.
d. İçişleri Bakanlığı tarafından hazırlanan "Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri" dokümanında belirtilen "İz Kaydı Alınması Gereken Sistemler" e ilave olarak diğer sistemlerden de (kullanıcı terminalleri, balküpü sistemi, veri kaçağı önleme sistemi, URL filtreleme vb.) iz kaydı alınması tavsiye edilir.

4.1.4 Diğer Sorumluluklar

a. Kurumsal SOME, siber olay öncesi, esnası ve sonrasındaki görev ve sorumlulukları ile kurumun diğer birimlerle ilişkilerini düzenler, siber olay yönetim talimatlarını (siber olay müdahale, siber olay bildirim süreci vb.) hazırlar.
b. Ulusal Siber Güvenlik Tatbikatı başta olmak üzere tatbikatlara katılırlar.

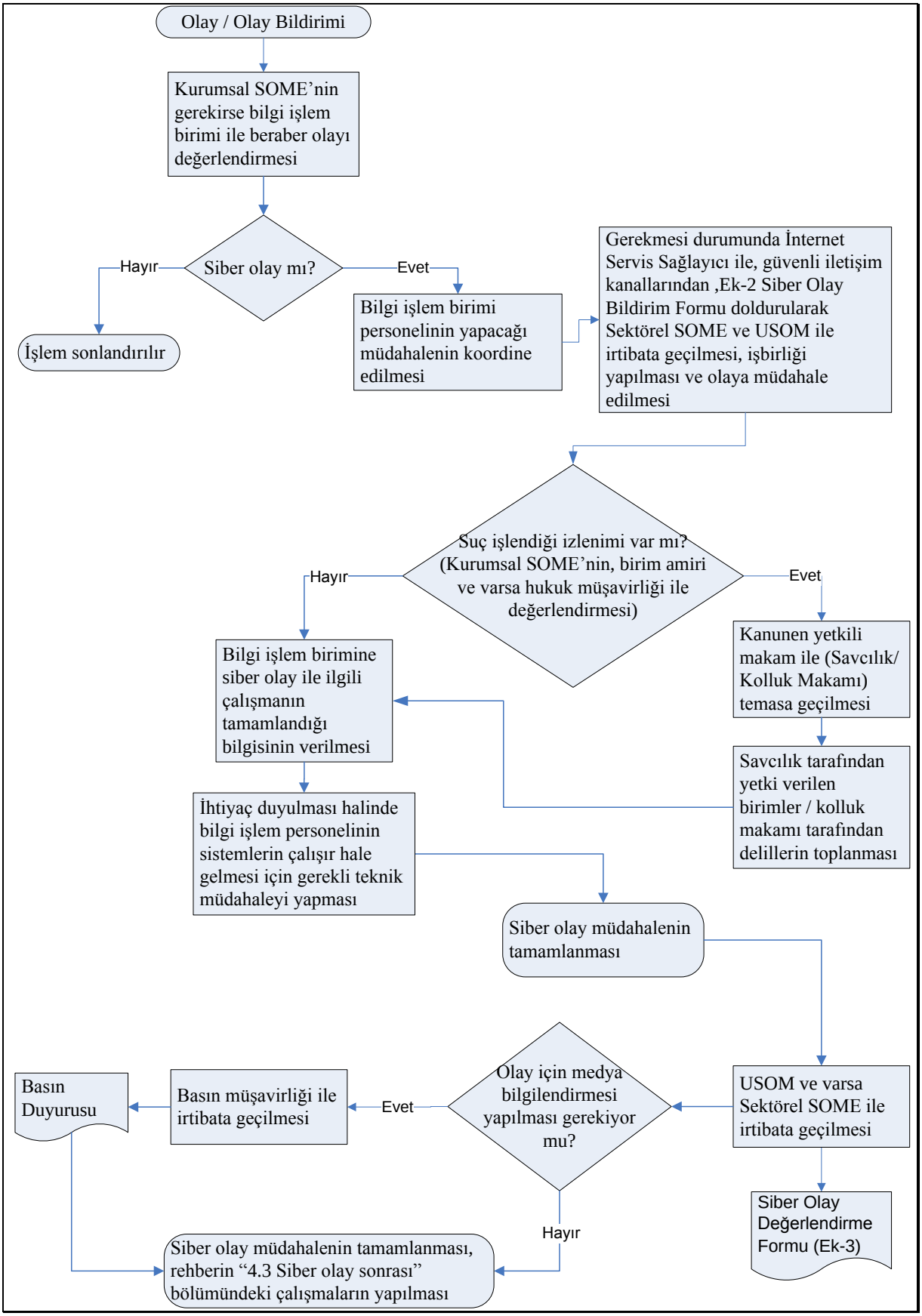
c. USOM ve varsa bağlı olduğu Sektörel SOME tarafından önerilen/düzenlenen toplantı ve etkinliklere katılırlar.
d. Güvenlik ürünlerinin (saldırı tespit sistemi, güvenlik duvarı, balküpü sistemi vb.) belirlenmesi sürecinde bilgi işleme destek verir.
e. Güvenlik ürünlerinin uygulama seviyesi işletimi ile ilgili politikaları bilgi işlem ile koordineli şekilde belirler.

