SİVİL HAVACILIK İŞLETMELERİNE YÖNELİK SİBER GÜVENLİK TALİMATI (SHT-SİBER)

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

Amaç

MADDE 1 -(1) Bu Talimatın amacı; sivil havacılık işletmelerinin siber tehditlere karşı alması gereken önlemleri ve havacılık işletmelerince kurulması gereken Kurumsal Siber Olaylara Müdahale Ekibi'nin işletme organizasyonu içerisindeki yerini, kapasite planlamasını, personelin niteliklerini, alması gereken eğitimleri, işletmelerin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları, iç ve dış paydaşlar ile iletişime ilişkin usul ve esaslarını belirlemektir.

Kapsam

MADDE 2 -(1) Bu Talimat, Genel Müdürlük tarafından yetkilendirilen tüm sivil havacılık işletmelerini 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, 2020-2023 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 tanımların açıklamaları aşağıda belirtildiği gibidir;

a) **1'inci Grup Havacılık İşletmeleri:** Havayolu işletmeleri, havalimanı işletmeleri, terminal işletmeleri, seyrüsefer hizmet sağlayıcıları,

b) **2'nci Grup Havacılık İşletmeleri:** A grubu Yer hizmeti kuruluşları, 100 kişiden daha fazla kişinin çalıştığı hava aracı bakım ve üs bakım kuruluşları ve SHGM tarafından belirlenerek resmi yazı ile bildirilen havacılık işletmeleri,

c) **3'üncü Grup Havacılık İşletmeleri:** 1'inci ve 2'nci Grup Havacılık İşletmeleri dışında kalan tüm sivil havacılık işletmeleri,

ç) **7x24 Esası:** Bir haftanın 7 günü 24 saat boyunca aralıksız olarak ilgili sistemin işletilmesi,

d) **A Grubu Yer Hizmeti Kuruluşları:** SHY-22 Havalimanları Yer Hizmetleri Yönetmeliği kapsamında A grubu çalışma ruhsatına sahip işletmeler,

e) **Balküpü :** Bilgi sistemlerine yetkisiz erişim sağlamak isteyen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sistemler (sunucu, uygulama, servis vb.),

f) **Beyaz Liste Yazılımlar:** İşletme bilgi teknolojileri ve operasyonel teknolojileri varlıklarına yüklenmesi uygun bulunan yazılımların listesi,

g) **Bilgi Teknolojileri İş Süreklilik Komitesi:** Bilgi teknoloji kritik varlık ve süreçlerin iş

sürekliliğinin sağlanması adına üst yönetimin liderliğinde kurulan ve ilgili tüm paydaş yönetici ve ihtiyaç duyulması halinde uzmanlarının katılım sağladığı komitedir.

ğ) **Bilinmesi Gerektiği Kadar Prensibi:** Bir varlığı, süreci veya bilgiyi sadece görev ve sorumlulukları gereği öğrenmekle, incelemekle, gereğini yerine getirmekle ve korumakla sorumlu bulunanların yetkileri düzeyinde bilgi sahibi olması ve nüfuz etmesini ifade eder.

h) **BT Varlıkları:** Bilgi teknolojileri varlıkları,

ı) **Genel Müdür:** Sivil Havacılık Genel Müdürü,

i) **Genel Müdürlük:** Sivil Havacılık Genel Müdürlüğü,

j) **Görevler Ayrılığı İlkesi:** Görevler ayrılığı ilkesi hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi amacıyla görevlerin farklı personel tarafından yapılmasının sağlanması,

k) **Havacılık İşletmeleri:** Sivil havacılık sektöründe faaliyet gösteren işletmeler,

l) **Hizmet Alınan Kuruluş:** Siber güvenlik ile ilgili işletmeye hizmet veren kurum veya kuruluşlar,

m) **İşletme:** Sivil havacılık sektöründe faaliyet gösteren işletmeler,

n) **İşletme Yönetimi:** İşletme üst yönetimi ve varsa yönetim kurulu,

o) **İz kaydı:** Operasyonel bir işlemin başlangıcından bitişine kadar adım adım takip edilmesini sağlayacak kayıtlar,

ö) **Kara Liste Yazılımlar:** İşletme bilgi teknolojileri ve operasyonel teknolojileri varlıklarına yüklenmesi uygun bulunmayan yazılımların listesi,

p) **Katmanlı Güvenlik Mimarisi:** Bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği güvenlik mimarisi,

r) **Kırmızı Takım Çalışması:** Bir işletmenin güvenlik cihazlarını, ağlarını, çalışanları, uygulamalarını ve fiziksel güvenlik kontrollerini gerçekte bir saldırıya ne kadar dayanabileceğinin ölçülmesi için tasarlanan tam kapsamlı ve çok katmanlı saldırı simülasyon çalışmalarının tümü,

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

ş) **Kritik Bilgi veya Veri:** Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara neden olabilecek, gizlilik, bütünlük ve erişilebilirliğinin olumsuz yönde etkilenmesinin işletmeye çok ciddi maddi veya manevi zarar vereceği yada iş sürekliliği kesintisine uğratabilecek her türlü bilgi, veri ve kişisel verilerin tümü,

t) **Kritik Varlıklar:** İşletmenin iş sürekliliğini ciddi anlamda sekteye uğratabilecek ve çalışmaması durumunda Türk Sivil Havacılık Sektörünü veya işletmeyi maddi ve itibari yönden zedeleyebilecek sistem, bilgi, belge vb. bütünü,

u) **Kurumsal SOME:** Temel görevleri Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ'inde ve bu Talimatta yer alan, görev yaptığı işletmelerde bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibi,

ü) **Kurumsal SOME Yöneticisi:** 1'inci Grup Havacılık İşletmelerinde siber güvenlikten sorumlu yetkili yönetici, 2'nci Grup Havacılık İşletmelerinde bilgi teknolojileri birimindeki en yetkili yönetici,

v) **Minimum Yetki Prensibi:** Bir varlığa veya kişiye sadece iş ihtiyacını karşılayacak ölçüde yetki verilmesi,

y) **Minimum Zaman Prensibi:** Bir varlığa veya kişiye sadece iş ihtiyacını karşılayacak sürede yetki verilmesi,

z) **OT Varlıkları:** Havacılık sektörü operasyonlarının sürdürülebilmesi için kullanılan tüm sistem, uygulama ve verileri sağlayacak kayıtları,

aa) **SHGM Hizmet Tarifesi:** SHGM web sayfası üzerinden yıllık olarak yayınlanan Ulaştırma ve Altyapı Bakanı onaylı hizmet tarifesi dokümanı,

bb) **Siber Güvenlik Durumsal Farkındalığı:** Bulunulan zaman diliminde işletme sistemlerinin gizlilik, bütünlük ve erişilebilirlik açısından durumu,

cc) **Siber Olay:** Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi veya ihlal teşebbüsünde bulunulması,

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

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

ee) **Tedarikçi Çıkış Stratejisi:** Hizmet alınan bir tedarikçi firmanın hizmet veya servis verememesi yada işletmenin bir tedarikçi firma ile çalışmayı durdurma kararı alması durumunda alınması planlanan aksiyonların dokümante edilmiş hali,

ff) **Tehdit Avcılığı :** Tehdit istihbarat verilerini temel alan, mevcut güvenlik çözümlerinden kaçan olası siber güvenlik ihlal olaylarının reaktif, proaktif ve tekrarlı olarak arama, tespit etme ve izole etme süreci,

gg) **Trafik Işığı Protokolü:** Ek-20'de yer alan ve işletmenin dış paydaşlarıyla bilgi paylaşması durumunda, paylaşılacak bilginin gizlilik derecesini ve hangi paydaşlar ile paylaşılmasının uygun olduğunu ifade eden protokol,

hh) **Veri İşleme:** Verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem,

ıı) **Yetkili Otorite:** Sivil Havacılık Genel Müdürlüğü

(2) Bu Talimatta geçen kısaltmaların açıklamaları aşağıda belirtildiği gibidir**;**

a) **ATM:** Hava Trafik Yönetimi,

b) **BGYS:** Bilgi Güvenliği Yönetim Sistemi,

c) **BT:** Bilgi teknolojileri,

ç) **CEH:** Etik Hacker Sertifikası,

d) **CISA:** Bilgi Sistemleri Denetçi Sertifikası,

e) **CISM:** Bilgi Sistemleri Yöneticisi Sertifikası,

f) **CISSP:** Bilgi Sistemleri Profesyoneli Sertifikası,

g) **CRISC:** Risk ve Bilgi Sistemleri Kontrol Sertifikası,

ğ) **DMZ:** Savunmasız bölge,

h) **ECSA:** EC-Council Güvenlik Analisti Sertifikası,

ı) **EKS:** Endüstriyel Kontrol Sistemi,

i) **FKM:** Felaket Kurtarma Merkezi,

j) **GIAC:** Küresel Bilgi Güvencesi Sertifikasyonu,

k) **GSEC:** GIAC Güvenlik Temelleri,

l) **IEC:** Uluslararası Elektroteknik Komisyonunu,

m) **ISO:** Uluslararası Standartlar Organizasyonu,

n) **MBCO:** En küçük iş sürekliliği hedefi,

o) **NTP:** Ağ zaman protokolü,

ö) **OT:** Operasyonel teknoloji,

p) **RPO:** Olası bir felaket anında kabul edilebilir kayıp miktarı,

r) **RTO:** Olası bir felaket anında normal düzene geri dönüş için kabul edilen kesinti süresi,

s) **SCADA:** Merkezi denetleyici kontrol ve veri toplama sistemi,

ş) **SGSYY:** Siber Güvenlikten Sorumlu Yetkili Yönetici,

t) **SHGM:** Sivil Havacılık Genel Müdürlüğü,

u) **SİP:** SOME İletişim Platformu,

ü) **SLA:** Hizmet seviyesi anlaşması,

v) **SOME:** Siber Olaylara Müdahale Ekibi,

y) **TSE:** Türk Standartları Enstitüsü,

z) **USOM:** Ulusal Siber Olaylara Müdahale Merkezi.

(3) Bu Talimatta belirtilmeyen tanımlar için, 14/10/1983 tarihli ve 2920 sayılı Türk Sivil Havacılık Kanunu ile 15/07/2018 tarihli ve 4 sayılı Cumhurbaşkanlığı Kararnamesi'nde, ilgili diğer mevzuatta ve ülkemizin üyesi bulunduğu uluslararası sivil havacılık kuruluşları tarafından yayımlanan dokümanlarda belirtilen tanımlar geçerlidir.

İKİNCİ BÖLÜM
Genel Hususlar ve Uygulama Esasları

Siber güvenlik kapsamında yönetim sorumluluğu

MADDE 5 -(1) Havacılık işletmeleri aşağıdaki belirtilen durumlardan sorumludur:

a) Bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele alır.

b) Bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağını tahsis eder.

c) Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini sağlar.

ç) Bilgi sistemlerinin kullanımından kaynaklanan siber risklerin yönetilmesi için etkin bir gözetim yürütür.

(2) İşletme bünyesinde siber güvenliğin sağlanmasında nihai sorumluluk işletme üst yönetimi ve varsa yönetim kurulundadır. İşletme yönetimi, bilgi sistemlerine ve operasyonel sistemlere ilişkin siber güvenlik önlemlerinin alınması hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında işletme yönetimi, işletmenin tamamında, SHGM düzenlemelerine uygun olarak, uygulanmasını gözetmekle yükümlü olduğu bir ISO 27001 Bilgi Güvenliği Yönetim Sistemi tesis eder. Söz konusu yönetim sisteminin aşağıdaki faaliyetleri de içermesi esastır:

a) Etkin bir varlık değerlendirme sürecinin oluşturulması ve bu sürecin sürekli olarak güncel kalmasının sağlanması,

b) İşletme varlıklarına yönelik olarak düzenli bir şekilde siber güvenlik risk ve tehdit değerlendirme çalışmalarının yapılması,

c) Siber güvenliğin sağlanması amacıyla oluşturulan politika, prosedür ve süreç dokümanlarının işletmenin tamamında uygulanmasının sağlanması,

ç) Olası siber güvenlik ihlallerini tespit etme, engelleme ve olay müdahale mekanizmalarının kurulması,

d) İşletme genelinde belirlenen varlık veya süreç envanterine uygun olarak tüm bilgi teknolojileri ve havacılık sektörü hizmetleri, EKS ve SCADA sistemlerinde görevler ayrılığı prensibi ile tutarlı etkin bir kimlik doğrulama ve erişim yönetiminin tesis edilmesi,

e) Siber güvenliğin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların siber güvenlik açısında test edilmesi, denetlenmesi ve sonuçlarının takip edilerek raporlanması sürecinin oluşturulması ve işletilmesi,

f) İşletme varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli güncellemelerinin ve yama işlemlerinin gerçekleştirilmesi,

g) Üst yönetim de dahil olmak üzere tüm işletme çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi işletmenin siber güvenliğini ilgilendiren tüm paydaşlarına yönelik siber güvenlik farkındalığını artıracak çalışmalar yapılması,

ğ) İşletme siber güvenlik kritik süreçlerin veya operasyonların sürekliliğini sağlamak üzere bilgi teknolojileri ve bilgi teknolojileri kullanan sistemler ile ilgili tüm süreçlerin iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve işletme yönetimi onaylı bir bilgi sistemleri süreklilik planı hazırlanması, süreç sorumlusu atanması ve Bilgi Teknolojileri İş Süreklilik Komitesi tesis edilmesi,

h) Dış hizmet alımlarının yönetimi kapsamında siber güvenliği ilgilendiren hususlarda Kurumsal SOME biriminin değerlendirme süreçlerinde yer almasının sağlanması ve tedarikçi değerlendirme süreçlerinde siber güvenlik unsurlarının değerlendirilmesi,

ı) Havacılık işletmeleri, işletme BT ve OT süreçlerini etkileyebilen, BT ve OT varlıklarına erişebilen, veri işleyebilen, saklayabilen , aktarabilen tüm süreçlerine yönelik dış hizmet alımlarında yüklenici firmadan alacakları hizmet ve sistemi sağlayan birimleri kapsaması zorunlu olmak koşuluyla en az işletmenin siber güvenlik kapsamında uyması gereken ulusal ve uluslararası standart ve düzenlemelerin zorunlu kıldığı siber güvenlik seviyesine uygun hizmet talep edilmesi ve denetim faaliyetleri icra edilmesi.

Siber güvenlik strateji planı

MADDE 6 -(1) 1'inci Grup Havacılık İşletmeleri, işletme yönetimi tarafından onaylanacak bir Siber Güvenlik Strateji Planı oluşturur.

(2) Siber Güvenlik Strateji Planı;

a) Mevcut siber güvenlik yapılanması analizi,

b) Siber güvenlik yapılanması kaynak-ihtiyaç analizi,

c) Güncel siber tehditler ve siber atak yüzeyi değişimi değerlendirilmesi,

ç) Siber güvenlik yapılanmasının iyileştirilmesi için planlanan eylem maddelerinin; proje başlangıç tarihi, proje bitiş tarihi, sorumlu paydaşlar ve proje içeriği detayları

hususlarını içerecek şekilde hazırlanır ve SHGM'ye resmi yazı ile gönderilir.

ATM güvenlik planı

MADDE 7 -(1) Seyrüsefer hizmet sağlayıcı işletmeler, Ek-1'de yer alan ATM Güvenlik Planı Kapsamına uygun olarak havalimanı bazında ATM güvenlik planlarını oluşturur. Söz konusu plan;

a) Havacılık Acil Durum Koruma ve Güvenlik Şefliği Birim Sorumlusu,

b) Elektronik Şefliği Birim Sorumlusu,

c) Terminal Elektronik ve BT Şefliği Birim Sorumlusu,

ç) Hava Seyrüsefer Şefliği Birim Sorumlusu

Koordinesi ile oluşturulur ve,

d) Kurumsal SOME Yöneticisi,

e) Havalimanı Müdürü

tarafından imzalanır.

(2) ATM Güvenlik Planı, Ek-2'de yer alan ATM Güvenlik Planı Kontrol Formunun eksiksiz doldurulmuş hali ve SHGM Hizmet Tarifesinde belirtilen ücret dekontu ile birlikte SHGM'ye onay için resmi yazı ile gönderilir.

(3) ATM Güvenlik Planında bir değişiklik olması durumunda Seyrüsefer Hizmet Sağlayıcı İşletmeler güvenlik planını revize ederek en geç 30 gün içerisinde SHGM onay işlemlerini tekrarlar.

Siber güvenlik kapsamında organizasyonel yapı

MADDE 8 -(1) 1'inci ve 2'nci Grup Havacılık İşletmeleri, işletme siber güvenlik faaliyetlerini yürütecek bir Kurumsal SOME birimi kurmakla yükümlüdür.

(2) 1'inci ve 2'nci Grup Havacılık İşletmeleri, Ek-3'te yer alan Kurumsal SOME Kurulum ve Yönetim Rehberi'nin Ek-5'inde yer alan Kurumsal SOME'ler için Gereksinim Listesi'ne uygun şekilde görevlerini icra eder.

(3) 1'inci Grup Havacılık İşletmeleri, doğrudan işletmenin Yönetim Kurulu Başkanına veya Genel Müdürüne bağlı bir Siber Güvenlikten Sorumlu Yetkili Yönetici atayarak, bu yönetici liderliğinde Kurumsal SOME yapılanmasını oluşturur. Bu yönetici, yapacağı uygulamalardan işletme yönetimine ve SHGM'ye karşı sorumludur. SGSYY işletmenin organizasyon şemasında yer alır ve işletme üst yönetim toplantılarında bulunur.

(4) İşletme yönetimi tarafından atanmış olan SGSYY Kurumsal SOME yönetim görevini üstlenir ve işletme bünyesinde görevlerin ayrılığı ilkesi kapsamında Kurumsal SOME biriminin BT ve OT süreçlerinde icra ettiği denetim ve gözetim görevleri dışında hiçbir görev alamaz.

(5) 2'nci Grup Havacılık İşletmeleri Kurumsal SOME birimlerini bilgi teknolojileri birimindeki en yetkili yöneticiye bağlı bir yapıda oluşturur.

(6) 3'üncü Grup Havacılık İşletmelerinin Kurumsal SOME birimi oluşturma zorunluluğu bulunmamakla birlikte, söz konusu işletmeler mevcut bilgi teknolojileri yapılanmaları kapsamında siber güvenlik yapılanmalarını oluşturur.

Kurumsal SOME kapsamında insan kaynağı

MADDE 9 -(1) İşletmenin, Kurumsal SOME kapsamında sorumlu olduğu görevler konunun önemi ve hassasiyeti nedeniyle işletme bünyesinde yürütülmelidir. Kurumsal SOME yönetim fonksiyonu dışında kalan görevler hizmet alımı yoluyla temin edilebilir.

(2) Kurumsal SOME görevlerinin bir firmadan hizmet alımı yoluyla temin edilmesi durumunda firma ile SLA ve gizlilik sözleşmesi yapılır.

(3) Kurumsal SOME Yöneticisi hiçbir şekilde hizmet alımı yoluyla temin edilemez. Bu nedenle, Kurumsal SOME Yöneticisi işletme çalışanı olmak zorundadır.

(4) İşletmeler, Kurumsal SOME görevlerini yerine getirmek üzere yeteri kadar personel görevlendirir veya yeteri kadar personel ile hizmet alımı yapar.

(5) Bu Talimatta belirtilen Kurumsal SOME Görev ve Sorumlulukları işletme içerisindeki başka birimlere devredilemez.

(6) 1'inci Grup Havacılık İşletmelerinde, Kurumsal SOME yapılanması kapsamında görevlendirilmesi planlanan personelin nitelik ve nicelik anlamında yeterliliği SGSYY tarafından değerlendirilir.

(7) Kurumsal SOME' de görev yapan personelin görev tanımları yazılı olarak dokümante edilerek ilgili personele tebliğ edilir.

(8) Kurumsal SOME' de görev yapması planlanan personelin görev tanımlarında bu Talimatın Kurumsal SOME Görev ve Sorumlulukları başlığı altında yer alan Kurumsal SOME görevleri dışında görev yapmalarına olanak sağlayacak hiçbir madde bulunamaz.

(9) 2'nci Grup Havacılık İşletmelerinde kurulması planlanan Kurumsal SOME birimlerinde yönetim görevini yerine getirecek Kurumsal SOME Yöneticisi Madde 9.8'de istenen zorunluluktan muaftır.

(10) Kurumsal SOME yapılanması hususunda değişiklik olması durumunda en geç 5 iş günü içerisinde SHGM'ye resmi yazı ile bildirim yapılır.

Siber güvenlikten sorumlu yetkili yöneticinin atanması

MADDE 10 -(1) 1'inci Grup Havacılık İşletmeleri, faaliyette bulundukları sürece SGSYY bulundurur. Bu yönetici, yapacağı uygulamalardan işletme yönetimine ve SHGM'ye karşı sorumludur.

Siber güvenlikten sorumlu yetkili yönetici onay süreci

MADDE 11 -(1) SGSYY'nin uygunluğu, SHGM tarafından aşağıdaki belge ve bilgiler değerlendirilerek belirlenir, uygun olanlara "Siber Güvenlikten Sorumlu Yetkili Yönetici Personel Onay Belgesi" düzenlenir. SGSYY'nin onaylanmasında aranacak şartlar ve istenilen belgeler şunlardır:

a) En az lisans derecesine sahip olduğunu gösteren diploma,

b) Doldurulmuş ve imzalanmış Ek-4'te yer alan Form-4 başvuru formu,

c) İş Sözleşmesi,

ç) İletişim bilgilerini de içerecek şekilde hazırlanmış özgeçmiş,

d) Nüfus cüzdanı örneği,

e) 08.06.2009 tarih ve SHT-17.1 talimat kodlu Tüm Havaalanları Giriş Kartı Talimatı'nın 14'üncü maddesindeki şartları taşımak,

f) Ek-5'de yer alan uluslararası geçerliliğe sahip siber güvenlik sertifikalarından en az 1 tanesine sahip olmak,

g) SHGM Hizmet Tarifesine göre yatırılmış ücret dekontu

Siber güvenlikten sorumlu yetkili yöneticinin görev ve sorumlulukları

MADDE 12 -(1) SGSYY'nin başlıca görevleri ve sorumlulukları aşağıda belirtilmiştir.

a) Kurumsal SOME birimini yönetmek,

b) Havacılık sektörünü etkileyen ulusal ve uluslararası siber güvenlik mevzuatını takip ederek, yeni kuralları ve tavsiyeleri yürürlüğe koymak,

c) Yürürlüğe koyulan politika, prosedür ve uygulamaların yerine getirildiğini denetlemek,

ç) Politika ve prosedürlerin yeterliliğini ve işletme içi uyumu gözlemlemek,

d) Siber güvenlik konusunda, işletmeye ait Genel Müdürlük, diğer BT ve OT operasyonlarının yürütüldüğü işletmeye ait diğer ofis ve merkezler, havalimanı ve temsilciliklerde sorumlu olmak,

e) İşletmenin siber güvenlik strateji planını hazırlamak, yazılı olarak hazırlanan stratejik planı üst yönetime onaylatmak,

f) Siber güvenlik strateji planı ile belirlenmiş eylem maddelerinin gerçekleştirilmesini takip etmek, ilgili eylem maddelerinin gerçekleşmemesi veya değiştirilmek istenmesi durumunda işletme üst yönetimine Ek-6'da yer alan formu kullanarak raporlamak,

g) İşletme öz kaynakları veya hizmet alım yöntemi ile temin edilen hizmetlerin siber güvenlik denetimlerini gerçekleştirilmesini sağlamak, düzeltici faaliyetlerin yerine getirilmesini koordine etmek,

ğ) Düzeltici faaliyetler ile ilgili raporlama ve kayıt sistemini oluşturmak,

h) ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı dahilinde yapılan iç denetlemelerin ve tetkiklerin koordinasyonunu sağlamak,

ı) Siber güvenlik alanında gereksinim duyulan kaynakları araştırılarak üst yönetime sunmak,

i) SHGM ile siber güvenlik ile ilgili tüm konularda iletişim noktası olup koordinasyonu sağlamak,

j) Gerek Kurumsal SOME personelinin gerekse işletme bünyesinde görev alan diğer personelin siber güvenlik farkındalığını ve işletme siber güvenlik kültürünü artıracak eğitim, seminer vb. programları düzenlemek,

k) Siber güvenlik risk analizi ve tehdit değerlendirmesi yaparak, alınacak ilave önlemleri belirlemek, planlamak ve uygulamak,

l) Siber güvenlik ile ilgili diğer faaliyetlerin kayıtlarının tutulmasını sağlamak,

m) İşletme siber güvenlik faaliyetlerini denetlemek ve iyileştirme çalışmaları gerçekleştirmek,

n) Olası bir siber ihlal durumunda siber olay müdahale sürecini yönetmek,

o) Kurumsal SOME ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi faaliyetlerinin yeterlilik ve uygunluğunu ölçmek amacıyla performans değerlendirmeleri yapmak, sonuçları üst yönetime ve SHGM'ye raporlamak.

Siber güvenlikten sorumlu yetkili yöneticinin görevden alınması

MADDE 13 -(1) SHGM tarafından yapılan inceleme ve denetlemelerde, siber güvenlik yönetiminde gerekli faydayı belirli bir süreçte sağlayamayan veya uygulamalarda olumsuzluk ya da havacılık güvenliğini direk etkileyen bir kusur tespit edildiğinde, işletme SGSYY'sinin değiştirilmesi

veya siber güvenlik yapılanmasının gözden geçirilmesi, SHGM tarafından istenebilir.

(2) SGSYY'nin aşağıda belirtilen suçlar ve kanunlarda belirtilen suçlardan hüküm giymesi halinde, işletme tarafından derhal SGSYY görevinden alınır ve ivedilikle SHGM'ye bilgilendirme yapılır.

a) Türk Ceza Kanunu'nda tanımlanan Göçmen Kaçakçılığı ve İnsan Ticareti Suçları, Yağma, Nitelikli Dolandırıcılık Suçları, Uyuşturucu Alıp Satma, Aracılık Etme Suçları, Suç İşleme Amacıyla Örgüt Kurma Suçu, Zimmet, İrtikap, Rüşvet, Kamu Görevine Ait Araç ve Gereçleri Suçta Kullanma Suçları, 4. Kısmında belirtilen Millete ve Devlete Karşı İşlenen Suçlar başlıklı 3.Bölümde yer alan Devletin Egemenlik Alametlerine ve Organlarının Saygınlığına Karşı Suçlar, 4. Bölümde; Devletin Güvenliğine Karşı Suçlar, 5. Bölümde yer alan Anayasal Düzene ve Bu Düzenin İşleyişine Karşı Suçlar, 6. Bölümde yer alan Milli Savunmaya Karşı Suçlar, 7. Bölümde yer alan Devlet Sırlarına Karşı Suçlar ve Casusluk ve 8. Bölümde yer alan sayılan Yabancı Devletlerle Olan İlişkilere Karşı Suçlar, Fuhuş ve Cinsel Dokunulmazlığa Kast İşlenen Suçlar,

b) 1567 sayılı Türk Parasının Kıymetini Koruma Hakkındaki Kanun,

c) 2313 sayılı Uyuşturucu Maddelerin Murakabesi Hakkındaki Kanun,

ç) 2863 Sayılı Kültür ve Tabiat Varlıklarını Koruma Kanunu (Tarihi Eser Kaçakçılığı hükümlerini kapsar),

d) 3713 Sayılı Terörle Mücadele Kanunu,

e) 4208 sayılı Kara Paranın Aklanmasının Önlenmesi Kanunu,

f) 5607 sayılı Kaçakçılıkla Mücadele Kanunu'ndan hüküm giymesi durumunda ve

g) Terör örgütlerine veya Milli Güvenlik Kurulunca Devletin milli güvenliğine karşı faaliyette bulunduğuna dair karar verilen yapı, oluşum veya gruplara üyeliği, mensubiyeti veya iltisakı yahut bunlarla irtibatı olduğu tespit edilmesi ve bu gerekçelerle kamu görevinden ihraç edilmesi durumunda.

(3) SHGM tarafından görevden alınan SGSYY görevden alınması tarihi itibari ile 5 yıl süre boyunca ilgili işletme Kurumsal SOME biriminde görev alamaz.

(4) SGSYY'nin değiştirilmesi veya istihdamın sonlandırılması durumunda yeni atanan SGSYY Madde 11.1'de belirtilen bilgi ve belgeler ile 30 gün içinde SHGM'den onay istenir.

Kurumsal SOME personel nitelikleri

MADDE 14 -(1) 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 veya siber güvenlik konusunda bilgi ve tecrübeye sahip olması gerekmektedir.

(2) Lisans programı mezunu personelde en az bir yıl bilgi işlem veya siber güvenlik alanında bilgi ve tecrübeye sahip olması gerekmektedir.

(3) Siber güvenlik alanında yüksek lisans veya doktora yapmış personelde tecrübe aranması zorunlu değildir.

Kurumsal SOME personelinin eğitimi

MADDE 15 -(1) İşletme, Kurumsal SOME personellerinin Kurumsal SOME'de görevlendirilmesinden itibaren 6 ay içerisinde birimdeki görevleri kapsamına uygun olarak Ek-7'de yer alan eğitimleri eksiksiz bir biçimde almalarını veya almış olmalarını sağlar, söz konusu eğitimlerin Ek-7'de belirtilen tazeleme süreleri dahilinde tekrar alınması sağlanır.

(2) İşletme, siber güvenlik faaliyetlerinde görev alacak personellerinin görevlerini icra edebilmesi için gerekli her türlü eğitimi almalarını sağlar.

(3) İşletme, Kurumsal SOME personelinin görev ve sorumluluklarını yerine getirebilmesi için gerekli olan temel yetkinliklere sahip olabilmesi amacıyla güncel teknolojiyi takip etmesini sağlar.

ÜÇÜNCÜ BÖLÜM
Kurumsal SOME Görev ve Sorumlulukları

Kurumsal SOME görev ve sorumlulukları

MADDE 16 -(1) Bu Talimat kapsamında Kurumsal SOME birimleri için aşağıda belirtildiği şekilde belirlenmiş 15 temel görevi bulunmaktadır:

a) Kurumsal SOME yönetim görevi,
b) Siber güvenlik politika ve prosedürleri oluşturma ve güncel tutma görevi,
c) Siber güvenlik kültürü oluşturma ve takip etme görevi,
ç) Siber güvenlik risk analizi ve yönetimi görevi,
d) BT kritik alanların fiziksel güvenliğinin sağlanması görevi,
e) Siber güvenlik kapsamında erişim yönetimi görevi,
f) Siber güvenlik kapsamında işletim güvenliği görevi,
g) Siber güvenlik tedarikçi yönetimi görevi,
ğ) İç ve dış kaynaklı sistem temin, geliştirme görevi,
h) BT süreçlerinde iş sürekliliğinin sağlanması görevi,
ı) Siber güvenlik tehdit istihbaratı toplama ve değerlendirme görevi,
i) Siber olay izleme ve tespit etme görevi,
j) Siber olay müdahale ve yönetimi görevi,
k) Siber güvenlik test ve denetleme görevi,
l) İç ve dış paydaşlarla iletişim görevi.

Kurumsal SOME yönetim görevi

MADDE 17 -(1) 1'inci Grup Havacılık İşletmelerinde Kurumsal SOME yönetim görevi SGSYY tarafından gerçekleştirilir.

(2) 2'nci Grup Havacılık İşletmelerinde Kurumsal SOME yönetim görevi bilgi teknolojileri birimindeki en yetkili yönetici tarafından gerçekleştirilir.

(3) Kurumsal SOME Yöneticisi, Kurumsal SOME birimi görevlerinin etkin ve sürdürülebilir bir şekilde yerine getirilmesinden sorumludur.

Siber güvenlik politika ve prosedürleri oluşturma ve güncel tutma görevi kapsamında politika ve prosedür oluşturma

MADDE 18 -(1) Kurumsal SOME, bilgi sistemlerinin ve operasyonel sistemlerin kullanımından kaynaklanan siber güvenlik risklerini yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden siber güvenlik politika, prosedür ve süreç dokümanlarını oluşturur. Bu madde kapsamında oluşturulan tüm dokümanlara, dokümanların gizlilik derecesi ve işletme çalışanlarının görev ve sorumluluklarının uygunluğu nispetinde erişim imkanı verilir. Dokümantasyon içerisinde ilgili teknik veya idari tedbirler dışında, asgari olarak doküman kodu, dokümanın gizlilik derecesi, dokümanı onaylayan, yenilenme tarihi, gözden geçirme tarihi, yenilenme tarihçesi bilgileri yer alır.

(2) Siber güvenlik politika, prosedür, süreç ve siber güvenlik strateji planının gerekleri, işletmenin organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözden geçirme faaliyetleri senede az 1 kere gerçekleştirilir ve gerekli görülmesi durumlarında iyileştirme çalışmaları yapılır. Bu kapsamda, politika ve prosedürlerin işletilmesinin takibinden Kurumsal SOME Yöneticisi sorumludur.

(3) Oluşturulan veya güncellenen tüm siber güvenlik ile alakalı politika ve prosedürler Kurumsal SOME Yöneticisinin yazılı veya dijital onayından geçerek işletme yönetimi onayına

sunulur.

Siber güvenlik politika ve prosedürleri oluşturma ve güncel tutma görevi kapsamında politika ve prosedürlere uyulmaması durumunda disiplin sürecinin işletilmesi

MADDE 19 -(1) İşletme siber güvenlik politika veya prosedürlerine uygun hareket edilmemesi durumunda ilgili personele uygulanacak disiplin mekanizması belirlenir, dokümante edilir ve işletilir.

(2) 1'inci Grup Havacılık İşletmelerinde, işletme siber güvenlik politika veya prosedürlerine uygun hareket edilmemesi durumunda personele uygulanacak disiplin cezasına karar verilecek heyette SGSYY de asil üye olarak görev alır.

Siber güvenlik politika ve prosedürleri oluşturma ve güncel tutma görevi kapsamında siber güvenlik farkındalığı eğitimi

MADDE 20 -(1) Kurumsal SOME, işletme bütününde bir siber güvenlik kültürü oluşturmak amacıyla siber güvenliğini ilgilendiren tüm iç ve dış paydaşlarına yönelik siber güvenlik farkındalık programı oluşturur, yürütür ve denetler.

(2) Kurumsal SOME, bilgi teknolojileri kaynaklarına ve sistemlerine fiziksel veya dijital erişimi olan iç ve dış kaynaklı tüm personelin siber güvenlik farkındalık seviyesini artırmak ve işletme genelinde siber güvenlik kültürü oluşturmak için kapsamlı bir siber güvenlik farkındalığı eğitim programı oluşturur.

(3) Siber güvenlik farkındalığı eğitim programı, siber güvenlik politikaları ve standartları ile birlikte, siber güvenlik konusundaki bireysel sorumlulukların neler olabileceği, bilgi varlıklarını korumak için alınması gereken önlemler ve ilgili siber güvenlik politika veya prosedürlerine uyulmaması halinde işletme personelinin karşılaşacağı disiplin süreçleri hakkında bilgi içerir.

Siber güvenlik politika ve prosedürleri oluşturma ve güncel tutma görevi kapsamında siber güvenlik farkındalığı çalışmaları

MADDE 21 -(1) Kurumsal SOME, işletme içi siber güvenlik farkındalık çalışmaları kapsamında aşağıda belirtilen hususları içerecek bir çalışma programı hazırlar.

a) İşletme personeline örgün, uzaktan veya bütünleşik eğitim yöntemi ile rol ve sorumluluk kriterlerine göre sınıflandırılmış bir siber güvenlik farkındalık eğitim programının hazırlanması ve bu eğitimlerin en az senede bir tazeleme eğitimlerinin verilmesi,

b) İşletme personeline rol ve sorumluluklarına göre maruz kalabilecekleri siber saldırı çeşitlerinin tanıtılması ve örnekler üzerinden bilgilendirme yapılması,

c) İşletme personeline sunulmak üzere siber güvenlik farkındalığı ve siber hijyen ile ilgili el kitaplarının oluşturulması ve personel kullanımına sunulması,

ç) Siber güvenlik eğitim materyallerinin en az senede bir gözden geçirilmesi ve güncel siber tehditler kapsamında güncellenmesi,

d) Siber güvenlik farkındalık eğitimi sonrasında eğitimi alan personelin yetkinlik seviyesinin Kurumsal SOME tarafından değerlendirilmesi,

e) İşletme çalışanlarına yönelik siber güvenlik ile ilgili bilgilendirme bültenlerinin hazırlanması ve çalışanlar ile paylaşılması,

f) 1'inci Grup Havacılık İşletmelerinde; İşletmenin bilişim sistemlerine erişimi olan bütün çalışanlarına yönelik 3 ayda bir sosyal mühendislik testlerini yapması veya yaptırması ve yönetici özetlerinin testin bitiminden en geç 1 ay sonra SHGM'ye gizli resmi yazı ile bildirmesi,

g) 2'nci Grup Havacılık İşletmelerinde; İşletmenin bilişim sistemlerine erişimi olan bütün çalışanlarına yönelik 6 ayda bir sosyal mühendislik testlerini yapması veya yaptırması ve yönetici özetlerinin testin bitiminden en geç 1 ay sonra SHGM'ye gizli resmi yazı ile bildirmesi,

ğ) Siber güvenlik farkındalığı konusunda yetersiz görülen personellerin tespit edilmesi ve bu personellerin siber güvenlik farkındalığının arttırılabilmesi için eğitim süreçlerinin gözden

geçirilerek işletme çalışan profiline uygun eğitim doküman ve yöntemleri ile siber güvenlik farkındalık eğitimlerinin tekrarlanması,

h) İşletme personelinin gözlemledikleri siber ihlal durumlarını, şüpheli hareketleri ve işletme siber güvenlik kültürünü arttırma yönündeki önerilerini raporlayabilecekleri bir raporlama sisteminin oluşturulması gerekmektedir.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında varlık envanterinin oluşturulması

MADDE 22 -(1) İşletme tüm bilgi teknolojileri varlıklarına ilişkin varlık envanterini oluşturmak, bu varlıkları EK-8'de yer alan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi madde 2.1.'e uygun bir şekilde gruplamak ve yönetmek ile yükümlüdür.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında siber güvenlik risk yönetim süreci

MADDE 23 -(1) Kurumsal SOME, alan uzmanları ile birlikte, siber güvenlik risklerini analiz eder, azaltmak, takip etmek ve raporlamak üzere bir siber güvenlik risk yönetim süreci tesis eder.

