Kurumsal Siber Olaylara Müdahale Ekibi Talimatı
(SHT-SİBER)

BİRİNCİ BÖLÜM
Amaç, Kapsam, Tanım ve Kısaltmalar, Hukuki Dayanak

Amaç

MADDE 1 - (1) Bu Talimatın amacı; Kurumsal Siber Olaylara Müdahale Ekibi (SOME)'nin kurum organizasyonu içerisindeki yerini, kapasite planlamasını, personelin niteliklerini, alması gereken eğitimleri, Kurumsal SOME'nin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları ve kurum içi/kurum dışı paydaşlarla iletişimine ilişkin usul ve esaslarını belirlemektir.

Kapsam

MADDE 2 - (1) Bu Talimat, Genel Müdürlük tarafından yetkilendirilen havayolu işletmelerini, yer hizmet kuruluşlarını ve havaalanı/terminal işleticilerini, 10 kişiden daha fazla kişinin çalıştığı havaaracı üs bakım kuruluşları ve seyrüsefer hizmet sağlayıcılarını kapsar.

Dayanak

MADDE 3 - (1) Bu Talimat; 20/10/2012 tarih ve 28447 sayılı Resmi Gazetede yayımlanan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararına, 11/11/2013 tarih ve 28818 sayılı Resmi Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğine, 14/10/1983 tarih ve 2920 sayılı Türk Sivil Havacılık Kanunu'na, 15/07/2018 tarihli ve 30479 sayılı Resmi Gazetede yayımlanan Bakanlıklara Bağlı, İlgili, İlişkili Kurum Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında 4 sayılı Cumhurbaşkanlığı Kararnamesine, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'na ve Milli Sivil Havacılık Güvenlik Programı Ek 19- Siber Tehditlere Karşı Yapılacak İşlemler Talimatı'na dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Talimatta geçen**;**

a) Genel Müdürlük: Sivil Havacılık Genel Müdürlüğünü,

b) SHGM: Sivil Havacılık Genel Müdürlüğünü

c) Genel Müdür: SHGM Genel Müdürünü,

ç) Havacılık Sektörü İşletmeleri (İşletme): Hava taşıma işletmelerini, havaalanı işletmelerini, terminal işletmelerini, yer hizmetleri kuruluşlarını, hava seyrüsefer hizmet sağlayıcılarını,

d) Kurumsal SOME: Temel görevleri Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ'inde yer alan, kurumunda bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibini,

e) Havacılık Sektörel SOME: Düzenlemekle yükümlü olduğu havacılık sektöründe bulunan kritik altyapı veya kamu sistemlerini siber olaylardan korumak için çeşitli çalışmalar yapan Sektörel Siber Olaylara Müdahale Ekibini,

f) Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya ihlal teşebbüsünde bulunulmasını,

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

ğ) USOM: Temel görevleri, "Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esasları"nda yer alan Ulusal Siber Olaylara Müdahale Merkezini,

h) TSE: Türk Standartları Enstitüsünü,

ı) ISO: International Organization for Standardization (Uluslararası Standartlar Organizasyonunu),

i) IEC: International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonunu),

j) CISA: Certified Information System Auditor

k) CISSP: Certified Information System Professional

l) CISM: Certified Information System Manager

m) CRISC: Certified In Risk and Information Systems Control

n) ECSA: EC-Council Certified Security Analyst

o) GSEC: GIAC Security Essentials

ö) CEH: Certified Ethical Hacker

p) SGSYY: Siber Güvenlikten Sorumlu Yetkili Yöneticiyi,

r) Hizmet Alınan Kuruluş: Siber Güvenlik ile ilgili işletmeye hizmet veren kurum/kuruluşları,

s) Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

ş) Kritik Varlıklar: İşletmenin iş sürekliliğini ciddi anlamda sekteye uğratabilecek ve çalışmaması durumunda Türk Havacılık Sektörünü maddi ve itibari yönden zedeleyebilecek sistem/bilgi/belge vb. bütününü,

t) İz kaydı: Bilişim sistemlerinin işletilmesi esnasında veya siber olaya maruz kalması durumunda ürettiği kayıtları,

u) A Grubu Havacılık Sektörü İşletmeleri:

-Havayolu işletmesi ise; Filosunda en az 20 adet uçak bulunduran havayolu işletmelerini,

-Bir önceki yılın (iç hat yolcu sayısı x 1)+(dış hat yolcu sayısı x 2) sayısı 10 milyon yolcudan fazla olan Havalimanı/Terminal işletmelerini,

-Seyrüsefer Hizmet Sağlayıcılarını,

ü) B Grubu Havacılık Sektörü İşletmeleri:

-Filosunda 20'den az uçak bulunduran havayolu işletmelerini,

-Bir önceki yılın (iç hat yolcu sayısı x 1)+(dış hat yolcu sayısı x 2) sayısı 10 milyon yolcuya eşit veya az olan Havalimanı/Terminal işletmelerini,