4.2 Siber Olay Esnası

Kurumda herhangi bir siber olayın gerçekleştiği durumlarda, Kurumsal SOME'ler Şekil 5'de yer alan akış diyagramına göre görevlerini icra ederler. Şekilde Kurumsal SOME'lerin olay müdahale esnasında bilgi işlem birimi, internet servis sağlayıcı, Sektörel SOME, USOM, hukuk müşavirliği, savcılık, kolluk kuvveti ve basın müşavirliği ile birlikte gerçekleştirebileceği işlemler açıkça belirtilmiştir.

Kurumsal SOME olay müdahale esnasında bilişim sistemlerine yetkisiz erişim yapılmaması için gerekli tedbirleri alır, aldırır.

Siber olay müdahale akışı içinde suç unsuruna rastlanması halinde savcılık, kolluk makamı vb. makamlara haber verilmesi hem kanuni yükümlülüğün yerine getirilmesi, hem de ulusal siber güvenlik kapsamında caydırıcılığın sağlanması açısından önem arz etmektedir.



Şekil 5: Siber Olay Müdahale Akış Diyagramı

4.3 Siber Olay Sonrası

Kurumda bir siber olay gerçekleştikten ve olaya müdahale edildikten sonra Kurumsal SOME'ler aşağıdaki görevleri icra ederler:

a. Zaman geçirmeden olaya neden olan açıklık belirlenir ve çıkarılan dersler kayıt altına alınır.
b. Kurumsal SOME, siber olay ile ilgili bilgileri USOM tarafından belirlenen kriterlere uygun şekilde (Ek 3 Siber Olay Değerlendirme Formunu doldurarak) USOM'a ve varsa bağlı olduğu Sektörel SOME'ye gönderir ve kayıt altına alır.
c. Olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler kurum yönetimine arz edilir.
d. Yaşanan siber olayların türleri, miktarları ve maliyetleri ölçülüp izlenir.
e. Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu hazırlanır, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilir.

Ek 1: Kurumsal SOME İletişim Bilgileri Formu

(*) işareti zorunlu alanları belirtmektedir.

<table>
<tr><th colspan="7">KURUMSAL SOME İLETİŞİM BİLGİLERİ FORMU</th></tr>
<tr><td colspan="2">Kurum Adı*</td><td colspan="3"></td><td colspan="2">Tarih:</td></tr>
<tr><td colspan="2" rowspan="2">SOME Takımı
7/24 İletişim Bilgileri*</td><td>Telefon</td><td>Cep telefonu</td><td>Faks</td><td colspan="2">Kurumsal e-posta</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="2">Hizmet aldığı ISS*</td><td colspan="5"></td></tr>
<tr><td colspan="2">ISS’ten almış olduğu güvenlik hizmetleri*</td><td>DDOS</td><td colspan="4">Diğer:</td></tr>
<tr><td colspan="2">Hangi tür Güvenlik Cihazları kullanılıyor</td><td>IPS</td><td>WAF</td><td>FW</td><td colspan="2">Diğer:</td></tr>
<tr><td colspan="2">Kurum IP Adres Aralığı</td><td colspan="5"></td></tr>
<tr><td rowspan="6">SOME Personelinin*</td><td>Adı Soyadı</td><td>Ünvanı</td><td>Telefonu</td><td>Cep telefonu</td><td colspan="2">Kurumsal e-posta adresi</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="5">İzlenmesi Talep Edilen Sistemlerin</td><td>Alan Adı</td><td>IP Adresi</td><td colspan="4">Açıklama</td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
</table>