(2) Kurumsal SOME, siber güvenlik risk analizi sonuçlarına göre tespit edilen her bir siber güvenlik riskine ilişkin, bu risklerin ilişkili olduğu varlıkların değerine ve işletmenin risk limitlerine uygun olacak şekilde risk indirgeme ve kontrol stratejileri belirler. Söz konusu bu varlıkların değerleri ele alınırken bu varlıkların ilişkili olduğu iş hedeflerini ve iş süreçleri ile bunların bağlı olduğu diğer iş hedeflerini ve iş süreçlerini dikkate alır. Risk indirgeme ve kontrol stratejilerinin belirlenmesi aşamasında, Kurumsal SOME koordinesinde riskin ilgili olduğu iş tarafının temsilcileriyle beraber siber güvenlik risk analizi sonucu oluşturulur.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında siber güvenlik risk analiz çalışması kapsamı

MADDE 24 -(1) Söz konusu siber güvenlik risk analizi kapsamında aşağıda belirtilen faaliyetler yerine getirilir:

a) Tespit edilen varlıklara veya süreçlere ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle siber güvenlik risklerin belirlenmesi,

b) Tespit edilen tehdit ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,

c) Siber güvenlik risklerin gerçekleşmesi durumunda ilişkili varlığın gizlilik, bütünlük, erişilebilirlik kriterlerine yönelik etki ve risk hesaplaması yapılması,

ç) Siber güvenlik risk analizinde gerçekleştirilen çalışmaların bütününü temsil ederek özetleyecek ve aşağıdaki hususları içerecek şekilde yazılı veya dijital bilgi varlıklarına ilişkin siber güvenlik risk değerlendirme raporunun oluşturulması:

1) Varlık veya süreç,

2) Varlık veya süreç sahibi,

3) Varlığın veya sürecin etkilediği diğer varlıklar veya süreçler,

4) Risk kategorisi,

5) Tehdit,

6) Güvenlik açığı,

7) Mevcut kontroller,

8) Risk seviyesi,

9) Etki analizi sonucu,

10) Alınması planlanan kontroller.

11) Risk indirgeme planlanan tarihi,

12) İndirgeme faaliyeti durumu.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında siber güvenlik risk indirgeme çalışmaları

MADDE 25 -(1) Risk indirgeme ve kontrol stratejilerinin belirlenmesi aşamasında risklerin nasıl ele alınacağına Kurumsal SOME biriminin önderliğinde karar verildikten sonra bu kararların uygulanmasını sağlayacak siber güvenlik risk aksiyon planları oluşturulur. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin belirlenmesinde, risk analizi aşamasında tespit edilen risk dereceleri dikkate alınır.

(2) Risk aksiyon planında belirlenen aksiyonların alınması risk analizi sonucu tespit edilen riskleri ortadan kaldırmıyorsa, aksiyon planının uygulanması sonucu kalacak artık riskler tespit edilir ve risk aksiyon planı güncellenir.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında siber güvenlik risk envanteri

MADDE 26 -(1) Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek işletmenin siber güvenlik risk envanteri oluşturulur.

(2) İşletme, yılda en az bir defa siber güvenlik risk analizlerini tekrarlar. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve siber güvenlik risk envanterinin güncellenmesi sağlanır.

(3) İşletme bünyesinde gerçekleştirilen siber güvenlik iç kontrol-iç denetim çalışmalarının, tüm Kurumsal SOME faaliyetlerinin, iç ve dış kaynaklar ile gerçekleştirilen sızma testi sonuçlarının, sistem test sonuçlarının ve SHGM denetimleri sonucunda tespit edilen bulguların risk envanterine girdi teşkil etmesi sağlanır.

(4) İşletme bilgi sistemlerinde meydana gelecek önemli değişikliklerden sonra siber güvenlik risk değerlendirmesini tekrarlar.

(5) İşletme, siber güvenlik risk yönetimi çalışmalarına, bütüncül bir güvenlik bakış açısıyla, işletme varlıklarına yönelik olarak gizlilik, bütünlük, erişilebilirlik kriterleri doğrultusunda aktif katkı sağlar.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında risk kabulü

MADDE 27 -(1) 1'inci Grup Havacılık İşletmelerinde bir siber güvenlik riskinin kabul edilebilmesi için SGSYY'nin ve söz konusu siber güvenlik riskine sahip iş tarafının en üst düzey yöneticisinin yazılı veya dijital inkar edilemez onayının bulunması ve söz konusu riskin Sivil Havacılık Genel Müdürlüğü mevzuatlarına aykırılık teşkil etmemesi şarttır. Ayrıca, kabul edilen her bir siber güvenlik riskinin kabul edilme durumunun devam etmesi için, söz konusu siber güvenlik riskinin detaylı olarak İşletme Genel Müdürüne YGG toplantısı kapsamında anlatılması ve Genel Müdür onayının alınması gerekmektedir.

(2) 2'nci Grup Havacılık İşletmelerinde bir siber güvenlik riskinin kabul edilebilmesi için söz konusu siber güvenlik riskine sahip iş tarafının en üst düzey yöneticisinin ve İşletme Genel Müdürünün yazılı veya dijital inkar edilemez onayının bulunması ve söz konusu riskin Sivil Havacılık Genel Müdürlüğü mevzuatlarına aykırılık teşkil etmemesi şarttır.

(3) Kurumsal SOME, kabul edilen siber güvenlik riskleri için, sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin önceki siber güvenlik risk değerlendirmelerine göre artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı, önceden kabul edilmiş olan siber güvenlik risklerini periyodik olarak yılda en az bir defa gözden geçirir ve yapılan çalışmaları dokümante eder.

Siber güvenlik risk analizi ve yönetimi görevi kapsamında üst yönetimin siber güvenlik riskleri hakkında bilgilendirilmesi

MADDE 28 -(1) Kurumsal SOME, işletme üst yönetimini ve BGYS iç paydaşlarını yönetim gözden geçirme toplantılarında siber güvenlik risk değerlendirmesi hakkında detaylı bir şekilde bilgilendirir.

BT kritik alanların fiziksel güvenliğinin sağlanması görevi

MADDE 29 -(1) Kurumsal SOME, hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanları korumak için güvenlik sınırlarını belirler.

(2) Kurumsal SOME, belirlemiş olduğu hassas veya kritik bilgi ve bilgi işleme olanaklarını barındıran alanları korumak için gereken güvenlik kontrollerini işletme fiziksel güvenliğinden sorumlu birim veya birimler ile birlikte belirleyerek dokümante eder.

(3) Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır. Bu alanlara erişim, sadece erişim yetkisine sahip olması gereken personelle sınırlandırılır, Kurumsal SOME erişim haklarını düzenli olarak gözden geçirir ve günceller.

(4) Kritik bilgi sistemlerini içeren fiziksel alanda görev yapan personel dışında herhangi bir işletme personeli, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, bunların erişim ve sonrası faaliyetleri detaylı bir şekilde izlenir ve veri merkezindeki çalışmaları boyunca mutlaka kendilerine refakat edilir. Bu çerçevede, veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur.

(5) Kurumsal SOME, işletme fiziksel güvenlik birimi ile koordineli bir şekilde çalışarak, kritik BT ve OT varlıklarının bulunduğu alanlara yönelik alınan fiziksel güvenlik kontrollerinin yeterliliğini, etkinliğini ve uygulanmasını denetler.

Erişim yönetimi görevi kapsamında kimlik doğrulama süreci

MADDE 30 -(1) Kurumsal SOME, işletme tüm bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş kullanıcılarca ve bu kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrol kuralları uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini denetler.

(2) Kurumsal SOME, bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde tesis edilmesini sağlar ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alındığını denetler.

(3) Kurumsal SOME, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri aldırır.

Erişim yönetimi görevi kapsamında erişim haklarının gözden geçirilmesi

MADDE 31 -(1) Kurumsal SOME, son kullanıcıların işletme kritik varlıklarını etkileyebilecek sistemler üzerindeki erişim hakları matrisini ilgili iş birimleri ile koordineli bir şekilde oluşturulmasını sağlar ve bu yetki erişim matrisini en az 3 ayda bir gözden geçirir.

(2) Kurumsal SOME, varlıklarının kritiklik seviyesini de göz önünde bulundurarak, her bir işletme varlığı için yetki erişim denetleme süre ve süreçlerini belirler.

(3) Kurumsal SOME, ayrıcalıklı kullanıcıların işletme sistemleri üzerindeki erişim hakları matrisini ilgili iş birimleri ile koordineli bir şekilde oluşturulmasını sağlar ve bu yetki erişim matrisini en az ayda bir gözden geçirir.

(4) Kurumsal SOME, ayrıcalıklı erişim hakkına sahip kullanıcıların standart kullanıcı hesaplarının olmasını ve ayrıcalıklı erişim haklarına ihtiyaç duyulmayan işlerde standart kullanıcı hesaplarının kullanmasını sağlar ve denetler.

Erişim yönetimi görevi kapsamında erişim yönetiminde minimum yetki, minimum süre prensibi

MADDE 32 -(1) İşletme verilen tüm erişim haklarında minimum yetki prensibini uygular.

(2) İşletme verilen tüm erişim haklarında işin gereksinimini dikkate alarak minimum süre

kapsamında yetki tanımlaması yapar.

(3) Erişim hakkı verilme ve alınma işlemleri siber güvenlik değişiklik yönetimi sürecine dahil edilerek Kurumsal SOME Yöneticisi koordinasyonunda yürütülür.

Erişim yönetimi görevi kapsamında uzaktan erişim

MADDE 33 -(1) Kurumsal SOME, kurum içi ve dışı paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin güvenli kanallar üzerinden olduğunu denetler.

İşletim güvenliği görevi kapsamında kapasite yönetimi

MADDE 34 -(1) Kurumsal SOME, işletme kritik altyapı ve siber güvenliği ilgilendiren bilgi teknolojileri varlıklarına, personeline ve çalışma ortamlarına ait kapasite gereksinimleri ile ilgili çıkarımlar ve analizleri ilgili iş birimleri ile koordine kurarak yapar ve üst yönetime sunar.

İşletim güvenliği görevi kapsamında uygulama yönetimi

MADDE 35 -(1) Kurumsal SOME, BT ve OT varlıklarına yüklenebilecek uygulamalar için beyaz liste ve kara liste oluşturur ve uygulandığını denetler.

(2) Beyaz liste sadece iş gereksinimleri kapsamında ihtiyaç duyulan uygulamaları içerir. Geçerli bir iş gereksinimi bulunmayan uygulamalar beyaz listeye eklenemez.

(3) Kurumsal SOME, işletmede kullanılan uygulama ve sistemlerin en güncel veya en kararlı versiyonlarının kullanıldığını süreklilik esasına uygun olarak takip eder.

(4) İhtiyaç duyulan versiyon güncellemeleri merkezi bir yapıdan uygulanır.

(5) İşletme lisanssız yazılım kullanmamalıdır. Kullanılan açık kaynaklı yazılımlarda söz konusu ürünün açık kaynaklı kod lisansı kullanılabilir.

İşletim güvenliği görevi kapsamında yerel yönetici hakları

MADDE 36 -(1) Zorunlu bir iş gereksinimi olmadıkça ve Kurumsal SOME Yöneticisi tarafından yazılı veya elektronik bir şekilde onaylanmadıkça personelin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenir.

İşletim güvenliği görevi kapsamında değişiklik yönetimi süreci

MADDE 37 -(1) İşletme, meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indirecek, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir siber güvenlik değişiklik yönetimi süreci tesis eder. Kurumsal SOME, işletme tarafından tesis edilen ve işletilen siber güvenlik değişiklik yönetim süreçlerini denetler, etkin ve sürdürülebilir bir siber güvenlik değişiklik yönetim sürecinin tesis edildiğinden emin olur.

(2) İşletme bilgi teknolojileri veya siber güvenlik süreçlerini etkileyen her değişiklikte siber güvenlik değişiklik yönetim sürecini uygular.

(3) Siber güvenlik değişiklik yönetimi çalışmaları, görevler ayrılığı prensibine uygun olarak icra edilir, test edilir, gerçekleştirilir, kayıt altına alınır, geri dönüş planları hazırlanır ve tüm süreç dokümante edilir. Siber güvenlik değişiklik yönetim süreçleri ile ilgili kayıtlar Kurumsal SOME tarafında kontrol edilir ve denetlenir.

(4) Değişiklik yönetimi kapsamındaki tüm değişikliklerin kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılır, bunlar için yeterli iz kaydı tutulur ve tutulan iz kayıtları düzenli olarak gözden geçirilir.

İşletim güvenliği görevi kapsamında değişiklik yönetimi sürecinde Kurumsal SOME onayı

MADDE 38 -(1) BT, OT veya siber güvenlik süreçlerini etkileyen değişikliklerde Kurumsal

SOME Yöneticisi onayı alınır.

İşletim güvenliği görevi kapsamında yama yönetimi

MADDE 39 -(1) İşletme, havacılık sektörü faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığın azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir yama yönetimi süreci tesis edilmesini sağlar. Yama yönetim sürecinin uygunluğu ve etkinliği Kurumsal SOME tarafında kontrol edilir ve denetlenir. Kurumsal SOME yama yönetim sürecinde aşağıdaki faaliyetleri yerine getirir;

a) Uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanılması,

b) İşletme tarafından kullanılan sistem, yazılım ve cihazlarda yer alan güvenlik açıklarının ve bu açıklara yönelik yamaların tespit edilmesi,

c) Tespit edilen yamaları uygulamanın ya da uygulamamanın etkisinin değerlendirilmesi,

ç) Yamaların nasıl uygulanacağına ilişkin metotların tanımlanması,

d) Uygulanacak yamaların uygulama öncesi test edilmesi,

e) 1'inci Grup Havacılık İşletmelerinde uygulanan ya da uygulanmamasına karar verilen yamalarla ilgili SGSYY'nin yazılı veya dijital onayının alınması,

f) Yamaların uygulanması ya da yanlış uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotların tanımlanması,

g) Uygulanamayan yamaların gidermeye çalıştığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontrollerin tesis edilmesi.

(2) Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık yamalanamadığında, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde söz konusu sistem, yazılım ve cihazlar kullanımdan kaldırılır.

Siber güvenlik tedarikçi yönetimi görevi kapsamında tedarikçi yönetimi süreci

MADDE 40 -(1) İşletme, siber güvenlik direncinin arttırılması ve işletme bilgi teknolojileri sistemleri ve bilgi teknolojilerinin kullanıldığı süreçlerin iş sürekliliğinin sağlanması amacıyla BT, OT ve havacılık sektörü süreçlerinin işleyişini ve siber güvenliğini etkileyen tüm tedarikçilerinin kapsama dahil edildiği etkin bir siber güvenlik tedarikçi yönetim süreci tesis eder.

(2) Kurumsal SOME, işletme kritik tedarikçilerini ve bu tedarikçilerin etkilediği süreçleri Ek-9'da yer alan Siber Güvenlik Kritik Tedarikçi Envanteri'ne uygun bir şekilde dokümante eder.

(3) Kurumsal SOME, siber güvenlik kritik tedarikçi envanterini en az senede bir gözden geçirir ve ihtiyaç halinde günceller.

Siber güvenlik tedarikçi yönetimi görevi kapsamında siber güvenlik gereksinimlerinin belirlenmesi

MADDE 41 -(1) Kurumsal SOME, işletmenin verisine erişebilen, verilerini işleyebilen, depolayabilen, iletebilen veya işletmenin bilgisi için bilgi teknolojileri altyapı bileşenlerini temin edebilen tedarikçilerine yönelik siber güvenlik gereksinimlerini belirler.

Siber güvenlik tedarikçi yönetimi görevi kapsamında tedarikçilerin denetlenmesi

MADDE 42 -(1) Kurumsal SOME, senede en az 1 kere kritik tedarikçilerinin sunduğu hizmeti siber güvenlik açısından denetler, denetlettirir veya Kurumsal SOME tarafından belirlenmiş kapsamda yapılan bağımsız denetim sonuçlarını değerlendirir.

Siber güvenlik tedarikçi yönetimi görevi kapsamında tedarikçi yönetiminde iş sürekliliği hususları

MADDE 43 -(1) İşletme tarafından yapılan siber güvenlik ve bilgi teknolojileri iş sürekliliği

risk ve etki çalışmaları tedarikçi yönetim süreçlerini de içerir.

Siber güvenlik tedarikçi yönetimi görevi kapsamında tedarikçi hizmetlerinde değişikliklerin yönetilmesi

MADDE 44 -(1) İşletme tedarikçi hizmetlerindeki değişiklikleri yönetmek için tedarikçi çıkış stratejileri oluşturur, söz konusu bu çıkış stratejilerini periyodik aralıklar ile gözden geçirir ve ihtiyaç duyulması halinde günceller.

Siber güvenlik tedarikçi yönetimi görevi kapsamında tedarikçi sözleşmelerinde siber güvenlik hususlarının belirtimi

MADDE 45 -(1) Siber güvenlik tedarikçi yönetim süreci kapsamında, Kurumsal SOME birimi tarafından belirlenmiş olan siber güvenlik kriterlerinin sözleşmelere dahil edilmesi sürecinin işletme genelinde uygulanması Kurumsal SOME tarafından denetlenir, tespit edilen uygunsuzluklar işletme üst yönetimine yazılı bir şekilde iletilir, tedarikçi yönetim süreci işletilir.

İç ve dış kaynaklı sistem temin, geliştirme görevi kapsamında ortam ve görevlerin ayrıştırılması

MADDE 46 -(1) Bilgi sistemlerinin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesinde, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlanır. Bu kapsamda sistem ve uygulamaların geliştirilme süreci, kaynak kodlarının tek bir kişi tarafından hazırlanıp derlenerek geliştirme, test ve üretim ortamları arasında taşınmasına imkân vermeyecek şekilde görevler ayrılığı prensibine uygun olarak işletilir.

İç ve dış kaynaklı sistem temin, geliştirme görevi kapsamında Kurumsal SOME onayı

MADDE 47 -(1) İç veya dış kaynaklar kullanılarak geliştirilmesi planlanan her tür yazılım ve sistem geliştirme veya temin etme süreçlerinde Kurumsal SOME'den söz konusu geliştirmenin siber güvenlik açısından uygunluğu kapsamında yazılı veya dijital onay alınır.

İç ve dış kaynaklı sistem temin, geliştirme görevi kapsamında SHGM güvenli yazılım geliştirme rehberine uyum

MADDE 48 -(1) İşletme iç veya dış kaynaklar kullanılarak geliştirilen uygulamalarda Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberine uygun bir şekilde süreci yönetir.

BT süreçlerinde iş sürekliliğinin sağlanması görevi kapsamında BT süreçlerinde iş sürekliliği sürecinin tesis edilmesi

MADDE 49 -(1) 1'inci Grup Havacılık İşletmelerinde havacılık sektörü faaliyetlerini yürütmede kullanılan bilgi teknolojileri ve süreçlerinin sürekliliğini sağlamak üzere, SGSYY ve İşletme Genel Müdürü veya Yönetim Kurulu tarafından onaylı bilgi teknolojileri iş sürekliliği yönetimi ve planının bir parçası olan bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumluları atanır ve Bilgi Teknolojileri İş Sürekliliği Komitesi tesis edilir.

(2) 2'nci Grup Havacılık İşletmelerinde havacılık sektörü faaliyetlerini yürütmede kullanılan Bilgi Teknolojileri süreçlerinin sürekliliğini sağlamak üzere, İşletme Genel Müdürü veya Yönetim Kurulu tarafından onaylı bilgi teknolojileri iş sürekliliği yönetimi ve planının bir parçası olan bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumluları atanır ve İş Sürekliliği Komitesi tesis edilir.

(3) İş Sürekliliği Komitesi ilgili alan uzmanları ve teknik uzmanlarda dahil olmak üzere tüm paydaşların temsilcilerinden oluşur ve işletme Genel Müdürü veya Yönetim Kurulu Başkanı bu komiteye başkanlık eder. İş Sürekliliği Komitesi meydana gelen siber olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür.

(4) Bilgi teknolojileri iş sürekliliği komitesi ilgili iş sürekliliği yönetim sürecini tesis ederken kendisini etkileyen tüm iç ve dış etkenleri değerlendirir.

BT süreçlerinde iş sürekliliğinin sağlanması görevi kapsamında iş sürekliliği yönetim sistemi

MADDE 50 -(1) BT süreçlerinde iş sürekliliğinin sağlanmasında işletme, ISO 22301 İş Sürekliliği Yönetim Sistemi Standardını temel alır ve bu standardın gereksinimlerini yerine getirir.

BT süreçlerinde iş sürekliliğinin sağlanması görevi kapsamında BT iş sürekliliği faaliyetleri

MADDE 51 -(1) Kurumsal SOME, BT iş sürekliliği çalışmaları kapsamında aşağıdaki faaliyetlerin yerine getirilmesini koordine eder;

a) İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi teknolojileri iş sürekliliği yönetim sürecinin tesis edilmesi,

b) İş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde bilgi teknolojileri iş sürekliliği planının geliştirilmesi, Ek-11'de yer alan forma uygun olarak dokümante edilmesi ve kurtarma için gerekli olan kritik işlemlerin belirlenmesi,

c) Bilgi teknolojileri iş sürekliliği planının uygulanabilir olmasının sağlanması,

ç) Yılda en az bir defa, iş sürekliliği denetimleri, tatbikatları ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemlerinin sürekliliğini etkileyen değişikliklerden sonra planın gözden geçirilerek güncellenmesi,

d) Bilgi teknolojileri iş sürekliliği planının ilgili diğer planlarla ve mevzuat gereksinimleriyle uyumlu olmasının sağlanması,

e) Yaşanan acil durum ve felaketlerden kaynaklanan yasal konuların ele alınması, halkla ilişkiler ve basın ile olan iletişimin yürütülmesine destek verilmesi,

f) İlgili ekiplere ve çalışanlara iş sürekliliği planı kapsamında eğitim verilmesi ve iş sürekliliği farkındalığın artırılması,

g) İş sürekliliği çalışmalarının görevler ayrılığı ilkesi de gözetilerek objektif bir şekilde değerlendirilmesi.

BT süreçlerinde iş sürekliliğinin sağlanması görevi kapsamında yedeklilik

MADDE 52 -(1) İşletme, bir yada daha fazla kritik sürecin beklendiği gibi çalışmadığı durumlarda, tüm sistemin veya havacılık sektörü faaliyetlerinin bir bölümünün çalışamaz hale gelmesini önlemek adına kritik sistem ve uygulama süreçleri için veri yedekleme, yedekli çalışma ve hazırda bekleme mekanizmalarını kurar.

BT süreçlerinde iş sürekliliğinin sağlanması görevi kapsamında felaket kurtarma merkezi

MADDE 53 -(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 kurar veya yurtiçinde farklı bir risk bölgesinde felaket kurtarma merkezi hizmeti veren firmalardan hizmet alır.

(2) İşletme, FKM kurulumu sürecinde Ek-12'de yer alan Felaket Kurtarma Merkezi Kurulumu Rehberine uygun bir şekilde hareket eder.

(3) İşletmeler, veri merkezlerinin ve felaket kurtarma merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz önünde bulundurur. Binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmamasını sağlar.

(4) İşletme, veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistem ve sensörler kullanır, bunların bakımlarını düzenli olarak yapar. Bu destek sistemi ve sensörlerin ilgili veri merkezlerinin bütünüyle

devre dışı kalmalarına neden olabilecek tek bir arıza noktası içermemesi sağlanır.

Siber güvenlik tehdit istihbaratı toplama ve değerlendirme görevi

MADDE 54 -(1) 1'inci Grup Havacılık İşletmelerinde; Kurumsal SOME, işletmenin siber güvenliğini tehdit eden mevcut ve potansiyel saldırılar hakkında bilgilerin toplanacağı ve analiz edileceği bir siber istihbarat toplama ve değerlendirme süreci oluşturur ve yürütür.

Siber olay izleme ve tespit etme görevi kapsamında iz kayıt yönetimi

MADDE 55 -(1) Kurumsal SOME; Ek-3'de yer alan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde bulunan "Olay Sonrasında İncelenmek Üzere Güvenilir Delillerin Elde Edilmesi İçin Tutulacak Kayıtların Asgari Nitelikleri" dokümanına uygun olarak, iz kayıtlarını merkezi bir şekilde tutar ve yönetir. Görevler ayrılığı prensibi çerçevesinde, merkezi iz kayıt sistemi yönetilerek korale edilir ve bu işlem iz kayıtlarını üreten bilişim sistemlerinin sorumlularından bağımsız olarak yapılır.

(2) 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 personeli, yazılım geliştiriciler ve denetçilere ait görev ve sorumluluklar görevlerin ayrılığı ilkesi kapsamında belirlenir.

(3) Kurumsal SOME, iz kayıtlarını ve oluşan alarmları günlük olarak izler ve incelemesini yaparak inceleme sonuçlarını aylık olarak dokümante eder.

(4) Kurumsal SOME, iz kayıtları üzerinde aylık analiz ve ilişkilendirme çalışması yapar; çalışma sonucunda oluşturduğu raporu Kurumsal SOME Yöneticisine sunar.

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

Siber olay izleme ve tespit etme görevi kapsamında iz kayıtlarının güvenliğinin sağlanması

MADDE 56 -(1) Siber olaylara ilişkin tutulan iz kayıtlarına, "bilinmesi gerektiği kadar" prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşması sağlanır.

(2) Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri yapılandırılarak kayıt üreten ortamlardaki iz kayıtlarının güvenliği sağlanır.

(3) Kayıt üreten ortamlarla iz kayıtları saklama merkezleri arasında teknik imkanlar dahilinde verinin şifreli olarak transfer edilmesi sağlanır.

(4) İz kayıtlarının tek yönlü kriptografik özet değerleri hesaplatılır ve iz kayıtları güvenli ortamlarda saklanır.

(5) Merkezi iz kaydı sunucuları BT ve OT sistemlerinden ayrık bir yapıda oluşturulur.

(6) Merkezi iz kaydı sunucusunun kayıtları, olayların olduğu sistem dışında merkezi bir sunucuda saklanır.

(7) İşletme kritik olaylarını belirler. Kritik olayların iz kayıtları merkezi sunucuya anlık olarak gönderilir, kritik olarak değerlendirilmeyen olayların iz kayıtları da işletmenin belirlediği aralıklarda merkezi sunucuya iletilir.

(8) Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi sunucularda yedeklenir, silinmelerine ve değiştirilmelerine izin verilmez.

(9) Merkezi iz kaydı sunucuları sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir, iz kayıtlarının silinmesi veya değiştirilmesi amaçlı erişimlere kapalı olur.

(10) İz kayıtları periyodik olarak yedeklenir ve yedekler uygun şekilde muhafaza edilir.

Siber olay izleme ve tespit etme görevi kapsamında iz kayıtlarının saklanması

MADDE 57 -(1) İz kayıtlarının saklanma süresi belirlenmesinde; iz kayıtlarından sağlanacak fayda ve ilgili iz kaydının kritikliği parametreleri göz önünde bulundurulur. İşletmelerin tabi oldukları yasal mevzuatları gereği uyması gereken süreler saklıdır.

Siber olay izleme ve tespit etme görevi kapsamında ağ zaman protokolü

MADDE 58 -(1) Kayıtların toplandığı bütün sistemlerin aynı zaman değerine sahip olması sağlanır. Bütün sistemlerin zamanlarının aynı yapılması işlemi için Ağ Zaman Protokolü sunucusu kurulup kayıt üreten farklı sistemlerin zamanlarını bu sunucu ile senkronize etmesi sağlanır. Bunun yanında farklı ülkelerde birimleri olan işletmeler için saat dilimi de dikkate alınır.

Siber olay izleme ve tespit etme görevi kapsamında tespit ve müdahale mekanizması

MADDE 59 -(1) 1'inci Grup Havacılık İşletmelerinde, Kurumsal SOME, işletme siber güvenlik durumsal farkındalığını sağlamak amacıyla 7x24 prensibine uygun bir tespit ve müdahale mekanizması kurar veya kurdurur.

(2) 2'nci Grup Havacılık İşletmelerinde, Kurumsal SOME, işletme siber güvenlik durumsal farkındalığını sağlamak amacıyla 7x24 prensibine uygun tespit mekanizması kurar veya kurdurur.

Siber olay izleme ve tespit etme görevi kapsamında aldatma çözümleri

MADDE 60 -(1) 1'inci Grup Havacılık İşletmeleri, tehdit avcılığı ve balküpü mekanizmalarını kurar veya kurdurur.

Siber olay izleme ve tespit etme görevi kapsamında anomali tespiti

MADDE 61 -(1) 1'inci Grup Havacılık İşletmelerinde Kurumsal SOME, kullanıcı ve network bazında anomali tespit sistemlerini kurar ve işletir.

Siber olay müdahale ve yönetimi görevi kapsamında siber olay yönetim süreci

MADDE 62 -(1) İşletme bünyesinde yaşanabilecek bir siber olay ihlal durumuna karşın, Kurumsal SOME siber olay ihlal durumlarını önceden belirler, olay müdahale senaryolarını oluşturur ve dokümante eder.

(2) Kurumsal SOME, siber güvenlik saldırı eğilimlerini takip eder ve siber olay müdahale süreçlerini ve dokümanlarını güncel tutar.

(3) Kurumsal SOME, işletmenin olası bir siber olay durumunda faaliyetlerinin en az etkilenmesini ve mümkün olan en kısa sürede hizmetlerin normal işleyişine döndürülmesini sağlayacak bir siber olay müdahale süreci yürütür.

(4) Kurumsal SOME, gerçekleşen siber olaylar için bir kök neden ve etki analizi yapar ve benzer olayların tekrarlanmasını önlemek için iyileştirici önlemler alır ve dokümante eder.

Siber olay müdahale ve yönetimi görevi kapsamında siber olay yönetim görevi

MADDE 63 -(1) Olası bir siber güvenlik ihlal durumunda olay yönetim sürecini Kurumsal SOME Yöneticisi yönetir.

Siber olay müdahale ve yönetimi görevi kapsamında yetkili otoriteye yapılması gereken zorunlu bildirimler

MADDE 64 -(1) İşletme aşağıda belirtilen durumlarda SHGM'yi ivedilikle bilgilendirir.

a) Yaşanan bir siber olayın büyüyerek bir krize dönüşmesi,

b) Kritik verilerin ya da kişisel verilerin sızması ya da ifşası ile sonuçlanması,

c) Kritik bilgi teknolojileri varlıklarının gizliliğinin etkilenmesi,

ç) Kritik bilgi teknolojileri varlıklarının bütünlüğünün etkilenmesi,

d) Kritik bilgi teknolojileri varlıklarının erişilebilirliğinin etkilenmesi,

e) Bilgi Teknolojileri İş Sürekliliği Planı'nın devreye alınması,

f) FKM sistemlerinin devreye alınması

(2) Madde 64.1'de bahsedilen siber güvenlik ihlallerinin olması durumunda işletme, ivedilikle

yaşanan siber güvenlik olayı hakkında bir adli bilişim çalışması yürütür ve olay kök neden analizi yapar.

(3) İşletme, yapılan çalışma sonucunda söz konusu olayın bir daha tekrarlanmaması adına alınması gereken önlemleri de belirleyerek SHGM'ye siber olay tespit edilme tarihinden itibaren en geç 15 iş günü içerisinde Ek-13'de yer alan formata uygun siber olay analiz raporunu gizli resmi yazı ile sunar.

(4) İşletme, madde 64.1 dışında kalan siber güvenlik olaylarını ve teşebbüslerini dokümante eder ve Ek-14'de bulunan formu kullanarak 3 aylık periyotlar ile bulundukları yılın mart, haziran, eylül, aralık aylarının son gününe kadar yılda toplam 4 defa SHGM'ye resmi yazı ile gönderir.

Siber güvenlik test ve denetleme görevi kapsamında siber güvenlik test ve denetim akışı

MADDE 65 -(1) İşletme, bilişim sistemleri güvenlik testlerini Ek-15'de belirtilen şekilde gerçekleştirir.

Siber güvenlik test ve denetleme görevi kapsamında geniş kapsamlı sızma testi

MADDE 66 -(1) Kurumsal SOME, yılda en az bir defa TSE onaylı sızma testi firmalarına Ek-16'da yer alan TSE Sızma Test Metodolojisine uygun bir şekilde geniş kapsamlı sızma testlerini yaptırır.

(2) Geniş Kapsamlı sızma testleri en az Ek-17'de yer alan Geniş Kapsamlı Sızma Testi Kapsam Dokümanı içeriğine uygun bir şekilde gerçekleştirilir.

(3) 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 kişiler tarafından gerçekleştirilemez.

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

(5) 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.

Siber güvenlik test ve denetleme görevi kapsamında dar kapsamlı sızma testi

MADDE 67 -(1) Kurumsal SOME, dar kapsamlı sızma testi kapsamında; en az 6 ayda bir test ve denetimleri yapar veya yaptırır.

(2) Dar kapsamlı sızma testi aşağıdaki hususları içerir.

a) İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması,

b) Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması,

c) Dışa açık web uygulamalarının sızma testleri,

ç) Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri ayarları,

d) Veri tabanı yapılandırma testleri ayarları.

(3) Kurumsal SOME, işletmenin bilgi işlem altyapısında köklü bir değişiklik olması durumunda 6 aylık süreyi beklemeden dar kapsamlı sızma testini yapar veya yaptırır.

Siber güvenlik test ve denetleme görevi kapsamında siber güvenlik doğrulama testi

MADDE 68 -(1) Kurumsal SOME, dar ve geniş kapsamlı sızma testleri sonrasında tespit edilen zafiyetler kapatıldıktan sonra doğrulama testlerini yapar veya yaptırır. Zafiyetin kapatıldığının doğrulaması zafiyeti kapatan kişi tarafından yapılamaz.

Siber güvenlik test ve denetleme görevi kapsamında yazılım siber güvenlik kabul testi

MADDE 69 -(1) Kurumsal SOME, işletme personeli veya hizmet alımı yoluyla temin edilen,

üretilen, güncellenen yazılımların kullanıma geçmeden önce yazılımın siber güvenliği ile ilgili testleri yapar veya yaptırır ve bu test sonuçlarını dokümante eder.

(2) Kurumsal SOME, iç veya dış kaynaklar ile geliştirilen veya güncellenen yazılımların siber güvenlik testlerinin yapılması veya yaptırılması sürecinde Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberini kullanır.

Siber güvenlik test ve denetleme görevi kapsamında OT sistemlerine yönelik sızma testi

MADDE 70 -(1) 1'inci Grup Havacılık İşletmeleri en az 2 senede bir kez olmak üzere işletme bünyelerinde yer alan EKS ve SCADA sistemlerinin sızma testini yaptırır.

Siber güvenlik test ve denetleme görevi kapsamında siber güvenlik iç tetkik süreci

MADDE 71 -(1) Kurumsal SOME, ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında yapılması gereken siber güvenlik iç tetkik süreçlerini yürütür.

Siber güvenlik test ve denetleme görevi kapsamında kırmızı takım faaliyetleri

MADDE 72 -(1) Kurumsal SOME, işletme BT ve OT süreçlerinin gizlilik, bütünlük ve erişilebilirlik unsurlarının güvenlik seviyesini arttırmak, sürdürülebilir bir siber güvenlik operasyon süreci oluşturmak ve mevcut siber güvenlik ekosisteminde aksayan noktaları zamanında tespit ederek, gerekli düzeltici eylemleri zamanında uygulamak amacıyla sürekli bir kırmızı takım siber güvenlik denetim süreci kurgular ve uygular.

Siber güvenlik test ve denetleme görevi kapsamında ağ ve haberleşme güvenliği

MADDE 73 -(1) Kurumsal SOME, işletmenin iç veya dış ağlardan gelebilecek siber güvenlik tehditlerinden korunması için proaktif yapıda ağ kontrol ve güvenlik sistemlerini tesis etmesini sağlar ve denetler. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisini esas alır.

(2) Hassas verilere sahip tüm sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. DMZ sistemleri, özel iç ağdaki sistemlerle yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurar.

(3) İnternet üzerinden veya işletme dış ağından görünür olan tüm sunucu ve sistemler, görünür olmalarını gerektirecek geçerli bir iş ihtiyacının olup olmadığı açısından düzenli olarak kontrol edilir ve eğer gerekli değilse bu sunucu ve sistemlerin işletme iç ağına taşınır.