-Yer hizmeti kuruluşlarını,

-10 kişiden daha fazla kişinin çalıştığı havaaracı üs bakım kuruluşlarını,

v) Seviye 1 Bulgu: Faaliyetin genel işleyişini etkilemeyen ancak daha iyi bir hizmet sunulmasını engelleyebilecek bulguları,

y) Seviye 2 Bulgu: Faaliyetin çıktılarının kalitesini etkileyen, yürütülmesinde gecikmelere ve sorunlara neden olabilecek bulguları,

z) Seviye 3 Bulgu: Faaliyetin yürütülmesinde uzun süreli gecikmelere ve ciddi sorunlara neden olabilecek bulgular bu grupta değerlendirilir. Risk ve etkileri değerlendirildiğinde, kurum faaliyetlerini sekteye uğratacak veya kurumun önemli mali kayıplarla karşılaşmasına neden olacak bulguları,

aa) Seviye 4 Bulgu: Risk ve etkileri değerlendirildiğinde, can kayıplarına veya bedensel bütünlüğe zarar vermesi, kurumun faaliyetlerini durdurması veya büyük mali kayıplara neden olması, havacılık sektörünün ve ülkemizin imajı açısından ciddi anlamda olumsuz etkide bulunması gibi sonuçlara neden olabilecek bulguları,

bb) Kırmızı Takım Çalışması: Bir işletmenin güvenlik cihazlarını, ağlarını, çalışanlarını, uygulamalarını ve fiziksel güvenlik kontrollerini gerçekte bir saldırıya ne kadar dayanabileceğinin ölçülmesi için tasarlanan tam kapsamlı ve çok katmanlı saldırı simülasyon çalışmalarını,

cc) Some İletişim Platformu(SİP): USOM tarafından SOME'lerin iletişimi için oluşturulmuş güvenli iletişim platformunu (www.sip.gov.tr),

dd) SHGM BYS: SHGM Bilgi Yönetim Sistemini(https://otomasyon.shgm.gov.tr/shgmSeam/) ifade eder.

(2) Bu Talimatta belirtilmeyen tanımlar için, 14/10/1983 tarihli ve 2920 sayılı Türk Sivil Havacılık Kanunu ile 10/11/2005 tarihli ve 5431 sayılı Sivil Havacılık Genel Müdürlüğü Teşkilat ve Görevleri Kanunu'nda, ilgili diğer mevzuatta ve ülkemizin üyesi bulunduğu uluslararası sivil havacılık kuruluşları tarafından yayımlanan dokümanlarda belirtilen tanımlar geçerlidir.

İKİNCİ BÖLÜM
Genel Hükümler

Kurumsal SOME Kurması Gereken İşletmeler

MADDE 5 - (1) Genel Müdürlük tarafından yetkilendirilen havayolu işletmeleri, yer hizmet kuruluşları, havaalanı/terminal işleticileri, hava aracı üs bakım kuruluşları ve seyrüsefer hizmet sağlayıcıları Kurumsal SOME kuracaktır.

Kurumsal SOME Temel Prensipleri ve Kurulum Aşamaları

MADDE 6 - (1) Kurumsal SOME kurması zorunlu kılınan A grubu Havacılık Sektörü İşletmeleri, doğrudan işletmenin yönetimine (Yönetim kurulu başkanı veya Genel Müdür) bağlı bir Siber Güvenlikten Sorumlu Yetkili Yönetici (SGSYY) atayarak, bu yönetici liderliğinde Kurumsal SOME yapılanmasını oluşturur. B grubu Havacılık Sektörü İşletmeleri ise mevcut BT yöneticilerini SGSYY olarak atayarak Kurumsal SOME yapılandırmasını oluşturmakla mükelleftir. SGSYY yönetimindeki Kurumsal SOME işletmenin organizasyon yapısında yer alır. SGSYY Kurumsal SOME birimi yönetim fonksiyonunu icra eder. SGSYY yönetim fonksiyonunun yanı sıra bu madde de belirtilen SOME fonksiyonlarından bir ya da bir kaçını da yerine getirebilir.

(2) SGSYY'nin uygunluğu, Genel Müdürlük tarafından bu talimatın 6 ncı maddesinin üçüncü fıkrasında belirtilen bilgi ve belgelerin değerlendirilmesi sonucunda onaylanır.

(3) İşletme tarafından atanan SGSYY'nin Genel Müdürlük tarafından onaylanması esnasında istenilen belgeler ve şartlar;

a) Doldurulmuş ve ıslak imzalanmış Siber Güvenlikten Sorumlu Yetkili Yönetici Değerlendirme Formu (Ek-1),

b) Personelin işletmede çalıştığını gösteren SGK sigortalı hizmet listesi

c) Bilgi Güvenliği/Siber Güvenlik alanında en az 5 yıllık tecrübe sahibi olduğunu gösteren belgeler (Siber Güvenlik alanında Yüksek Lisans 1, Doktora 2 yıl tecrübe sayılacaktır.),

ç) Bilgi Güvenliği/Siber Güvenlik alanında uluslararası geçerliliği olan aşağıdaki sertifikalardan en az 1 tanesi:

1) CISA
2) CISSP
3) CISM
4) CRISC
5) ECSA
6) GSEC
7) CEH
8) TSE Kıdemli Sızma Test Uzmanı Sertifikası
9) ISO 27001 Baş Denetçi Sertifikası

d) En az lisans derecesine sahip olduğunu gösteren diploma,

e) İletişim bilgilerini ve TC Kimlik Numarasını da içerecek şekilde hazırlanmış özgeçmiş,

f) SHGM Hizmet Tarifesine göre yatırılmış ücret dekontu

Genel Müdürlük onayına resmi yazı ile sunulur. Genel Müdürlük bu bilgi ve belgelerden uygun olanları talep etmeyip teyit edebilir.

(4) Kurumsal SOME, işletmenin/kuruluşun bilgi işlem biriminden ve mevcut diğer birimlerinden tamamen bağımsız bir şekilde SGSYY'nin altında kurulur.