Ek 2: Siber Olay Bildirim Formu

SİBER OLAY BİLDİRİM FORMU

1. Bildirimi yapan SOME:

2. Bildirimi yapan personelin

Ad, Soyad :
Unvan/Birim :
Telefon :
E-posta :

3. Olay türü:

□ Servis dışı bırakma (DDoS)
□ Bilgi Sızdırma (Data Leakage)
□ Zararlı Yazılım (Malware)
□ Dolandırıcılık (Fraud)
□ Port Tarama
□ SQL Injection
□ Web Defacement
□ Sosyal Mühendislik
□ Spam
□ Şifre Ele Geçirme
□ Kimlik taklidi
□ Oltalama (Phishing)

□ Diğer (Lütfen açıklayınız):

_____

4. Olay sistem kesintisine sebep oldu mu? □ Evet □ Hayır

5. Olayın:

Tahmini başlangıç zamanı

Tarih : …….. Saat : ……..

Tespit edildiği zaman

Tarih : …….. Saat : ……..

6. Eklemek istedikleriniz:

Ek 3: Siber Olay Değerlendirme Formu

SİBER OLAY DEĞERLENDİRME FORMU		
1. Bildirimi yapan SOME:		
2. Bildirimi yapan personelin **Ad, Soyad :** **Unvan/Birim :** **Telefon :** **E-posta :**		
3. Olay türü: □ Servis dışı bırakma (DDoS) □ Bilgi Sızdırma (Data Leakage) □ Zararlı Yazılım (Malware) □ Dolandırıcılık (Fraud) □ Port Tarama □ SQL Injection □ Diğer (Lütfen açıklayınız): _____	□ Web Defacement □ Sosyal Mühendislik □ Spam □ Şifre Ele Geçirme □ Kimlik taklidi □ Oltalama (Phishing)	
4. Olay sistem kesintisine sebep oldu mu? □ Evet □ Hayır		
5. Etkilenen sistemler: □ Uygulama Sunucusu □ Posta Sunucusu □ Güvenlik Duvarı □ Diğer (Lütfen açıklayınız): _____	□ Veritabanı Sunucusu □ Web Sunucusu	□ DNS □ Dosya Sunucusu
6. Olayın kısa tanımı:		
7. Olayı bildiren kişi/kurum ve tespit edilme yöntemi : □ Kurum dışı bildirim □ Kurumsal SOME çalışanı □ Diğer (Lütfen açıklayınız): _____	□ Kurum çalışanı	□ Bilgi işlem birimi

Tespit edilme yöntemini açıklayınız:

_____

8. Olayın:

Tahmini başlangıç zamanı

Tarih : …….. Saat : ……..

Tespit edildiği zaman

Tarih : …….. Saat : ……..

9. Siber olaylara ait iz kayıtları tespit edildi mi?

□ Hayır

□ Evet

Kaynak IP : _____

Hedef IP : _____

Port : _____

Diğer : _____

10. Alınan Karşı Önlemleri Açıklayınız:

11. Eklemek istedikleriniz

Ek 4: Eğitim İçerikleri

Güvenli Yapılandırma Denetimi Eğitimi

Ön Şartlar

- □ Temel ağ bilgisi
- □ İşletim sistemleri bilgisi (Windows ve Unix)
- □ Sınır güvenliği yapılarını tanıma.