(4) İşletme, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır.

(5) İç ağdan gelebilecek tehditlerin etkisini azaltmak ve işletme iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere işletme iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde kurum iç ağına kritiklik ve görev bazında ağ segmentasyonu uygulanır. Farklı ağ segmentleri arasındaki hassas veri trafiği kontrol edilir ve güvenliği sağlanır.

(6) İç ağa sadece yetkilendirilmiş cihazların erişebilmesi sağlanır. Dış hizmet alım yöntemi ile icra edilen havacılık ve bilgi teknolojileri operasyonlarının yürütülmesi de bu madde kapsamında değerlendirilir.

(7) EKS ve SCADA sistemleri BT networkünden ayrılır.

(8) EKS ve SCADA sistemlerine kritiklik veya görev bazlı bir ağ segmentasyonu uygulanır.

Siber güvenlik test ve denetleme görevi kapsamında ağ trafiğinin izlenmesi

MADDE 74 -(1) Kritik ağ segmentlerine yapılan tüm bağlantılar sürekli olarak izlenerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz tüm bağlantıların

sonlandırılması sağlanır. Benzer şekilde, ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alarak önemli tüm sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portlar kapatılır.

Siber güvenlik test ve denetleme görevi kapsamında yapılandırma dokümanlarının oluşturulması

MADDE 75 -(1) Kurumsal SOME, tüm masaüstü, dizüstü, mobil cihazlar, iş istasyonu makineleri ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi tüm kritik bilgi teknolojileri varlıkları için sıkılaştırılmış ve test edilmiş güvenli standart yapılandırma bilgilerini oluşturur ve dokümante eder.

Siber güvenlik test ve denetleme görevi kapsamında zararlı yazılımlara karşı tedbirler

MADDE 76 -(1) Kurumsal SOME, tüm masaüstü, dizüstü ve iş istasyonu makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit edecek etkin araçlar kullanır.

Siber güvenlik test ve denetleme görevi kapsamında kriptografik kontroller

MADDE 77 -(1) Kurumsal SOME, bilginin gizliliği, aslına uygunluğu ve bütünlüğünün korunması için kriptografinin doğru ve etkin kullanımın temin edildiğini denetler.

Siber güvenlik test ve denetleme görevi kapsamında test ve denetim faaliyetleri sonucu siber risklerin güncellenmesi

MADDE 78 -(1) Kurumsal SOME, yaptığı veya yaptırdığı tüm sistem test ve denetim faaliyetleri sonrasında kurumsal siber güvenlik değerlendirme ve risk analizi raporunda gerekli güncellemeleri yapar.

Siber güvenlik test ve denetleme görevi kapsamında bulgu yönetimi

MADDE 79 -(1) Kurumsal SOME, tüm sistem test ve denetim faaliyetleri sonrasında tespit edilen zafiyetlerin ilgili bilgi işlem personeli veya hizmet alınan firma tarafından kapatılması sürecini yönetmek üzere dokümante edilmiş bir bulgu yönetim süreci tesis eder.

(2) Kurumsal SOME tarafından oluşturulmuş siber güvenlik bulgu yönetim süreci aşağıdaki unsurları içerir:

a) Bulgu No,

b) Bulgu Açıklama,

c) Bulgu Tespit Edilme Yöntemi,

ç) Bulgu Tespit Edilme Tarihi,

d) Bulgunun İlgili Birime Bildirilme Tarihi,

e) Zafiyet Sonucu Etkilenmesi Muhtemel Sistem veya Süreçler,

f) Bulgu Kök Neden,

g) Bulgunun İlişkilendirildiği Siber Güvenlik Risk No,

ğ) Bulguyla İlgili Oluşturulan Siber Güvenlik Risk No,

h) Varlık veya Süreç Sahibi Birim,

ı) Kapatmak İçin Alınacak Aksiyonlar,

i) Bulgu Kapatma Son Tarihi,

j) Bulgu Kapatma Aksiyonunu Gerçekleştirecek Kişi veya Birim,

k) Bulgu Takibini Gerçekleştiren Kurumsal SOME Personeli,

l) Bulgu Son Durum Açıklama

Siber güvenlik test ve denetleme görevi kapsamında adli süreçlerin yönetilmesi

MADDE 80 -(1) Kurumsal SOME, yapılan siber güvenlik testleri sonucunda suç olabilecek iz, delil ve emare (zararlı yazılım, sızma vb.) görülmesi durumunda Kurumsal SOME Yöneticisi ve işletmenin hukuk müşavirliği ile görüşerek gecikmeksizin kanunen soruşturmaya yetkili makamlara (savcılık veya kolluk), SHGM'ye ve USOM'a bildirimde bulunur.

İç ve dış paydaşlarla iletişim görevi

MADDE 81 -(1) Kurumsal SOME, bir prosedür veya talimatta Kurumsal SOME'lerin kurum içi ve dışı paydaşlar ile iletişim esaslarını oluşturur.

(2) Kurumsal SOME; siber olay öncesi, esnası ve sonrasında, siber güvenlik çalışmalarını yönetmek amacıyla kurumdaki bilgi işlem birimi ve varsa hukuk ve basın ve halkla ilişkiler müşavirlikleri ve benzeri birimler ile birlikte çalışır.

İç ve dış paydaşlarla iletişim görevi kapsamında iç ve dış paydaşlar ile iletişim esasları

MADDE 82 -(1) İşletme dış paydaşlar ile gerçekleştireceği siber güvenlik ile alakalı ihlal olayı, istihbarat ve bilgi paylaşımlarında trafik ışığı protokolü esasına göre bir sınıflama yapar.

(2) SHGM ile yapılan veri paylaşımlarında işletmenin trafik ışığı protokolüne göre olan tercihi değerlendirilmeye alınır. SHGM gerekli gördüğü hallerde söz konusu bu sınıflandırmayı göz ardı edebilir.

İç ve dış paydaşlarla iletişim görevi kapsamında trafik ışığı protokolünün kullanılması

MADDE 83 -(1) Kurumsal SOME, tüm Kurumsal SOME personelinin iletişim bilgilerini USOM ve SHGM'ye SİP uygulaması üzerinden bildirmek ve güncel tutmak ile yükümlüdür.

İç ve dış paydaşlarla iletişim görevi kapsamında siber güvenlik faaliyet raporu

MADDE 84 -(1) Kurumsal SOME, yıllık Siber Güvenlik Faaliyet Raporlarını Ek-18'de yer alan Yıllık Siber Güvenlik Faaliyet Raporu Formatına uygun bir şekilde hazırlayarak SHGM'ye en geç izleyen yılın 31 Ocak tarihine kadar eksiksiz bir şekilde gönderir.

DÖRDÜNCÜ BÖLÜM
Diğer Hükümler

Yasal uyum

MADDE 85 -(1) İşletme kendisini siber güvenlik alanında etkileyen tüm yasal mevzuat ve sözleşmeden doğan şartlarını değerlendirir mevcut süreç ile karşılaştırarak dokümante eder.

(2) 1'inci ve 2'nci Grup Havacılık İşletmeleri, Ek-3'de yer alan Kurumsal SOME Kurulum ve Yönetim Rehberi'nde belirtilen gereksinimlere uyar.

(3) Havacılık işletmeleri, Cumhurbaşkanlığı Dönüşüm Ofisi Tarafından hazırlanan Ek-8'de bulunan Bilgi ve İletişim Güvenliği Rehberine uyum sağlamakla yükümlüdür.

ISO 27001 bilgi güvenliği yönetim sistemi standardı uyumluluğu

MADDE 86 -(1) 1'inci ve 2'nci Grup Havacılık İşletmeleri işletme bilgi teknolojileri varlıkları, operasyonel teknoloji varlıkları ve havacılık sistemlerini etkileyen tüm süreçlerini ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı kapsamında belgelendirir.

Siber güvenlik kapsamında iç denetim

MADDE 87 -(1) İşletme, siber güvenlik faaliyetlerinin yeterliliğini ve siber direncini ölçmek için görevler ayrılığı ilkesini gözeterek senede en az 1 defa olmak üzere Ek-19'da yer alan Havacılık Sektörü Siber Güvenlik İç Kontrol Metodolojisini kullanarak iç denetim faaliyeti gerçekleştirir.

Yönetim gözden geçirme

MADDE 88 -(1) İşletme, siber güvenlik faaliyetlerinin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için en az senede bir olmak üzere Genel Müdür veya Yönetim Kurulu Başkanı başkanlığında ve tüm BGYS paydaşlarının katılım sağlayacağı bir gözden geçirme toplantısı düzenler.

(2) Yönetim Gözden Geçirme toplantıları aşağıdaki hususları kapsar.

a) Önceki yönetimin gözden geçirme toplantılarında belirlenmiş görevlerin durumu,

b) Kurumsal SOME görev ve sorumluluklarını ilgilendiren iç ve dış konulardaki değişiklikler,

c) En az aşağıdaki hususları kapsayacak şekilde işletme siber güvenlik faaliyetleri performansına dair geri bildirim yapması gerekmektedir:

1) Uygunsuzluklar ve düzeltici faaliyetler,

2) İzleme ve ölçme sonuçları,

3) İç ve dış kaynaklı tüm tetkik ve denetim sonuçları,

4) Siber güvenlik Stratejik Plan hedeflerinin durumu,

ç) İç ve dış paydaşların siber güvenlik süreçleri ile ilgili geri bildirimleri,

d) Siber güvenlik risk değerlendirme sonuçları ve risk işleme planının durumu ve sürekli iyileştirme için fırsatlar,

e) Ek-19'da yer alan Havacılık Sektörü Siber Güvenlik İç Kontrol Metodolojisine göre yapılmış değerlendirme sonuçlarının analizi.

(3) Tüm toplantı katılımcılarının ıslak veya dijital imzasını içeren yönetim gözden geçirme toplantısı sonuç tutanağı, toplantının bitiminden itibaren en geç 5 iş günü içerisinde gizli resmi yazı ile SHGM'ye gönderilir.

Siber güvenlik çalışmalarında yerli-milli ürün kullanımının yaygınlaştırılması

MADDE 89 -(1) İşletme bilgi teknolojileri süreçlerinde dışa bağımlılığın ve dışa bağımlılığın oluşturabileceği siber risklerin azaltılması amacıyla yerli-milli ürün kullanımına önem verir.

BEŞİNCİ BÖLÜM
Cezai Yaptırımlar

MADDE 90 -(1) 1'inci ve 2'nci Grup Havacılık İşletmeleri SHGM tarafından haberli veya habersiz olarak denetlenir. SHGM tarafından yapılan risk ve önceliklendirme çalışmalarına göre yüksek riske sahip olduğu belirlenen 3'üncü Grup Havacılık İşletmeleri de SHGM tarafından denetime tabi tutulabilir. Yapılan siber güvenlik denetimleri sonucunda;

a) Tespit edilen bulgular EK-21'de yer alan Bulgu Önem Seviyesine göre sınıflandırılarak, SHGM tarafından belirlenen bulgu kapatma sürelerine uygun bir şekilde kapatılması için işletmeye bildirilir.

b) SHGM tarafından uygun görülen tarihte eksiliklerin giderilmemiş olması durumunda ilgili işletmeden savunma talep edilir. Söz konusu savunmanın incelenmesi ve SHGM tarafından yeterli görülmemesi durumunda SHGM, 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.

(2) SHGM tarafından yapılan inceleme ve denetlemelerde adli soruşturmaya konu olabilecek

hususlara rastlanılması durumunda adli makamlara suç duyurusunda bulunulur.

ALTINCI BÖLÜM
Son Hükümler

Yürürlükten Kaldırılan Genelge

MADDE 91 -(1) Bu Talimatın yürürlüğe girmesi ile birlikte 02/08/2016 tarihli Genel Müdürlüğümüz HGD/2015-1 Genelgesi yürürlükten kalkacaktır.

Yürürlük

MADDE 92 -(1) Bu talimat 01.04.2023 tarihinde yürürlüğe girer.

Yürütme

MADDE 93 -(1) Bu Talimat hükümlerini Sivil Havacılık Genel Müdürü yürütür.

EKLER:

EK-01 - ATM Güvenlik Planı Kapsamı
EK-02 - ATM Güvenlik Planı Kontrol Formu
EK-03 - Kurumsal SOME Kurulum ve Yönetim Rehberi
EK-04 - Siber Güvenlikten Sorumlu Yönetici Başvuru Formu (Form-4)
EK-05 - SGSYY Siber Güvenlik Sertifikası Kabul Listesi
EK-06 - Siber Güvenlik Strateji Planı Durum Bildirim Formu
EK-07 - Kurumsal SOME Eğitim Listesi
EK-08 - Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi
EK-09 - Siber Güvenlik Kritik Tedarikçi Envanteri
EK-10 - Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberi
EK-11 - BT Süreçleri İş Sürekliliği Planı
EK-12 - Felaket Kurtarma Merkezi Kurulumu Rehberi
EK-13 - Siber Olay Analiz Formatı
EK-14 - Siber Olay İstatistiksel Bildirim Formu
EK-15 - Bilişim Sistemleri Güvenlik Test Süreci
EK-16 - TSE Sızma Test Metodolojisi
EK-17 - Geniş Kapsamlı Sızma Testi Kapsam Dokümanı
EK-18 - Yıllık Siber Güvenlik Faaliyet Raporu Formatı
EK-19 - Havacılık Sektörü Siber Güvenlik İç Kontrol Metodolojisi
EK-20 - Trafik Işığı Protokolü
EK-21 - Bulgu Önem Seviyesi

Ek-1. ATM Güvenlik Planı Kapsamı

Birinci Bölüm

1. Amaç
2. Kapsam
3. Dayanak
4. Yetki
5. Sorumluluk
   5.1. Üst Yönetim Sorumluluğu
   5.2. Havalimanı İşletmesi Sorumluluğu
   5.3. Kurumsal SOME Sorumluluğu

İkinci Bölüm

6. Tanımlar
7. Genel Esaslar

Üçüncü Bölüm

8. ATM Güvenliğinin Amaçları
9. Güvenlik Yönetim Sistemi
   9.1. Güvenlik Yönetimi Politikası
   9.2. ATM Varlık Envanteri
   9.3. Güvenlik Risk Değerlendirme ve Planlama
   9.4. Uygulama ve Operasyon
   9.5. ATM Sistemlerinin Yasa Dışı Müdahaleden Korunması
      9.5.1. Personel Güvenliği
      9.5.2. Fiziksel Güvenlik
      9.5.3. Siber Güvenlik
   9.6. Kontrol ve Düzeltici Faaliyetler
   9.7. İlgili Otorite ve Paydaşlar ile Koordinasyon
   9.8. ATM Güvenliğinde Rol ve Sorumluluklar
   9.9. Kriz Yönetimi
   9.10. Yönetim Gözden Geçirme

Dördüncü Bölüm

10. Eğitim
11. Yürürlülük
12. Yürütme
13. Onay

Ek-2. ATM Güvenlik Planı Kontrol Formu

Kurum Adı :	
Havalimanı :	

ÜST YÖNETİM SORUMLULUĞU						
No	**Soru**	**Sorumluluk**	**Referans**	**İşletme Yetkilisi**	**SHGM Yetkilisi**	
				Mevcut Mu?	**Mevcut Mu?**	**Yeterli Mi?**
1	Üst Yönetim Sorumluluğu	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->Md.5.1			
FİZİKSEL GÜVENLİK						
No	**Soru**	**Sorumluluk**	**Referans**	**İşletme Yetkilisi**	**SHGM Yetkilisi**	
				Mevcut Mu?	**Mevcut Mu?**	**Yeterli Mi?**
2	Hassas/kritik bilgi ve bilgi işleme olanakları barındıran alanların tanımlanması	Havalimanı Yönetimi	ISO 27001-->A.11.1.1 BİGR-->Md.3.6			
3	Güvenli alanların yetkili personele yönelik erişim izni-giriş/çıkış yetkilendirilmesi	Havalimanı Yönetimi	ISO 27001-->A.11.1.2 BİGR-->Md.3.6			
4	Kısıtlı alan giriş/çıkış kayıt logları ve analizleri	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.11.1.2 BİGR-->Md.3.6			
5	Dış etkenlere yönelik fiziksel koruma prosedürü	Havalimanı Yönetimi	ISO 27001-->A.11.1.3 BİGR-->Md.3.6			
6	ATM güvenlik kritik noktalarının fiziksel izolasyonu	Havalimanı Yönetimi	ISO 27001-->A.11.1.6 BİGR-->Md.3.6			

Ek-2. ATM Güvenlik Planı Kontrol Formu

7	Fiziksel güvenlik iç tatbikatı	Havalimanı Yönetimi	ISO 27001-->Md.9.1,Md.9.2			
SİBER GÜVENLİK						
				İşletme Yetkilisi	**SHGM Yetkilisi**	
No	**Soru**	**Sorumluluk**	**Referans**	**Mevcut Mu?**	**Mevcut Mu?**	**Yeterli Mi?**
8	Siber İstihbarat Toplama	Kurumsal Some	ISO 27001-->A.12.6.1 HGD-2015/1-->Md.2,Md.3 KSKYR-->Md.4.1.2			
9	Penetrasyon Testleri	Kurumsal Some	ISO 27001-->A.12.7.1 BİGR-->Md.3.1.11, Md.2.3.2 HGD-2015/1-->Md.2,Md.3 EK-19-->Md.8,Md.12			
10	Anomali Tespit Sistemleri	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.12.7.1,A.18.2.1., A.18.2.2,A.18.2.3,Md.10.1, Md.10.2 BİGR-->Md.3.1.11,Md.3.4.5, Md.2.3.2 HGD-2015/1-->Md.2,Md.3, KSKYR-->Md.4.1.2,Md.4.1.3 EK-19-->Md.8,Md.12			
11	Bilgi Güvenliği İş Sürekliliği	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.17.1.1,A.18.1.1 BİGR-->Md.3.1.12 HGD-2015/1-- >Md.2,Md.3,Md.4.1.a KSKYR-->Md.4.1.4			

12	Siber Güvenlik Olay Yönetimi	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.5.1.1,A.16.1.1, A.16.1.2,A.16.1.3,A.16.1.5 BİGR-->Md.3.1.10 HGD-2015/1-->Md.2,Md.3 KSKYR-->Md.4.1.4 EK-19-->Lahika-1			
13	Varlık Yönetimi	Havalimanı Yönetimi	ISO 27001-->A.8.1.1 BİGR-->Md.2.1.1, Md.2.1.2, Md.3.1.1, Md.3.1.2			
14	Siber Risk Yönetimi	Kurumsal Some	ISO 27001-->Md.6.1.2,Md.6.1.3 BİGR-->Md.3.1.3.6			
15	Otoriteler ve özel ilgi grupları ile iletişim kanalları	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.6.1.3,A.6.1.4 KSKYR-->Md.3.2,Md.3.3			
16	Tedarikçi Yönetimi	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.15.1.1,A.15.1.2, A.15.2.1 DOC 30->Md.14.2.4.2			
17	Erişim Kontrol Politikası	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.9.1.1			
18	İz Kayıt Analizi	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.12.4.1,A.12.4.2, A.12.4.3,A.12.4.4			
19	Ağ Segmentasyonu	Kurumsal Some	ISO 27001-- >A.9.1.2,Md.A.13.1.3 DOC 30->Md.14.2.4.1 BİGR->Md.3.1.7.4			

Ek-2. ATM Güvenlik Planı Kontrol Formu

20	Kriptografik Kontroller	Kurumsal Some	ISO 27001-->A.10.1.1 BİGR->Md.3.1.7.4			
21	Kötücül Yazılımlardan Korunma	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.12.2.1			
22	Saat Senkronizasyonu	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.12.4.4			
23	Ağ ve Haberleşme Güvenliği Prosedürü	Kurumsal Some	ISO 27001-->A.13,A.9.1.2			
24	Firewall, IDS/IPS vb. Güvenlik Cihazları	Kurumsal Some	BİGR->Md.3.1.6.19			
25	DoS/Ddos Önlemleri	Kurumsal Some	BİGR->Md.3.1.6.7			
26	Beyaz Liste/Kara Liste Uygulaması	Kurumsal Some	BİGR->Md.3.1.6.4			
27	Çalışanların Güvenlik Soruşturmaları	Havalimanı Yönetimi	DOC 30->Md.14.2.4.5 ISO 27001->Md.A.7.1.1			
28	Siber Güvenlik Farkındalık Çalışmaları	Kurumsal Some/Havalimanı Yönetimi	ISO 27001->Md.A.7.2.2 BİGR->Md.3.5.2.1			
29	Hizmet Alımı Güvenlik Soruşturmaları, Gizlilik Anlaşmaları	Kurumsal Some/Havalimanı Yönetimi	KSKVYR->Md.3.1			

Ek-2. ATM Güvenlik Planı Kontrol Formu

YGG VE DENETİM SÜREÇLERİ						
				İşletme Yetkilisi	SHGM Yetkilisi	
No	**Soru**	**Sorumluluk**	**Referans**	**Mevcut Mu?**	**Mevcut Mu?**	**Yeterli Mi?**
30	Havalimanı Üst Yönetimi ATM Güvenlik Gözden Geçirmesi	Havalimanı Yönetimi	ISO 27001-->Md.9.3 HGD-2015/1-->Md.2,Md.3,			
31	İç Tetkik Süreçleri	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.17.1.3 HGD-2015/1-->Md.2,Md.3, Md.4.1.a			
32	ISO 27001 Denetim Süreçleri	Kurumsal Some/Havalimanı Yönetimi	ISO 27001-->A.18.1.1,A.18.1.2., A.18.2.3 HGD-2015/1-->Md.2,Md.3			

Yukarıdaki kontrol listesinde bulunan bilgilerin doğruluğunu taahhüt ederiz.

Kurumsal SOME Yöneticisi

Ad-Soyad

Tarih

İmza

Havalimanı Baş Müdürü/Meydan Müdürü

Ad-Soyad

Tarih

İmza

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

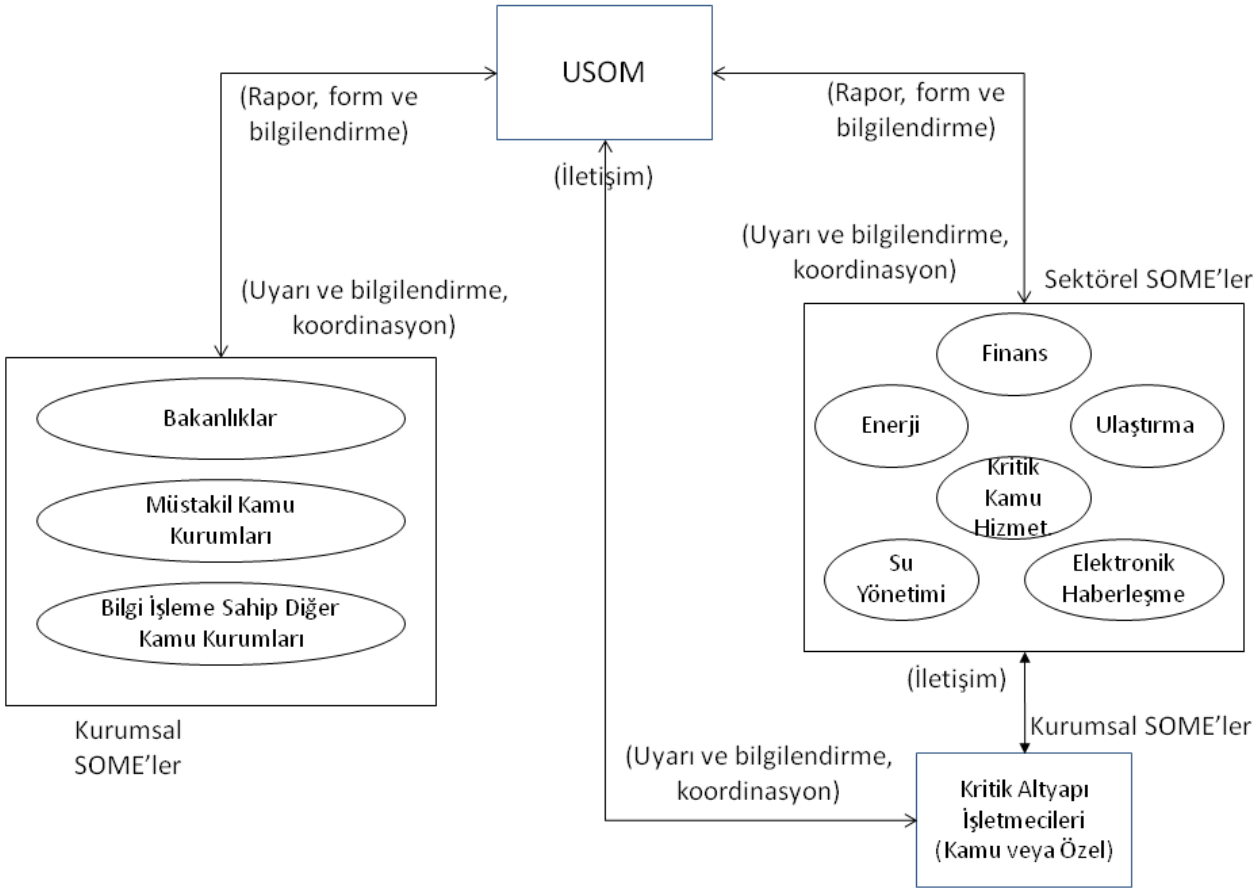
Tablo 2 - Hizmet Alanları

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

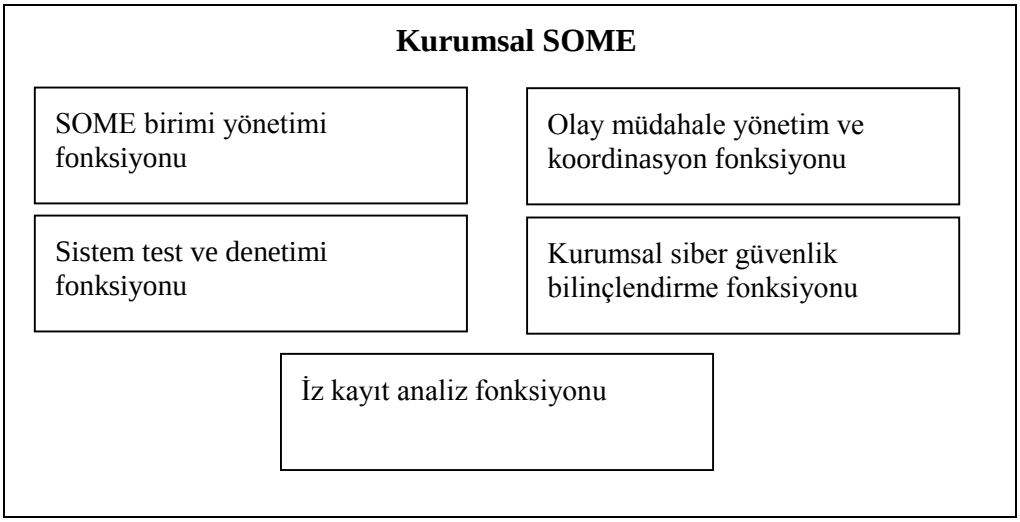
3.1 Kurum İçerisindeki Yeri ve Kapasite Planlaması

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.

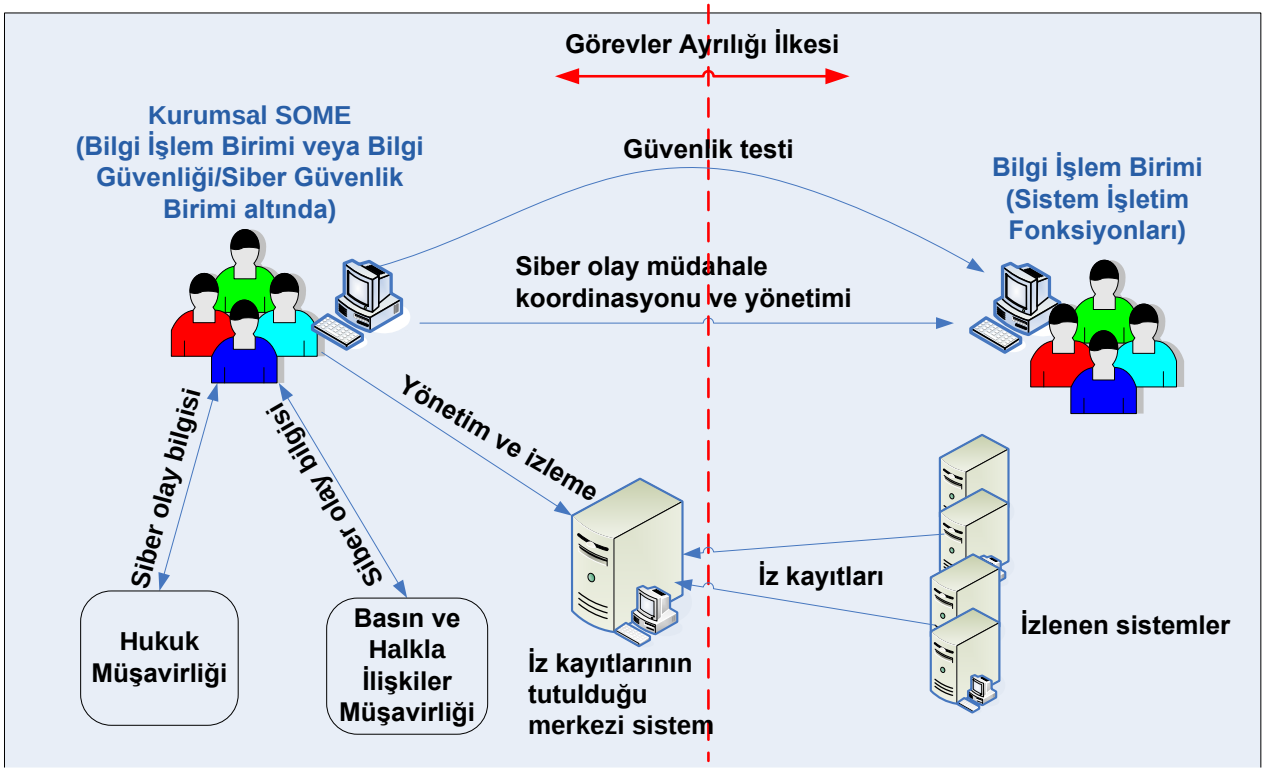
Kurumlar personel ihtiyacını firmalardan hizmet alımı yolu ile de temin edebilirler. Firmadan temin edilen personel için kurumun gereksinimleri çerçevesinde güvenlik soruşturması (adli sicil kaydı, şahıs güvenlik belgesi v.b.) yaptırılır, firma personeline gizlilik sözleşmesi imzalatılır ve bu şekilde 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

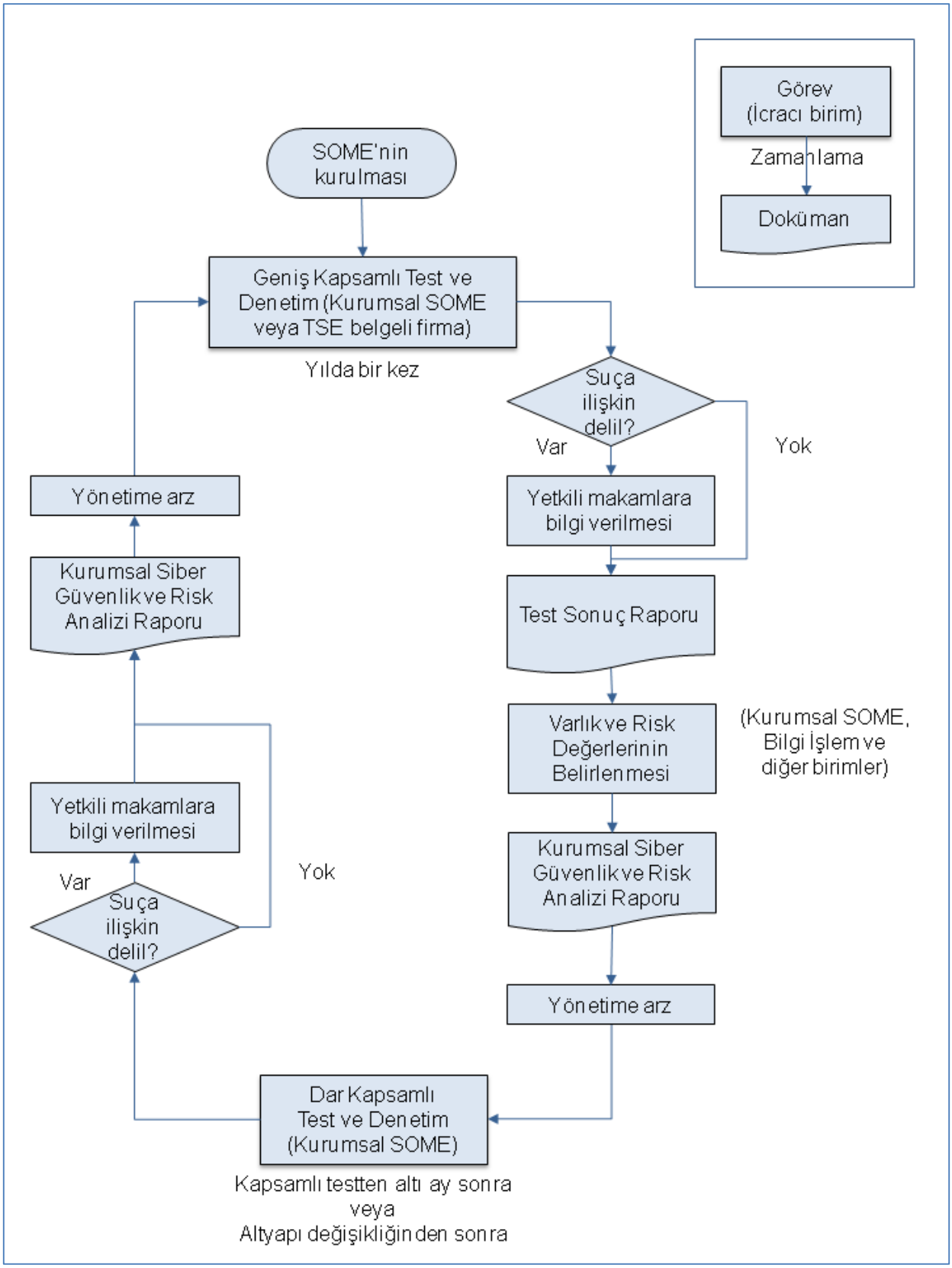
Kurumsal SOME'lerin, farkındalık çalışmaları kapsamında;

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.