(5) Kurumsal SOME temel olarak aşağıda belirtilen altı fonksiyonu icra eder:

a) SOME birimi yönetimi fonksiyonu

b) Olay müdahale yönetim ve koordinasyon fonksiyonu

c) Sistem test ve denetimi fonksiyonu

ç) Kurumsal siber güvenlik bilinçlendirme fonksiyonu

d) İz kayıt analiz fonksiyonu

e) Siber istihbarat toplama fonksiyonu

(6) İşletmenin bu talimatın 6 ncı maddesinin beşinci fıkrasında belirtilen fonksiyonları, konunun önemi ve hassasiyeti nedeniyle işletme bünyesinde yürütülmesi tercih edilmelidir. Ancak zorunlu hallerde hizmet alımı yoluyla temin edilebilir. SOME birimi yönetim fonksiyonu/SGSYY hiçbir şekilde hizmet alımı yoluyla temin edilemez. Bu nedenle, SGSYY kurum çalışanı olmak zorundadır. Kurumsal SOME'de görev yapan personellerin görev tanımları açık bir şekilde yapılmalıdır. Yapılan görev tanımlarında Kurumsal SOME fonksiyonları dışında görev yapmalarına olanak sağlayacak hiçbir madde bulunamaz.

(7) Kurumsal SOME fonksiyonlarının bir firmadan hizmet alımı yoluyla temin edilmesi durumunda firma ile gizlilik sözleşmesi yapılması zorunludur.

(8) İşletmeler, Kurumsal SOME yönetim fonksiyonu/SGSYY görevi haricindeki fonksiyonlarını yerine getirmek üzere yeteri kadar personel görevlendirir veya yeteri kadar personel ile hizmet alımı yapar.

(9) Kurumsal SOME'nin görev ve sorumluluklarının gerçekleştirilebilmesi için, Kurumsal SOME'de çalışacak personelin en az ön lisans programlarından mezun olması ve en az iki yıl bilgi işlem ve/veya bilgi güvenliği/siber güvenlik konularında bilgi ve tecrübeye sahip olması gerekmektedir.

(10) İşletmeler, Kurumsal SOME Kurulum ve Yönetim Rehberi'nin Ek-5'inde yer alan Kurumsal SOME'ler için Gereksinim Listesi'ne uygun şekilde görevlerini icra etmek zorundadır.

Kurum İçi Paydaşlarla İletişim Esasları

MADDE 7 - (1) Kurumsal SOME; siber olay öncesi, esnası ve sonrasında, siber güvenliği yönetmek amacıyla kurumdaki bilgi işlem birimi ve varsa hukuk ve basın/halkla ilişkiler müşavirlikleri ve benzeri birimler ile birlikte çalışır.

(2) Bilişim sistemlerinin yönetimini ve sürekliliğini sağlayan bilgi işlem ekibinin görevleri ile siber güvenliğe ilişkin belirlenen politikalara uygun şekilde faaliyet gösteren, ihtiyaç durumunda yetkili makamlarla iletişime geçen, kayıt vb. veriyi yetkili makamlara aktaran ve müdahaleyi yapan/yapılmasına yardımcı olan Kurumsal SOME'nin görevleri birbirinden farklı görevler olup bu görevleri yapan ekipler arasında "görevler ayrılığı" ilkesinin uygulanması ve farklı personel tarafından yapılması zorunludur. Bu amaçla iş gücü kapasitesinin artırılması ve iyileştirilmesi için işletme gerekli tedbirleri alır.

(3) Kurumsal SOME; siber olay esnasında, işletmenin yapacağı müdahaleyi bilgi işlem birimi ile koordine eder. İhtiyaç duyulması halinde, bilgi işlem birimine teknik destek sağlayabilir.

(4) Kurumsal SOME; siber olay sonrasında, olay ile ilgili siber olay sonrası değerlendirme çalışmasını ilgili birimler ile birlikte yürütür ve ilgili paydaşları bu talimata uygun bir şekilde bilgilendirir.

(5) İşletmeler, bu talimatın 7 nci maddesinde yer alan hususlar göz önüne alınarak düzenlenen bir prosedür/talimatta Kurumsal SOME'lerin kurum içi paydaşlar ile iletişim esaslarını oluşturmakla yükümlüdür.

Kurum Dışı Paydaşlarla İletişim Esasları

MADDE 8 - (1) Kurumsal SOME, tüm Kurumsal SOME personelinin iletişim bilgilerini USOM ve Havacılık Sektörel SOME'sine Some İletişim Platformu (SİP) üzerinden bildirmek ile yükümlüdür.

(2) Söz konusu platformda yer alan bilgilerde değişiklik olması durumunda Kurumsal SOME bu değişikliği gecikmeksizin SİP üzerinden güncellemekle yükümlüdür.

(3) Kurumsal SOME, işletmelerine yapılan bir siber saldırı esnasında vakit kaybetmeden Havacılık Sektörel SOME'si ve USOM'a bilgi vermek zorundadır.

(4) Kurumsal SOME, yıllık Siber Güvenlik Faaliyet Raporlarını Ek-2'de belirtilen formata göre hazırlayarak Havacılık Sektörel SOME'sine en geç izleyen yılın 31 Ocak tarihine kadar eksiksiz bir şekilde gönderir.

Siber Güvenlik ile İlgili Eğitimlerin Alınması

MADDE 9 - (1) İşletme, Kurumsal SOME personellerinin görevlerini icra edebilmesi için gerekli her türlü eğitimi almalarını sağlamak ile yükümlüdür.

(2) İşletme, Kurumsal SOME personellerinin Kurumsal SOME'de görevlendirilmesinden itibaren 1 yıl içerisinde birimdeki görevleri kapsamına uygun olarak Ek-3'te yer alan eğitimleri eksiksiz bir biçimde almalarını sağlar.