Ana Konular

- □ Zafiyet, tehdit tanımları
- □ Açık kaynak kodlu güvenlik zafiyet tarayıcıları ve bu araçların kullanımı
- □ Windows işletim sistemi denetimi
- □ Unix/Linux sistemlerin denetimi
- □ Bir ağın topolojisini çıkartma
- □ Sınır sistemleri denetimi

Sızma Testleri Eğitimi

Ön Şartlar

- □ Temel ağ bilgisi
- □ İşletim sistemleri bilgisi (Windows ve Unix)
- □ Etki alanı bilgisi
- □ Sınır güvenliği yapılarını tanıma

Ana Konular

- □ Pentest tanımı, amacı, dikkat edilmesi gereken hususlar
- □ Dış ağ taramaları ve aktif bilgi toplama
- □ Keşif ve zafiyet tarama
- □ Zafiyet istismar etme (exploitation)
- □ Etki alanı ve son kullanıcı bilgisayarları sızma testleri
- □ İstismar sonrası yapılması gerekenler (post-exploitation)
- □ Veritabanı sızma testleri
- □ Network bileşenleri sızma testleri ve ikinci katman saldırıları
- □ Güvenlik mekanizmaları atlatma yöntemleri
- □ Sosyal mühendislik
- □ Web uygulamaları sızma testleri

Saldırı Teknikleri Eğitimi

Ön Şartlar

- Temel TCP/IP bilgisi
- Temel işletim sistemi bilgisi

Ana Konular

- Güvenlik Testlerinde Bilgi Toplama
- TCP/IP İletişiminde Oturuma Müdahale
- Güvenlik Duvarları
- Saldırı Tespit ve Engelleme Sistemleri
- Güvenlik Duvarı, Saldırı Tespit ve Önleme Sistemleri ile İçerik Filtreleme Sistemlerini Atlatma
- Host/Ağ/Port Keşif Ve Tarama Araçları
- Zafiyet Tarama ve Bulma Sistemleri
- Exploit Çeşitleri ve Metasploit Kullanımı
- Kablosuz Ağlar ve Güvenlik
- Web Uygulama Güvenliği ve Hacking Yöntemleri
- VPN ve Şifreleme Teknolojileri
- Son Kullanıcıya Yönelik Saldırı Çeşitleri ve Yöntemleri
- Güvenlik Amaçlı Kullanılan Firefox Eklentileri
- Linux sistem yönetimi ve güvenliği
- TCP/IP Protokol Ailesi Zafiyet Analizi
- Paket Analizi, Sniffing

Saldırı Tespit ve Kayıt Yönetimi Eğitimi

Ön Şartlar

- Temel işletim sistemi bilgisi
- Temel TCP/ IP bilgisi
- Temel Linux bilgisi

Ana Konular

- Trafik Analizi Temelleri
- Uygulama Protokolleri ve Trafik Analizi
- Açık Kaynak Kodlu Saldırı Tespit Sistemi
- Ağ Trafiği Analizi ve İzleme
- Uygulama protokolleri için saldırı tespit metotları
- Kayıt Yapılandırma Ayarları
- Kayıt Analiz Yöntemleri ve Teknikleri
- Kayıt Yönetimi
- Büyük Boyutlu Kayıtların İşlenmesi
- Kayıtları İzleme
- Olay Müdahalesi için Kayıtlar
- Adli Analiz Kayıtları
- Uyumluluk için Kayıt
- Kayıt Toplamada En Sık Yapılan Yanlışlar
- Kayıt Standartları

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 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 Sistemleri Adli Analizi Eğitimi

Ön Şartlar

- □ Temel Linux ve Windows işletim sistemi bilgisi.