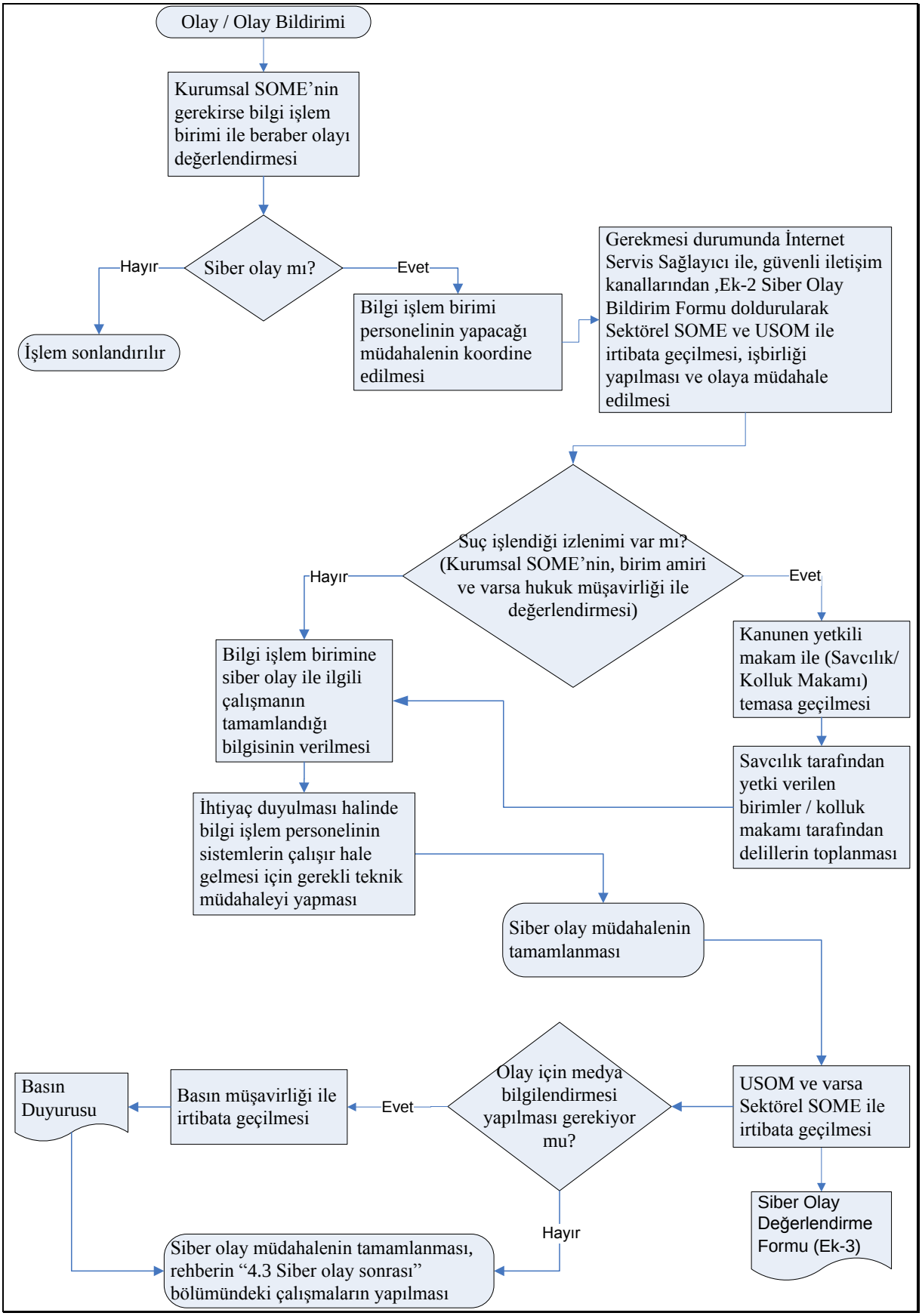
c. USOM ve varsa bağlı olduğu Sektörel SOME tarafından önerilen/düzenlenen toplantı ve etkinliklere katılırlar.
d. Güvenlik ürünlerinin (saldırı tespit sistemi, güvenlik duvarı, balküpü sistemi vb.) belirlenmesi sürecinde bilgi işleme destek verir.
e. Güvenlik ürünlerinin uygulama seviyesi işletimi ile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

Sivil Havacılık Genel Müdürlüğü
Directorate General of Civil Aviation

SİBER GÜVENLİKTEN SORUMLU YETKİLİ YÖNETİCİ ONAY FORMU (FORM – 4)

Form-4

Aşağıda yer alan mevzuatta belirlenen kriterlere göre
Yönetici Personel gerekliliklerinin detayları;
(Details of Management Personnel required to be accepted as specified in):

1. Adı / Soyadı *First Name / Surname*:

… Başvuru sahibinin adı ve soyadı……

2. Görevi *Position*:

… Başvuru sahibinin görevi……

3. Göreviyle ilgili nitelikler *Qualifications relevant to the item (2) position*:

… Başvuru sahibinin görevini ifa etmesi için sahip olduğu nitelikler……

4. Görevi ile ilgili iş deneyimi *Work experience relevant to the item (2) position*:

… Başvuru sahibinin yapacağı görev ile ilgili geçmiş tecrübeleri……

5. Daha önceki herhangi bir Form-4 sahiplik durumu *Previous ownership of any Form-4*:

… Başvuru sahibinin şu an ve geçmişinde herhangi bir Form-4 sahiplik durumu ……

6. İşletmenin Ticari Ünvanı *Organization*:

… İşletmenin ticari ünvanı …… ……

7. Başvuru Sahibi imzası, Tarih – *Signature of Applicant, Date*

… Başvuru sahibinin imzası ve günün tarihi……

8. Sorumlu Müdür imzası, Tarih – *Signature of Accountable Manager, Date*

… Başvuru sahibinden sorumlu olacak müdürün imzası ve günün tarihi……

Tamamlandıktan sonra lütfen bu formu taratıp SHGM-BYS otomasyon sistemine SHT-SİBER Madde 11'de yer alan belgelerle beraber yükleyiniz…
(On completion, please upload this form to SHGM-BYS system with relevant documents as indicated in the article 11 of SHT-SIBER)

Ek-5. SGSYY Siber Güvenlik Sertifikası Kabul Listesi

1. CISA (Bilgi Sistemleri Denetçi Sertifikası)
2. CISM (Bilgi Sistemleri Yöneticisi Sertifikası)
3. CISSP (Bilgi Sistemleri Profesyoneli Sertifikası)
4. CRISC (Risk ve Bilgi Sistemleri Kontrol Sertifikası)
5. GSEC (GIAC Güvenlik Temelleri)
6. TSE Kıdemli Sızma Test Uzmanı Sertifikası
7. ISO 27001 Baş Denetçi Sertifikası
8. ISO 22301 Baş Denetçi Sertifikası

Ek-6. Siber Güvenlik Strateji Planı Durum Bildirim Formu

No	Strateji Planı Maddesi	Hedeflenen Tamamlanma Tarihi	Durum*	Açıklama

* : İlgili alanı “Gerçekleştirildi”, “Gerçekleştirilmedi” veya “Değiştirildi” ifadelerinden birisini kullanarak doldurunuz.

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	1
Eğitim Adı	:	Güvenli Yapılandırma Denetimi Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	50
Uygulama (%)	:	50
Eğitim Toplam Süre	:	3 gün/24 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitim Alması Gereken SOME Rolleri	:	▪ Siber Güvenlik Test/Denetleme Görevi ▪ Siber Güvenlik Tedarikçi Yönetimi Görevi
Eğitim İçeriği		

- 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

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	2
Eğitim Adı	:	Sızma Testleri Eğitimi
Eğitim Verilme Türü	:	Uygulama
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	-
Uygulama (%)	:	100
Eğitim Toplam Süre	:	5 gün/40 saat
Eğitim Tazeleme Süresi	:	1 yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Güvenlik Test/Denetleme Görevi
Eğitim İçeriği		

- 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
- Desktop uygulamaları sızma testleri
- DNS servisi testleri
- E-posta servisi testleri
- Dağıtık servis dışı bırakma (DDoS) testleri
- Sanallaştırma sistemleri testleri
- Kablosuz ağ testleri
- Güvenlik duvarı testleri
- URL ve içerik filtreleme testleri
- EKS/SCADA sızma testleri

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	3
Eğitim Adı	:	Saldırı Teknikleri Eğitimi
Eğitim Verilme Türü	:	Teorik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	100
Uygulama (%)	:	-
Eğitim Toplam Süre	:	2 gün/16 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi ▪ Siber Olay İzleme ve Tespit Etme Görevi ▪ Siber Olay Müdahale ve Yönetimi Görevi ▪ Siber Güvenlik Test/Denetleme Görevi ▪ Siber Güvenlik Kültürü Oluşturma ve Takip Etme Görevi ▪ Siber Güvenlik Risk Analizi ve Yönetimi Görevi ▪ BT Süreçlerinde İş Sürekliliğinin Sağlanması Görevi ▪ Siber Güvenlik Tedarikçi Yönetimi Görevi

Eğitim İçeriği

- Güvenlik testlerinde bilgi toplama
- TCP/IP iletişiminde oturuma müdahale
- Güvenlik duvarları
- Saldırı tespit ve engelleme sistemleri
- Güvenlik duvarı, saldırı tespit ve önleme sistemleri ile içerik 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
- Linux sistem yönetimi ve güvenliği
- TCP/IP protokol ailesi zafiyet analizi
- Paket analizi, sniffing

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	4
Eğitim Adı	:	Saldırı Tespit ve Kayıt Yönetimi Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	20
Uygulama (%)	:	80
Eğitim Toplam Süre	:	2 gün/16 saat
Eğitim Tazeleme Süresi	:	1 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Olay İzleme ve Tespit Etme Görevi

Eğitim İçeriği

- Trafik analizi temelleri
- Uygulama protokolleri ve trafik analizi
- Açık kaynak kodlu saldırı tespit sistemi
- Ağ trafiği analizi ve izleme
- Uygulama protokolleri için saldırı tespit metotları
- Kayıt yapılandırma ayarları
- Kayıt analiz yöntemleri ve teknikleri
- Kayıt yönetimi
- Büyük boyutlu kayıtların işlenmesi
- Kayıtları izleme
- Olay müdahalesi için kayıtlar
- Adli analiz kayıtları
- Uyumluluk için kayıt
- Kayıt toplamada en sık yapılan yanlışlar
- Kayıt standartları
- Log türleri
- Uygulama kayıt türleri
- İşletim sistemi kayıt türleri
- Nitelikli log nedir
- Gerekli GPO ayarları
- Pattern yakalama ve log analizi
- Kullanım senaryosu oluşturma uygulaması

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	5
Eğitim Adı	:	Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Türü	:	Sınıf
Teorik (%)	:	90
Uygulama (%)	:	10
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi ▪ Siber Olay İzleme ve Tespit Etme Görevi ▪ Siber Olay Müdahale ve Yönetimi Görevi

Eğitim İçeriği

- Merkezi Kayıt Yönetimi sistemleri
- SIEM sistemleri
- SIEM çözümlerine örnekler
- Envanter analizi ile yüksek riske sahip varlıkların belirlenmesi
- Açık kaynak kodlu merkezi güvenlik izleme yazılımı (OSSIM)
- OSSIM mimarisi ve entegre araçlar
- OSSIM konfigürasyonu
- OSSIM web konsolu
- Güvenlik politikalarının ve raporlarının düzenlenmesi
- OSSIM ajanı ile bilgi toplama
- SYSLOG ile bilgi toplama
- Güvenlik olaylarının korelasyonu
- Güvenlik istihbaratı için olay analitik iş akışlarının optimize edilmesi
- Olay analizi ve müdahale
- Sistem bakımı ve güncelleme

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	6
Eğitim Adı	:	Siber Olaylara Müdahale Ekibi Kurulum ve Yönetimi Eğitimi
Eğitim Verilme Türü	:	Sınıf
Teorik (%)	:	100
Uygulama (%)	:	-
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	1 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Tüm Kurumsal SOME Rolleri

Eğitim İçeriği

- Giriş (Tarihçe, örnek bilgisayar olayları, örnek SOME'ler ve organizasyonlar)
- SOME temel konuları (SOME nedir, SOME çerçevesi, SOME servis çerçevesi)
- SOME görev ve sorumlulukları
- SOME gereksinimleri
- Siber olay müdahale süreci (olay müdahale servis tanımı ve servis işlevleri)
- SOME operasyonel elemanları (yazılım, donanım, politika ve prosedürler)
- SOME proje planı
- Havacılık 4.0
- Denetim teknikleri
- Ulusal ve uluslararası regülasyonlar

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	7
Eğitim Adı	:	Bilişim Sistemleri Siber Olay Analiz Eğitimi
Eğitim Verilme Türü	:	Sınıf
Teorik (%)	:	80
Uygulama (%)	:	20
Eğitim Toplam Süre	:	0,5 gün/4 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Olay Müdahale ve Yönetimi Görevi
Eğitim İçeriği		

- 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

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	8
Eğitim Adı	:	Bilgisayar Siber Olay Analizi-Derinlemesine Windows Eğitimi
Eğitim Verilme Türü	:	Sınıf
Teorik (%)	:	20
Uygulama (%)	:	80
Eğitim Toplam Süre	:	0,5 gün/4 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Olay Müdahale ve Yönetimi Görevi
Eğitim İçeriği		

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

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	9
Eğitim Adı	:	Ağ Siber Olay Analizi Eğitimi
Eğitim Verilme Türü	:	Online + sınıf
Teorik (%)	:	80
Uygulama (%)	:	20
Eğitim Toplam Süre	:	0,5 gün/4 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Olay Müdahale ve Yönetimi Görevi
Eğitim İçeriği		

- 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

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	10
Eğitim Adı	:	Zararlı Yazılım Analiz Yöntemleri Eğitimi
Eğitim Verilme Türü	:	Uygulama
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	0
Uygulama (%)	:	100
Eğitim Toplam Süre	:	2 gün/16 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Olay Müdahale ve Yönetimi Görevi ▪ Siber Güvenlik Test/Denetleme Görevi
Eğitim İçeriği		

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

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	11
Eğitim Adı	:	DDoS Saldırıları ve Korunma Yöntemleri Eğitimi
Eğitim Verilme Türü	:	Teorik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	100
Uygulama (%)	:	-
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Güvenlik Test/Denetleme Görevi

Eğitim İçeriği

- Dos/DDoS saldırıları
- Havacılık sektörüne yönelik hizmet dışı bırakma tehditleri
- Dos/DDoS saldırı trendleri
- DoS/DDoS saldırı türleri
- DoS/DDoS tespit etme ve korunma yöntemleri
- DDoS korunma hizmeti minimum gereksinimleri

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	12
Eğitim Adı	:	Bilişim Hukuku Eğitimi
Eğitim Verilme Türü	:	Teorik
Eğitim Verilme Şekli	:	Dijital
Teorik (%)	:	100
Uygulama (%)	:	0
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi

Eğitim İçeriği

- 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 sağlayıcıları
- 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

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	13
Eğitim Adı	:	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	50
Uygulama (%)	:	50
Eğitim Toplam Süre	:	5 gün/40 saat
Eğitim Tazeleme Süresi	:	1 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Tüm Kurumsal SOME Rolleri

Eğitim İçeriği

- BGYS kavramı
- PUKO döngüsü
- 27000 ailesi
- 27001 temel şartlar
- İşletmenin bağlamı
- Liderlik
- Planlama
- Destek
- Operasyon
- Performans değerlendirme
- İyileştirme
- 27001 EK-A maddeleri
- 27701 temel giriş
- Olay inceleme uygulaması

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu		:	14
Eğitim Adı		:	EKS Siber Güvenlik Eğitimi
Eğitim Verilme Türü		:	Bütünleşik
Eğitim Verilme Şekli		:	Sınıf
Teorik (%)		:	70
Uygulama (%)		:	30
Eğitim Toplam Süre		:	2 gün/16 saat
Eğitim Tazeleme Süresi		:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri		:	▪ Siber Güvenlik Test/Denetleme Görevi
Eğitim İçeriği			

- EKS Giriş
- Proses modelleri
- IT ve OT İhtiyaçlarını anlama
- EKS özelinde fiziksel güvenlik
- EKS katmanlı güvenlik mimarisi
- EKS saldırı yüzeyini anlama
- EKS saldırı ağacı
- EKS temel zafiyetler
- EKS bilgi toplama
- EKS yönelik güncel tehditler
- EKS sunucu güvenliği
- EKS sunucu ve iş istasyonları
- Windows tabanlı sistemler
- Unix/Linux tabanlı sistemler
- EKS özelinde güncelleme ve yama yönetimi
- Yedekleme ve yedeklik
- Sıkılaştırma
- Sunucular otomasyon ve denetim
- Uç bileşenlerin korunması
- Veritabanı ve historian güvenliği
- EKS ağ güvenliği
- Ağ yönetimi giriş
- Ethernet
- TCP/IP
- TCP tabanlı EKS protokolleri
- IT firewall, OT firewall, Data Diode'ları
- EKS ağlarında wireless
- Saha bileşenleri

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	15
Eğitim Adı	:	Bilgi Teknolojileri İş Sürekliliği Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	80
Uygulama (%)	:	20
Eğitim Toplam Süre	:	1 gün/ 8 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi ▪ Bilgi Teknolojileri Süreçlerinde İş Sürekliliğinin Sağlanması Görevi

Eğitim İçeriği

- Bilgi teknolojileri iş sürekliliği kavramı
- Neden uygulanmalıdır
- Bilgi teknolojileri iş sürekliliği süreçleri
- PÜKO döngüsü
- Bilgi teknolojileri iş sürekliliğinde süreç yaklaşımı
- Bağlam analizi
- Liderlik
- Planlama(risk ,hedefler vs.)
- Destek(kaynaklar,yeterlilikler,farkındalık vs.)
- İşletim
- Performans değerlendirme
- İyileştirme
- Bilgi teknolojileri iş sürekliliği planlama, tatbikat ve değerlendirme uygulama

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	16
Eğitim Adı	:	Siber Güvenlik Risk Yönetimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	50
Uygulama (%)	:	50
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi ▪ Siber Güvenlik Risk Analizi ve Yönetimi Görevi
Eğitim İçeriği		

- Risk yönetim sistemi'nin rolü, önemi ve faydaları
- Risk yönetiminin temel kavramları
  - Varlık/süreç
  - Risk metodolojisi
  - Etki değerlendirmesi
  - Olasılık belirleme
  - Risk indirgeme çeşitleri
  - Risk takibi
  - Siber güvenlik risk yönetim sistemi
- Risk yönetim prensipleri, çerçevesi ve süreci
- ISO 31000, 27005
- ISO 31000'in kurumsal risk yönetiminde uygulanması
- Siber güvenlik risk vaka analizi

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	17
Eğitim Adı	:	Tedarikçi Yönetimi Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Verilme Şekli	:	Sınıf
Teorik (%)	:	80
Uygulama (%)	:	20
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	3 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi ▪ Siber Güvenlik Tedarikçi Yönetimi Görevi

Eğitim İçeriği

- Tedarikçi yönetimi nedir
- Tedarikçi sınıflandırması
- Tedarikçilere yönelik siber güvenlik riskleri
- Tedarikçi siber güvenlik risk-tehdit analizi
- Tedarikçi bilgi güvenliği kriterlerinin belirlenmesi
  - Olay inceleme uygulaması
- Tedarikçi sözleşmelerinde siber güvenlik gereksinimlerinin belirtimi
- Tedarikçi değerlendirme süreci
- Çıkış stratejisi

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	18
Eğitim Adı	:	Siber Güvenlik Bilinci Oluşturma Eğitimi
Eğitim Verilme Türü	:	Bütünleşik
Eğitim Veriliş Şekli	:	Sınıf
Teorik (%)	:	80
Uygulama (%)	:	20
Eğitim Toplam Süre	:	1 gün/8 saat
Eğitim Tazeleme Süresi	:	2 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Kurumsal SOME Yönetim Görevi ▪ Siber Güvenlik Kültürü Oluşturma ve Takip Etme Görevi
Eğitim İçeriği		

- Temel tasarım yöntemleri
- Sosyal mühendislik saldırı türleri
- Sosyal mühendislik denetim teknikleri
  - Uygulama: Sosyal mühendislik saldırıları senaryolarının hazırlanması(phishing, phone phishing,kimlik hırsızlığı, omuz sörfü vb.)
  - Uygulama: Son kullanıcı siber güvenlik farkındalık mülakatı
- Eğitim hazırlama yöntemleri
- Eğitim ölçme-değerlendirme süreci

Ek-7. Kurumsal SOME Eğitim Listesi

Eğitim Kodu	:	19
Eğitim Adı	:	Siber Tehdit İstihbarat Eğitimi
Eğitim Verilme Türü	:	Teorik
Eğitim Veriliş Şekli	:	Sınıf
Teorik (%)	:	100
Uygulama (%)	:	-
Eğitim Toplam Süre	:	2 gün/16 saat
Eğitim Tazeleme Süresi	:	1 Yıl
Eğitimi Alması Gereken SOME Rolleri	:	▪ Siber Güvenlik Tehdit İstihbaratı Toplama ve Değerlendirme Görevi

Eğitim İçeriği

- Siber tehdit istihbarat türleri
- Siber tehditler ve zincir metodolojisi
- Tehdit istihbaratı veri toplama ve işleme
- IoC
- Veri analizi
- Tehdit istihbaratı analizi
- İstihbarat raporlama
- Trafik ışığı protokolü

Ek-7. Kurumsal SOME Eğitim Listesi

	SOME Rolleri														
No	Eğitim Adı	1.Kurumsal SOME Yönetim Görevi	2.Siber Güvenlik Politika/Prosedür Oluşturma ve Güncel Tutma Görevi	3.Siber Güvenlik Kültürü Oluşturma ve Takip Etme Görevi	4.Siber Güvenlik Risk Analizi ve Yönetimi Görevi	5.BT Kritik Alanların Fiziksel Güvenliğinin Sağlanması Görevi	6.Siber Güvenlik Kapsamında Erişim Yönetimi Görevi	7.Siber Güvenlik Kapsamında İşletim Güvenliği Görevi	8.Siber Güvenlik Tedarikçi Yönetimi Görevi	9.İç ve Dış Kaynaklı Sistem Temin, Geliştirme Görevi	10.BT Süreçlerinde İş Sürekliliğinin Sağlanması Görevi	11.Siber Güvenlik Tehdit İstihbaratı Toplama ve Değerlendirme Görevi	12.Siber Olay İzleme ve Tespit Etme Görevi	13. Siber Olay Müdahale ve Yönetimi Görevi	14. Siber Güvenlik Test/Denetleme Görevi	15.İç ve Dış Paydaşlar ile İletişim Görevi
1	Güvenli Yapılandırma Denetimi Eğitimi								x						x	
2	Sızma Testleri Eğitimi														x	
3	Saldırı Teknikleri Eğitimi	x		x	x				x		x		x	x	x	
4	Saldırı Tespit ve Kayıt Yönetimi Eğitimi												x			
5	Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi	x											x	x		
6	Siber Olaylara Müdahale Ekibi Kurulum ve Yönetimi Eğitimi	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
7	Bilişim Sistemleri Adli Analizi Eğitimi													x		
8	Bilgisayar Adli Analizi – Derinlemesine Windows Eğitimi													x		
9	Ağ Adli Analizi Eğitimi													x		
10	Zararlı Yazılım Analiz Yöntemleri Eğitimi													x	x	
11	DDoS Saldırıları ve Korunma Yöntemleri Eğitimi														x	
12	Bilişim Hukuku Eğitimi	x														
13	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
14	EKS Eğitimi														x	
15	İş Sürekliliği Eğitimi	x									x					
16	Siber Güvenlik Risk Yönetimi	x			x											
17	Tedarikçi Yönetimi Eğitimi	x							x							
18	Siber Güvenlik Bilinci Oluşturma Eğitimi	x	x	x												
19	Siber Tehdit İstihbarat Eğitimi											x				

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

EK-8 - Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

SHT-Siber talimatı EK-8'de yer alan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi'ne https://bulut.shgm.gov.tr/index.php/s/9moU9f1ESVZX4XG adresi üzerinden ulaşabilirsiniz.

Ek-9. Siber Güvenlik Kritik Tedarikçi Envanteri

No	Tedarikçi Firma	İlgili Süreç	Etkilenen Süreçler	Tedarikçi Kritiklik Seviyesi

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

HAVACILIK SEKTÖRÜ GÜVENLİ YAZILIM GELİŞTİRME REHBERİ

HAVACILIK GÜVENLİĞİ DAİRE BAŞKANLIĞI-SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ

Havacılık Sektörü Güvenli Yazılım Geliştirme Rehberi

Aralık,2020/Ankara

İçindekiler

1.YAZILIM GELİŞTİRME SÜREÇLERİ

1.1.Analiz

Bu aşamanın amacı sistemin işlevlerini ve kesin gereksinimleri açıklığa kavuşturmak ve sonucunda bunları belirli bir formatta dokümante etmektir. Bu çalışma müşteri, yazılım mühendisi, sistem analisti, iş analisti, ürün yöneticisi, Kurumsal Some görevlisi vb. rollerin bir araya geldiği gruplar tarafından yapılabilir. Çeşitli yazılım geliştirme metodolojilerinde bu aşamada kullanım dokümanları ve test plan dokümanları da oluşturulabilir.

1.2.Tasarım

Gereksinimlerin tamamlanmasıyla beraber sistem tasarım aşamasına başlanır. Yazılım ürün tasarımı, gereksinim ve isteklerini karşılamak üzere yazılım ürününün özellikleri, yetenekleri ve ara yüzlerinin belirlenmesi etkinliğidir. İki tür tasarımdan bahsetmek mümkündür (Yüksek düzeyde tasarım — Mimari tasarım ve Detaylı tasarım). Mimari tasarım, yazılım modüllerinin genel yapıları ve organizasyon içerisindeki etkileşimleri ile ilgilenir. Sonucunda mimari tasarım dokümanları oluşturulur. Detaylı tasarım aşamasında Mimari tasarım dokümanları genelde revize edilirler. Tasarım ve analiz aşamalarının ayrımı "Problem Ne?/Problem Nasıl Çözülür?" sorularının kullanımı ile ilgilidir. Gereksinimlerin belirlendiği analiz aşaması problemin ne olduğu ile ilgilidir.

1.3.Kodlama

Tasarım aşamasının belirli bir olgunluğa ulaşmasıyla birlikte kodlama aşaması başlar. Teslim edilecek projeyi programlama aşamasıdır.

1.4.Test

Kodlama süresince ve kodlama sonrasında yapılan diğer önemli aşama test'tir. Erken test et yaklaşımı ile hareket edip, analiz aşamasından itibaren test bakış açısına sahip olmamız hata yapma oranımızı ve maliyetleri düşürecektir. Birim testleri, duman testleri, yanlış değer testleri, kabul testleri, kullanım senaryo testleri, yük testleri, kullanıcı kabul testi, yoldan geçen adam testi, test otomasyonu gibi sürece ve duruma göre uygulanabilecek çok farklı kategoride ve derinlikte test türü bulunmaktadır.

1.5.Bakım

Tüm test aşamaları tamamlandıktan sonra yazılım ürünün sahaya teslim edilebilir bir versiyonu çıkartılır ve teslim aşaması gerçekleştirilir. Teslim çıktısı olarak ürün tek başına yeterli değildir. Mutlaka son kullanıcılar için kullanım kılavuzu ve versiyon fark dokümanı oluşturulmalıdır. Teslim ile birlikte bakım aşaması da başlar. Hata giderici, önleyici, altyapıyı iyileştirici, ürüne yeni özellikler ekletici gibi farklı bakım faaliyetleri mevcuttur.

2.GÜVENLİ YAZILIM GELİŞTİRME

2.1.Girdi Doğrulama

Günümüzde bilinen ve gelecekte de muhtemel tehditlerin çoğu kötü niyetli girdi ile başlamaktadır. Bununla birlikte; basit girdi doğrulama yöntemleri ile büyük güvenlik tehditlerinin önlenmesi mümkündür.

Girdi doğrulama yöntemlerini "beyaz kutu" ve "kara kutu" olmak üzere ikiye ayırmak mümkündür. Beyaz kutu yönteminde bilinen bir şablon girdi olarak kullanılmakta, bu şablonun dışındaki tüm girdiler kötü niyetli olarak kabul edilmektedir. Şablonun kontrolü çok kolay olduğundan bu yöntem oldukça etkili bir yöntemdir. Kara kutu yöntemi ise daha az etkili olmasına rağmen daha çok tercih edilen bir yöntemdir. Bu yöntemde kullanılan belirli bir şablon yoktur, sadece bilinen saldırıların bir listesi mevcuttur. Eğer girdi bilinen bir saldırıya benziyor ise o zaman girdi reddedilecek, onun dışındaki tüm girdiler ise kabul edilecektir. Tüm atak çeşitlerini belirlemek zor iken gelecekteki atakları bilip filtrelemek daha da zor olacağından bu yöntemin etkinliğinin daha az olacağı açıktır. Dolayısıyla veri yapıları, mümkün olduğunca belli bir şablona uygun tasarlanarak geçerleme daha güçlü kılınmalıdır.

İstemci-sunucu uygulamalarında doğrulama hem istemci hem de sunucu tarafında yapılabilmektedir. Bununla birlikte; bir saldırgan istemci tarafındaki doğrulama kontrolünü kolay aşabileceğinden istemci tarafındaki doğrulama hiçbir zaman yeterli bir güvenlik önlemi olarak ele alınmamalıdır. Bunun yerine daha çok sunucu tarafında doğrulama kontrolü yapılarak güvenlik seviyesi arttırılmalıdır. Güvenilir olmayan bir kaynaktan gelen veriler mutlaka onaylanmalıdır.

2.2.Kimlik Doğrulama

Kimlik doğrulama, varlıkların kimlik kontrolünden geçmesi işlemidir ve farklı kimlik doğrulama yöntemleri bulunmaktadır. Genellikle yazılımlar önceleri sadece kullanıcı adı ve şifre kullanması şeklinde zayıf doğrulama yöntemleri kullanılmakta idi. Eğer bir "domain" yapısı varsa, kullanıcılar "Active Directory" kullanılarak doğrulanmakta, "domain" dışında ise kimlik yönetimine ilişkin veritabanı uygulanmaktadır. Daha güçlü doğrulama yöntemleri olarak da biyometrik metotlar veya akıllı kartlar kullanılabilir. Bir diğer doğrulama yöntemi ise üçüncü bir tarafın doğrulama işini yapması ve bu üçüncü tarafa güven duyulması şeklindedir.

2.3.Yetkilendirme

Kullanıcıların tanımlanması aşaması olan kimlik doğrulamadan sonra kullanıcının kimliği doğrultusunda erişim haklarının belirlendiği ve kontrolünün gerçekleştiği aşama yetkilendirmedir.

2.4.Konfigürasyon Yönetimi

Konfigürasyon, uygulama ile ilgili hassas bilgileri içermektedir. Örnek olarak, veri tabanına erişim için gerekli bağlantı bilgilerini içeren dosyalar bu kapsamdadır. Konfigürasyona müdahale uygulamanın işleyişini değiştirebilir veya çalışmamasına sebep olabilir. Konfigürasyon dosyalarının sunucularda saklanıyor olması yeterli güvenlik önlemlerinin alındığı anlamına gelmemektedir. Konfigürasyon dosyaları hassas bilgi olarak nitelendirilmeli, şifrelenmiş bir şekilde tutulmalı ve bu dosyalara erişim kayıt altında tutulmalıdır.

2.5.Kritik Bilgi Yönetimi

Kritik bilginin ne olduğunun belirlenebilmesi için uygulamanın ve işin bir arada ele alınması gerekir. Uygulama geliştirici işin niteliğini tam olarak bilemediğinden, diğer yandan işin sahibi de uygulamanın teknik altyapısı hakkında sınırlı bilgiye sahip olacağından bu iki taraf tek başlarına kritik bilgi için yeterli tanımlama yapamayacaklardır. İki tarafın ve kurumsal some yetkililerinin bir araya gelmesiyle hassas bilgileri içeren bir liste oluşturulmalı ve bu listeyi koruyacak bir politika oluşturulmalıdır.

2.6.Kriptografi

Veriyi korumanın yollarından biri de şifrelemedir. Hassas bilgiler bilinen ve test edilmiş şifreleme yöntemleri ile saklanmalıdır. Daha önce kırılması uzun zaman alan algoritmalar günümüzde daha kısa zamanda çözülebilmektedir. Dolayısıyla uygulama içindeki algoritmalar zamanla gözden geçirilmeli ve güncellenmelidir.

2.7.Parametre Manipülasyonu

Dağıtık algoritmalar modüller arasında parametre gönderirler. Eğer bu parametreler arada değiştirilirse, saldırı gerçekleştirilmiş olur.

2.8.Hata Yönetimi

Bazı teknolojiler hataları kullanarak hata yönetimi gerçekleştirmektedirler. Hatalar geliştiriciler ve sistem yöneticileri için uygulama ile ilgili birçok önemli bilgi ihtiva ettiği için çok önemlidirler. Bununla birlikte; geliştirici için bu derece önemli olan bilgi kullanıcı açısından problem oluşturabilmektedir. Her ne kadar kullanıcılar bu hataların ne demek olduğunu anlamasalar da saldırganlar için büyük ipuçları, yazılımla ilgili önemli bilgiler içermektedir. Bundan dolayı sadece genel bir hata mesajının dönmesi, hataların kayıt altında tutulması ve gerçek hataya sadece yöneticiler ulaşmasını sağlayacak sürecin oluşturulması gerekmektedir.

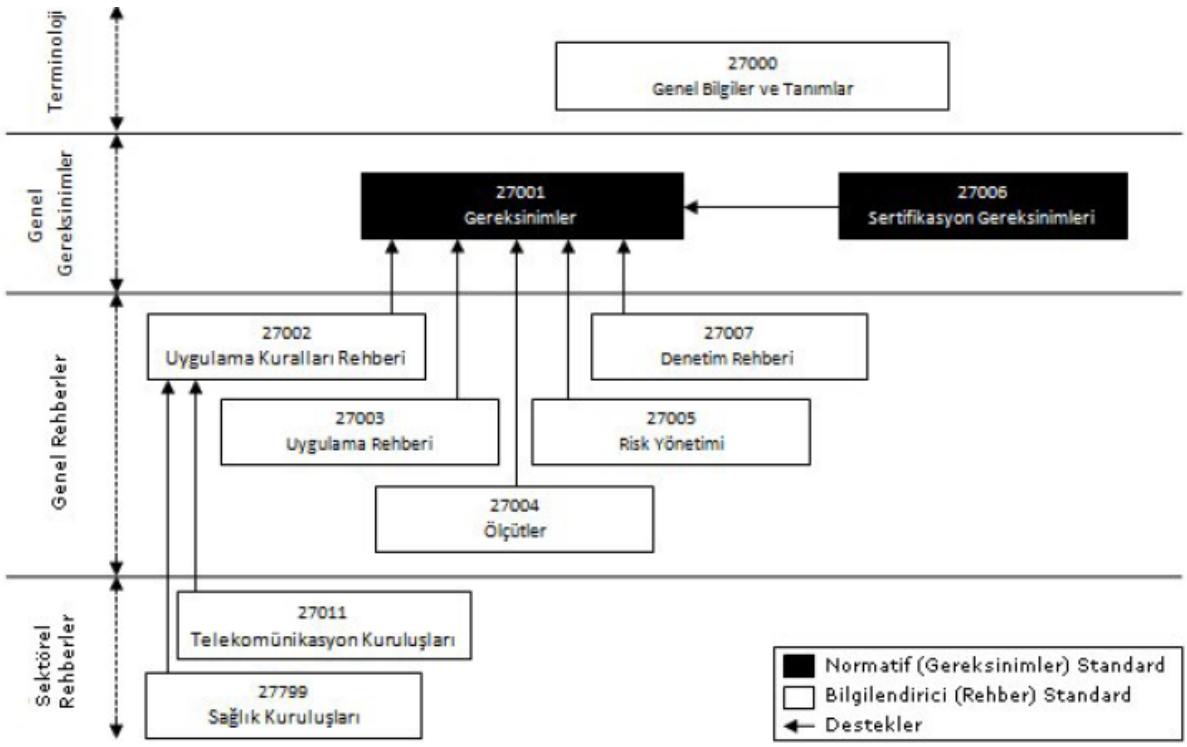
2.9.Kayıt Tutma ve Denetim

Uygulama veya uygulamanın yöneticileri saldırı altında olduklarını anlamalıdır. Bu durum aslında neyin normal neyin anormal olduğunun belirlenmesi ile sağlanır. Bir uygulamaya ilişkin normal süreç ve şablon tanımlanmalı ve bunu dışında bir olay olduğunda saldırı ihtimali, kurumsal some yetkilileri ile birlikte, ele alınmalıdır.

3.ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE GÜVENLİ YAZILIM GELİŞTİRME

Bilgi güvenliği, yazılı, sözlü, elektronik ortam gibi farklı ortamlardaki bilginin gizlilik, bütünlük ve erişilebilirlik bakımından güvence altına alınması ve bu güvence durumunun sürekliliğinin sağlanmasıdır. Bilgi sistemlerinin hayata geçmesiyle ortaya çıkan depolama ve işleme imkânlarının artması, izinsiz erişimler, bilginin yetkisiz imhası, yetkisiz değiştirilmesi veya yetkisiz görülmesi ihtimallerinin artması gibi hususlar nedeniyle bilgi güvenliği kavramı gündeme gelmektedir. Bilgi güvenliği işletmenizdeki tüm yazılı ve dijital bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir.

Bilgi güvenliği ile ilgili olarak ISO 27000 serisi güvenlik standartları, kullanıcıların bilinçlenmesi, güvenlik risklerinin azaltılması ve de güvenlik açıklarıyla karşılaşıldığında alınacak önlemlerin belirlenmesinde temel bir başvuru kaynağıdır.



ISO 27001, gerek yazılım geliştirme süreçleriyle doğrudan ya da dolaylı ilişki içerisinde olan birçok kontrol içermektedir.

4.YAZILIM GELİŞTİRME AŞAMALARINA İLİŞKİN KONTROLLER

4.1.Analiz Aşamasına İlişkin Kontroller

Yazılım geliştirme sürecinin en önemli aşamasıdır. Bu aşamada yapılacak yanlışlıklar yazılım projesinin başarısını en yüksek düzeyde etkilemektedir. Bu aşamada kurumun mevcut bilgi teknolojileri, varsa sistem veri tabanı yapısı, sistem veri yapıları tanımlanmalıdır. Kullanıcı uygulama ihtiyaçları doğrultusunda yazılım ihtiyaç tanımları, veri yapılarını güncelleyen giriş bilgileri, uygulama yazılım ara yüz tanımları, yazılımın üreteceği çıktı bilgileri, yazılım için istenen sorgular gibi tanımlar belirlemelidir.

Bu kapsamda;

- Yazılım için devreye alınacak yeni bilgi sistemleri için iş gereksinimleri bildirgeleri ya da mevcut bilgi sistemlerine yapılan iyileştirmeler güvenlik kontrolleri için gereksinimleri belirlemelidir.
- Yeni bilgi işleme tesisleri için, bir yönetim yetki süreci tanımlanmalı ve gerçekleştirilmelidir.
- Yetkilendirilmiş kullanıcıların sistemde neler yapabileceği uygun şekilde belirtilmelidir, aksi durumlarda başka kullanıcı haklarını kullanma, yetkisiz olduğu halde verilere erişebilme gibi sakıncalar doğabilir. Kuruluş içinden ya da dışından sağlanmış olsun tüm ağ hizmetlerinin güvenlik özellikleri, hizmet seviyeleri ve yönetim gereksinimleri tanımlanmalıdır.
- İletişimin bütün türlerinin kullanımıyla ve bilgi değişimini korumak için resmi değişim politikaları, süreçleri ve kontrolleri oluşturulmalıdır.
- Yazılımda kullanılacak harici materyaller için fikri mülkiyet haklarına göre materyallerin kullanımı ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalarla doğan gereksinimlere uyum sağlanmalıdır.
- Kuruluşun dış taraflarla yapacağı bilgi ve yazılım değişimi için anlaşmalar yapılması gerekir, bu gereksinim analiz aşamasında karşılanmalıdır.