(3) İşletme, Kurumsal SOME personellerinin Ek-3'te yer alan söz konusu eğitimlerin 5 senede bir tazeleme eğitimlerini almalarını sağlar.

(4) Yukarıda belirtilen eğitimler birleştirilebilir. Bu durumda eğitim içeriği Havacılık Sektörel SOME'sine bildirilmelidir.

(5) İşletme, Kurumsal SOME personeline sağladığı eğitim olanakları ile sınırlı kalmamalı. Söz konusu personelin sistemli bir şekilde kayıt analizi ve yönetimi yapabilmesi, işletmenin bilişim sistemlerindeki önemli güvenlik zafiyetlerini tespit edebilmesi ve siber olay müdahale koordinasyonu yapabilmesi için gerekli olan temel yetkinliklere sahip olabilmesi amacıyla güncel teknolojiyi takip etmesini sağlamakla yükümlüdür

Kurum İçi Siber Güvenlik Kültürü Oluşturma ve Farkındalık Çalışmalarının Gerçekleştirilmesi

MADDE 10 - (1) Kurumsal SOME, kurum içi farkındalık çalışmaları kapsamında;

a) İşletme personeline Siber Güvenlik Farkındalık Eğitiminin verilmesi ve bu eğitimin her sene tazelenmesi,

b) İşletme tarafından Siber Güvenlik Farkındalık Eğitimi verilen personelin yetkinlik seviyesinin Kurumsal SOME tarafından değerlendirilmesi,

c) İşletme çalışanlarına bilgi güvenliğiyle ilgili bilgilendirme e-postaları gönderilmesi,

ç) İşletmenin bilişim sistemlerine erişimi olan bütün çalışanlarının en az %25'ini kapsayacak şekilde 3 ayda bir yılda en az 4 kez olmak üzere sosyal mühendislik testlerini yapması/yaptırması ve sonuçlarını Ek-4'te belirtilen formata uygun bir şekilde testin bitiminden en geç 1 ay sonra Genel Müdürlüğe gizli resmi yazı ile bildirmesi,

d) İşletmedeki personellerin bilgi güvenliği farkındalığını ölçecek anketlerin/çalışmaların senede en az 1 kere yapılması (minimum (işletme toplam çalışan sayısı/100)*2) senaryo ile),

e) Siber Güvenlik Farkındalığı konusunda yetersiz görülen personellerin tespit edilmesi ve bu personellerin siber güvenlik farkındalığının arttırılabilmesi için gerekli çalışmaların yapılması,

f) Senede en az bir kere işletmedeki personellerin siber güvenlik farkındalıklarını ölçmek üzere fiziksel kırmızı takım çalışmaları yapmaları/yaptırmaları
faaliyetlerini yapar/yaptırır.

(2) 10 uncu madde birinci fıkrada belirtilen faaliyetlerin dışında Kurumsal SOME'nin;

a) İşletmenin yemekhane, toplantı odaları gibi ortak kullanılan bölgelerine bilgi güvenliğiyle ilgili posterler asılması,

b) Siber güvenlik ile ilgili periyodik olarak kurum içi bülten hazırlanması ve bu bültenin personeller ile paylaşılması,

c) Varsa işletmenin iç portalında siber güvenlik ile ilgili bir bölüm oluşturulması,

ç) Siber güvenlikle ilgili ekran koruyucuların ve arka plan resimleri vb. materyallerin hazırlanması

faaliyetlerini de Siber Güvenlik Farkındalık Çalışması kapsamında yapması önerilir.

Bilişim Sistemleri Güvenlik Testlerinin Gerçekleştirilmesi

MADDE 11 - (1) Bilişim sistemleri güvenlik testleri Ek-5'te belirtilen şekilde gerçekleştirilir.

(2) Geniş kapsamlı test ve denetim kapsamında;

a) Kurumsal SOME, yılda en az bir defa TSE onaylı sızma testi firmalarına testlerini ve denetimlerini yaptırır. Bu testlerin/denetimlerin kapsamı şu şekilde olmalıdır:

1) İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması

2) Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması

3) Dışa açık web uygulamalarının sızma testleri

4) Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri

5) Veri tabanı yapılandırma testleri

6) Kuruma özel geliştirilmiş yazılımlar

7) DNS servisi testleri

8) E-posta servisi testleri

9) Sosyal mühendislik testleri

10) Sadece kurum içinden erişilen web uygulamaları sızma testleri

11) Dağıtık servis dışı bırakma (DDoS) testleri

12) Sanallaştırma sistemleri testleri

13) Kablosuz ağ testleri

14) Güvenlik duvarı testleri

15) URL ve içerik filtreleme testleri

b) Geniş Kapsamlı Sızma Testleri sadece TSE onaylı sızma testi firmalarına yaptırılabilir.

c) Gerçekleştirilen geniş kapsamlı test sonuç raporlarının içermesi gereken minimum bilgiler:

1) Yönetici Özeti

a) Sızma Testini Gerçekleştiren Firma Bilgileri

b) Sızma Testini Gerçekleştiren Şahıs Bilgileri

c) Sızma Testi Kapsamı

ç) Sızma Testi Metodolojisi ve Test Esnasında Kullanılan Sistem/Program/Ürün Bilgileri

d) Sızma Testi Sonucunda Tespit Edilen Bulguların Kritiklik Seviyesine Göre Dağılımı