Ana Konular

- □ Bilgisayar olaylarına müdahale
- □ Bilgisayar adli analizi hazırlık aşamaları
- □ İşletim sistemlerinde dosyalama sistemleri (NTFS, FAT32, ext2, ext3) hakkında bilgiler (Dosyaların bu sistemlerde ne şekilde oluşturulduğu, saklandığı, silindiği vb.)
- □ Bilgisayarların çeşitli bölümleri için (RAM, "Stack" alanı, sabit diskler vb.) verilerin kalıcılığı ve veri çıkarma şekilleri
- □ Linux üzerinde bilgisayar olayı adli analizi yapılması ve ilgili araçların tanıtımı
- □ Uygulamalı kısımda adli analiz çalışma ortamının kurulması ve araçlarla şüpheli dosya incelemesi yapılması
- □ Windows üzerinde bilgisayar olayı adli analizi yapılması ve ilgili araçların tanıtımı
- □ Adli analizle ilgili yasal çerçeveler ve delillerin mahkemeye sunulabilecek şekilde saklanması

Bilgisayar Adli Analizi – Derinlemesine Windows Eğitimi

Ön Şartlar

- Bilişim sistemleri Adli Analizi Eğitimi

Ana Konular

- Sayısal Adli Analiz Temelleri ve Kanıt Toplama
- Uygulamalı: Temel Windows Adli Analizi Bölüm 1 - Dizi Sorguları, Veri madenciliği ve E-posta Adli Analizi
- Uygulamalı: Temel Windows Adli Analizi Bölüm 2 – Kayıt Defteri ve USB Analizi
- Uygulamalı: Temel Windows Adli Analizi Bölüm 3 – Kayıt Dosyası Analizi
- Uygulamalı: Temel Windows Adli Analizi Bölüm 4 – Web Tarayıcı Analizi
- Uygulamalı: Sayısal Adli Analiz Yarışması

Ağ Adli Analizi Eğitimi

Ön Şartlar

- Katılımcıların (VirtualBox veya VMWare) üzerinde çalıştırılacak sanal işletim sistemini sıkıntısız çalıştırabilecek bir bilgisayarının olması.
- Katılımcıların Linux işletim sistemi temelleri ve uygulamaları hakkında bilgili olması.
- Katılımcıların Linux işletim sistemlerinde basit kurulum ve bağlantı işlemlerini yapabilir düzeyde olması (IP Adresi atama, log dosyası takip etme, editör kullanımı vb.).
- Katılımcıların genel ağ protokolleri (IP, HTTP, TCP, UDP, vb.) ve ağ dinleme araçları (wireshark, tcpdump vb.) hakkında giriş seviyesinde bilgisinin olması.

Ana Konular

- Dijital kanıtların ağ kaynaklarından elde edilmesi
- Analiz sürecinde elde edilecek sonuçların tekrar üretilebilir olması ve elde edilen kanıtların güvenilir olması
- Ağ analizinde farklı amaçlar için kullanılabilecek araçlar, teknolojiler ve süreçler
- Mobil cihaz güvenliği
- Uygulamalar

Zararlı Yazılım Analiz Yöntemleri Eğitimi

Ön Şartlar

- Temel işletim sistemi bilgisi

Ana Konular

- Uygulamalı: Zararlı Yazılım Araçları ve Yöntemleri
- Uygulamalı: Zararlı Yazılım Analizi Temelleri
- Uygulamalı: Diğer Zararlı Yazılım Analiz Yöntemleri
- Uygulamalı: Zararlı Kod Analizi
- Uygulamalı: Zararlı Yazılımlardan Korunma Yöntemleri

DDoS Saldırıları ve Korunma Yöntemleri Eğitimi

Ön Şartlar

- Temel TCP/IP bilgisi

Ana Konular

- DDoS saldırı çeşitleri
- DDoS saldırı analizi
- DDoS ile mücadele

Bilişim Hukuku Eğitimi[4]

Ön Şartlar

□ Belirli bir ön şart yoktur.

Ana Konular

□ Adli Sürecin yürütülmesi temel eğitimi
□ 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

[4] Eğitim içeriği Ankara Barosu İnternet Sitesinden alınmıştır.