4.2.Tasarım Aşamasına İlişkin Kontroller

Tasarım aşamasında, uygulanacak geliştirme safhaları, her safha için girdiler, çıktılar ve kontrol metotları, iş zaman planları, uygulama planlarının yanı sıra yapılacak işlerin neler olduğu, bu işler için gerekli zaman ve kaynak ihtiyaçlarının tespiti, ilerlemenin izlenmesi için kullanılacak metotlar belirlenmelidir. Bu kapsamda;

- Tüm yazılım kullanıcıları için her türlü yazılım sistemine erişim kullanıcı isimleri ve şifreler ile sağlanmalı, bu şifre ve kullanıcı isimleri her kullanıcı için tek ve benzersiz olacak şekilde tasarlanmalıdır.

- Tasarımda kullanıcılar işlevlerine ve sorumluluk alanlarına göre gruplandırılmalı, grup bazında programlara ve veri tabanlarına erişim hakları verilerek yetkisiz kişilerin sistemi kullanmasına imkân verilmemelidir.
- Bilgi sistemlerinin birbirine bağlantısı ile ilişkili bilgiyi korumak için politikalar ve prosedürler geliştirilmeli ve gerçekleştirilmeli, bilgi sızması fırsatları önlenmelidir.
- Yüksek riskli uygulamalara ek güvenlik sağlamak için bağlantı sürelerinde sınırlandırmalar kullanılması gerektiği hesaba katılmalıdır.
- Tehditlerden korunmak için ve iletilmekte olan bilgi dâhil ağı kullanan sistemler ve uygulamalar için güvenliği sağlamak amacıyla ağlar uygun şekilde yönetilmeli ve kontrol edilmelidir.
- Kullanıcılar ve destek personeli tarafından bilgi ve uygulama sistem işlevlerine erişim, oluşturulması önerilen tanımlanmış erişim kontrol politikasına uygun olarak kısıtlanmalıdır.

4.3.Kodlama Aşamasına İlişkin Kontroller

Yazılımlarda kodlamalar yapılırken güvenli yazılım kodlama teknikleri kullanılmalıdır. Bu kapsamda;

- Yazılımlar, modüler planlanmalı, modüler arası ilişkilerde yapısallık göz önünde bulundurulmalı ve programcı müdahalesi asgari seviyede olacak şekilde parametrik hazırlanmalıdır.
- Sisteme yeni modülerin ilavesi, modüllerin değiştirilmesi ya da silinmesi durumda sistemin bütünü etkilenmemelidir.
- Tutarsız kod ve verilerin girişine engel olacak tedbirler alınmalı, veri tipleri ile kullanıcıların giriş yaptıkları alanların birbirleri ile tutarlı olma durumu kod içinde yapılan düzenlemeler ile giriş anında kontrol edilmelidir.
- Uygulamalara gerçekleşen veri girişinin, bu verinin doğruluğunun ve uygunluğunun geçerlenmesi gerekmektedir.
- Kayıt olanakları ve kayıt bilgisi kurcalanma ve yetkisiz erişime karşı korunmalıdır.
- Yazılımda çıkış verisi sistem hakkında bilgi vermemeli veri sızıntısına açıklık bırakmamalıdır.
- Bir uygulamadan gerçekleşecek veri çıktısı, depolanan bilginin işlenmesinin koşullara göre doğruluğunun ve uygunluğunun sağlanması için geçerlenmelidir.
- Veri işleme hataları veya kasıtlı eylemler nedeniyle herhangi bir bilgi bozulmasını saptamak için geçerleme kontrolleri uygulamalar içine dâhil edilmelidir.
- Uygulamalarda verinin kimliğinin doğruluğunu sağlama ve mesaj bütünlüğünü koruma gereksinimleri tanımlanmalı bunlarla ilgili uygun kontroller tanımlanmalı ve gerçekleştirilmelidir.
- Kötü niyetli koda karşı korunmak için saptama, önleme ve kurtarma kontrolleri ve uygun kullanıcı farkındalığı prosedürleri gerçekleştirilmeli, elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.
- Kriptografi teknikleri yazılımlarda güvenliği sağlamada faydalanılan önemli tekniklerdir. Bilginin korunması için kriptografik kontrollerin kullanımına ilişkin bir politika geliştirilmeli ve gerçekleştirilmelidir.
- Kriptografi için yeterli rastgeleliği sağlayan kriptografik tekniklerin kullanım desteklenmeli ve anahtar yönetimi bulunmalıdır.

- Yazılım geliştirme hizmetinin kuruluş dışından sağlanması durumunda, hizmeti sunan şirketin hareketleri ve yaptığı işler denetlenmeli ve izlenmelidir.

4.4.Test Aşamasına İlişkin Kontroller

Kodlama aşamasından sonra gerçekleştirilecek test aşamasında yazılım uygulaması modüllerinin nitelik ve nicelik testleri uygulanmalıdır. Bu kapsamda;

- Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmalıdır.
- Veri tabanının büyüklüğü ve listelenen, sorgulanan kayıt sayısı ile sistemin performans ilişkisi kontrol edilmelidir.
- Test verisi dikkatlice seçilmeli, korunmalı ve kontrol edilmelidir.
- Yazılım ürünlerinin, sistemin ve alt sistemlerin modül, fonksiyon, entegrasyon ve performans testlerinden sonra testlerde ortaya çıkan değerlere uygun olarak gerçek bilgi ve verilerle, gerçek kullanıcı donanım ve işletim ortamında tüm ihtiyaçların karşılandığı kontrol edilmelidir.
- Test aşaması bitip uygulama devreye alınırken tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi ve bilgi işleme olanaklarına olan erişim hakları, istihdam, sözleşme veya anlaşmalarının sonlandırılmasıyla birlikte kaldırılmalı ya da değiştirilmesiyle birlikte ayarlanmalıdır.

4.5.Bakım Aşamasına İlişkin Kontroller

Yazılım geliştirme sürecinin son aşaması, bakım aşamasında da alınması gereken bir takım güvenlik önlemlerinden söz etmek mümkündür. Bu kapsamda;

- Yazılım paketlerine yapılacak değişiklikler, belirli bir incelemeden geçirilmeli, gerek duyulanlar gerçekleştirilmeli, bunun dışındakiler önlenmelidir. Tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.
- Kullanıcıların erişim hakları da resmi bir proses kullanarak düzenli aralıklarda gözden geçirmelidir.
- Yazılım Kaynak kodlarının bozulma riskini azaltmak ve bilgi kaybından korumak amacı ile kaynak kodları yazılım uzmanlarının işletim sistemleri içinde değil sunucu terminal üzerinde bulunmalıdır. Program kaynak koduna erişim kısıtlı olmalıdır.
- Yedekleme için kurtarılabilir veri saklama yöntemleri uygulanmalı, bilgi ve yazılımlara ait yedekleme kopyaları düzenli olarak alınmalı ve alınan yedekler belirlenecek bir politikaya göre uygun şekilde düzenli olarak test edilmelidir.
- Eğer yetkilendirme varsa ve bilgi içeren ortamın, kuruluşun fiziksel sınırları ötesinde taşınması söz konusu ise taşıma esnasında, bilgiler yetkisiz erişime, kötüye kullanıma ya da bozulmalara karşı korunmalıdır.
- Bilgisayar donanımlarının depolama ortamı içeren tüm parçaları, elden çıkarılmadan önce, herhangi bir hassas veri ve lisanslı yazılım varsa kaldırılmasını veya güvenlişekilde üzerine yazılmasını sağlanmalıdır.

- İşletim sistemleri değiştirildiğinde, kurumsal işlemlere ya da güvenliğe hiçbir kötü etkisi olmamasını sağlamak amacıyla iş için kritik uygulamalar gözden geçirilmeli ve test edilmelidir.
- Kurumların ve şirketlerin operasyonel sistemlerindeki yazılımların kurulmasını kontrol etmek için prosedürler bulunmalıdır.

5.Ulaştırma ve Altyapı Bakanlığı Güvenli Yazılım Geliştirme Kontrol Listesi

Gözden Geçiren		**Proje Adı**	
Gözden Geçirme Süresi	(Harcanan Toplam Süre Saat Olarak Yazılır)	**İş Büyüklüğü**	
Gözden Geçirme Tarihleri		**Gözden Geçirilen İş Ürünü**	

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
Mimari, Tasarım ve Tehdit Modelleme					
1	Uygulamanın mimarisi Güvenli Yazılım Geliştirme Kılavuzunda belirtilmiş olan güvenli yazılım ilkelerine uygun olmalıdır.	Yüksek			
2	Uygulamadaki bileşenler hata durumlarında varsayılan olarak güvenli durumlara geçmelidir.	Yüksek			
3	Uygulamaya yapılan tüm erişim istekleri hem istek hem de yanıt zamanında yetkilendirmeye tabi tutulmalıdır.	Yüksek			
4	Uygulama bileşenleri birbirlerinden iyi tanımlanmış güvenlik mekanizmalarıyla ayrılmalıdır. Bu bağlamda sanallaştırma, uygulama konteyneri, ağ ayrımı, güvenlik duvarı veya bulut tabanlı güvenlik grupları gibi mekanizmalar kullanılmalıdır.	Yüksek			
Bilgi Toplama					

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
5	Web, uygulama ve veri tabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler (sunucu adı ve sürümü, kullanılan program sürümü vb.) gizlenmelidir.	Orta			
6	Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.	Orta			
7	Uygulamaların üzerinde koştukları sunucular, servis verdikleri dizinlerin içeriklerini listelememelidir.	Orta			
8	Arama motorları tarafından görüntülenmemesi istenen dizinler varsa, bunlar için robots.txt ile önlem alınmalıdır. Yalnız, sayfa içerisinde köprülenmeyen bağlantıların/dizinlerin (örneğin yönetim sayfası) güvenlik sorunu oluşturmaması adına robots.txt dosyasına eklenmemesi gerekmektedir.	Orta			
Yapılandırma Yönetimi					
9	Uygulama çatısı, veri tabanı, uygulama sunucusu ve web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.	Kritik			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
10	Uygulama, güncelleme bildirimlerini ya da güvenlik uyarılarını e-posta, SMS veya alternatif iletişim kanallarıyla iletebilmelidir.	Yüksek			
11	Uygulama, başarısız sistem başlatma, başarısız sonlandırma veya başarısız kapatma gibi işlemlerde güvenli bir duruma geçmelidir.	Yüksek			
12	Ana sistem için gereksiz olan dosyalara (örneğin yedekleme, arşiv, test, geliştirme için kullanılan dosyalar) erişim engellenmeli ve sistemdeki gereksiz uygulamalar kaldırılmalıdır.	Yüksek Yüksek			
13	ASP.NET, PHP, STRUTS gibi kullanılan uygulama çatılarının güvenlik özellikleri aktif hale getirilmelidir.	Yüksek			
14	Ön tanımlı kullanıcı hesapları sistemden, veri tabanından ve uygulamadan kaldırılmalıdır.	Yüksek			
15	Hassas bilgiler içeren web sayfalarının tarayıcılarda belleğe alınmaması için autocomplete, cache-control, pragma gibi gerekli HTTP/HTML başlıkları kullanılmalıdır.	Yüksek			
16	Güvenli web trafiği için (SSL) güçlü şifreleme algoritmaları kullanılmalıdır, güvensiz algoritmalar inaktif hale getirilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
17	SSL sunucusunun "renegotiation" özelliği kapatılarak sunucu servis dışı bırakma ve Man In The Middle (MITM) saldırılarına karşı korunaklı hale getirilmelidir.	Yüksek			
İletişim Güvenliği					
18	Güvenilen bir sertifika otoritesinden her Transport Layer Security (TLS) sunucu sertifikasına bir güven zinciri oluşturulabilmeli ve her sunucu sertifikası geçerli olmalıdır.	Yüksek			
19	Kimlik doğrulaması yapılmış, hassas veriler ya da işlevler içeren ve güvensiz ya da şifrelenmemiş protokollerle yapılan tüm bağlantılar (iç ve dış) için TLS protokolünün yaygın kullanılan son sürümü üzerinden yapılmalıdır.	Yüksek			
20	Uygulamada, ağı dinleyen saldırganların trafiği kaydetmesini engellemek için ileri gizlilik şifrelemeleri kullanılmalıdır.	Yüksek			
21	Uygulama, Çevrimiçi Sertifika Durum Protokolü Damgalama (OCSP stapling) gibi yöntemlerle sertifika iptal denetimi gerçekleştirebilecek şekilde yapılandırılmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
22	Sertifikalarda ve sertifikanın tüm hiyerarşisinde yalnızca güçlü algoritmalar ve protokoller kullanılmalıdır.	Yüksek			
23	Uygulama, kimliği doğrulanmış iletişim oturumlarının güvenilir olarak sonlandırıldığını belirten ve kolay anlaşılabilen bir çıkış iletisi görüntülemelidir.	Yüksek			
Kimlik Doğrulama					
24	Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası maskelenmeli ve açık olarak görünmemelidir.	Yüksek			
25	Tüm şüpheli kimlik doğrulama kararları için özet veri içerecek şekilde iz kaydı oluşturulmalıdır.	Yüksek			
26	Yazılım altyapısında ya da herhangi bir bileşen için kullanılan teknolojide üzerinde varsayılan parolalar yer almamalıdır.	Yüksek			
27	Zayıf parolaların kullanımına izin verilmemelidir.	Kritik			
28	Kullanılan parolalar ve parolamı unuttum kontrol soru ve cevapları gibi diğer hassas veriler açık metin olarak saklanmamalıdır.	Kritik			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
29	Uygulama ile son kullanıcı arasında aktarılan kullanıcı adı, parola gibi hassas veriler HTTPS protokolü üzerinden aktarılmalıdır.	Kritik			
30	Herkese açık olmayan bütün kaynaklara ve sayfalara erişim için sunucu tarafında kimlik doğrulaması yapılmalıdır.	Yüksek			
31	Parola Hash değerleri oluşturulurken salt verisi de kullanılmalıdır.	Yüksek			
32	Kullanıcılara (SMS, e-posta yoluyla) dağıtılan başlangıç parolalar, kullanıcılar uygulamaya ilk giriş yaptıklarında değiştirilmeye zorlanmalıdır.	Yüksek			
33	Uygulama üzerinden yapılan kritik işlemler hem uygulama seviyesinde hem de sunucu seviyesinde kayıt altına alınmalıdır.	Kritik			
34	Kullanıcı adı ve parola ile kimlik doğrulamasının yapıldığı kontroller tek tip hata mesajı vermek suretiyle kullanıcı adları listeleme saldırılarına engel olmalıdırlar.	Yüksek			
35	Önceden belirlenmiş hatalı giriş sayısından sonra hesap pasif hale getirilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
36	Uygulama giriş yapan kullanıcıya profil bilgilerini (şifre, email adresi) düzenleme imkanı verilmelidir.	Orta			
37	Şifremi unuttum mekanizması olmalıdır ancak bu mekanizma güvenlik zafiyeti içermemelidir.	Yüksek			
38	Uygulama erişim için kullanıcıya otomatik üretilip verilen ilk parola güçlü, benzersiz ve geçerlilik süresine sahip olmalıdır.	Yüksek			
39	Parolalar en az 8 karakterden oluşmalıdır, en az bir büyük bir küçük harf içermeli, en az 1 rakam içermeli, en az bir özel karakter içermeli aynı karakterler peş peşe kullanılmamalıdır.	Yüksek			
40	Parolalar geçerlilik süresi olmalıdır (standart kullanıcı için tavsiye edilen 180 gün).	Yüksek			
41	Parola değiştirilmesi için mutlaka eski parola doğrulanmalıdır.	Yüksek			
Oturum Yönetimi					
42	Kullanıcı oturumu kapattığında tüm oturumlar geçersiz hale getirilebilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
43	Oturum kimlikleri yeterince uzun olmalı, rastgele olmalı ve etkin oturumlar içerisinde tekil olmalıdır.	Yüksek			
44	Oturum sonlandığında oturum ile ilgili tüm geçici depolama alanları ve çerezler uygulama tarafından silinmelidir.	Yüksek			
45	Uygulama her ürettiği oturum kimliğini yalnızca bir kez kullanmalıdır.	Yüksek			
46	Oturum tekil tanımlayıcısı (Session ID) URL'de gönderilmemeli veya referrer başlığı* içine dâhil edilmemelidir.	Yüksek			
47	Oturum bilgisi zaman aşımına uğrayacak şekilde yapılandırılmalıdır.	Yüksek			
48	Uygulamalarda başarılı kimlik doğrulama ve tekrarlayan kimlik doğrulama (re-authentication) neticesinde her zaman yeni bir oturum bilgisi oluşturulmalıdır. Çıkış işleminden sonra da var olan oturum bilgisi geçersizleştirilmelidir.	Yüksek			
49	Kritik işlemlerde CSRF saldırılarına karşı "token" veya "CAPTCHA" gibi güvenlik önlemleri alınmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
50	Oturum bilgisini içeren çerezlerin (COOKIE) domain ve yol (path) bilgileri ilgili site için en uygun şekilde sınırlandırılmalıdır.	Yüksek			
51	Kullanılan çerez değerleri için *httponly* parametresi tanımlı olmalıdır. Buna ek olarak, HTTPS protokolü kullanılan bağlantılarda kullanılan çerez değerleri için *secure* parametresi tanımlı olmalıdır.	Yüksek			
52	Başarılı login işlemleri sonrası kullanıcı HTTP 302 ile dahili sayfalara yönlendirilmelidir.	Orta			
53	Başarılı kimlik doğrulaması sonucu erişilen uygulamalarda sistemden tekrar çıkmak (logout) için gerekli linkler sağlanmalıdır.	Orta			
Yetkilendirme					
54	Yetkilendirme yaparken “Rol bazlı” yetkilendirme tercih edilmelidir.	Yüksek			
55	Uygulama, kurumsal bilgi sistemlerinde saklanan ve kendi sorumluluğunda olmayan verilerin değiştirilebilmesini engellemelidir.	Yüksek			
56	Kullanıcı yetkileri, sadece sistem yöneticisi veya yetkilendirilmiş kişiler tarafından yapılmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
57	GET ve POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.	Kritik			
58	Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır.	Yüksek			
59	Veri tabanı kullanıcısının sadece uygulamanın kullandığı veri tabanı kaynaklarına erişim hakkı olmalıdır.	Yüksek			
60	Veri tabanı kullanıcısının veri tabanına sadece uygulama sunucu IP adresinden bağlantı hakkı olmalıdır.	Yüksek			
61	Web tabanlı istatistiksel bilgi sağlayan uygulamalara erişim herkese açık olmamalı, rol tabanlı yetkilendirme yapılmalıdır.	Orta			
62	Kısıtlı erişim gerektiren bütün URL'lere, fonksiyonlara, obje referanslarına, servislere, uygulama verilerine, kullanıcı bilgilerine, güvenlik yapılandırma dosyalarına erişim denetlenmelidir.	Yüksek			
63	Yetki hakkının artık gerekmediği durumlarda (görevden ayrılma, projede rol değiştirme gibi) en kısa sürede ilgili haklar iptal edilmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
64	Bir kullanıcıya bağlı birden fazla rol varsa oturum kapatılmadan roller arası geçiş yapılabilmesi sağlanmalıdır.	Yüksek			
65	Yetkilendirme dinamik olmalı ve yetki kaldırıldığında kullanıcın ilgili sayfaya erişimi mümkün olmamalıdır.	Yüksek			
66	Uygulama dokümante edilmişse sistemin çalışmasını etkileyebilecek parametreleri ya da kullanıcı hesaplarını içermemelidir.	Yüksek			
67	Her bir İş nesnesi(business object)* için read/write/modify/delete gibi yetkiler tanımlanmalıdır.	Yüksek			
İş Mantığı					
68	Yönetim paneli gibi kritik dizinlerin isimleri kolay tahmin edilebilir olmamalıdır. (admin, yönetici, administrator, yönetim, panel v.b.).	Orta			
69	Uygulama domain isimlerine ait hassas bilgilerin google/bing gibi arama motorları tarafından indekslenmediği kontrol edilmelidir.	Yüksek			
70	Uygulama iş mantığını doğru bir şekilde gerçekleştirmeli, iş mantığındaki akışlar yazılımda beklenen sırada gerçekleşmeli,	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
	gereken adımlar atlanmamalı, adımların insanların yapabileceği süreler içinde gerçekleştirildiği kontrol edilmeli ve çok yüksek sıklıkla gönderilen istekler tespit edilmelidir.				
Dosyalar ve Kaynakların Güvenliği					
71	Uygulama, ayar ve denetim dosyaları kullanıcı verisiyle aynı konumda depolamamalıdır.	Yüksek			
72	Uygulama, paylaşılan kaynaklar üzerinden yapılan istenmeyen bilgi akışlarını engellemelidir.	Yüksek			
73	URL yeniden yönlendirmelerinin sadece bilinen "beyaz liste" adreslerine yapılması, bilinmeyen adreslere yönlendirme gerekiyorsa kullanıcının uyarılarak onayının alınması sağlanmalıdır.	Yüksek			
74	Güvenilmeyen kaynaklardan alınan dosyaların türü doğrulanmalı ve zararlı bir içeriğe sahip olup olmadığı kontrol edilmelidir.	Yüksek			
75	Güvenilmeyen verinin dinamik olarak yüklenerek çalışan koda dahil edilmesi engellenmelidir.	Yüksek			
76	Karşı alanlar arası kaynak paylaşımında (Cross-domain Resource Sharing, CORS) güvenilmeyen veri kullanılmamalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
77	Web veya uygulama sunucularının, kendi sınırları dışında bulunan kaynak ve sistemlere uzak bağlantı ve erişimi varsayılan olarak engellenmelidir.	Yüksek			
78	Uygulama, güvenilmeyen kaynaklardan alınmış veriyi çalıştırılabilir kod olarak koşturmamalıdır.	Yüksek			
Veri Denetimi					
79	Kullanıcıdan gelen tüm girdiler sunucu tarafında veri kontrolünden geçmelidir.	Yüksek			
80	Kullanıcıdan gelen veriler işletim sistemi komut satırına girmeden kontrol edilmeli ve düzgünleştirme işleminden (escape) geçirilmelidir.	Kritik			
81	Bütün veritabanı sorguları, parametre olarak yapılmalı ve veritabanına erişimde kullanılan dile karşı (SQL, NoSQL vb.) enjeksiyon saldırılarını önleyebilecek denetimler yapılmalıdır.	Kritik			
82	XSS saldırılarına karşı bütün kullanıcı girdileri dışarı aktarılmadan önce sunucu tarafında özel karakter kodlama (output encoding) işleminden geçirilmelidir.	Yüksek Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
83	Güvensiz kaynaklardan veri alarak aritmetik işlem yapan uygulamalar, gerekli tam sayı üst sınır ve alt sınır kontrollerini gerçekleştirmelidirler.	Yüksek			
84	Web uygulamalarında kullanıcıların girmiş olduğu verilerin ver tabanına kaydetmeden önce istenen şartları sağlayıp sağlamadığını kontrol etmek için validation kontrolleri kullanılmalıdır. Bilgi tekrarını önlemek ve veri tutarlılığını sağlamak için de veri tabanına normalizasyon işlemi uygulanmalıdır.	Yüksek			
85	Karşıdan dosya yükleme işlemlerinde yüklenilen dosya üzerinde isim, boyut, tip ve içerik kontrolü yapılmalıdır.	Yüksek			
86	Kullanıcı parametrelerini kullanarak farklı sitelere yönlendirme yapan uygulamalarda ilgili parametrelere pozitif girdi denetimi uygulanmalı ve bu sayede olta saldırılarına engel olunmalıdır.	Yüksek			
87	Kullanıcıdan veri alarak LDAP'a bağlanan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri LDAP düzgünleştirme işleminden (escape) geçirmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
88	Kullanıcıdan gelen CR/LF karakterleri uygulama tarafında oldukları gibi HTTP cevap başlıklarında kullanılmamalıdır.	Yüksek			
89	Uygulamalar, uygun olan her sayfada çerçeve engelleyici önlemleri (frame busting) almalıdırlar.	Orta			
90	Uygulama hizmete girmeden önce sızma testleri yapılmalıdır.	Yüksek			
91	Uygulama, yetki onaylama hizmetlerinin (LDAP, Active Directory) enjeksiyonu açıklıklarını önleyici güvenlik denetimlerini yapmalıdır.	Yüksek			
92	HTML form alanlarının veri girdileri, REST çağrıları, HTTP üst başlıkları, çerezler, toplu işlem dosyaları, RSS beslemeleri gibi veri girdileri için doğrulama denetimi yapılmalıdır.	Yüksek			
Güçlü Kriptografik Mekanizmaların Kullanımı					
93	Tüm kriptografik modüllerin, güvenli bir şekilde hataya düştüğü doğrulanmalıdır. Hata yönetimi “Oracle Padding” atağına imkan tanımayacak şekilde olmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
94	Tüm anahtar ve şifreler kullanımları tamamlandığında, tamamen sıfırlanarak yok edilmelidir.	Yüksek			
95	Tüm rastgele üretilen sayılar, dosya isimleri, global eşsiz değerler (GUID) ve karakter dizilerinin saldırgan için tahmin edilemez olması sağlanmalıdır. Rastgele sayıların yüksek entropiye sahip olarak üretilmelidir	Yüksek			
96	Uygulamada şifreleme, anahtar değişimi, dijital imzalama veya özet alma gibi fonksiyonlar bulunuyorsa TS ISO/IEC 19790-24759 onaylı kriptografik modüller ve rasgele sayı üreteçleri kullanılmalıdır.	Yüksek			
Verinin Korunması					
97	Sunucu üzerinde saklanan önemli verilerin ön belleklenmiş ya da geçici üretilmiş kopyaları şifreli ve güvenli bir şekilde saklanmalıdır.	Yüksek			
98	Bellekte tutulan önemli veriler gereksinimi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde silinmelidir.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
99	Uygulama herhangi bir metodu çalıştırmadan önce güvenlik metodlarını çalışır ve ayakta olduğunu garanti etmelidir.	Yüksek			
100	Silinmiş verilere uygulama bileşenleri üzerinden tekrar ulaşım engellenmelidir. Bellekte ye da disk sisteminde oluşturulan nesnelerin (objects)* gizli veri içermesi engellenmelidir.	Yüksek			
101	Uygulama tablolar arasında veri bütünlüğünü garanti altına almalıdır.	Yüksek			
102	Gerçek veri tabanı asla test ortamı için kullanılmamalıdır.	Yüksek			
103	Uygulama, iş tanımlama dokümanında ya da güvenlik gereksinimlerinde belirtilmesi durumunda, uygulama ara yüzlerinden işlenen ya da saklanan bütün verilerin yedeklerinin alınabilmesine imkân sağlamalıdır.	Yüksek			
Hizmet Dışı Bırakma					
104	DoS saldırısı barındıracak veya şifre deneme-yanılma gibi kaba kuvvet saldırılarına açık tüm formlara CAPTCHA kontrolleri uygulanmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
105	Genelde uygulamaların arama özelliğini kötüye kullanarak veri tabanı üzerinde çok detaylı arama yaptırarak işlemciyi meşgul eden SQL genel arama karakter (%,* vb.) saldırılarına karşı arama süresini kısıtlamak suretiyle önlem alınmalıdır.	Orta			
Web Servisleri					
106	SOAP, Restful, XML-RPC gibi teknolojilerle geliştirilmiş web servislerine erişimlerde kimlik doğrulama kontrolü uygulanmalıdır.	Kritik			
107	Web servisleri için kullanılan çatıların klasik XML saldırılarına (örneğin çok büyük XML verileri, çok sık tekrarlanan XML tag'leri) ve parametre manipülasyonlarına karşı korunaklı olmaları sağlanmalıdır.	Yüksek			
108	Uygulama, web servislerini iyi yapılandırılmış en az TLS v1.2 ve muadil güvenlik önlemi sunan bir protokol ile sunacak şekilde tasarlanmalıdır.	Yüksek			
109	Uygulama, web servis girdilerini kullanmadan önce gidilerin şeklini (XML ve JSON şemalarına uygunluk, parametre beyaz listesi) uygunluğunu ve içeriğini çeşitli saldırılara karşı (XML	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
	bombalama, dış varlık saldırısı, kusurlu XML yapısı, tekrarlamalı girdi vb.) kontrol etmelidir.				
110	Uygulama, web servisi ile gönderilen veride betik (script) içermeyecek şekilde tasarlanmalıdır.	Yüksek			
111	Uygulama, web servislerinden şifreli olarak paylaşılan verileri yine şifreli olarak saklayacak şekilde tasarlanmalıdır.	Yüksek			
İzleme ve Denetim					
112	İz kayıtlarının doğru zaman bilgisi ile oluşturulması sağlanmalıdır.	Yüksek			
113	İzleme kayıtlarının yetkisiz silinmeden ve/veya değiştirilmeden korunması gerekmektedir.	Yüksek			
114	İzleme kayıtlarına erişim de, erişim denetimine tabii olmalıdır. Bu bilgilere sadece güvenlik yöneticilerinin erişmeleri sağlanmalıdır.	Yüksek			
115	İzleme kayıtlarının arşivlenmesi ve bu arşivlerin bakımı mümkün olmalıdır.	Yüksek			
116	İzleme kayıtları, güvenlik yöneticisinin belirlediği ya da uygun bir standarda göre belirlenmiş bir süre zarfı müddetince tutulmalıdır.	Yüksek			

#	Değerlendirme Listesi	Seviye	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)	Açıklama	Uygun (U), Uygun Değil (UD), Kapsam Dışı (KD)
117	İz kaydı bilgileri 5651 sayılı kanuna uygun şekilde elektronik olarak imzalanmalıdır.	Yüksek			
Kişisel Verilerin Korunması					
118	Uygulama, kişisel veriler üzerinde işlem yapılması ana amaç olmayan durumlarda kişisel verileri maskeleyerek görüntülemeli, aktarmalı veya işlemelidir.	Yüksek			
119	Uygulama, kişisel verileri şifreli olarak saklamalı ve bu verilerin taşınmasında korumalı iletişim kanallarını kullanmalıdır.	Yüksek			
120	Kullanılan veritabanının dışarıya aktarımı ancak veritabanı yönetim yetkisi olan hesaplarla yapılmalı ve öncesinde veritabanındaki kişisel verilerin silinmesi sağlanmalıdır.	Yüksek			

***Seviye**

4-Kritik: Bu seviyedeki güvenlik açıkları saldırganlar tarafından genellikle kötüye kullanılabilir, bütün uygulamanın ve sistemin ele geçirilmesiyle veya en azından hassas bilgilerin açığa çıkmasıyla sonuçlanabilir.

3-Yüksek: Bu seviyedeki güvenlik açıkları saldırganlar tarafından kötüye kullanılabilir ve uygulamadaki/sunucudaki güvenlik ve sistem yapılandırma bilgilerinin ele geçirilmesiyle sonuçlanabilir.

2-Orta: Bu seviyedeki güvenlik açıkları saldırganların hassas sistem ve program sürüm bilgilerini ele geçirmesine neden olabilir.

1-Düşük: Bu seviyedeki güvenlik açıkları saldırganların sistemin basit bilgilerini (portlar, servisler, sürüm) ele geçirilmesine neden olabilir.

6.Yararlanılan Kaynaklar

- Dayıoğlu, Burak, “Yazılım Geliştirme Yaşam Döngüsü ve Güvenlik”
- Kartın, Esma, “Güvenli Yazılım Geliştirme”
- Özbilgin, Dr.İzzet Gökhan, “Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi”
- Yılmaz, Yrd.Doç.Dr. Güray, “Yazılım Mühendisliği Gerçeği”,
- Beydağlı, Erkut, “Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler Standartı”
- Alparslan, Erdem, “Güvenli Yazılım Geliştirme Modelleri”
- Michael, C.C., Radosevich, Will, “Risk-Based and Functional Security Testing”,
- “Yazılım Güvenliği Yaklaşımı”, Labris Teknoloji,
- Cohen, Manu, “Practical Application Security”
- Çetinkaya, Mehtap, “Kurumlarda Bilgi Güvenliği Yönetim Sistemi’nin Uygulanması”
- International Standard, “ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements”
- Ottekin, Fikret, “Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri”
- Calder, Alan, Bon, Jan Van,“Implementing Information Security based on ISO 27001/ISO 17799 - A Management Guide”
- International Standard, ISO/IEC 27000:2009: Information technology –Security techniques – Information security management systems – Overview and vocabulary
- Layton, Timothy P. “Information Security: Design, Implementation, Measurement and Compliance”,
- Brooks, F.P., “No Silver Bullet Essense and Accidents of Software Engineering”
- Microsoft Security Lifecycle (SDL) Version 3.2
- COBİT, IT Governance Institute

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Ek-11 - BT Süreçleri İş Sürekliliği Planı

SHT-Siber talimatı Ek-11'de yer alan BT Süreçleri İş Sürekliliği Planı'na https://bulut.shgm.gov.tr/index.php/s/rlhIHIGYFGjRPjq adresi üzerinden ulaşabilirsiniz.

FELAKET KURTARMA MERKEZİ KURULUMU REHBERİ

1. KAPSAM VE AMAÇ

1.1. Felaket Kurtarma Merkezi Kurulumu nedir?

Felaket kurtarma merkezinin fiziksel olarak kurulması, iklimlendirme sistemleri, yapısal kablolama, enerji alt yapısı, yangın algılama ve söndürme sistemleri, ısı ve nem takip sistemleri, aydınlatma, fiziksel geçiş kontrol sistemleri, kamera sistemleri, izolasyon ve yükseltilmiş zemin, vb. faaliyetlerin belirli standartlara uygun yapılmasını kapsamaktadır.

1.2. Felaket kurtarma merkezi için durum raporu hazırlandı mı?

Felaket kurtarma merkezi yerinin seçimi, kullanılacak teknolojilerin ve kapasitelerinin belirlenmesi amacıyla bir durum raporunun hazırlanması gerekmektedir.

Hazırlanacak durum raporunda; felaket kurtarma merkezinin coğrafi lokasyonu, kurulum yapılması planlanan yerin fiziksel altyapısı göz önünde bulundurularak gerekli enerji altyapısı, sunucu kapasitesi, yükseltilmiş taban sistemleri, yangın söndürme sistemleri, trafo, kesintisiz güç kaynağı, jeneratör, fiziksel güvenlik ve ortam izleme gibi kriterler belirlenmelidir.

Durum raporunun hazırlanmasında, Felaket Kurtarma Merkezi Geliştirme / İyileştirme Fizibilitesi Rehberi'nden faydalanılabilir.

1.3. Uygun yer seçimi raporu hazırlandı mı?

Felaket kurtarma merkezinin seçileceği coğrafi mekân önemlidir. Felaket kurtarma merkezinin, mümkünse sistem odası/veri merkezi ile aynı il sınırları içerisinde olmaması tercih edilmelidir. Bu sayede deprem, sel, terör gibi her iki veri merkezini de kötü etkileyecek risklerin azaltılması sağlanabilir. Uygun yer seçimi raporunun hazırlanmasında, Felaket Kurtarma Merkezi Geliştirme / İyileştirme Fizibilitesi Rehberi'nden faydalanılabilir.

1.4. Felaket kurtarma merkezi mimari, elektrik ve mekanik konsept dizaynları hazırlandı mı?

Felaket kurtarma merkezi kurulumu aşamasında detaylı mimari (örneğin kabinetlerin yerleşimi UPS, jenaratör yerleştirilmesi gibi), inşai (yükseltilmiş zemin yangın kapısı gibi), elektrik (şebeke ve UPS elektrik kablolaması, topraklama), güvenlik (yangın algılama, kapı geçiş ve kamera sistemleri) ve mekanik projelerin hazırlanması (yangın ve klima sistemlerinin borulaması), yapısal kablolama altyapısının projelendirilmesi gerekmektedir.

Bu proje çizimleri üzerinden kurulumların yapılması ve projelendirilmesi uygulanacağından bir bütünlük oluşturması açısından önem arz etmektedir.

2. YAPILACAK İŞİN TANIMI

2.1. Felaket kurtarma merkezi network altyapısı planlandı mı?

Felaket kurtarma merkezi ile veri merkezi arasında iletişim için bulunan internet hat kapasitesinin yüksek olması veya ihtiyacı karşılaması önemlidir.

Network altyapısında yedekliliğin nasıl sağlandığı da sorgulanmalıdır. Bir veri merkezinin "Operatör Yedekliliğinin" olması, sadece tek bir operatörün internet hizmetine bağımlı kalmadan istediğiniz zaman internet servis sağlayıcınızı değiştirmenize imkân sağlar. Ayrıca, veri merkezinin fiber ve metro ethernet ağ altyapısına yakınlığı stratejik önem taşımaktadır.

Network planlaması yapılırken FKM'nin çalışma prensibinin de belirlenmesi gerekmektedir. Aktif-Aktif ve Aktif-Pasif network topolojilerinden hangisi ile çalışılacağı veri merkezinin fiber ve metro ethernet ağ altyapısına yakınlığına göre belirlenebilir.

Felaket kurtarma merkezinde, ANSI/TIA-942 standartlarına uygun olarak yapısal kablolama planları hazırlanmalıdır. Yapısal kablolama sistemindeki bakır kablolama ürünlerinde TIA-568-C2 ve ISO/IEC 11801 standardı, fiber kablolama ürünlerinde de TIA-568-C3 ve ISO/IEC 11801 standartlarının sağlandığına dikkat edilmelidir. Teknolojik gelişmelere paralel olarak kullanılan ürünlerdeki standartlar da değişebileceğinden dolayı yeni sürümler ve modeller takip edilmeli ve kullanılmalıdır.