2) Teknik Özet

a) Zafiyetin Önem Derecesi (Acil, Kritik, Yüksek, Orta, Düşük)

b) Zafiyetin Etkisi

c) Zafiyetin Bulunduğu Bileşenler

ç) Zafiyetin Nedeni ve Nasıl Tespit Edildiği Hakkında Açıklama

d) Alınması Gereken Önlemler

ç) Kurumsal SOME'nin yılda en az bir kez TSE tarafından belgelendirilmiş onaylı sızma testi firmalarına yaptırması gereken geniş kapsamlı sızma testleri iki sene üst üste aynı denetçiler tarafından yapılamaz.

d) Kurumsal SOME, geniş kapsamlı sızma testlerini yaptırdığı firma ve bu testlerde görev alan firma personelleri ile gizlilik sözleşmesi imzalar.

e) İşletme, Kurumsal SOME fonksiyonlarını icra etmek için hizmet aldığı kuruluşlara ve o kuruluşların hisse sahibi olduğu diğer kuruluşlara hizmet alımı süresince Geniş Kapsamlı Sızma Testi yaptıramaz.

f) İşletme, Geniş Kapsamlı Sızma Testi sonucunda bu maddeye uygun olarak oluşturduğu raporun tamamının yüklenici firma tarafından işletmeye tesliminden sonra en geç 7 iş günü içerisinde gizli resmi yazı ile Genel Müdürlüğe gönderir.

(3) Dar Kapsamlı Test;

a) Kurumsal SOME, dar kapsamlı test kapsamında; en az 6 ayda bir aşağıdaki kapsamda test ve denetimleri yapmak veya yaptırmak ile yükümlüdür:

1) İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması

2) Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması

3) Dışa açık web uygulamalarının sızma testleri

4) Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri

5) Veri tabanı yapılandırma testleri

b) Kurumsal SOME, işletmenin bilgi işlem altyapısında köklü bir değişiklik olması durumunda da 6 aylık süreyi beklemeden aynı test adımlarını gerçekleştirmek ile yükümlüdür.

c) Kurumsal SOME,işletme personeli tarafından üretilen yazılımların kullanıma geçmeden önce yazılım güvenliği ile ilgili testlerin yapılması/yaptırılmasından ve bu test sonuçlarının dokümante edilmesinden sorumludur.

(4) A grubu havacılık işletmeleri en az senede bir kez olmak üzere işletme bünyelerinde yer alan EKS/Scada sistemlerinin sızma testini yaptırmak zorundadır.

(5) B grubu havacılık işletmeleri en az 3 senede bir kez olmak üzere işletme bünyelerinde yer alan EKS/Scada sistemlerinin sızma testlerini yaptırmak zorundadır.

(6) Kurumsal SOME, yapılan güvenlik testleri sonucunda suç olabilecek iz, delil ve emare (zararlı yazılım, sızma vb.) görülmesi durumunda SGSYY ve işletmenin hukuk müşavirliği ile görüşerek gecikmeksizin kanunen soruşturmaya yetkili makamlara (savcılık/kolluk), Havacılık Sektörel SOME'sine ve USOM'a bildirimde bulunur.

(7) Kurumsal SOME, bu maddenin ikinci ve üçüncü fıkralarında tanımlanan faaliyete müteakip Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi raporunda gerekli güncellemeleri yapar.

(8) Kurumsal SOME, dar ve geniş kapsamlı sızma testleri sonrasında tespit edilen zafiyetlerin ilgili bilgi işlem personeli/hizmet alınan firma tarafından kapatılması sürecini yönetir ve takip eder.

(9) Kurumsal SOME, dar ve geniş kapsamlı sızma testleri sonrasında tespit edilen zafiyetler kapatıldıktan sonra doğrulama testlerini yapar/yaptırır. Zafiyetin kapatıldığının doğrulaması zafiyeti kapatan kişi tarafından yapılamaz. Zafiyetin kapatılmasına müteakip zafiyeti kapatan kişi/kişiler tarafından bir form düzenlenir ve bu form SGSYY'ye sunulur.

(10) Kurumsal SOME'nin, dar ve geniş kapsamlı sızma testlerinin yanı sıra gelişigüzel aralıklarla zafiyet taraması yapması/yaptırması tavsiye edilir.

(11) Kurumsal SOME, işletmenin belirlediği geniş kapsamlı test tarihlerini, test kapsamını ve testi yapacak firmanın yetkinlik sertifikalarını test tarihinden en az 1 ay önce Havacılık Sektörel SOME'sine resmi yazı ile bildirmek ile yükümlüdür. Tarihte bir değişiklik olması durumunda işletme Sektörel SOME'ye ivedilikle e-posta yoluyla bilgilendirme yapar.

(12) İşletmeler, sahip oldukları bilişim sistemlerinin ve belge/bilgilerin gizlilik, bütünlük ve erişilebilirlik yönünden güvenliğini sağlamakla yükümlüdür.

Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi

MADDE 12 - (1) Kurumsal SOME, başta bilgi işlem birimi olmak üzere işletmenin ilgili birimleri ile koordineli bir şekilde çalışarak işletmenin varlık/süreç değerlerini belirler ve söz konusu verinin gizlilik-bütünlük ve erişilebilirlik kriterlerini de gözeterek varlık/süreç ve risk değerlerini hesaplar.

(2) Kurumsal SOME, işletmenin siber güvenlik riskleri ile ilgili "Kurumsal Siber Güvenlik

Değerlendirme ve Risk Analizi" raporunu hazırlar ve üst yönetimin onayına sunar.