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
  - o Güvenlik politikası
  - o Bilgi güvenliği organizasyonu
  - o Varlık yönetimi
  - o İnsan kaynakları güvenliği
  - o Fiziksel ve çevresel güvenlik
  - o İletişim ve işletim yönetimi
  - o Erişim kontrolü
  - o Bilişim sistemi edinim, geliştirme ve bakımı
  - o Bilgi güvenliği olay yönetimi
  - o İş sürekliliği yönetimi
  - o Uyum
□ ISO 27001'e uygunluk denetimi
  - o Denetim planlama
  - o Denetim kontrol listeleri
  - o Uygunsuzluklar ve raporlama
□ Çeşitli uygulamalar

Ek 5: Kurumsal SOME'ler İçin Gereksinim Listesi

Genel Öğeler
1. Görev Alanının Tanımlanması: Kurumsal SOME'nin sorumlu olacağı bilişim varlıkları ile hizmet vereceği kurum/birim(ler) net bir şekilde belirlenmelidir.
2. Görev ve Yetkilerin Belirlenmesi: Kurumsal SOME'lerin görev ve yetkileri SOME'nin temel hedeflerini de içerecek şekilde açıkça belirlenmelidir.
3. Organizasyon Şeması: Kurumsal SOME'nin kurulduğu kuruma ait organizasyon şemasındaki yeri belirtilmelidir.
4. Kurumsal SOME Organizasyonu: Kurumsal SOME amir ve personelinin görev ve sorumlulukları ile kurumdaki yeri detaylandırılmalıdır. Tüm ekip çalışanları aynı birimde bulunmuyorsa bu durum Kurumsal SOME organizasyon şemasında belirtilmelidir.
Politika
1. Bilginin Sınıflandırılması ve Korunması: Hassas, gizli veya halka açık bilgilerin sınıflandırıldığı, ayrı ayrı bu bilgilerin nasıl saklanacağı, nakledileceği, erişilebileceği, vb. gibi konuların açıklandığı politikalar hem elektronik hem de basılı kopyalar şeklinde oluşturulmalıdır.
2. Kayıt Tutma: Tutulan elektronik veya basılı kayıtların sınıflarına göre ne kadar süre saklanması gerektiği, yedeklemenin nasıl yapılacağı, yedeklerin nasıl nakledileceği ve arşivleneceğini belirten politikalar hazırlanmalıdır.
3. Kayıt Yok Etme: Sayısal veya basılı kayıtların sınıflarına göre ne şekilde ve kim tarafından yok edilebileceğini belirten politikalar oluşturulmalıdır.
4. Bilgi Dağıtımı ve Erişimi: Dağıtılabilecek bilginin türü ve metodunun açıklandığı, hangi bilgiye kimlerin ulaşabileceğinin belirtildiği politikalar oluşturulmalıdır.
5. Kurumsal SOME Sistemlerinin Kullanımı: Kurumsal SOME çalışanlarının ekipman ve sistemlerini günlük işlerde nasıl kullanacağı detaylı olarak açıklanmalıdır. Ekipman ve sistemlere ait aşağıdaki konularda politikalara açıklık getirilmelidir: □ İzinsiz erişime karşı nasıl korunuyor? □ Kişisel amaçlı kullanılabilir mi? □ Hangi sitelere giriş yapılabilir veya yapılamaz? □ Kişisel yazılımlar indirilip yüklenebilir mi? □ Virüs ve casus yazılım taraması hangi sıklıkla yapılıyor? □ Yazılım güncellemeleri hangi sıklıkla yapılıyor?
6. Olay Müdahale Politikası: Kurumsal SOME sorumluluklarının detaylıca belirtildiği, hangi durumlarda kolluk kuvvetleri ya da USOM ve varsa bağlı Sektörel SOME'den yardım istenebileceğinin açıklandığı politikalar hazırlanmalıdır.