Sistem odası ve veri merkezi yapısal kablolamasında kullanılacak olan bakır ve fiber kablolama ürünlerinin fabrikasyon sonlandırma olması kayıpları azaltacağından performansı arttıracak ve arıza oranlarını azaltacaktır.

Yapısal kablolama ürünleri uçtan uca etiketlenmelidir. Kullanılacak etiketlerin, sıcağa, soğuğa ve neme dayanıklı olması gerekmektedir. Etiketlemenin TIA-606-A standartlarına göre yapılması önerilmektedir.

Ayrıca bakır kablolama ürünlerinde, şimdiki teknolojiye göre Cat6A ve Cat7 kategorilerindeki kablolama ürünlerinin zırhlı veya folyo kaplı olması data kayıplarının azaltılmasında fayda sağlayacaktır. Zırhlı ve folyolu kablolarda doğru topraklama yapılması önem arz etmektedir.

2.2. Felaket kurtarma merkezi enerji altyapısı planlandı mı?

Felaket kurtarma merkezinin kullanacağı trafoların maksimum besleme kapasitesi öğrenilmelidir. Eğer trafo besleme kapasitesi veri merkezindeki sistemlerin çekeceği güç için yeterli değilse veri merkezi kapasitesine göre trafo planlanmalıdır. Bu planlama yapılırken ileride veri merkezine eklenecek yeni sistemler (kabinet, storage, klima, ağ cihazları, sunucu vb) de düşünülerek şimdiki ihtiyaçtan daha yüksek besleme güçlü trafo planlanabilir. Dağıtım trafolarının otomatik geçişli ve bire bir yedekli olması, şebeke enerjisinin kesildiği

anlarda yedekliliği sağlayacaktır.
Jeneratörlerin adedi, kapasitesi ve besleme süreleri iş sürekliliği açısından önem arz etmektedir. Jeneratör kapasite planlamalarında klimaların iç ve dış ünite demeraj akımları planlamaya dahil edilmelidir. Jeneratör sistemlerinde birçok marka ve model içten yanmalı motor bulunmaktadır. Dizel jeneratörlerin verimliliği yüksekken, uzun vadeli tasarruf için doğalgaz beslemeli motorlar da tercih edilebilir.

Felaket kurtarma merkezinde kullanılan UPS sistemlerinin yedekliliği sağlanmalıdır. Ortalama bir veri merkezi UPS besleme süresi 10 dakika olarak planlanmalıdır. Daha yüksek besleme sürelerinin batarya maliyetlerini ve bakım maliyetlerini arttıracağı unutulmamalıdır. Günümüzde kullanılan veri merkezlerindeki UPS sistemleri statiktir. Veri merkezindeki yüksek enerji ihtiyaçlarında yeni teknoloji dinamik UPS sistemleri de kullanılabilmektedir. Dinamik UPS sistemlerinin avantajları ise; aşırı ısı üretmez, iklimlendirme ihtiyaçları yoktur, verimliliği yüksektir, akü maliyetleri yoktur.

Çözüm	Güç Bileşenleri		Enerji Depolama Aracı		Dizel Kullanımı
	Elektronik	Döner Elektrik Makinası	Aküler	Kinetik Enerji	Dizel
Dinamik UPS	Hayır	Evet	Hayır	Evet	Evet
Hibrit Dinamik UPS	Evet	Evet	Hayır	Evet	Evet
Statik UPS	Evet	Hayır	Evet	Hayır	Evet

Elektrik dağıtım panoları mevcut enerji altyapısına yetecek ve en az %20 genişleme kapasitesi ile tasarlanmalıdır. Dağıtım panolarındaki tüm bağlantıların klemensler vasıtasıyla irtibatlandırılması gerekmektedir. Elektrik panolarındaki şalt malzemelerin TSE standartlarını sağlaması riskleri azaltmak açısında önemlidir. Panolar üzerinde enerji analizörleri konumlandırılarak giriş/çıkış elektriksel farklılıkların ve dalgalanmaların takip edilmesi oluşabilecek sorunların önceden engellenmesi için faydalı olacaktır.

Felaket kurtarma merkezi aydınlatmasında elektronik balastlı ürünlerin kullanılması elektriksel parazitlenmenin önüne geçecektir. Yeni teknolojilerden Led aydınlatma sistemleri ile de enerji verimliliği sağlanması planlanmalıdır. Acil aydınlatma ve yönlendirme sistemlerinin kendilerine ait batarya sistemi olması gerekmektedir. ANSI/TIA-942 standardına göre yatayda 500 lüx, dikeyde 200 lüx aydınlatma gerekliliği sağlanmalıdır.

Kabinet içine yerleştirilecek aktif cihazların enerji tüketim değerleri doğru hesaplanmalı ve uygun bir PDU seçilmelidir. Örnek vermek gerekirse; hangi kabinete, kaç adet ve ne tip sunucu veya switchler yerleştirilecek). Yanlış yapılacak seçimler mevcut PDU'ların yeterli kapasitede kullanılamamasına sebep olacaktır. Mümkün oldukça, yönetilebilir PDU tercih edilmelidir. Yönetilebilir PDU'lar soket bazında enerji tüketimi, akım, voltaj

vb gibi değerleri sağlamaktadır. Cihazların uzaktan kapatılıp açılmasında yönetilebilir PDU'lar önemli rol oynamaktadır. Yönetilebilir PDU'lar üzerine sıcaklık ve nem sensörleri konularak kabinet içi değerler uzaktan izlenebilmekte veya raporlanabilmektedir.

Felaket kurtarma merkezi içerisinde yer alan elektriksel elemanların bir merkezden kontrolü, yaşanan olayların kayıt altına alınması ve izlenmesi önem kazanmaktadır. Enerji izleme yazılımı ile elektriksel raporlamalar ve hatta faturalama işlemleri yapılabilmektedir. FKM için PUE (Power Usage Effectiviness) hesaplaması yapılabilmektedir.

2.3. Felaket kurtarma merkezi iklimlendirme sistemi planlandı mı?

Bir FKM'de çalışan çok sayıda ekipmandan (sunucu, switch, depolama cihazı, vb.) dolayı ortam ve cihazların aşırı ısınması söz konusu olabilmektedir. Bu nedenle iklimlendirme sistemi, sıcaklık ve nem kontrolü için önemlidir.

Oda tipi, koridor tipi, kabinet içi, kabinet arkası, kabinet üstü, vb. gibi farklı biçimlerde kullanılabilen iklimlendirme sistemleri bulunmaktadır.

Günümüzde en yaygın soğutma yöntemi soğuk hava (Klima) ile yapılmaktadır. Su ile soğutma (Green Data Center) yeni bir çözüm olarak karşımıza çıkmaktadır. ANSI/TIA-942 standardı, soğutmada en öncelikli yapılması gereken çalışmayı, kabinlerin yerleşimlerinin düzenlenmesi olarak ortaya koymaktadır. Bu çözümde dikkat edilmesi gereken sıcak ve soğuk hava koridorları oluşturmaktır. Kabin ve Klima yerleşimlerinde cihazların soğuk havayı çektiği ve sıcak havayı boşalttığı alanlar bir koridor gibi oluşturulmalıdır. Sıcak hava öz kütleden dolayı yükseleceği için klimalar bu havayı çekebilecek konumda olmalıdır. Soğuk hava ise yükseltilmiş zeminin altından kabin önlerindeki menfezlerden cihazlara ulaşmalıdır. Devamlılığın öneminden dolayı klimaların yedekliliği de son derece önemlidir. Klimalar sık arızalanan bir yapıya sahiptir bu yüzden yedeklilik son derece önemlidir.

ANSI/TIA-942 standartlarına göre koridorların asgari genişliği 100 cm, kabinet arkası genişlik ise en az 60cm olarak belirlenmelidir.

FKM iklimlendirme sisteminin döşeme altından soğutması planlanıyorsa elektrik kablolamasının döşeme altında hava akışını engellemeyecek şekilde planlanması gerekmektedir. Data kablolaması ise kabinet üstünden tel tava ve fiber kanallar ile çekilerek havalandırmayı engellememesi sağlanmış olmalıdır.

Bir başka iklimlendirme yöntemi olan "Free Cooling", iklimlendirmede kullanılan suyun soğutulması için dış ortamda yer alan düşük sıcaklıktaki havanın kullanılması ile soğutmayı mümkün kılar. Soğuk gece ve kış aylarında bu işlemle enerji tüketiminde %70'e kadar tasarruf sağlanabilmektedir. Ortalama sıcaklığın yüksek olduğu coğrafi bölgelerde bu sistem verimlilik sağlamamaktadır.

2.4. Felaket kurtarma merkezi fiziksel güvenliği düşünüldü mü?

FKM'ne giriş/çıkışlar kontrol altına alınmalı, yetkisiz personelin FKM'ne girişi engellenmelidir. Dışarıdan gelen bir kişinin yetkili personelin gözetimi olmadan FKM içerisinde çalışma yapmaması sağlanmalıdır. Bu bilgi güvenliği açısında da önemlidir. FKM içerisine giriş çıkışlar kayıt altına alınmalı, periyodik olarak raporlanmalı ve FKM yöneticileri tarafından değerlendirilmelidir. FKM'ne giriş/çıkış kontrolü için kullanılabilecek farklı sistemler bulunmaktadır. Günümüzde en sık kullanılan yöntemler kart okuyuculu cihazlar ve parmak izi okuyuculu cihazlar ile oluşturulan giriş kontrol sistemleridir.

Güvenlik kamera sistemleri ile veri merkezinde ölü alan kalmayacak şekilde izleme yapılmasına imkân sağlayacak kamera tasarımları yapılmalı ve FKM sürekli izlenmelidir. Aynı şekilde UPS odaları, trafo odaları ve jeneratör odaları gibi kritik alanlar sürekli izlenmeli ve kayıt altına alınmalıdır. Günümüz teknolojisine göre IP (network) tabanlı yüksek çözünürlüklü kamera sistemleri kullanılmaktadır. İhtiyaç durumuna göre hareketli veya sabit kameralardan yararlanılmalıdır. Karanlık mekânlarda veya ışık seviyesi düşük mekânlarda gece görüş özellikli kameralar tercih edilmelidir.

FKM'nin bulunduğu odada pencere var ise bu pencerelerin ısı ve yangın yalıtımlı duvarlar ile kapatılması önerilmektedir.

FKM odasının kapıları yangına dayanıklı ve geçiş güvenliği olan (kartlı, parmak izi, retina) kapılar olması tercih edilmelidir.

2.5. Felaket kurtarma merkezi için yangın algılama ve söndürme sistemi düşünüldü mü?

FKM'de bulunan elektronik cihazlara ve personele zarar vermeyecek yangın söndürme çözümleri seçilmelidir. Mümkünse, uygun duman algılama sensörleri ile yangının hangi alanda çıktığı öğrenilebilmeli ve yangın söndürmenin hangi sunuculara/sistemlere yapıldığı bilinmelidir. Yangın söndürme çözümlerinde sık kullanılan gazlar FM200, FE25, Argon ve Novec 1230 gazlarıdır.

Novec 1230, elektriksel iletkenliği olmayan, kokusuz, renksiz, hızla buharlaşan söndürme sıvısıdır. Ozon yok etme katsayısı sıfırdır. Atmosferik ömrü sadece 5 gündür ve çevre dostudur.

FM200 gazı, Halon 1301 gazının kullanımının yasaklanması sonrasında piyasaya sürülmüştür. Kullanımı en yaygın gazdır. Özellikle narin elektrikli ve elektronik cihazların bulunduğu, insanlı ortamlarda en etkin çözüm olarak kullanılmaktadır. FM 200 gazı yangında önemli rol üstlenen kimyasal reaksiyonları kırma ve ısı enerjisini absürde etme özelliği ile yangınları söndürmektedir. Gazlı söndürme sisteminde amaç içeride bulunan oksijeni emmektir. Bu yüzden sensörler bir yangın algıladığında ilk yapacağı hamlelerden biri içeride bulunan personelin tahliye edilmesi ve klimaların kapatılması olmalıdır. Bu içerdeki personelin zarar görmesini, dumanın tüm ortama yayılmasını ve yangın şiddetinin artmasını engelleyecektir.

Yangın algılama ve söndürme sistemi NFPA standartlarında olmalı ve 7/24 çalışmalıdır.

Sistem odası ve veri merkezi dışına çıkan boru, elektrik ve veri güzergahlarındaki boşluklar uygun yangın izolasyon malzemeleri ile doldurularak dışarıdaki bir yangının içeri ulaşması engellenmelidir.

FKM girişlerinde konumlandırılacak yangın kapılarının TS-EN 1634-1 sertifikasına sahip olması önemlidir. Tüm yangın kapılarının montajı tamamlandıktan sonra oda sızdırmazlık raporlarının alınması önerilmektedir.

2.6. Doğal afetlere karşı önlemler alındı mı?

FKM'nin her türlü afete hazır olması gerekmektedir. Elektrik kesintileri, su baskını, fırtına, deprem, terör ve diğer olağanüstü durumlar için gerekli önlemler alınmalıdır.

Yaşanabilecek bir sel felaketi veya yangın, sensörler ve dedektörler kullanılarak sürekli takip edilmeli, FKM'nin otomasyon sistemi aracılığı ile sesli uyarı ve ikaz cihazları çalışmalı, ihtiyaç halinde gerekli kişiler mail veya sms yoluyla bilgilendirilmelidir.

FKM binası deprem yönetmeliğine uygun ve FKM donanımlarının ağırlıklarını taşıyacak şekilde tasarlanmalıdır. İhtiyaç halinde bina kolon ve sütunlarında gerekli güçlendirme çalışmaları planlanmalıdır.

FKM'de kullanılan kabinetlerin iç tasarımlarında ağır cihazların alt kısımlara ve hafif cihazların kabinet üstüne yerleştirilmesine dikkat edilmelidir. Kabinet içine yerleştirilecek cihazların ağırlıkları kabinet seçiminde dikkate alınmalıdır.

Yükseltilmiş döşeme sistemlerinin üzerinde bulunan kabinetlerin deprem anında salınımını azaltmak için kabinetlere deprem ayakları takılarak zemine sabitlenmelidir.

İklimlendirme sulu soğutma sistemi kullanılacak şekilde tasarlanmış ise bina birleşim yerlerinde (dilatasyon noktaları) mekanik borulamada esnek bağlantı birimleri kullanılmalıdır.

2.7. FKM ortam izleme sistemi düşünüldü mü?

FKM güvenliğini izleme ve oluşabilecek kötü durumların önceden tespit edilmesini sağlama amacıyla ortam izleme sisteminden yararlanılır.

FKM 7/24 kamera sistemi ile izlenmeli ve kayıt altına alınmalıdır. Olası istenmeyen bir durumda izlemeyi gerçekleştiren personel, yaşanan durumun önemine göre sorumlu olan personelle irtibata geçmeli ya da kendisi veri merkezine müdahale edebilmelidir.

Buna ilave olarak FKM'inde yangına karşı ısı ve duman, su baskınına karşı su sensörü, nem durumunu takip

edebilmek için nem sensörü, kapı giriş çıkış ve açık kalma senaryolarının yapılması için kuru kontakları, gerekirse sismik sensör kullanımı ile ortam anlık olarak izlenebilmektedir.

2.8. FKM yükseltilmiş döşeme sistemi ve kablo kanalları planlandı mı?

FKM kurulumunda bu iki adım birbiriyle paralel ilerlemelidir. Kablo kanalları döşeme işlemi bittikten sonra zemin döşeme işlemi yapılmalıdır. Yük durumunda, elektrik kabloları etrafında oluşacak manyetik alan data kablosunda kayıplara sebep olabilmektedir. Bu nedenle, enerji ve data kablo tavaları birbirinden ayrı ve belirli mesafelerde çekilmelidir.

TIA ve TSE standartlarına göre FKM tüm kablolar düşük halojenli LSZH veya L0ZH tipi olmalıdır.

Zemin döşemesi kablo kanallarına ve soğuk hava akışına imkân verecek şekilde uygun bir yükseklikte (asgari 50 cm) yapılmalıdır. Kullanılacak döşeme malzemeleri kabinlerdeki tam dolu olma durumu göz önünde tutularak en az 1000 kg kadar basınca dayanabilecek sağlamlıkta seçilmelidir. Günümüz kabinlerinin 1500 kg kadar yük taşıma kapasitelerine sahip olabildikleri göz önünde bulundurulmalıdır. Zemin altında karoları tutan destek ayakları mümkün olduğunca kabin ayaklarının basacağı noktaların altına veya yakınına konarak kabin yüklerinin taşınması kolaylaştırılmalıdır. Kabinlerin sallanması gibi ihtimallere karşı bu ayaklar yerlerinden kolayca oynamayacak ve birbirine destek olabilecek şekilde yerleştirilmelidir.

Yükseltilmiş zeminde, kabin önlerine açılacak menfezler ile klimadan çıkan soğuk hava en sağlıklı şekilde ulaştırılmalıdır. Zemin altında yangın sensörleri bulundurulmalıdır.

Yükseltilmiş zemin panelleri yanmaz özellikte kalsiyum sülfat özlü olmalıdır. Kalsiyum sülfat özlü paneller diğer sunta özlü panellerden daha fazla yük taşıma endeksine sahiptir. Panellerin üst yüzeyleri antistatik özellikte olmalı, kolay çizilmeyen ve yırtılmayan HPL türü malzemeler ile kaplı olması tercih edilmelidir. Panellerin alt yüzeylerinin çelik sac ile kaplı olması ayrıca yük dayanımını arttırmaktadır.

3. İŞ MODELİ

3.1. Felaket kurtarma planı hazırlandı mı?

Felaket kurtarma planı, kurumun bir felaket yaşanması durumunda, gerçekleştirilecek faaliyetleri içeren planlardır. Bu plan içerisinde, kurum için önemli hizmetlerin ve bu hizmetleri oluşturan bileşenlerin bir felaket durumunda (genellikle bir Felaket Kurtarma Merkezi) içerisinde nasıl çalışır hale getirileceği detaylı bir şekilde tarif edilir.

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.

TÜBİTAK-BİLGEM-YTE

Felaket kurtarma planı aynı zamanda veri yedeklerinin de saklanmasını ve gerekli durumlarda bu yedeklerden geriye dönülebilmesini de öngörmeli ve mümkünse veri kaybının olmamasını sağlamalıdır.

Felaket kurtarma planının doğruluğu ve güncelliği, belirli aralıklarla, kapsamlı testlerle denenmelidir. Kurumlarda yaşanan değişikliklerin, planı etkilemesi durumunda, plan değişikliklere göre uyarlanmalı ve yeniden test edilmelidir. Bu plan yalnızca felaket anında kullanılan bir belge değil, aynı zamanda kurumun iş ve hizmet sürekliliği ile ilgili işleyişinde ve süreçlerinde aksaklık ve eksiklerin tespit edilmesini sağlayan, felaketlerin önlenmesi ve etkilerinin azaltılması yönünde iyileştirmeleri de mümkün kılan bir belge olmalıdır. Hizmetleri ve hizmetleri oluşturan bileşenleri, bir felaket durumunda kurtarabilmek için farklı teknolojilerden yararlanılabilir. Kullanılabilecek teknolojiler, kurumun var olan teknik altyapısına göre değişir. Kullanılan sunucular, işletim sistemleri, uygulamalara göre farklı çözümler kullanabilir. Temel olarak kullanılan bazı teknolojiler şunlardır:

- Sanallaştırma; sunucuların donanım bağımsız olmasını sağlamaktadır.
- Cluster (kümeleme) çözümleri; bir sistemin benzer başka sistemler ile birlikte (yedekli) çalışmasını sağlayan çözümlerdir.
- Storage replikasyon; depolama üniteleri arasında verilerin birebir kopyalanmasını sağlayan çözümlerdir.
- Backup (Yedekleme) çözümleri; verilerin bir yedeğinin saklanıp gerektiğinde tekrardan alınmasını sağlayan çözümlerdir.
- Bağlantı çözümleri; verilerin Felaket Kurtarma Merkezi'ne sağlıklı bir şekilde aktarılabilmesi için kullanılacak bağlantı teknolojileri önemlidir. Felaket Kurtarma Merkezi'nin bulunduğu yere göre Fiber, Noktadan-noktaya MetroEthernet, Noktadan-noktaya G.SHDSL, VPN ve GSM üzerinden APN vb. teknolojiler kullanılabilir.

Özet olarak, felaket kurtarma amacıyla kullanılacak sistemler, kurumun var olan BT altyapısı ve Felaket Kurtarma Merkezi'nin yerine göre şekillendirilebilir

3.2. FKM'nin yapılanmasında uygulanacak yöntem belirlendi mi?

FKM ile ana veri merkezi/sistem odasının birlikte nasıl çalışacağı (aktif-pasif (asimetrik) ya da aktif-aktif (simetrik)) belirlenmelidir.

Aktif-pasif modelde, veri merkezi tarafı aktiftir ve tüm işlemleri kendisi üstlenmiştir. Pasif taraftaki FKM ise hazırda bekleme durumunda ve veri merkezinin yedeği olarak görev yapar. Herhangi bir felaket durumunda FKM devreye girer ve işlemlerinin devam etmesini sağlar.

Aktif-aktif modelde ise veri merkezi ve FKM tarafı birbirinden bağımsız fakat birlikte işlemleri yürütmektedir. Bir felaket durumunda, herhangi bir tarafın durması sonucu diğer taraf yükü üzerine alır, tüm işlemleri üstlenir. Duran taraf onarıldığı ve ayağa kaldırıldığı zaman tekrar kendi işlerini üstlenerek çalışmasına devam eder.

3.3. Farklı üretici çözümleri değerlendirildi mi?

İklimlendirme sistemleri, yapısal kablolama, enerji alt yapısı, yangın algılama ve söndürme sistemleri, ısı ve nem takip sistemleri, aydınlatma, fiziksel geçiş kontrol sistemleri, kamera sistemleri, izolasyon ve yükseltilmiş zemin sistemleri ile ilgili üreticilerle temasa geçilip bilgiler alınmalı ve yaklaşık maliyetlendirmesi üreticilerden talep edilmelidir.

İhtiyaç duyulan sistemler farklı üretici ve yüklenici tarafından farklı çözümler sunularak sağlanabilir. Bu nedenle aynı kategorideki farklı üreticilerin çözümleri değerlendirilip, avantaj ve dezavantajlarına göre en uygun ürün seçilmelidir. Farklı üreticilerin sunduğu çözümler bir test, pilot veya PoC ortamında gözlemlenerek hangi çözümün neler sağlayabileceği detaylı olarak değerlendirilmelidir. Bu çalışmayla önerilen çözümlerin avantajları ve kurumun ihtiyaçlarını ne düzeyde karşıladığı gibi konular gözlemlenebilir. Böylelikle, ihtiyacı tam olarak karşılamadığı düşünülen noktalar varsa bunlar tedarik öncesinde daha detaylı olarak değerlendirilebilir.

Projelerde farklı kriterlerin ağırlığı hesaplanarak bir teknik değerlendirme tablosu hazırlanabilir. Bu değerlendirme tablosunda fiyat, çözümün teknik yeterliliği, ölçeklenebilirlik, yönetilebilirlik, süreklilik, uyumluluk ve ileride duyulacak ek ihtiyaçlar gibi faktörlerin çözüm içinde hangi önem ağırlığında olduğunun netleştirilmesi daha efektif bir karar verilmesini sağlayacaktır.

Çok sayıda çözümün değerlendirilmesi, hem zaman ihtiyacı gerektirdiği, hem de kaynak sayısını arttıracağı için PoC testi yapılacak ürünler, bu ürünleri kullanan diğer kurumların memnuniyet durumlarına göre sayıca kısıtlanabilir. Böylelikle önerilen çözümler tüm özellikleriyle daha detaylı değerlendirilmiş olacaktır.
Seçilecek çözüm içerisinde yer alacak ürünlerin ileride ihtiyaç duyulabilecek bir ölçeklenme çalışması sırasında farklı marka ürünlerle olan uyumluluğu incelenmeli ve mümkün olduğu kadar üretici bağımlılığından kaçınılmalıdır.

Alınması planlanan çözüm (ve içerisinde yer alan sistemler/ürünler) için bağımsız değerlendirme kuruluşlarının veya organizasyonlarının hazırladığı raporlarının incelenmesi faydalı olur. Bu kuruluş ve organizasyonlar ilgili ürünleri kendi test ortamlarında eşit şartlarda değerlendirmeye tabi tutarlar ve test sonucu teknik rapor oluştururlar. Buna ek olarak, ürünlerle ilgili farklı karşılaştırmalar da (ürünün geleceği hakkındaki planları, güçlü yönleri, zayıf yönleri ve dikkat edilmesi gerekli noktalar vb.) bu incelemede yer alır. Bu değerlendirmeler dikkatli incelenirse doğru ürünü bulmada yol gösterecektir.

3.4. Farklı Kurumlarda bulunan FKM'ler ziyaret edildi mi?

FKM'si olan kamu kuruluşları araştırılarak yapılan çalışmalar ve modellemeler araştırılarak değerlendirilmelidir. Yapının nasıl kurulduğu ve işletildiği öğrenilmelidir. Diğer kamu kurumlarının bilgi ve tecrübeleri dinlenerek doğru çözümlerin konumlandırılması sağlanmalıdır. Bir FKM'si bulunan kurumların, FKM kurulumu öncesi ve FKM kurulumu sonrası varsa yaşadığı sıkıntılar ve öneriler, gerek çözüm seçiminde,

gerekse FKM kurulumunda yol gösterici olacaktır.

3.5. FKM yönetimini yapacak yeterli sayı ve yetkinlikte personel bulunuyor mu?

FKM'nin verimli olarak yönetilebilmesi, işletim sırasında oluşabilecek aksaklıkların hızlı ve kolay çözülebilmesi için Kurum'un personel ihtiyacı göz önüne alınmalıdır. Personel yetkinliğinin arttırılması gerekiyorsa alınacak eğitimler planlanarak anlaşma kapsamına eklenmelidir. FKM kurulumu ve işletim sürecinde yeterli personel yoksa dışardan bir kaynak alımı planlanması önemli olacaktır.

3.6. Personel eğitimi planlaması yapıldı mı?

Personel yetkinliğinin arttırılması için eğitimler planlanarak anlaşma kapsamına eklenmelidir. Bu eğitimler kurulacak FKM içerisinde yer alan yönetim araçlarının ve ekipmanların doğru bir biçimde kullanılması ve arıza durumunda nasıl bir yönerge izleneceğinin bilinmesi açısından fayda sağlayacaktır. Aynı zamanda sorunlara müdahale ve çözüm süresini kısaltacaktır.

3.7. Üretici veya danışmanlık verecek yüklenici firma değerlendirildi mi?

FKM kurulumunda birlikte çalışılacak firma (ya da firmalar) için karar verilirken, aşağıdaki maddeler göz önüne alınarak bir değerlendirme formu hazırlanabilir:

- İlgili alandaki pazar payı,
- İlgili teknolojiler konusunda standardizasyon belirlenmesine yapılan katkıları,
- Kurumsal sertifikasyon sahipliği,
- Sektördeki tanınırlığı,
- Arge'ye yaptığı yatırım oranı,
- İlgili alanlardaki patent ve buluşları,
- Çözüm geliştirme aşamalarında üniversitelerle olan ortak çalışmaları,
- Çözümlerinin bilinirlik düzeyleri,
- Üretim merkezlerinin yaygınlığı ve lojistik, bayi, distribütör ve kanal yapısının yeterliliği,
- İlgili çözüm ve projeyi stratejik olarak görüp görmedikleri,
- Kalite belgeleri ve hangi standartlarla uyumlu oldukları,
- Sertifikalı personel sayısı ve personelin nitelikleri,
- Yerleşik ofisi bulunup bulunmadığı ve yakın konumda çalıştırdığı personel sayısı,
- Faaliyete başladığı yıl,
- Daha önce yapılmış benzer projelerdeki referansları,
- Referans projenin büyüklüğü, karmaşıklığı, hangi noktalarda altyüklenici veya dış kaynak kullandığı/kullanacağı,
- Referans listesinde yer alan kurumlardan görüş alınması,
- Servis ağının yaygınlığı,
- Teknik destek elemanlarının yetkinliği ve uzmanlık sertifikaları,
- Çağrı merkezi, yedek parça ve çağrı takip süreçlerinin bulunması,

- Danışmanlık hizmeti verebilmesi,
- İlgili alanlardaki kalite belgeleri

Uzun süreli ve detaylı projelerde birlikte çalışılacak firmanın finansal durumunun proje sürecini ve kapsamını belirlenen süre içinde yürütebilecek yeterlikte olup olmadığı değerlendirilmelidir.

4. ÇIKTILAR

4.1. FKM topolojisi hazırlandı mı?

Uygulanan yöntemin (aktif-aktif veya aktif-pasif) topolojisinin bilgileri ve çalışma prensipleri dokümante edilerek saklanmalıdır. İleride yapıyı bilmeyen personele kaynak başvurusu olabilecektir.

4.2. Felaket kurtarma planı hazırlandı mı?

Felaket kurtarma planının son hali belge durumuna getirilerek saklanmalı ve ilgili personel ile paylaşılmalıdır. Hazırlanan felaket kurtarma planı dahilinde gerekli testler yapılarak doküman güncelleme ihtiyaçları düzenlenmelidir.

4.3. Proje çizimleri var mı?

FKM mekanik, elektrik, yapısal kablolama, yangın söndürme, inşaat ve kablo kanalları gibi sistemlerin proje çizimlerinin sağlanması (şartname oluşturulma aşamasında) gerekmektedir.

Proje sonunda yüklenici veya üreticiden as-build (son durum) çizimleri alınmalıdır. Bu çizimlerin ilerideki değişikliklerde veya modernizasyonda kullanılması için saklanması önemlidir.

4.4. Eğitim dokümanları ve kullanıcı kitapçıkları var mı?

Firmalardan alınan eğitimlerden elde edilen dokümanlar ve ürünlerin kullanıcı kitapçıkları ileride oluşabilecek herhangi bir sorunda danışılabilmesi için saklanmalıdır.

Ek-13. Siber Olay Analiz Formatı

Firma Adı	
Tarih	
Raporu Hazırlayan	
Raporu Onaylayan	

1.Siber Olay Hakkında Özet Bilgi

Olay Türü		
Olay Gerçekleşme Saat Aralığı		
Olay Açıklama		
Kesinti Süresi		
Etkilenen Hizmetler/Süreçler		
Tahmini Maddi Kayıp		

2.Siber Olay Süreci Detaylı Anlatım

3.Kök Neden Analizi

4.Olayın Tekrarlanmaması İçin Alınacak Aksiyonlar

5.Alınacak Aksiyonların Projelendirme Süreçleri

No	Düzeltici Faaliyet	Proje Başlama Tarihi	Proje Bitiş Tarihi

Kurumsal SOME Yöneticisi
Tarih

İmza

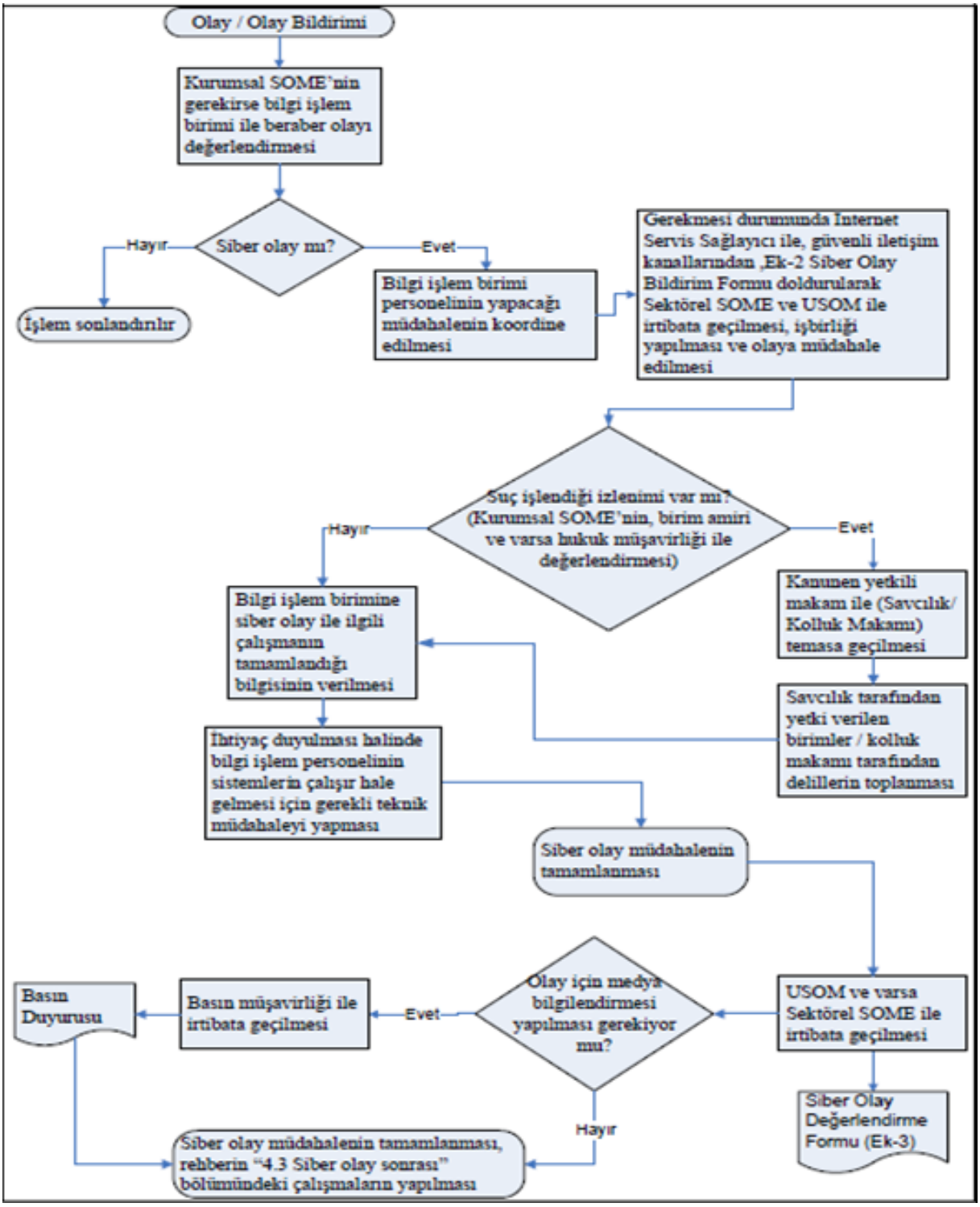
İşletme Genel Müdürü
Tarih

İmza

Ek-14. Siber Olay İstatistiksel Bildirim Formu

No	Çeyrek	Saldırı Türü	Toplam Saldırı Sayısı	Engellenen Saldırı Sayısı	Engellenemeyen Saldırı Sayısı

Ek-15. Bilişim Sistemleri Güvenlik Test Süreci



SIZMA TESTİ HİZMETİ VEREN PERSONEL VE FİRMALAR İÇİN YETKİLENDİRME PROGRAMI

İlk yayınlanma: 01.10.2013
R2: 05.01.2014
R3: 24.03.2014
R4: 15.04.2014
R5: 02.05.2014
R6: 16.05.2014
R7: 28.05.2014
R8: 20.02.2015
R9: 20.03.2015
R10:14.05.2015
R11:14.09.2015

Bu dokümana aşağıdaki web sayfasından erişilebilir:

- Türk Standardları Enstitüsü Resmi web sitesi (TSE) (bilisim.tse.org.tr).

İÇİNDEKİLER

0. GİRİŞ

Bilgi, içinde bulunduğumuz iletişim çağında bir kurumun en önemli varlıklarından biridir. Bu kapsamda Bilgi'nin temel güvenlik özellikleri olan Gizlilik, Bütünlük ve Erişilebilirlik özelliklerinin korunması çok kritik ve kaçınılmazdır. Bu özelliklerden herhangi birinin zarar görmesi etki seviyesine göre kuruma zarar verir. Bu sebeple bilginin işlendiği sistemler ve uygulamalar düzenli olarak güvenlik testlerine tabi tutulmak suretiyle dışarıdan ve içeriden gelebilecek saldırılara karşı, bu sistem ve uygulamalardaki zafiyetler tespit edilerek kapatılmalıdır. Bu program dokümanında sızma testi yapan firmalara ve personellere ait kriterler ve şartlar ortaya konulmaktadır.

Sızma testi, bilgisayar ve ağ güvenliğini dışarıdan veya içeriden yapılan bir saldırı ile değerlendirme yöntemidir.

Sızma testlerinin kuruluşlara çeşitli yararları vardır. Bunlardan bazıları aşağıda sıralanmıştır:

- Belirli bir saldırı vektör kümesinin olabilirliğinin belirlenmesi,
- Belirli bir sıralamada kullanılan düşük riskli açıklıkların bir kombinasyonundan kaynaklanan yüksek riskli açıklıkların tespit edilmesi,
- Otomatize ağ veya uygulama açıklık tarama yazılımları ile tespit edilmesi güç veya imkânsız olan açıklıkların tespit edilmesi,
- Başarılı saldırıların, olası iş etkisi ve işletimsel etkilerinin büyüklüğünün anlaşılması ve değerlendirilmesi,
- Ağ koruma cihazlarının ve uygulamalarının saldırıları başarı ile tespit etme ve karşılık verme kabiliyetlerini test etme,
- Güvenlik personeli ve teknolojisine yönelik artan yatırımlara gerekçelendirme sağlanması.