(3) Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi raporunun içermesi gereken minimum bilgiler şunlardır:

a) Yönetici Özeti

1) Risk Değerlendirme Metodolojisi

2) Siber Güvenlik Risklerinin Önem Derecesine Göre Sayısal Dağılımı

b) Teknik Rapor

1) Riskin Tanımı

2) Varlık/Süreç Değeri

3) Riskin Önem Derecesi (Acil, Kritik, Yüksek, Orta, Düşük)

4) Riskin Olası Etkisi

5) Riskin Bulunduğu Bileşenler

6) Riskin Gizlilik-Bütünlük-Erişilebilirlik Değerleri

7) Riskin Toplam Değeri

8) Alınması Gereken Önlemler

9) Riskin Sahibi

10) Risk Üzerinde Uygulanması Planlanan Kontrol/Kontrollerin Son Tarihi

(4) İşletme, üst yönetim tarafından onaylanan Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi Raporu'nu 7 gün içinde eksiksiz bir şekilde Genel Müdürlüğe resmi yazı ile gönderir.

(5) Kurumsal SOME, geniş ve dar kapsamlı sızma testleri sonucunda elde ettikleri bulgulara göre Kurumsal Siber Güvenlik Değerlendirme ve Risk Analiz Raporunu günceller. Güncellenen Kurumsal Siber Güvenlik Değerlendirme ve Risk Analiz Raporu'nu 7 gün içinde Genel Müdürlüğe resmi yazı ile gönderir.

ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi

MADDE 13 - (1) Kurumsal SOME kurmakla yükümlü işletmeler, kişisel verilerin, uçuş operasyon ve havayolu operasyon bilgilerinin, bilişim sistemlerinin ve endüstriyel kontrol sistemlerinin tamamını içeren ISO/IEC 27001:2013 sertifikasyonlarını TÜRKAK'a ya da ülkemizde bilinirliği olan uluslararası eşdeğerlerine akredite olmuş belgelendirme firmalarına 31.12.2020 tarihine kadar yaptırmakla yükümlüdür.

(2) İşletmeler, 13 üncü madde birinci fıkrada belirtilen kapsamdaki sertifikalarını alana kadar ISO/IEC 27001:2013 hakkındaki çalışmalarını ve iş süreçlerini 6 aylık süreler ile Genel Müdürlüğümüze raporlar.

Felaket Kurtarma Merkezi

MADDE 14 - (1) İşletme, olası bir felaket, kriz veya kesinti yaşanması durumunda iş sürekliliğinin aksamaması amacı ile farklı bir risk bölgesinde yer alan bir felaket kurtarma merkezi kurmakla veya yurtiçinde felaket kurtarma merkezi hizmeti veren firmalardan hizmet almakla yükümlüdür.

(2) Kurumsal SOME, Kurumsal Siber Güvenlik Değerlendirme ve Risk Analiz Raporu'nu da dikkate alarak felaket, kriz veya kesinti yaşanması durumunda etkin önlem alınabilmesi; itibarın, marka değerinin, değer yaratan faaliyetlerin ve paydaşların çıkarlarının korunabilmesi amaçlarıyla belirlenen operasyonların sürekliliğinin temin edilmesi veya hedeflenen zaman diliminde kurtarılabilmesinin sağlanması ve kriz öncesi duruma dönülebilmesine yönelik bir felaket kurtarma planı hazırlar. Felaket kurtarma planı, ilgili iş birimleri ile birlikte hazırlanmalı, mümkün olduğunca kapsamlı olmalı, kritik iş süreçlerinin felaket sonrası devamını, diğer önemli süreçlerin en kısa sürede başlatılabilmesini ve devamında kurumun normal işleyişe dönebilmesini sağlamalıdır.

İz Kayıtlarının Merkezi Olarak Yönetilmesi

MADDE 15 - (1) Kurumsal SOME; Kurumsal SOME Kurulum ve Yönetim Rehberi'nde yer

alan "Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri" dokümanına uygun olarak, iz kayıtlarının 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.

(2) Kurumsal SOME, iz kayıtlarının günlük olarak izleme ve incelemesini yaparak bunu dokümante eder.

(3) Kurumsal SOME, iz kayıtları üzerinde aylık analiz ve ilişkilendirme çalışması yapar; çalışma sonucunda oluşturduğu raporu SGSYY'ye sunar.

(4) Kurumsal SOME, aylık olarak yaptığı iz kayıt analiz ve ilişkilendirme çalışmasında olağan dışı herhangi bir duruma rastlarsa, bu konuda düzeltici/önleyici aksiyon alır.

İz Kayıtlarının Güvenliği

MADDE 16 - (1) Siber olaylara ilişkin tutulan iz kayıtlarına, "bilinmesi gerektiği kadar" 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 verinin şifreli olarak transfer edilmesi sağlanmalıdır.

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

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

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

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

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

İz Kayıtlarının Yönetimi ile İlgili Roller

MADDE 17 - (1) İz 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, Kurumsal SOME personelleri, yazılım geliştiriciler ve denetçilere ait görev ve sorumluluklar belirlenmelidir.

İz Kayıtlarının Saklanma Süresi

MADDE 18 - (1) İz kayıtlarının saklanma süresi belirlenmesinde; iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği parametreleri göz önünde bulundurulmalıdır. İşletmelerin tabi oldukları yasal mevzuatları gereği uyması gereken süreler saklıdır.

Ortak Zaman Sunucusu Kullanımı

MADDE 19 - (1) 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 işletmeler için saat dilimi (timezone) de dikkate alınmalıdır.

Siber Olay Öncesi Diğer Sorumluluklar

MADDE 20 - (1) Kurumsal SOME; siber olay öncesi, esnası ve sonrasındaki görev ve sorumlulukları ile işletmenin diğer paydaşları ile ilişkilerini koordine ederek siber olay yönetim ve bilgi güvenliği ile ilgili talimatlarını (siber olay müdahale, siber olay bildirim süreci vb.) hazırlar.