Çalışma Ortamı

1. **Fiziksel Güvenlik:** Kurumsal SOME birimlerine ait çalışma yeri, haberleşme altyapısı ile bilginin ve çalışanların korunmasını dikkate alarak düzenlenmelidir.
2. **Depolama:** Kurumsal SOME ekibi depolamaları gereken fiziksel varlıklarını güvenli bir şekilde saklamalıdır. Bu varlıkların nasıl ve nerede saklanacağı, bu materyale kimlerin erişebileceği ile ilgili yöntemler belirlenmelidir.
3. **E-posta ile güvenli iletişim yöntemi (PGP Kullanımı):** Kimlerin anahtarları olmalı, anahtarlar nasıl üretilmeli ve saklanmalı konuları netleştirilmelidir.
   - □ Kimlerde anahtar olacaktır (amir, personel, vb.)?
   - □ Anahtarlar nasıl oluşturulacak, yönetilecek ve saklanacaktır?
   - □ Anahtar yönetimi konuları:
     - o Anahtarları kim oluşturacaktır?
     - o Hangi tür anahtar oluşturulacaktır?
     - o Anahtar boyutu ne olacaktır?
     - o Son kullanma tarihleri belirlenecektir
     - o İptal sertifikası gerekli olacak mıdır?
     - o Anahtarlar ve iptal sertifikaları nerede saklanacaktır?
     - o Anahtarlar nasıl iptal edilecektir?
     - o Anahtarları kim imzalamalıdır?
   - □ Parola politikası var mıdır?

Olay Yönetimi

1. **Olay Müdahale Planı:** İzlenmesi gereken adımlar şu şekilde sıralanabilir:
   - □ Olay atama
   - □ Olay analiz
   - □ Olay önceliği yükseltme
   - □ Olayı kapama
   - □ Olaydan alınan dersler

   Ayrıca şu hususlara dikkat edilmelidir:
   - □ Olayla ilgili kayıtları kim tutuyor, bilgiyi kim takip ediyor?
   - □ Olay sırasında sürekli bilgilendirilmesi gereken denetmenler var mı?
   - □ Olay sırasında olayın derecesini yükseltmek için bir politika mevcut mu?
   - □ Bir olayı kapatmak için hangi kriterlere bakılır?
2. **Raporlama:** Kurumsal SOME'nin kurum içi ve kurum dışı paydaşlar arasındaki bilgilendirme süreci tanımlanmalıdır. Olay sonrası USOM'a rapor verilmelidir.

Ek 6: Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri

"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" 3. Maddesi çerçevesinde **"Siber Olayların Delillendirilmesi"** eyleminin **"Olay sonrasında incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin belirlenmesi"** alt eyleminde İçişleri Bakanlığı sorumlu kuruluş olarak belirlenmiştir.

İçişleri Bakanlığı'nın eşgüdümünde ve ilgili kurum/kuruluşların katılımı ile tamamlanan **"Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri"**ne ilişkin çalışma tamamlanmıştır.

Bu çalışma kurumlar için bir kılavuz niteliğinde olup, kurumların kendi sistemlerine ilişkin risk değerlendirmesi yaparak hangi sistemleri kuracaklarını ve hangi sistemlerden, ne seviyede kayıt toplayacaklarını belirlemeleri gerekmektedir.

Çalışma sonucunda oluşturulan rapor 7 başlık altında toplanmış olup bunlar aşağıdaki gibidir:

1. **İz Kayıtlarının Alınması Gereken Sistemler**
2. **İz Kayıtlarında Bulunması Gereken Asgari Nitelikler**
3. **İz Kayıtlarının Güvenliği**
4. **İz Kayıtlarının Yönetimi ile İlgili Roller**
5. **İz Kayıtlarının Saklanma Süresi**
6. **Ortak Zaman Sunucusu Kullanımı**
7. **Merkezi İz Kayıtları Yönetiminin Sağlanması**

1. İz Kaydı Alınması Gereken Sistemler

A. Fiziksel ortam kayıtları:

1) Kritik Bilişim sistemleri odaları giriş-çıkış kayıtları,
2) Kritik Bilişim sistemleri odaları giriş-çıkış kamera kayıtları,
3) Çalışma ortamları giriş-çıkış kayıtları,
4) Çalışma ortamları giriş-çıkış kamera kayıtları.