Sızma testleri genellikle tam güvenlik denetimlerinin bir parçası olmakla beraber (örneğin; PCI DSS standardı hem yıllık olarak hem de devamlı olarak (sistem değişikliklerinden sonra) sızma testi gerektirmektedir. Benzer şekilde, ISO/IEC 27001:2005 standardı kapsamı dâhilinde sızma testi yapılması gerekmektedir) tek başına da yapılabilir.

Sızma testlerinde bazı riskler ve dikkat edilmesi gereken noktalar da vardır:

- Test yapılırken, sisteme aşırı yüklenme veya hata oluşturma sonucunda işletimsel sistemde çökme veya hatalı çalışma gibi sorunların yaşanması,
- Kurumsal verilerin kasti veya kasıtsız olarak test esnasında değiştirilmesi,
- Daha önce yaptırılan testlere ait sonuçların, 3.tarafların eline geçerek kötü niyetli olarak kullanılması.

Bu hususlarla ilgili kuruluşlara yönelik olarak bu dokümanda alınması gereken tedbirlere dair bilgilere de yer verilmiştir.

1.KAPSAM VE UYGULAMA ALANI

Bu kriter programı, sistemlerdeki açıklıkları tespit etmek, bu açıklıklardan yararlanılabildiğini göstermek ve bu açıklıkları raporlamak için sızma testi yapan kişi ve kuruluşların sahip olması ve yerine getirmesi gereken kriterleri kapsar. Sızma testi dışında kalan fakat sızma testleri ile ilintili olan; Tersine Mühendislik, Zararlı Yazılım Analizi, Exploit Geliştirme, Zafiyet Araştırma (Vulnerability Research) ve Adli Bilişim gibi konular bu programın kapsamı dahilindedir.

2.ATIF YAPILAN STANDARDLAR VE/VEYA DOKÜMANLAR

EN, ISO, IEC vb.No	Adı (İngilizce)	TS No	Adı (Türkçe)
ISO/IEC 27001:2013	Information technology – Security techniques – Information security management systems - Requirements	TS ISO/IEC 27001:2013	Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler

3.TERİM VE TARİFLER

Bu program için aşağıdaki terim ve tarifler geçerlidir.

3.1. Sızma testi ve türleri

Belirlenen sistemin veya ağın güvenlik açısından analiz edilmesi ve sistemin güvenlik açıklarının ve güvenlik boşluklarının bulunması, bu açıklardan faydalanılarak sistemlere sızılması. Otomatik tarama araçları ile gerçekleştirilen zafiyet taramaları sızma testinin bir aşamasıdır; ancak sızma testi değildir.

3.1.1. Beyaz kutu

Beyaz kutu ağ'daki tüm sistemlerden bilgi sahibi olarak yapılan sızma testi türüdür. Test uzmanının dışarıdan ya da içeriden ağa girmeye ve zarar vermeye çalışmasının simülasyonudur.

3.1.2. Siyah kutu

Siyah kutu testi saldırı yapılacak ağ hakkında hiçbir bilgi sahibi olmadan dışarıdan ağa ulaşmaya çalışan saldırganın verebileceği zararın boyutlarının algılanmasını sağlar.

3.1.3. Gri kutu

Gri kutu testi iç ağda bulunan yetkisiz bir kullanıcının sistemlere verebileceği zararın analiz edilmesini sağlar. Veri çalınması, yetki yükseltme ve ağ paket kaydedicilerine karşı ağ zayıflıkları denetlenir.

3.2. Kuruluş

Sızma testi yaptıran tüzel kişilik.

3.3. Firma

Sızma testi yapan tüzel kişilik.

3.4. Hizmeti aksatma testi (DOS)

Hedef sistemin kaynaklarının ya da bant genişliğinin meşgul edildiği saldırılardır.

3.5. Politika

Yönetim tarafından resmi olarak genel niyetin ve yönün ifade edilmesi.

3.6. Üçüncü taraf

Söz konusu olan konu ile ilgili, taraf bakımından bağımsız olarak kabul edilen kişi ya da kuruluş.

[ISO/IEC Guide 2:1996]

3.7. Tehdit

Bir sistem veya kuruluşta zarara neden olabilecek istenmeyen bir olayın potansiyel nedeni.

[ISO/IEC 13335-1:2004]

3.8. Zayıflık

Bir veya birden fazlar tehdit tarafından istismar edilebilecek bir veya bir grup varlığın zayıf noktaları.

4. KISALTMALAR

DDoS **:** Distributed Denial-of-Service
DoS **:** Denial-of-Service
DNS **:** Domain Name System
FTP **:** File Transfer Protocol
HTTP : Hyper Text Transfer Protocol
HTTPS : Hyper Text Transfer Protocol Secure
IP **:** Internet Protocol
ISO **:** International Organization for Standardization
OWASP **:** Open Web Application Security Project
PCI-DSS **:** Payment Card Industry - Data Security Standarts
SCADA : Supervisory Control and Data Acquisition
SSL **:** Secure Sockets Layer
TSE **:** Türk Standartları Enstitüsü
TCP/IP **:** Transmission Control Protocol/Internet Protocol
UDP **:** User Datagram Protokol

5. SIZMA TESTİ AŞAMALARI

5.1. Planlama

Test sürecinin planlanması aşağıdaki adımlardan oluşmalıdır. Her adımda uyulması gereken hususlar belirtilmiştir.

5.1.1. Test öncesi

Test öncesinde testi yaptıran kuruluş ile koordinasyon sağlanmalıdır. Bu koordinasyon bir sözleşme ve ekinde bir kapsam dokümanı ile belgelenmelidir. Örnek bir kapsam dokümanı Ek-2'de verilmiştir.

Sözleşme ve kapsam dokümanında aşağıdaki hususların olmasına dikkat edilir:

- İşin kapsamı ve tanımı,
- Testin türü (Siyah kutu, beyaz kutu, gri kutu veya belirli zaman aralıkları ile bunların karması olabilir.),
- Sızma testi hizmet türü,
- Testin gerçekleştirileceği sistemlere ait bilgiler (IP, Domain Adı vb.),
- Testin yapılacağı tarih ve saat dilimleri,
- Testi gerçekleştirecek uzmanlara ait bilgiler,

- Hangi ip adresinden testin gerçekleştirileceği,
- Açık bulunduğu taktirde Truva atı yüklenip yüklenemeyeceği,
- Acil Durum Kotarma safhasında iletişime geçilecek personel ve yönetici iletişim bilgileri.

Kuruluş, firma ve testi gerçekleştirecek personel ile bir gizlilik sözleşmesi imzalamalıdır. İmzalanacak olan gizlilik sözleşmesi, İş sözleşmesi kapsamında bazı ek maddeler şeklinde de ele alınabilir fakat gizlilik için ayrı ve detaylı bir sözleşmenin imzalanması tavsiye edilir. Eğer, teklif esnasında gizlilik dereceli bilgilerin paylaşımı söz konusu olacaksa Gizlilik Sözleşmesinin teklif alımından önce yapılması tavsiye edilir.

Firma bu aşamada kuruluştan feragatname isteyebilir. Örnek bir feragatname Ek-3'de verilmiştir.

NOT 1: Gri kutu testlerde testi gerçekleştirmek için gelecek personelin Kuruluşta çalışacağı tarih ve saat dilimleri de kapsam dokümanında belirtilir.

NOT 2: Gri kutu testlerini gerçekleştirmek için gerekli kullanıcı adı ve parola kapsam dokümanında belirtilir. Bu kullanıcı kimliği, firmaya geçici olarak temin edilebilir veya kalıcı bir test hesabının açılarak test dışında "disabled" olacak şekilde ayarlanabilir.

NOT 3: Bu aşamada, kapsam dokümanında yer alan güvenlik uzmanları kuruluş tarafından değerlendirilmeli ve onaylanmalıdır.

5.1.2. Test esnası

Güvenlik testi sürecinde açıklık derecelendirmesi uyarınca acil ya da kritik öneme sahip açıklıkların en kısa sürede kapatılması gerekebilir. Özellikle sızma testi sırasında bu bilgilerin kurum ile paylaşılması veya kapatılması güvenlik testinin bundan sonraki akışını etkileyebileceğinden, firma tarafından daha önce belirlenmiş standart bir form ile bildirimlerin kuruluşa gönderilmesi gerekmektedir.

Güvenlik testlerini yürüten takım ile müşteri kuruluş arasında güvenlik testleri sırasında güvenlik testi kapsamında yapılabilecek olası eklemeler ve güncellemeler için gelen talepler de standart bir form üzerinden yapılmalıdır.

Testler esnasında kuruluş tarafından sistem üzerinde yoğunluk oluşturacak (rapor alma, yığın işleme vb.) herhangi bir işlem yapılmaması tavsiye edilir. Bu tür bir işlem acil olarak gerçekleştirilmesi gerekiyorsa, kuruluş sorumluları firma ile iletişime geçerek, testlerin geçici olarak askıya alınmasını talep etmeleri tavsiye edilir.

5.1.3. Acil durum kurtarma

Testler esnasında sistemin işleyişinin kuruluş sorumluları tarafından izlenmesi ve sistemde bir sorun tespit edildiği takdirde, firma sorumlusuna konuyla ilgili bilgi verilerek testlere ara verilmesini istemesi tavsiye edilir. Sistemde tespit edilen sorun uzun süreli veya önemli ise testler daha sonraki bir tarihe ertelenebilir.

5.1.4. Test sonrası

Test sonrası aşama en önemli evredir; çünkü sızma testlerini gerçekleştiren test uzmanına tam sızma yapabilme yetkisi verilmiş ise test sonrasında sistemleri tekrar test öncesi aşamadaki durumlarına geri döndürmelidir. Hedef sisteme yüklenen dosyalar, kayıt defteri değişiklikleri ve oluşturulan zayıflıklar temizlenmelidir.

Testin tamamlanmasını müteakiben, bulunan açıklıklar ve başarılı olan sisteme sızma girişimleri ile ilgili olarak firma tarafından bir Sızma Testi Raporu (bk. Madde 5.3) hazırlanmalı ve kuruluşa iletilmelidir.

Sızma testi raporu sadece kuruluşun sorumluları ile paylaşılır. Kuruluşun bulunan açıklıkların kapatılmasına yönelik olarak bir takvim hazırlayarak açıklıkları kapatması gerekmektedir. Açıklıkların

kapatılmasına müteakip doğrulama testi, testi gerçekleştiren firma tarafından yapılarak kuruluşa iletilmelidir.

5.1.5. Test periyodu

Sızma testlerinin kuruluş tarafından düzenli olarak en az yılda 1 defa yaptırılması tavsiye edilir. Bunun dışında kritik uygulama ve sistemler daha sık aralıklarla test ettirilebilir. Ayrıca yeni hizmete girecek olan sistem ve uygulamalar için işletime alma öncesinde sızma testleri yaptırılması tavsiye edilir.

5.1.6. Test zamanlaması

Sızma testleri için mümkün olduğu kadar test edilecek sistemde yoğunluk olmayan saatlerin seçilmesi tavsiye edilir. Gün içinde çalışması kritik olan sistem ve yazılımlar için mesai saatleri dışında bir zaman diliminin tercih edilmesi tavsiye edilir. DoS/DDoS saldırı testi düzenlenecek ise, yine mesai saatleri dışının tercih edilmesi tavsiye edilir.

5.2. Uygulama

5.2.1. Sızma testi aşamaları

Sızma testlerini sekiz aşamada ele almak mümkündür. Bunlar;

1. Ön irtibat
2. Bilgi toplama
3. Tehdit modelleme
4. Zafiyet analizi
5. Sızma
6. Sızma Sonrası
7. Raporlama
8. Doğrulama Testi

Sızma testlerinin firmalar tarafından yukarıda belirtilen aşamalarda ele alınması tavsiye edilir.

Firma, bir sızma testi öncesinde o testte yer alacak personeli resmi olarak belirlemeli ve atamalıdır. Herhangi bir personel aynı anda 3 (üç)'ten fazla testte yer alamaz. Sızma testleri, Madde 5'de yer alan test süreci şartlarına uygun şekilde gerçekleştirilir.

Sızma testlerinde test araçlarının kullanımı, sızma testlerini kolaylaştırıcı bir etkendir. Araçların kullanımı uzmanın kendisinin uzun sürede yapabileceği testleri daha kısa sürede tamamlamasını sağlayacaktır. Ne var ki test araçlarının sonuçları güvenilir olmayabilir ve sadece test araçları ile yapılacak testler, kullanılabilir açıklıkları bulmada yetersiz kalacaktır. Bu kriter çerçevesinde firma sadece test araçlarını kullanarak test yapmamalı, dolayısıyla üretilecek olan test sonuç raporu sadece otomatik test araçlarının çıktısı olmamalıdır. İyi bir test yapılabilmesi için öncelikle uzmanlık temeline dayanan testler yapılmalıdır. Bu testlerin test araçlarının kullanımı ile desteklenmesi tavsiye edilir.

Kendi bünyesinde sızma testi yapan kuruluşların da bu standarda uyum sağlaması tavsiye edilir.

Özellikle kritik sistemlerde yapılacak sızma testleri için sigorta yaptırılarak riskin transfer edilmesi tavsiye edilir.

5.2.2. Sızma testi türleri

Sızma testlerinin çeşitli türleri vardır. Bunlardan bu program kapsamında ele alınanlar aşağıda başlıklar halinde belirtilmiştir.

Ağ ve sistem altyapısı sızma testleri

Hedef sistemin ağ ve sistem altyapısına yönelik gerçekleştirilen sızma testleridir. Özellikle aşağıdaki adımların uygulanması tavsiye edilir.

- Yerel ağ sızma testleri
- İnternet sızma testleri
- Güvenlik duvarı sızma testleri
- Saldırı tespit ve/veya engelleme sistemleri sızma testleri

Web uygulamaları ve veritabanları sızma testleri
Hedef sistemde kullanılan platform ve geliştirme dillerinden bağımsız olarak gerçekleştirilen sızma testleridir. Özellikle aşağıdaki adımların uygulanması tavsiye edilir.

- Bilgi toplama
- Yapılandırma yönetim testleri
- Veri doğrulama testleri
- Hizmet aksatma testleri
- İş mantığı testleri
- Oturum yönetimi testleri
- Web hizmetleri testleri
- Kimlik doğrulama testleri
- Yetkilendirme testleri
- Ajax testleri

Mobil uygulamalar sızma testleri
Akıllı telefon, tablet bilgisayar gibi sistemler ve bu sistemlerde çalışan uygulamalar üzerine yapılan sızma testleridir.

Kablosuz ağlar sızma testleri
Kablosuz ağları ve bu ağda yer alan cihazları hedef alan sızma testleridir. Özellikle aşağıdaki adımların uygulanması tavsiye edilir.

- Erişim Noktası (Access Point) cihazlarına yönelik testler
- Şifreleme kullanmayan sistemlere yönelik testler
- Şifreleme (WEP/WPA/WPA2) kullanan sistemlere yönelik testler
- Kablosuz ağa bağlı istemcilere yönelik testler

Endüstriyel kontrol sistemleri sızma testleri
Bir tesiste veya işletmede yer alan tüm ekipmanların merkezi denetleme kontrol ve veri toplama sistemlerine (SCADA) yönelik gerçekleştirilen sızma testleridir.

Hizmeti aksatma saldırıları (DoS/DDoS)
Hizmeti aksatma saldırıları bir sızma testi değildir. Ancak; bilgi güvenliğinin üç ana bileşeninden birisi olan erişilebilirliği doğrudan hedef aldığı ve günümüzde bu konunun önemi arttığı için bu program kapsamında bahsedilmiştir. Yaygın olarak kullanılan test çeşitleri aşağıda verilmiştir;

- Syn Flood Saldırıları
- ACK Flood Saldırıları
- FIN Flood Saldırıları
- TCP Connection Flood Saldırıları
- UDP Flood DDoS Saldırıları
- ICMP Flood DDoS Saldırıları
- HTTP GET, POST Flood Saldırıları

- DNS Flood DDoS Saldırıları
- Botnet Simülasyonu
- Rate Limiting, Karantina Özelliklerinin Test Edilmesi
- Uygulamalara Özel DoS Testleri
- SSL, HTTPS DoS Testleri

Sosyal mühendislik sızma testleri
Sosyal Mühendislik testleri, çeşitli yöntemlerle kullanıcıları aldatmaya yönelik testlerdir. Bu yöntemler telefon konuşması vb. sözlü iletişim ile olabildiği gibi, e-posta ile yapılan oltalama saldırıları gibi teknik araçlar kullanarak da yapılabilir.

Fiziksel sızma testleri
Bilişim sistemlerine yönelik sızma testleri genel olarak ağ iletişimi üzerine odaklansa da çok eski bir yöntem olan fiziksel sızmalar önemini korumaktadır. Fiziksel sızma testi, önemli bir cihaza yerinde müdahale edilmesi olabileceği gibi cihazın bulunduğu konumdan başka bir konuma nakledilmesi de olabilir.

5.3. Raporlama

Sızma Testi Raporu yapılan güvenlik testlerinin sonuçlarının detaylı olarak aktarıldığı belgedir. Genelde şifreli bir medya halinde test öncesi anlaşma yapılan kuruluş yetkilisine teslim edilmelidir. Kuruluş ile müşteri aralarında yaptıkları anlaşmada aksi belirtilmedikçe, testi yapan firma Test Doğrulama aşamasından sonra Sızma Testi Raporunu imha etmelidir. Gerek testi yaptıran gerekse testi yapan firma testin yapıldığına dair bilgileri paylaşmaktan kaçınmalı ve bu şekilde sistemin hedef haline gelmesi engellenmelidir. Sızma Testlerini yapan firmanın test yapılan kuruluşları referans olarak yayınlamaması tavsiye edilir. Bu şekilde hem test yapılan kurum hem de test yapan güvenlik firması risk altına girmekten korunabilir.

Sızma Testi sonuç raporu en az olmak üzere aşağıdaki şartları sağlamalıdır:

- Kapak Sayfası (testlerin yapıldığı zaman dilimini içeren) olmalıdır.
- Yönetici özeti bölümü olmalıdır. Yönetici özeti, özellikle kısa bir okuma ile rapordaki önemli bilgilere ulaşmak isteyen okuyuculara (özellikle yöneticilere) yönelik bir bölümdür. Yönetici özetinin aşağıdaki alt bölümleri içermesi tavsiye edilir:
- Genel Bilgiler
- Kapsam ve IP Adresleri
- Test Ekibi
- Genel Değerlendirme
- Genel Test Metodolojisi
- Risk Derecelendirme
- Genel Bulgular
- Tavsiye Özeti

Teknik Bilgiler bölümü olmalıdır. Teknik bilgiler raporun teknik detaylarının verildiği kapsamlı bir bölümdür. Teknik bilgilerin aşağıdaki alt bölümleri içermesi tavsiye edilir:

- Giriş
- Bilgi Toplama
- Açıklık Analizi
- Kullanma / Açıklık Onayı

- Kullanma Sonrası Etki
- Varsa Diğer Testler (Sosyal Mühendislik/Fiziksel Sızma Testi/DoS/DDoS v.b.)
- Kullanılan Araçlar

Açıklıklara ait bir risk derecelendirmesi olmalıdır. Derecelendirme sayısal olarak veya farklı renklendirme şeklinde yapılmalıdır. Risk derecelendirmesi, kuruluşun, risklerin giderilmesinde önceliklendirme yapmasına imkân vermek üzere hazırlanmalıdır.

Sızma Testi Raporları:

- A seviye firmalar için KIDEMLİ SIZMA TESTİ UZMANI
- B seviye firmalar için SERTİFİKALI SIZMA TESTİ UZMANI
- C seviye firmalar için KAYITLI SIZMA TESTİ UZMANI

Tarafından hazırlanmalı, imzalanmalı; raporların onaylanmaları ise bu uzmanların bir üst amirleri tarafından yapılmalıdır.

Örnek bir Sızma testi sonuç raporu Ek-1'de verilmiştir. Rapor, sızma testi yaptıran müşterinin ihtiyaçlarına göre değiştirilebilir.

6. YETKİNLİK ŞARTLARI

6.1. Personel yetkinlik şartları

Sızma testlerinin başarılı bir şekilde gerçekleştirilmesinde en temel etken uzmanlık olduğundan dolayı testlerin kalitesinde ve tutarlılığında en önemli kriter de testi yapan personelin uzmanlık seviyesi olarak görülmektedir.

6.1.1. Personel yetkinlik seviyeleri

Personel yetkinlik seviyeleri dört başlıkta değerlendirilecektir.

Stajyer Sızma Testi Uzmanı (ST.S.T.U.)
Kayıtlı Sızma Testi Uzmanı (KA.S.T.U.)
Sertifikalı Sızma Testi Uzmanı (SE.S.T.U.)
Kıdemli Sızma Testi Uzmanı (KI.S.T.U.)

Aşağıda bu yetkinlik seviyelerine dair açıklamalar ve şartlar belirtilmiştir:

6.1.1.1. Stajyer Sızma Test Uzmanı

Stajyer Sızma Testi Uzmanı, sektörde çalışmaya başlamış kişileri tanımlamaktadır. Stajyer Sızma Testi Uzmanlarında aşağıdaki şartlar aranmaktadır;

- Bir yıl içerisinde güvenlik konusunda en az bir (1) adet eğitim almış olmak[1],
- 6 ay bilgi güvenliği/bilişim alanında tecrübe veya Yazılı(Teorik) Sınavda Başarılı Olmak

[1] Eğitimler Belgelendirme/Eğitim kuruluşlardan alınmalıdır. Eğitim, Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ile Web Uygulaması ve Veritabanı Sızma Testi Uzmanlığı vb. alanlarında olmalıdır.

NOT-1: Firmanın çalıştırdığı stajyerleri genel sağlık sigortalı olarak çalıştırmaları kuvvetle önerilmekte olup, gerçekleştirdiği projelerde yer almak suretiyle tecrübe edindiklerini gösterebilmelidir.

NOT-2: Stajyer Test Uzmanlığı için (eğer 6 ay tecrübe yoksa), Yazılı(Teorik) Sınavda 100 üzerinden 50 puan başarılı olmak beklenmektedir.

6.1.1.2. Kayıtlı Sızma Test Uzmanı

Kayıtlı Sızma Testi Uzmanı olabilmek için aşağıdaki şartların yerine getirilmesi gerekmektedir.

- Belgelendirme/Eğitim Kuruluşu tarafından yapılan yazılı ve uygulamalı uzmanlık sınavında başarılı olmak,
- 1 yıl bilgi güvenliği/bilişim alanında çalışmış olmak veya 1 yıl sızma testi yapmış olmak ve bunu belgelendirmek,
- Madde 6.1.2'deki şartları taşımak,
- En az lise mezunu olmak.

Kayıtlı Sızma Testi Uzmanlığı;

- A1-Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı
- A2-Web Uygulamaları ve Veri tabanları Sızma Testi Uzmanlığı
- A3-Endüstriyel Kontrol Sistemleri Sızma Testi Uzmanı
- A4-Sosyal Mühendislik Sızma Testi Uzmanı
- A5-Fiziksel Sızma Testi Uzmanı
- A6-Mobil Uygulamalar Sızma Testi Uzmanı
- A7-Kablosuz Ağlar Sızma Testi Uzmanı
- A8-DOS/DDOS Testi Uzmanı
- A9-Adli Bilişim Uzmanı

olmak üzere 9 (dokuz) ana daldan oluşmakta olup, aşağıdaki notlara göre

Kayıtlı Sızma Testi Uzmanlığı da genel olarak;

- Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı,
- Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı

Sınıflandırılacaktır.

NOT-1: A1, A3, A5, A7, A8 uzmanlık alanları Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ile ilgili olup, sınavları ve sertifikasyonu ortak yapılacaktır.

NOT-2: A2, A4, A6, A8 uzmanlık alanları Web Uygulamaları ve Veri tabanları Sızma Testi Uzmanlığı ile ilgili olup, sınavları ve sertifikasyonu ortak yapılacaktır.

NOT-3: A9 uzmanlık alanında Sadece Eğitim verilecek olup, sınav yapılmayacak olup, Adli bilişim uzmanı; bilgisayar ve bilişim teknolojileri kullanılarak işlenen suçlarla ilgili olay yerinin analiz edilmesi, verilerin toplanması, bu verilerin incelenmesi, varsa eğer suç ile ilgili gerekli ilişkilendirmeler yapılarak sonuçların düzenli bir raporlama neticesinde adli makamlara sunulmasını sağlar.

NOT-4: Kayıtlı Test Uzmanlığı için, Teorik (Yazılı) sınav ve Uygulamalı (Pratik) sınav ortalamasının en az 100 üzerinden 50 puan olması gerekmektedir. Teorik Sınav 1/3, Uygulamalı sınav 2/3 ağırlığındadır.

6.1.1.3. Sertifikalı Sızma Test Uzmanı

Sertifikalı Sızma Testi Uzmanı olabilmek için aşağıdaki şartların yerine getirilmesi gerekmektedir:

- Madde 6.1.3'de belirtilen sertifikalardan en az birine sahip olmak ya da Belgelendirme/Eğitim Kuruluşu tarafından yapılacak yazılı ve uygulamalı sınavda başarılı olmak,
- 2 yıl bilgi güvenliği/bilişim alanında çalışmış olmak veya 2 yıl sızma testi yapmış olmak ve bunu belgelendirmek,
- En az 1 adet ulusal veya uluslararası düzeyde makale yayınlamak veya bir zafiyet keşfinde bulunup TSE'nin zafiyet bildirim programına bildirmek,
- Madde 6.1.2'deki şartları taşımak,
- En az üniversitelerin iki yıllık ön lisans bölümlerinden birinden mezunu olmak.

Sertifikalı Sızma Testi Uzmanlığı;

- Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı,
- Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı

olmak üzere iki ana daldan oluşmaktadır. Her bir uzmanlık için ayrı sertifikalandırma yapılmaktadır.

NOT: Sertifikalı Test Uzmanlığı için, Teorik (Yazılı) sınav ve Uygulamalı (Pratik) sınav ortalamasının en az 100 üzerinden 70 puan olması gerekmektedir. Teorik Sınav 1/3, Uygulamalı sınav 2/3 ağırlığındadır

6.1.1.4. Kıdemli Sızma Test Uzmanı

Kıdemli Sızma Testi Uzmanı olabilmek için aşağıdaki şartların yerine getirilmesi gerekmektedir.

- Belgelendirme/Eğitim Kuruluşu tarafından yapılan yazılı ve uygulamalı uzmanlık sınavında başarılı olmak,
- 4 yıl bilgi güvenliği alanında çalışmış olmak veya 4 yıl sızma testi yapmış olmak ve bunu belgelendirmek,
- En az 1 adet ulusal veya uluslararası düzeyde makale yayınlamak veya bir zafiyet keşfinde bulunup Belgelendirme/Eğitim Kuruluşunun zafiyet bildirim programına bildirmek yada siber güvenlik alanında yüksek lisans yapmış olmak.
- Madde 6.1.2'deki şartları taşımak,
- En az üniversitelerin dört yıllık lisans bölümlerinden birinden mezun olmak.

Kıdemli Sızma Testi Uzmanlığı;

- Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı,
- Web Uygulaması ve Veritabanı Sızma Testi Uzmanlığı

olmak üzere iki ana daldan oluşmaktadır. Her bir uzmanlık için ayrı sertifikalandırma yapılmaktadır.

Kayıtlı Sızma Testi Uzmanı, Sertifikalı Sızma Testi Uzmanı ve Kıdemli Sızma Testi Uzmanı için belge geçerlilik süreleri 3 (üç) yıldır. Üçüncü yılın sonunda yetkilendirilmiş personeller yetkilerini devam ettirebilmek için;

- Kayıtlı Sızma Testi Uzmanları, tekrar çoktan seçmeli ve uygulmalı sınavda başarılı olmalı,
- Sertifikalı Sızma Testi Uzmanları sahip oldukları sertifikaları devam ettirmeli, veya çoktan seçmeli ve uygulamalı sınavda başarılı olmalı,
- Kıdemli Sızma Testi Uzmanları çoktan seçmeli ve uygulamalı testte başarılı olmalıdır.

Not 1 - Sızma testi uzmanları, hizmet verdiği kurum ve kuruluşlardaki gizlilik içermeyen Sızma Testi Rapor Özetlerini (E-imza ile imzalaması önerilmektedir), gerektiğinde Belgelendirme/Eğitim Kuruluşu yetkililerine gönderebilmelidirler.

Not 2 - Kıdemli Sızma Testi Uzmanlığı için, Teorik (Yazılı) sınav ve Uygulamalı (Pratik) sınav ortalamasının en az 100 üzerinden 85 puan olması gerekmektedir. Teorik Sınav 1/3, Uygulamalı sınav 2/3 ağırlığındadır.

6.1.2. Özel şartlar

- Kamu kurumlarında ve kamu kurumu niteliğindeki kurumlarda test yapacak personellerde Türk vatandaşı olma ve kamu haklarından mahrum bulunmama şartları aranır. Bu şartları, kuruluşta takip etmelidir.
- Sızma testi yapacak kişilerin adli sicil kaydı ve/veya adli sicil arşiv kaydı olmamalıdır.

Ayrıca, ihtiyaç duyulan durumlarda kuruluşlar kendi güvenlik düzeylerine göre özel güvenlik, kişi güvenlik ya da klerans gibi belgeleri de isteyebilirler.

6.1.3. Eşdeğerlik çizelgesi

Sertifikalı Sızma Testi Uzmanı belgelendirmelerinde aşağıdaki uluslararası sertifikalar eşdeğer olarak kabul edilecektir. Belirtilen sertifikalar haricinde Madde 6.1.1.3 deki diğer şartların yerine getirilmesi gerekmektedir. Sertifikalı Sızma Testi Uzmanlığı için kabul edilecek sertifikalar Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ve Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı başlıkları altında iki ayrı tabloda verilmiştir.

Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı Eşdeğerlik Tablosu:

Sertifikalandırma Otoritesi	Sertifika Adı
EC-Council	Licensed Penetration Tester (LPT)
GIAC	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
GIAC	GIAC Penetration Tester (GPEN)
Offensive Security	Offensive Security Certified Professional (OSCP)

Çizelge 1 – Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı Eşdeğerlik Tablosu

Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı Eşdeğerlik Tablosu:

Sertifikalandırma Otoritesi	Sertifika Adı

GIAC	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
GIAC	GWAPT (GIAC Web Application Penetration Tester)
OWASP	OSWE (Offensive Security Web Expert)
Offensive Security	OSWE (Offensive Security Web Expert)

Çizelge 2 – Web Uygulamaları ve Veritabanları Sızma Testi Uzmanlığı Eşdeğerlik Tablosu

6.1.4 Genel Şartlar ve Uygulamalar

- Uygulamalı Eğitim ve Sınavlar genel olarak A1-Ağ ve Sistem Altyapısı Sızma Testi Uzmanlığı ve A2-Web Uygulaması ve Veri tabanı Sızma Testi Uzmanlıklarından yapılacak olup, diğer A3,A4,A5,A6,A7,A8,A9 uzmanlık alanlarından teorik(yazılı) eğitim ve sınav yapılacaktır.
- Tüm Uzmanlık alanlarında istenen bilgi güvenliği/bilişim/sızma testi tecrübeleri için, daha önceden bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında yükseköğretim kurumlarında alınıp başarılı olunan derslerin ve eğitimler (tekrar edilen dersler hariç) eğitimler gün/hafta/ay vb. süre olarak hesaplanıp*, tecrübeden sayılabilecektir.
- Stajyer ve Kayıtlı Test Uzmanlıkları için Ön lisans, Lisans, Y. Lisans ve Doktora öğrenimlerinde bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında alınan ve başarılı olunan dersler en fazla 1 yıl tecrübeye sayılabilecektir;
- Sertifikalı Test Uzmanlığı için Lisansın son 2 yılı, Yüksek Lisans ve Doktora öğreniminde bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında alınan ve başarılı olunan dersler en fazla 1 yıl tecrübeye sayılabilecektir;
- Kıdemli Test Uzmanlıkları için ise Yüksek Lisans ve Doktora öğreniminde bilgi güvenliği/siber güvenlik/bilişim/sızma testi alanlarında alınan ve başarılı olunan dersler en fazla 1 yıl tecrübeye sayılabilecektir.
-

*: Bilgi güvenliği/bilişim/sızma testi Tecrübesi

Tecrübe için hafta ve ay hesabı yapılır. Tecrübe= Ders kredisi x hafta sayısı (1 hafta 32 saat olarak Kabul edilmektedir)

Bilgi güvenliği/Bilişim Eğitimleri

1 gün 8 saat, 1 hafta 5 gün, 1 ay 4 hafta kabul edilerek sure hesaplanır.

Bilgi güvenliği/Bilişim Dersleri

1 gün 8 saat, 1 hafta 5 gün, 1 ay 4 hafta kabul edilerek sure hesaplanır.

6.2. Firma yetkinlik şartları

Aşağıdaki çizelgede personel sayıları ve uzmanlıkları temelinde firma seviyeleri ve ISO/IEC 27001:2013 şartı olup olmadığı verilmiştir.

Firma Seviyesi	KI.S.T.U.	SE.S.T.U.	KA.S.T.U.	ST.S.T.U.	ISO/IEC 27001:2013 Serifikasyonu
A	1	1	1	2	Zorunlu
B		1	1	1	Zorunlu
C			1		Kısmen

Çizelge 3 – Personel Sayılarına ve Uzmanlıklarına göre firma seviyeleri

A, B ve C seviyelendirmesi firmaların personel kapasiteleri göz önüne alınarak yapılmıştır. Bu seviyelendirme ile sızma testi yaptıran kuruluşların kendi büyüklüklerine uygun firmaları tercih edebilmesi amaçlanmaktadır.

Bu standard da belirtilen şartlara uyum sağladığını iddia eden firmalar TSE'ye başvurarak uyumlarını belgelendirirler. Firmalar, TSE tarafından yıllık olarak denetime tabii tutulur ve belgeleri yenilenir.

C seviyesi firmalar için ISO/IEC 27001:2013 sertifikasyonu zorunlu olmamakla birlikte, ISO/IEC 27001:2013 in aşağıda yer alan standard maddelerine ve ek kontrol maddelerine uyum sağlamaları gerekmektedir.

27001 FİRMA SINIFLANDIRMA TABLOSU

Firma Sınıfı	Standard Uyumluluk	Standard Maddeleri
C	ISO IEC 27001	6.1.2. Bilgi güvenliği risk değerlendirmesi 6.1.3. Bilgi güvenliği risk işleme A 5.1.1 Bilgi güvenliği için politikalar A 6.1.1 Bilgi güvenliği rolleri ve sorumlulukları A 6.1.2 Görevlerin ayrılığı A 7.1.1 Tarama A 7.2.2 Bilgi güvenliği farkındalığı ve eğitimi A 8.1.1 Varlıkların envanteri A 8.2.1 Bilgi sınıflandırması A 8.3.1. Taşınabilir ortam yönetimi A 8.3.2 Ortamın yok edilmesi A 9.1.1 Erişim kontrol politikası A 9.2.1 Kullanıcı kaydetme ve kullanıcı silme A 9.2.2 Kullanıcı erişimine izin verme A 9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi A 9.4.2 Güvenli oturum açma prosedürleri A 9.4.3 Parola yönetim sistemi A 9.4.5 Kaynak koduna erişim kontrolü A 11.1.2 Fiziksel giriş kontrolleri A 11.1.3 Ofislerin odaların ve tesislerin güvenliğinin sağlanması

		A 11.2.2 Destekleyici altyapı hizmetleri A 11.2.9 Temiz masa temiz ekran politikası A 12.1.2 Değişiklik yönetimi A 12.2.1 Kötücül yazılımlara karşı kontroller A 12.3.1 Bilgi yedeklemesi A 12.4.1 Olay kaydetme A 12.6.1 Teknik açıklıkların yönetimi A 13.1.1 Ağ kontrolleri A 13.2.1 Bilgi transfer politikaları A 15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası A 16.1.2 Bilgi güvenliği olaylarının raporlanması A 17.1 Bilgi güvenliği sürekliliği A 18.1 Yasal ve sözleşmeye tabi gereksinimler A 18.2.3 Teknik uyum gözden geçirmesi

Uygunluğu kontrol etmek için yapılan faaliyetlerin kayıtları tutulmalıdır.

Bütün kayıtlar okunaklı olmalı, zarar görmelerini veya bozulmalarını ve kaybolmalarını önlemek için uygun şartları sağlayabilecek mekanlarda kolayca ulaşılabilecek şekilde saklanmalı ve muhafaza edilmelidir. Kayıtların muhafaza edilme süreleri belirlenmelidir.

Not - Kayıtlar, basılı kopya veya elektronik kayıt gibi herhangi bir ortamda olabilir.

Saklanması gereken bütün kayıtlar, emniyetli bir şekilde ve gizlilik içinde muhafaza edilmelidir.