(2) Kurumsal SOME, Ulusal Siber Güvenlik Tatbikatı başta olmak üzere sektörel ve/veya ulusal kapsamda yapılan tatbikatlara katılmakla yükümlüdür.

(3) Kurumsal SOME, USOM ve Havacılık Sektörel SOME tarafından düzenlenen toplantı ve etkinliklere katılmakla yükümlüdür.

(4) Kurumsal SOME, siber güvenlik ürünlerinin (saldırı tespit sistemi, güvenlik duvarı, balküpü sistemi vb.) belirlenmesi sürecinde bilgi işlem birimi ile koordineli çalışır.

(5) Kurumsal SOME, güvenlik ürünlerinin uygulama seviyesi işletimi ile ilgili politikaları bilgi işlem ile koordineli şekilde belirler.

(6) İşletme, USOM ve Genel Müdürlüğümüz tarafından talep edilen her türlü bilgi/belge ve raporlamaları eksiksiz bir biçimde ve bildirim tarihi geçmeden belirtilen iletişim yoluyla bildirmek ile yükümlüdür.

(7) İşletme, USOM ve/veya Havacılık Sektörel SOME'si tarafından iletilen ihbarlar ile ilgili gecikmeksizin aksiyon almakla ve aldığı aksiyonları USOM ve Havacılık Sektörel SOME'sine bildirmekle yükümlüdür.

(8) İşletmeler, kendi içlerinde geliştirdikleri yazılımları Tübitak Bilgem Siber Güvenlik Enstitüsü tarafından yayımlanan Güvenli Yazılım Geliştirme Temel Kuralları dokümanına uygun bir biçimde geliştirmekle yükümlüdür.

(9) Kurumsal SOME'ler işletmeleri hakkında siber güvenlik istihbaratı toplar/toplatır.

Siber Olay Esnası Diğer Sorumluluklar

MADDE 21 - (1) Kurumsal Some, işletmede herhangi bir siber olayın gerçekleştiği durumda Ek-6'da yer alan akış diyagramına göre görevlerini icra eder.

(2) Kurumsal SOME; siber olay öncesi, müdahale esnası ve sonrasında bilişim sistemlerine yetkisiz erişim yapılmaması için gerekli tedbirleri almak/aldırmakla yükümlüdür.

(3) Kurumsal SOME, siber olay müdahale akışı içinde suç unsuruna rastlanması halinde savcılık, kolluk makamı vb. makamlara haber vermek zorundadır.

Siber Olay Sonrası Diğer Sorumluluklar

MADDE 22 - (1) İşletmede bir siber olay gerçekleştikten ve olaya müdahale edildikten sonra Kurumsal SOME aşağıdaki görevleri icra eder:

a) Zaman geçirmeden olaya neden olan açıklığı belirler/kapatır ve çıkarılan dersleri kayıt altına alır.

b) Siber olay ile ilgili bilgileri USOM tarafından belirlenen kriterlere uygun şekilde (Ek-7 Siber Olay Değerlendirme Formunu doldurarak) Havacılık Sektörel SOME'sine gönderir ve kayıt altına alır.

c) Olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler SGSYY'ye arz edilir.

ç) Yaşanan siber olayların türlerini, miktarlarını ve işletmeye maliyetini ölçüp kayıt altına alır.

d) Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporunı hazırlar; üst yönetim, Havacılık Sektörel SOME'sine resmi yazı ile iletir.

Diğer Sorumluluklar

MADDE 23 - (1) Kurumsal SOME, bu talimata ilaveten Milli Sivil Havacılık Güvenlik Programı eki olan "Siber Tehditlere Karşı Yapılacak İşlemler Talimatı"nda yer alan önlemleri de almakla yükümlüdür.

(2) Kurumsal SOME, görevlerini "Kurumsal SOME Kurulum ve Yönetim Rehberi" ve Ulusal

Siber Güvenlik Stratejisi ve Eylem Planlarına uygun şekilde yerine getirecektir.

Bilgi Sistemlerine İlişkin Destek Hizmeti Alımı Sürecinin Yönetimi

MADDE 24 - (1) İşletme üst yönetimi; bilgi sistemleri/siber güvenlik kapsamında alınacak destek hizmetlerine ilişkin olarak, söz konusu hizmetin destek hizmeti alımı yoluyla gerçekleştirilmesinin işletme açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve destek hizmeti kuruluşu ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak yeterli bir gözetim mekanizması tesis eder. Tesis edilecek gözetim mekanizması ile asgari olarak;

a) Bilgi sistemleri altyapısına ilişkin destek hizmeti alımının doğuracağı risklerin tüm yönleriyle değerlendirilmesini,

b) Destek hizmeti kuruluşunun seçiminde gerekli özenin gösterilmesini,

c) Destek hizmeti alımı kapsamındaki tüm sistem ve süreçlerin işletmenin kendi risk yönetimi, güvenlik ve müşteri mahremiyeti politikalarına uygun olmasını,

ç) Kritik varlıklar ile ilgili destek hizmeti kapsamında işletme verilerinin destek hizmeti kuruluşuna aktarılmasının gerekli olduğu durumlarda, destek hizmeti kuruluşunun güvenlik konusundaki prensip ve uygulamalarının en az işletmenin uyguladıkları düzeyde olmasını,

d) Kritik varlıklar ile ilgili destek hizmeti alımı kapsamındaki faaliyetlerin işletme bünyesinde gerçekleştirilmesi durumunda hangi denetimlere tabi tutulması öngörülüyorsa, herhangi bir kapsam daraltılmasına gidilmeden işletme tarafından yılda en az 1 kere aynı denetimlere tabi tutulması ve faaliyetin destek hizmeti alımı yoluyla gerçekleştirilmesi nedeniyle ek denetim ihtiyacı duyuluyorsa bunların da gerçekleştirilmesini,

e) Destek hizmeti alımına ilişkin hususların işletme iş süreklilik planı göz önünde bulundurularak düzenlenmesini ve gerekli önlemlerin alınmasını, destek hizmeti kuruluşunun bu kapsamdaki yükümlülüklerinin sözleşme ile netleştirilmesini
temin eder.