B. Sanal ortam kayıtları:

1) Güvenlik duvarları,
2) Antivirüs yazılımları,
3) Saldırı tespit/önleme sistemleri,
4) Yönlendiriciler ve anahtarlama cihazları,
5) Sunucular,
6) İş uygulamaları (Kritik Kurumsal projeler),
7) Veri tabanları,
8) Sanal özel ağ sistemleri

2. İz Kayıtlarında Bulunması Gereken Asgari Nitelikler

A. Kaydı Oluşturan Sistem

B. Kaydın Oluşturulma Zamanı (Tarih, saat, zaman dilimi)

C. Kaydı Oluşturan Olay

D. Kaydın İlişkili Olduğu Kişi (IP-Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı)

3. İz Kayıtlarının Güvenliği

A. Gizlilik

1) Siber olaylara ilişkin tutulan iz kayıtlarına, "bilinmesi gerektiği kadar" (need to know) prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabiliyor olması sağlanmalıdır.

2) Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri yapılandırılmalıdır.

3) Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında teknik imkanlar dahilinde trafiğin şifreli olarak transfer edilmesi sağlanmalıdır.

B. Bütünlük

1) İz kayıtlarının tek yönlü kriptografik özet değerleri (hash) hesaplatılmalı ve iz kayıtları güvenli ortamlarda saklanmalıdır.

2) Siber olaylara ilişkin iz kayıtlarının saklanması için kurulacak yapının kayıtları, olayların olduğu sistem dışında merkezi bir sunucuda saklanmalıdır. Kurum kritik olaylarını belirlemelidir. Kritik olayların iz kayıtları merkezi sunucuya anlık olarak (olay oluştuğu zaman) gönderilmeli, kritik olmayan olayların iz kayıtları da kurumun belirlediği aralıklarda merkezi sunucuya iletilmelidir.

3) Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi sunucularda yedeklenmeli, silinmelerine ve değiştirilmelerine izin verilmemelidir.

4) Merkezi iz kaydı sunucuları sadece yeni iz kayıtlarının saklanması için fonksiyonlar içermeli, iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere kapalı olmalıdır.

C. Erişilebilirlik

İz kayıtlarının periyodik olarak yedeklenmesi ve yedeklerin uygun şekilde muhafaza edilmesi sağlanmalıdır.

4. İz Kayıtlarının Yönetimi ile İlgili Roller

Kurumların iz kayıtlarının yönetimi; iz kayıtlarının üretilmesi, transfer edilmesi, depolanması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi aşamalarını kapsar. Bu süreçlerde sistem, veri tabanı, ağ ve güvenlik yöneticileri, Siber Olaylara Müdahale Ekipleri (SOME), yazılım geliştiriciler ve denetçilere ait görev ve sorumluluklar belirlenmelidir.

5. İz Kayıtlarının Saklanma Süresi

İz kayıtlarının saklanma süresi belirlenmesinde, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği parametreleri göz önünde bulundurulmalıdır. İz kayıtları bu bilgiler ışığında asgari olarak 1 yıl süre ile saklanmalıdır. Kurumların kendi mevzuatları gereği uyması gereken süreler saklıdır.

6. Ortak Zaman Sunucusu Kullanımı

Kayıtların toplandığı bütün sistemlerin aynı zaman değerine sahip olması gerekmektedir. Bütün sistemlerin zamanlarının aynı yapılması işlemi için Ağ Zaman Protokolü (NTP-Network Time Protocol) sunucusu kurulup kayıt üreten farklı sistemlerin zamanlarını bu sunucu ile senkronize etmesi sağlanmalıdır. Bunun yanında farklı ülkelerde birimleri olan kurumlar için saat dilimi (timezone) de dikkate alınmalıdır.

7. Merkezi İz Kayıtları Yönetiminin Sağlanması

Yukarıda asgari nitelikleri belirtilen iz kayıtlarının daha etkin, verimli ve güvenli bir şekilde toplanması, ilişkilendirilmesi, arşivlenmesi, raporlanması amacıyla Merkezi İz Kayıtları Yönetimi Mekanizmaları devreye alınmalıdır.