(2) Destek hizmeti alımının, planlananın dışında sonlanması veya kesintiye uğraması durumlarına ilişkin risklerin yönetilmesine uygun bir çıkış stratejisi belirlenir.

(3) Destek hizmeti alımına ilişkin koşul, kapsam ve her türlü diğer tanımlama ilgili destek hizmeti kuruluşunca da imzalanmış olacak şekilde sözleşmeye bağlanır. Sözleşme, asgari olarak aşağıdaki hususları içerir:

a) Hizmet seviyelerine ilişkin tanımlamalar

b) Hizmetin sonlanma koşulları

c) İşletmeye ait iş süreklilik planının sekteye uğramasını önleyecek şekilde destek hizmeti kuruluşunun alması gereken önlemlere ilişkin hükümler

ç) İşletmenin güvenlik politikası dâhilinde hassasiyet arz eden konulara ilişkin gereklilikler

d) Sözleşme kapsamında üretilecek olan ürünün sahipliğini ve fikri mülkiyet haklarını da göz önünde bulundurarak düzenleyen hükümler

e) Sözleşmede destek hizmeti kuruluşları için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler

f) Destek hizmeti alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler

g) İşletmenin tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde destek hizmeti kuruluşları için de uygulanmasını sağlayacak hükümler

(4) İşletme; güvenlik politikasındaki ilkeler doğrultusunda ve destek hizmeti alımından kaynaklanan riskleri kontrol altında tutmak üzere organizasyonuna ilişkin gerekli değişiklikleri yapar, idari prosedürler tanımlar, bu kapsamda alınacak önlemleri ilgili tüm bölümlerin günlük işlemlerine ve sistemlerine entegre eder, destek hizmeti kuruluşuyla ilişkileri yürütecek yeterli bilgi ve tecrübeye sahip bir sorumlu atar.

(5) Destek hizmeti kuruluşlarına verilen erişim yetkileri özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu yetkiler için risk değerlendirmesi yapılır, buna göre eğer gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim yetkisi, erişilen verinin değeri, destek hizmeti kuruluşu tarafından yürütülmekte olan kontroller ve bu erişimin işletme bilgilerinin güvenliği üzerindeki etkileri dikkate alınır.

(6) İşletme üst yönetimi, destek hizmeti alımı yoluyla gerçekleştirilen servisler için; servisin erişilebilirliğini, performansını, kalitesini, bu servis kapsamında gerçekleşen güvenlik ihlali olaylarını ve destek hizmeti kuruluşunun güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip eder.

ÜÇÜNCÜ BÖLÜM
Cezai Yaptırımlar

MADDE 25 - (1) İşletmeler Genel Müdürlük Sektörel SOME'si tarafından haberli veya habersiz olarak denetlenir. Yapılan denetimler sonucunda;

a) Tespit edilen bulgular, Ek-8 Bulgu Seviyeleri Listesi'nde belirtilen bulgu kapatma sürelerine uygun bir şekilde kapatılması için BYS sistemi üzerinden işletmeye bildirilir.

b) Genel Müdürlük tarafından uygun görülen tarihte eksiliklerin giderilmemiş olması durumunda ilgili işletmeden savunma talep edilir. Söz konusu savunmanın yeterli olmaması durumda Genel Müdürlük, ilgili işletmeye 2920 sayılı Türk Sivil Havacılık Kanunu'nun 143 üncü maddesi gereği Sivil Havacılık Genel Müdürlüğü Tarafından Verilecek İdari Para Cezaları Hakkında Yönetmelik (SHY-İPC) hükümlerine göre idari para cezası uygular.

c) Tespit edilen eksikliklerin önemi göz önüne alınarak bu maddede belirlenen adımlardan bir veya daha fazlası Genel Müdür onayı ile atlanabilir.

(2) Genel Müdürlük tarafından yapılan inceleme ve denetlemelerde adli soruşturmaya konu olabilecek hususlara rastlanılması durumunda adli makamlara suç duyurusunda bulunulur.

DÖRDÜNCÜ BÖLÜM
Son Hükümler

Yürürlükten Kaldırılan Genelge

MADDE 26 - (1) 02/08/2016 tarihli Genel Müdürlüğümüz HGD/2015-1 Genelgesi 01.01.2020 tarihinde yürürlükten kalkacaktır.

Yürürlük

MADDE 27 - (1) Bu talimat yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 28 - (1) Bu Talimat hükümlerini Sivil Havacılık Genel Müdürü yürütür.

EKLER:

EK-1 - SGSYY Form_4 (hgd)-SİBER

EK-2 - Siber Güvenlik Faaliyet Raporu Şablonu

EK-3 - Kurumsal SOME Personeline Yönelik Siber Güvenlik Eğitimleri ve İçerikleri

EK-4 - Sosyal Mühendislik Testi Sonuç Raporu
EK-5 - Bilişim Sistemleri Güvenlik Testleri Süreci
EK-6 - Siber Olay Müdahale Akış Diyagramı
EK-7 - Siber Olay Değerlendirme Formu
EK-8 - Bulgu Seviyesi Listesi