6.2.1. Kuruluş ile iletişim şartları

Sızma testlerinde olumsuz durumlar ile karşılaşılmaması (işletimsel sistemlerin göçmesi, dışarıya veri sızması vb.) ve testlerin etkin ve zamanlı bir biçimde gerçekleştirilmesinde kuruluş ile etkin iletişim çok önemli rol oynar. Hem sızma testi öncesinde hem de sızma testi esnasında kuruluş ile sürekli iletişim halinde olmak gerekir. Firma, sızma testi gidişatına göre verilmesi gereken kritik bazı kararlarda (Hizmet Aksatma testini devam ettirip ettirmeme vb.) mutlaka kuruluşun görüşünü almalıdır.

Sızma testleri esnasında, kuruluş gerçek siber saldırılara da maruz kalabilmektedir. Bu noktada kuruluşun, sızma testlerini izleyerek, testler ile siber saldırılar arasında ayrım yapabilmesi ve firma ile iletişim kurarak, testi durdurmasını istemesi önem arz etmektedir. Testin siber saldırı esnasında durdurulması, hem sistemi korumak açısından hem de sonradan yapılacak olan adli bilişim analiz çalışmasını da kolaylaştırması açısından önemlidir.

Aşağıdaki hususlara dikkat edilmelidir:

- Firma, sızma testine başlamadan önce kuruluşunun irtibat noktasını bilgilendirmelidir.
- Firma, kuruluş ile gizlilik dereceli veya hassas bilgilerin elektronik ortamdan paylaşımında yeterli seviyede güvenlik kontrollerini (dosyayı şifreli gönderme, e-postayı şifreli, elektronik imzalı gönderme, güvenli ftp vb.) uygulamalıdır.
- Firmanın, sızma testi öncesinde kuruluş ile çevrimiçi veya karşılıklı olarak bir toplantı yapması ve sızma testlerinde karşılaşılabilecek riskler ve alınabilecek önlemler konusunda kuruluşu bilgilendirmesi tavsiye edilir.
- Firma sızma testi öncesinde kapsamı net şekilde belirlemeli ve buna uygun olarak testleri gerçekleştirmelidir. Test esnasında kapsamın genişletilmesi söz konusu olursa firma bu kararı kuruluş ile görüşerek ve kuruluşun yazılı onayına istinaden alabilir ve buna göre testlerin kapsamını genişletebilir veya daraltabilir.

6.2.2. Gizlilik ve kayıt saklama şartları

Sızma testi ile ilgili gerek kuruluş tarafından doldurulan anket, form vb. dokümanlar gerekse firma tarafından üretilen sızma testi sonuç raporu vb. dokümanlar gizlilik derecesine haiz dokümanlardır. Bu tür dokümanlar üretim, kullanım ve saklama aşamalarında hassasiyetle ele alınmalı ve çalınma, yetkisiz erişim, kaybolma vb. risklere karşı korunmalıdır.

Test raporlarının saklanmasında kuruluşunun görüşü alınmalı ve buna göre hareket edilmelidir. Önceki yapılan testlere ait raporlar saklanacak ise, bu raporlar firma personelinin taşınabilir bilgisayarlarında veya taşınabilir ortamlarda (harici disk, flash disk vb.) bulundurulmamalı, gerek yazılı kopyaları gerekse elektronik kopyaları mutlaka güvenli bir ortamda saklanmalıdır.

Raporlar özellikle sunumlarda kullanılmamalı ve örnek mahiyetinde diğer kuruluşlara gösterilmemelidir. Raporların saklanması, bir sonraki testte daha önce bulunan açıklıkların kapatılıp kapatılmadığını anlamak açısından firma için yararlı olacaktır. Ne var ki raporların ele geçirilmesi veya çalınması da firma için yüksek bir güvenlik riski teşkil etmektedir.

Firma belirli bir teste ait sızma testi raporunu saklayabilmesi için testi yaptıran kuruluştan mutlaka resmi nitelikte yazılı olarak izin almalıdır. Bu izne binaen firma sızma testi raporlarını saklayabilir.

Firma, hangi personelinin hangi testlerde görev aldığını dair kayıtları tutmalı ve en az 2 yıl süre ile bu kayıtları saklamalıdır. Ayrıca sızma testlerinde yer alan personelin isimleri de Sızma testi raporunda belirtilmelidir.

Test raporlarına erişim, bilmesi gereken prensibine göre verilmeli, yetkilendirilmeli ve kontrol edilmelidir. Raporlara erişim sadece testi yapan veya doğrudan yöneten kişiler ile kısıtlı kalmalı ve bunlar haricinde erişim olmamalıdır. Bir önceki testin devamı niteliğinde yeni bir test yapılacak ise bu durumda yeni testi yapacak olan personel eski test raporuna erişmek üzere yetkilendirilebilir. Bu durumda yetkilendirmenin yetkili kişi tarafından onaylanması gerekir.

Yukarıdaki kriterler temelinde örneğin; firmanın muhasebe müdürü veya iş geliştirme müdürünün test raporlarına erişimi olmamalıdır. Yeni yapılacak bir sızma testi için atanan proje yöneticisi, sızma testi yapacak olan personele aynı kuruluşun bir önceki sızma testine dair erişim için yetkilendirebilir.

Firmanın farklı iş kollarında faaliyet göstermesi durumunda ISO/IEC 27001:2013 ek maddelerine uyum sadece ilgili birimi için aranır. İlgili birimin, diğer birimlerle çalışma alanı ve bilgi paylaşımı v.b. durumları söz konusu olduğunda gizlilik şartlarına uygunluk sağlanır.

6.2.3. Kapanış işlemleri

Firma yasal olarak faaliyetlerine son vermesi durumunda, kendisinde bulunan sızma testi sonuç raporlarını geri dönülemez şekilde imha etmelidir.

6.2.4. Bildirim şartları

TSE tarafından yetkilendirilmiş personeller, firma değiştirmeleri veya çalıştıkları firmadan ayrılmaları durumunda en geç 15 takvim günü içinde bu durumu TSE'ye bildirmelidirler. Aynı şekilde firmalar da, yetkilendirilmiş bir personel firmadan ayrıldığında veya firmada göreve başladığında bu durumu TSE'ye bildirmelidirler.

Firmadan ayrılan personel, firmanın belgelendirme sınıfı ile ilgili değişikliğe neden oluyor ise ayrılış tarihini müteakip iki (2) ay içerisinde eşdeğer yetkinliği sahip bir personel istihdam edilmelidir.

6.2.5. Yabancı uzman çalıştırma ile ilgili şartlar

Kamu kurumlarında ve kamu kurumu niteliğindeki kurumlarda test yapacak personellerde Türk vatandaşı olma ve kamu haklarından mahrum bulunmama şartları aranır. Bu şartları, kuruluşta takip etmelidir.

Sızma testlerinde çalışan uzmanların ne renk şapka taktıkları çok net olmayabildiğinden, özellikle çeşitli kötü niyetli organizasyonların hedefi haline gelebildiklerinden ve bu alanda yüksek meblağlar söz konusu olduğundan dolayı, yabancı uzman çalıştırma konusu hassasiyetle ele alınmalıdır.

Bu noktada her ne kadar yukarıdaki koşullar yerli uzmanlar açısından da geçerli olsa bile, hukuksal açıdan bakıldığında, kanunsuz bir davranış neticesinde ülke kanunlarının uygulanması uluslararası kanunlara göre çok daha kolay ve caydırıcı etkiye sahiptir. Ayrıca; teknik olarak bakıldığında yurtdışından yapılan saldırıların takip edilmesi de yine yurtiçinden yapılan saldırılara göre çok daha zor olabilmektedir.

Bu nedenle firmalar kamu kurum ve kuruluşlarına yaptıkları sızma testlerinde yabancı uzman çalıştırmamalıdırlar. Özel sektör kuruluşlarına yapılan testlerde de yabancı uzman çalıştırılmaması tavsiye edilir. Özel durumlarda (yurtiçinde belli bir alanda uzman bulunamıyor ise vb.) yabancı uzman çalıştırma yoluna gidilebilir fakat firmanın bunu net bir şekilde ve delilleri ile gerekçelendirebilmesi gerekmektedir. Gerekçelendirme delili, firmanın ilgili pozisyon için ilana çıkması ve ilanın en az 2 (iki) hafta askıda kalması fakat eleman bulamamasıdır.

7. Kişisel bilgilerin gizliliği

Firma yaptığı testler esnasında kuruluş çalışanlarının kişisel bilgilerine ulaşması durumunda, bu bilgileri kuruluş ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Sızma test raporunda kullanıcı adı ve parolaları maskelenmelidir.

8. Kanunlara ve mevzuata uyum

Testler yasadışı araçları veya yöntemleri içermemelidir. Örnek: DDOS için Botnet kiralama vb. Ayrıca; testler esnasında kuruluş ile sözleşmede veya teknik şartnamede belirlenmiş olan kapsam dışına kuruluşun yazılı izni olmadan çıkılmamalıdır.

Sızma testleri esnasında firma, sadece kuruluşa ait içeriklere erişim sağlanabildiğini göstermeli, bunun dışında kuruluşa ait içeriklerin tamamına erişim sağlayarak tüm içeriği kopyalamamalı ve üçüncü taraflar ile paylaşmamalıdır. Firmanın içeriklere erişim sağlandığını gösterebilmesi için gerekiyorsa örnek olarak birkaç kayıt delil sağlamak amacıyla kopyalayabilir.

Program kapsamında yetkilendirilen personeller için taahhütname, firmalar için ise belge kullanım sözleşmesi imzalanacaktır. Yetkilendirilmiş personel ve firmalar imzaladıkları taahhütname ve sözleşmedeki şartlara uymadıkları takdirde yetkilendirme belgeleri belgelendirme kuruluşu tarafından geri alınır.

9. Gözetim ve yeniden belgelendirme

Bu standardda belirtilen şartlara uyum sağladığını iddia eden firmalar belgelendirme kuruluşuna başvurarak uyumlarını belgelendirirler. Firmalar, belgelendirme kuruluşu tarafından yıllık olarak denetime tabii tutulur ve belgeleri yenilenir.

EK-1

ÖRNEK BİR SIZMA TESTİ SONUÇ RAPORU

XYZ LTD. ŞTİ.

ABC KURUMU

SIZMA TESTİ RAPORU

XYZ Bilgi Güvenliği Limited Şirketi
Cumhuriyet Mah. Demokrasi Sok. No: 17/6 ÇANKAYA/ANKARA
Telefon : 0 312 123 45 67
Faks : 0 312 123 45 68

1 Ocak – 31 Ocak 2013

İçindekiler

UYARI

Rapor içeriği gizli olup iki tarafın yazılı mutabakatı olmadan üçüncü taraflara basılı olarak ya da elektronik ortamda transfer edilemez veya paylaşılamaz.

Rapor, tarama süresi içinde varlığı bilinen veya tarafımızdan tespit edilen güvenlik açıklıklarını içerecektir. Tarama işlemi bittikten sonra rapor teslim edilene kadar geçen süre içerisinde çıkabilecek yeni güvenlik açıklarına dair eksikliklerden dolayı raporu hazırlayan firma sorumlu tutulamaz.

Rapor içinde yer alan çözüm önerilerine konu hakkında fikir verme amaçlı yer verilmiştir. Çözüm önerilerinin uygulanması sebebi ile çıkabilecek problemlerden raporu hazırlayan firma sorumlu tutulamaz. Önerilerde sunulan değişikliklerden gerçekleştirilmeden önce konu hakkında uzman kişilerden destek alınması tavsiye edilir.

1. YÖNETİCİ ÖZETİ

1.1. GENEL BİLGİLER

Bu rapor, XYZ Ltd. Şti. tarafından ABC Kurumu sistemleri üzerindeki güvenlik açıklarını ortaya çıkarmak amacı ile 1 Ocak - 31 Ocak 2013 tarihleri arasında gerçekleştirilen sızma testleri ve güvenlik değerlendirmeleri çalışmalarının detaylı sonuçlarını içermektedir.

Sızma testi kapsamında ABC Kurumu altyapısı ve sunucularının çalışmasını etkileyecek araçlar kurum yetkililerinin bilgisi olmadan kullanılmamış, hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Bilgi sistemleri, intranet ve internet olmak üzere iki ayrı taramaya tabii tutulmuştur. Internet üzerinden gerçekleştirilen testler, sistemler hakkında herhangi bir bilgisi olmayan personel tarafından gerçekleştirilmiştir. Intranet üzerinden gerçekleştirilen testlerde çeşitli seviyede yetkilendirilmiş kullanıcı hakları kullanılarak sistemler test edilmiş ve bunlardan doğabilecek riskler raporun ilerleyen kısımlarında açıklanmıştır.

Test ile sunucular üzerinde bulunabilecek muhtemel güvenlik açıklıklarının kötü niyetli saldırganlardan önce ortaya çıkartılması ve önlem alınması amaçlanmaktadır.

Rapor, bulunan her güvenlik açığının risk derecesini, açık hakkında açıklamaları, daha detaylı bilgi bulabileceğiniz bağlantıları, güvenlik açığının nasıl kapatılabileceği hakkında gerekli bilgiyi, açığın nasıl kötüye kullanılabileceği hakkında örnekleri ve uzman personelin yorum ve önerilerini içermektedir.

Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamalıdır.

Rapor okuyucunun TCP/IP ve kullanılan teknoloji hakkında temel bilgilere sahip olduğu düşünülerek hazırlanmıştır. Bu sebeple raporlarda kullanılan terimler ile ilgili her hangi bir açıklama yapılmayacaktır.

1.2. KAPSAM VE IP ADRESLERİ

Bu tarama kapsamında taramayı yaptıran ABC Kurumu tarafından belirlenen ve aşağıda listelenen sunuculara yönelik saldırı ve sızma testi gerçekleştirilmiştir. Bu testler esnasında, test edilen sunucular tarafından verilen hizmetlerin sekteye uğratılmaması amacıyla Denial of Service (DoS) saldırıları ayrı yapılmıştır. Denial of Service (DoS) saldırıları ile ilgili bilgi raporun ilerleyen kısımlarında özel bölüm olarak verilmiştir. Test edilen IP adresleri aşağıda listelenmiştir.

212.125.85.1-212.125.85.255 adres aralığı internet tarafında taranmıştır.

Sunucu Adı	IP Adresi	DNS Adı	Açıklama
MAIL	212.125.85.6	mail.abc.gov.tr	E-posta sunucusu
WEB	212.125.85.100	www.abc.gov.tr	Web Sunucusu
WEB	212.125.85.104	www.kml.gov.tr	Web Sunucusu
DNS	212.125.85.150	dns.abc.gov.tr	DNS Sunucusu

192.168.100.0-192.168.100.255 adres aralığı yerel ağ tarafında taranmıştır.

Sunucu Adı	IP Adresi	DNS Adı	Açıklama
DC	192.168.100.10	dc.abc.gov.tr	Etki Alanı Sunucusu
WEB	192.168.100.100	www.abc.net.tr	Intranet Uygulama Sunucusu
DNS	192.168.100.150	dns.abc.net.tr	DNS Sunucusu
SQL	192.168.100.101	Sql.abc.net.tr	Intranet Veri tabanı Sunucusu

1.3. TEST EKİBİ

Ahmet CAN	Kıdemli Sızma Testi Uzmanı*
Nur ÖZDEMİR	Sertifikalandırılmış Sızma Testi Uzmanı*
Cem ALPUN	Kayıtlı Sızma Testi Uzmanı*
Meryem YILMAZ	Stajyer Sızma Testi Uzmanı*
Ümit GÜZEL	Stajyer Sızma Testi Uzmanı*

* TSE XXX programına uygun uzmanlık seviyesidir.

1.4. GENEL DEĞERLENDİRME

Gerçekleştirilen kontroller, özellikle web uygulamalarının güvenlik açısından son derece sorunlu kodlara sahip olduğunu göstermiştir. Bu da testler neticesinde SQL Injection gibi önemli ve tehlikeli güvenlik açıklarının tespit edilmesine yol açmıştır. Kullanıcı tarafından yollanan verilerin, uygulama tarafından kullanılmadan önce sorun oluşturacak karakterler için kontrol edilmemesi SQL Injection, XSS (CrossSiteScripting) gibi web uygulama problemlerinin ortaya çıkmasına neden olmaktadır. Tespit edilen bu açıklar, yetkisiz kullanıcıların rahatlıkla web sitesine ait içeriği değiştirmesine, veri tabanında tutulan tüm kayıtlara erişim sağlamasına veya sunucu üzerinde istedikleri komutları çalıştırmasına izin verecek niteliktedir. Bu açıklardan başarı ile faydalanan bir saldırgan veri tabanının bulunduğu ağa erişim sağlayabilir. Elde edilen test sonuçları internet üzerinden bu açıklar sayesinde yerel ağa erişimin mümkün olduğunu göstermiştir. Yine web sunucuları üzerindeki yapılandırmada hatalar bulunması, detaylı hata mesajları vasıtası ile uygulama kaynak kodları gibi önemli bilgilerin elde edilmesine izin vermiştir.

Güncel olmayan işletim sistemleri sunucuların sağlıklı çalışmasını tehdit eden unsurlardan bir tanesidir. Sunucunun tamamen başkasının eline geçmesine kadar giden bu açıklıklar zamanında önlenmediği taktirde büyük sorunlara yol açmaktadır.

1.5. GENEL TEST METODOLOJİSİ

Günümüz bilgi güvenliğinde iki tür yaklaşım vardır. Bunlardan kabul göreni proaktif yaklaşımdır. Sızma testleri (pentest) ve zayıflık tarama (vulnerability assessment) konusu proaktif güvenliğin en önemli bileşenlerinden biridir.

Sızma testleri ve zayıflık tarama birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Sızma testi çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme) belirlenmesidir.

Zayıflık tarama daha çok otomatize araçlar kullanılarak gerçekleştirilir ve kısa sürer. Sızma testi çalışmaları zayıflık tarama adımını da kapsayan ileri seviye tecrübe gerektiren bir süreçtir ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.

1.6. RİSK DERECELENDİRME

Sızma testi çalışmalarında bulunan açıklar 5 risk seviyesinde değerlendirilmişlerdir. Bu değerlendirmede, PCI-DSS güvenlik tarama prosedürleri dokümanında[2] kullanılan beş seviye risk değerleri kullanılmıştır.

Aşağıdaki tablo **Tablo** kullanılan seviyelendirmeyi açıklamaktadır.

Risk	Seviyesi	Risk Puanı	Detay Açıklama
	**ACİL**	5	Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklık vektörleri bu kategoriye girerler.
	**KRİTİK**	4	Kritik öneme sahip açıklıklar, nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Ayrıca yansıtılan ve DOM tabanlı XSS açıklık vektörleri bu kategoriye girer.
	**YÜKSEK**	3	Yüksek öneme sahip açıklıklar, uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi (mesela, yönetici hakları olmayan bir işletim sistemi kullanıcısı veya e-posta sahteciliği) veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan ataklara sebep olan açıklıkları içermektedir.
	**ORTA**	2	Orta öneme sahip açıklıklar, yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir.
	**DÜŞÜK**	1	Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin (best practices) izlenmemesinden kaynaklanan eksikliklerdir.

Tablo 1- Raporda kullanılan risk seviyelendirmesi

[2] https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf

1.7. GENEL BULGULAR

1.7.1. SQL Injection Güvenlik Açıklıkları

SQL Injection web uygulamasında kullanılan parametrelere, kendi sorgulamalarımızı ekleyerek arka plandaki veri tabanına erişmemize ve SQL sorgulamaları yapmamıza olanak tanıyan açıktır. Genellikle web uygulaması üzerindeki formlar veya URL içindeki parametreler kullanılarak bu açıktan yararlanılır. Eğer web uygulamasının herhangi bir veri tabanı ile bağlantısı var ve uygulama üzerinde gerekli önlemler alınmamış ise bu tip saldırılar yapmak mümkün olabilir. Bu tip saldırılar neticesinde sistem üzerinde tam yetki sahibi olmak, yerel ağdaki sistemlere sızmak veya veri tabanı üzerinde tutulan kayıtlara erişmek ve değiştirmek mümkün olabilir.

1.7.2. Güncel Olmayan Sunucular

Sunucular, hizmetlerin sunulduğu genel platformlar olarak çeşitli işletim sistemleri koşturmaktadır. İşletim sistemleri, çıkan yama programlar ile zaman zaman güncellenmektedir. Güncelleştirmeler takip edilmediği taktirde telafi edilemeyen sorunlara yol açmaktadır.

1.7.3. Cross Site Scripting (XSS)

Dinamik olarak oluşturulan web sayfalarında, kullanıcı tarafından sağlanan bilgiler uygulama tarafından düzgün bir şekilde işlenemediği veya kontrol edilemediği durumlarda, yetkisiz kişileri istedikleri script kodlarının görüntülenecek sayfada çalışmasını sağlayabilirler. Söz konusu problem Cross Site Scripting (XSS) olarak adlandırılmaktadır. Bu tip saldırıların hedefi direkt olarak sunucuya bağlanan kullanıcılardır. Uygulamalardaki XSS açıklıkları kullanılarak, bağlanan kullanıcıların session id, cookie gibi bilgileri çalınmaya çalışır.

1.8. TAVSİYE ÖZETİ

Sızma testi neticesinde özellikle sql injection ve güncel olmayan sunucular tespit edilmiştir.

Yazılım geliştirme sürecini müteakip, yazılımı devreye almadan önce yapılacak kod analizlerinin sql injection açıklıklarını önleme de büyük fayda sağlamaktadır. Yazılımı geliştiren personele güvenli kod geliştirme eğitimlerinin temin edilmesi bu sürecin daha sağlıklı yürütülmesine ciddi derece de katkı sağlamaktadır.

Güncel olmayan işletim sistemleri her zaman sorun olmuştur. Güncelleştirme uyarıları halka açık olarak yayınlandığı için art niyetli kişiler tarafından da kolaylıkla takip edilip zafiyetler kullanılabilmektedir. Güncelleştirmelerin takip edilmesini sağlayan bir politika ve prosedür kurulması ile bu konudan kaynaklanan risklerin asgari seviyeye indirgendiği görülmektedir.

2. TEKNİK BİLGİLER

2.1. GİRİŞ

Güvenlik taramaları internet üzerinden erişilebilir sunucular için kurumdan en az bilgi temin edilerek gerçekleştirilmiş olup, sıradan bir kullanıcının ne gibi aktiviteler gerçekleştirebileceğini göstermektedir. Intranet üzerinden gerçekleştirilen sızma testlerinde kurum tarafından temin edilen çeşitli seviyelerde yetkilendirilmiş kullanıcı hakları kullanılmıştır. Testler sırasında çeşitli ticari tarama ürünleri, herkes tarafından temin edilebilecek açık kaynak kodlu programlar ve uzmanlarımız tarafından geliştirilmiş yardımcı program ve araçlar kullanılmıştır. Bu araçların listesi "Kullanılan Araçlar" bölümünde yer almaktadır.

2.2. BİLGİ TOPLAMA

2.2.1. Domain Sorgusu ve Whois Sorgusu

Bu aşamada domain sorgusu, dns sunucudan alan transferi ve whois veritabanı taramaları gerçekleştirildi.

2.2.2. Web Sitesi Analizi

Kurumun hangi dış bağlantıları ve etki alanlarının kullandığını belirlemek amacı ile kurumun web siteleri genel olarak incelendi. Daha sonra yapılacak detaylı incelemelere temel teşkil edecek bilgiler toplandı.

2.2.3. Arama Motorları

Arama motorları kullanılarak kurum ve kurum personeli hakkında araştırmalar yapıldı. Bu araştırmalar neticesinde kritik personelin üye olduğu gruplar sosyal paylaşım siteleri tespit edilerek kurum hakkında bilgi edinme çalışılması yapıldı. Bu çalışma kapsamında kurum hakkında yapılmış haberler de incelenerek faydalı olabilecekler ayıklandı.

2.2.4. Ağ Haritasının Çıkarılması

Bilgi toplamanın en önemli kısmı elde edilen bilgilerin birleştirilmesidir. Bu aşamada elde edilen bilgiler birleştirilerek kuruma ait güvenlik duvarı, uygulama sunucusu, veritabanı yönetimi sunucusu, aktif ağ cihazları gibi cihazların ip adresleri ve birbirleri ile olan bağlantıları tespit edildi.

2.2.5. Sosyal Mühendislik Çalışması

Kurumlara yapılan saldırıların en zayıf halkası genelde kullanıcılar olabilmektedir. Kurumda bilgi alınabilecek her türlü personel ile iletişme geçilerek (sahte e-postalar, telefon görüşmeleri veya benzer vasıtalar ile) temasa geçilerek bilgi edinim çalışması gerçekleştirildi.

2.2.6. Tahmin Çalışması

Kurumun faaliyet alanı, yapısı ve sistemleri temel alınarak, kurumda olabilecek servis ve uygulamaların bir listesi testte kullanılmak amacı ile oluşturuldu.

2.3. AÇIKLIK ANALİZİ

Bu kısımda açıklık analizi yapılan açıklıklar risk seviyesine göre sıralanır.

AÇIKLIK 1

Risk Seviyesi	Acil/Kritik/Yüksek/Orta/Düşük
Erişim Ortamı	İnternet/Intranet
Kullanıcı Profili	Internet Kullanıcısı/Intranet Kullanıcısı/Sistem Kullanıcısı/Diğer
Kullanılan Araçlar	Sqlmap
Zafiyet Türü	Web Uygulaması Açıklıkları/Hizmetler/Windows Açıklıkları
Zafiyet Adı	SQL Injection/OpenSSH Rastgele Komut İşletim Zafiyeti/Cross site scripting (XSS)
Etkilenen Sistemler ve portlar	212.125.85.100 - 5521
Tanım	Bazı uygulama yazılımlarında sql injection açıklıklarının olduğu tespit edilmiştir.
Çözüm önerileri	Kod geliştirme esnasında sql injection neden olabilecek hususlara dikkat edilmelidir. Uygulama kodlarına müdahale edilemeyen uygulamalar için uygulama katmanı güvenlik duvarı (web application firewall) kullanılmalıdır.
Referanslar ve İyi Uygulama Örnekleri	https://www.owasp.org/index.php/SQL_Injection

NOT: Tanım kısmında açıklık/zafiyet ile ilgili elde edilen ekran görüntüleri paylaşılabilir.

AÇIKLIK 2

Risk Seviyesi	Acil/Kritik/Yüksek/Orta/Düşük
Erişim Ortamı	İnternet/Intranet
Kullanıcı Profili	Internet Kullanıcısı/Intranet Kullanıcısı/Sistem Kullanıcısı/Diğer
Kullanılan Araçlar	Nessus
Zafiyet Türü	Web Uygulaması Açıklıkları/Hizmetler/Windows Açıklıkları
Zafiyet Adı	SQL Injection/OpenSSH Rastgele Komut İşletim Zafiyeti/Cross site scripting (XSS)
Etkilenen Sistemler ve portlar	172.16.32.25 - 5522
Tanım	Bazı Windows sistemlerinin güncel olmadığı belirlenmiştir.
Çözüm önerileri	Tüm sistemler için gerekli güncellemelerin yapılmış olduğundan emin olunmalı, güncelleştirmelerin düzenli olarak yapılması için gerekli düzenlemeler yapılmalıdır.
Referanslar ve İyi Uygulama Örnekleri	http://windowsupdate.microsoft.com http://www.microsoft.com/technet/security/default.mspx

NOT: Açıklıkların analizinde aşağıdaki çizelge de yer alan değerler kullanılabilir.

Risk Seviyesi	Erişim Ortamı	Kullanıcı Profili	Zafiyet Türü	Zafiyet Adı
Acil	İnternet	Internet Kullanıcısı	Web Uygulamaları	SQL Injection
Kritik	Intranet	Intranet Kullanıcısı	Windows Açıklıkları	OpenSSH Rasgele Komut İşletim Zaafiyeti
Yüksek	Kablosuz Ağ	Sistem Kullanıcısı	Linux Açıklıkları	Cross site scripting (XSS)
Orta	Mobil Ağ	Sistem Yöneticisi	Ağ Yapılandırmaları	Mantıksal Açıklık
Düşük	Diğer……	Diğer……	Diğer……	Girdi Doğrulama Zafiyeti
				Kimlik Doğrulama Zafiyeti
				Oturum Yönetimi Zafiyeti
				Yetkilendirme Zafiyeti
				AJAX Zafiyeti
				Diğer……

2.4. KULLANMA/AÇIKLIK ONAYI

AÇIKLIK 1

8 Ocak 2013 tarihli İdare yazısı ile açıklıktan nasıl faydalanılabileceğinin açıklanması amaçlı testin ilerletilmesi talep edilmiştir.

Risk Seviyesi	Acil/Kritik/Yüksek/Orta/Düşük
Erişim Ortamı	İnternet/Intranet
Kullanıcı Profili	Internet Kullanıcısı/Intranet Kullanıcısı/Sistem Kullanıcısı/Diğer
Kullanılan Araçlar	Sqlmap
Zafiyet Türü	Web Uygulaması Açıklıkları/Hizmetler/Windows Açıklıkları
Zafiyet Adı	SQL Injection/OpenSSH Rastgele Komut İşletim Zafiyeti/Cross site scripting (XSS)
Etkilenen Sistemler ve portlar	212.125.85.100 – 5521
Tanım	Bazı uygulama yazılımlarında sql injection açıklıklarının olduğu tespit edilmiştir.
Çözüm önerileri	Kod geliştirme esnasında sql injection neden olabilecek hususlara dikkat edilmelidir. Uygulama kodlarına müdahale edilemeyen uygulamalar için uygulama katmanı güvenlik duvarı (web application firewall) kullanılmalıdır.
Referanslar ve İyi Uygulama Örnekleri	https://www.owasp.org/index.php/SQL_Injection

2.5. KULLANMA SONRASI ETKİ

AÇIKLIK 1

Açıklık üzerinde yapılan testler ilerletilerek aşağıdaki personel bilgileri ve intranet uygulama kullanıcı adı ve parolaları elde edilmiştir. Ayrıca, web sunucusunun bu veri tabanını kullandığı tespit edildiğinden gerekli değişiklikler yapılarak web sayfası üzerinde görülmesi sağlanmıştır.

S. No	Adı Soyadı	Görevi	Kullanıcı Adı	Parola
1	*Yüksel UÇAR*	*Sağlık Mem.*	****	****
2	*Handan GÖKDEMİR*	*Tıbbi Teknolog*	****	****
3	*Cevahir KESEN ÜLKÜ*	*Ebe*	****	****
4	*Züleyha KAPLAN*	*Diyetisyen*	****	****

2.6. DENIAL of SERVICE (DoS) SALDIRILARI

DoS/DDoS testleri sırasında kurumun iş akışını aksatmamak amacıyla Kurum personeli ile koordineli bir çalışma yürütülmüştür. Bu çalışma kapsamında testler hafta sonu saat 02:00-04:00 arasında gerçekleştirilmiştir.

DoS/DDoS saldırıları yapılan sunucular aşağıda listelenmiştir.

Sunucu Adı	IP Adresi	DNS Adı	Açıklama
MAIL	212.125.85.6	mail.abc.gov.tr	E-posta sunucusu
WEB	212.125.85.100	www.abc.gov.tr	Web Sunucusu
DNS	212.125.85.150	dns.abc.gov.tr	DNS Sunucusu

Günümüz dünyasında şirketlerin internete olan bağlantıları hayati önem kazanmış durumdadır. Internet bağlantısının önem kazanmasıyla paralel olarak Internet dünyasının en eski ve etkili saldırı yöntemlerinden biri olan DoS saldırıları da tehdit sınıflandırmasında en üst sıralara yükselmiştir. DoS/DDoS saldırılarının birçok çeşidi bulunmaktadır. ABC Kurumu tarafından aşağıdaki saldırı çeşitlerinin yapılması istemiştir.

ABC Kurumu tarafından talep edilen DoS/DDoS saldırı çeşitleri:

- Syn flood ddos saldırıları
- ACK flood ddos saldırıları
- FIN flood ddos saldırıları
- TCP flood ddos saldırıları
- ICMP flood ddos saldırıları
- HTTP GET flood
- HTTP Post Flood
- UDP Flood
- DNS flood
- Fragmentatin flood

Bu testler neticesinde kurumun aşağıdaki DoS/DDoS çeşitlerine karşı herhangi bir korumasının olmadığı tespit edilmiştir:

- HTTP GET flood
- HTTP Post Flood
- UDP Flood
- DNS flood
- Fragmentatin flood

2.7. KULLANILAN ARAÇLAR

Raporda detayları sunulan sunuculara doğru gerçekleştirilen testlerde aşağıdaki listelenen ticari ve açık kaynak kodlu araçlar kullanılmıştır.

2.7.1. Ağ Tarayıcıları

Nessus – Açık kaynak kodlu zafiyet tarayıcısıdır. *http://www.nessus.org/*

Nmap – Nmap ("Network Mapper") network haritasının çıkartılmasında ve güvenlik denetiminde kullanılan açık kaynak kodlu bir araçtır. *www.insecure.org/nmap/*

2.7.2. Uygulamaya Yönelik Araçlar

AppTool - Uygulama düzeyindeki güvenlik açıklarının çıkartılmasında ve çözüm önerilerinin sunulmasında kullanılan lisanslı bir araçtır.

http://www.appsecurity.com/software/products/tr/tr/apptool-source/

2.7.3. Diğer Araçlar

Nemesis – Paket üreticisi bir program.

Ripe.net – Kamuya açık web sitesi.

EK-2

SIZMA TESTİ KAPSAM BELİRLEME FORMU ÖRNEĞİ

Bu form gerçekleştirilecek olan güvenlik testlerinin kapsamını belirlenmesi için hazırlanmıştır. Lütfen mümkün olduğu kadar detaylı şekilde doldurunuz. Lütfen gerekli yerleri **(x)** şeklinde işaretleyiniz.

Test yapılmasını istediğiniz sistemler arasında kuruluş dışında barındırılan sistemler var ise bu durum testi yapan firmaya bildirilmelidir.

Testin gerçekleştirileceği

Tarih aralığı : ...../...../..... - ...../...../.....

IP aralığı: ..... - .....

Talep Edilen Test Türü	
( ) Beyaz Kutu Testi ( ) Siyah Kutu Testi ( ) Gri Kutu Testi Gri Kutu Testi ..... saatleri arasında yapılmalıdır. Siyah Kutu Testi ..... saatleri arasında yapılmalıdır. Beyaz Kutu Testi ..... saatleri arasında yapılmalıdır.	
Talep Edilen Hizmetler	
( ) Internet Üzerinden Güvenlik Denetim Hizmeti ( ) Web Uygulamalarına Yönelik Güvenlik Denetim Hizmeti ( ) Yerel Ağ İçinden Güvenlik Denetim Hizmeti ( ) Diğer.....	
Internet Üzerinden Ağ Cihazları ve Sunucu Güvenlik Denetim Hizmeti	
Test Edilecek IP'ler ve Açıklama	"1.1.1.1 (DNS)" gibi
Firmaya Ait Test Edilecek Alan Adı	
Internet Üzerinden Test Edilecek Toplam Aktif Sunucu Sayısı	
Web Uygulamalarına Yönelik Güvenlik Denetim Hizmeti	
Test Edilecek Web Uygulama ve Sunucu Sayısı	

Test Edilecek Web Uygulamalarına Ait URL'ler	Uygulama URL'i	Teknoloji (.NET,PHP,JAVA)	Test Hesabı Verilecek mi?*

Yerel Ağ İçinden Gerçekleştirilecek Güvenlik Denetim Hizmeti Bilgileri			
Yerel Ağ İçinden Gerçekleştirilecek Güvenlik Denetim Hizmeti Bilgileri	Web Sunucu:	DNS Sunucu:	Firewall/VPN:
	Mail Sunucu:	SFTP Sunucu:	Veri Tabanı:
	Diğer:	Diğer:	Diğer:

Test Edilecek İstemci Sayıları ve Türü	
Test Edilecek IP'ler ve Açıklama	"1.1.1.1 (DNS)" gibi
Çalışmanın Gerçekleştirileceği Lokasyon	
Wireless Ağlara Sızma Testleri	
Test Edilecek Cihaz Sayısı	
Kimlik Doğrulama Yöntemleri	
İstenilen Testler	( ) WiFi Ağını İçeriden ve Dışarıdan Dinleme Testleri
	( ) WiFi Hotspot Testleri
	( ) Erişim Sağlanması Durumunda Diğer Sistemlere Erişim Testleri
	( ) Şifreleme Türünün Tespit Ve Kırılma Testleri
Acil Durum Kotarma İletişim Bilgileri	

Firma		Müşteri Kuruluş	
İdari		İdari	
Teknik		Teknik	

EK-3

SIZMA TESTİ ÖNCESİ

MÜŞTERİ FERAGATNAMESİ ÖRNEĞİ

Test Tarihleri: <gg.aa.yy> - <gg.aa.yy>

İşbu Sızma Testi Öncesi Müşteri Feragatnamesi ("Feragatname") <gg.aa.yy> tarihinde, <adres> adresinde mukim <müşteri tam adı> ("Müşteri") ile <adres> adresinde mukim yüklenici <firma> ("Firma") arasında imzalanmış olan hizmet alımına ilişkin sözleşmeye ek olmak üzere düzenlenerek taraflarca imzalanmıştır.

Müşteri işbu Feragatname ile firma tarafından Müşteri'ye verilecek saldırı simülasyonu hizmetleri ("Hizmet") kapsamında işbu Feragatname'yi imzalamayı kabul, beyan ve taahhüt eder. Saldırı simülasyonu kötü amaçlı bir saldırganın Müşteri sistemlerine verebileceği zararı Müşterinin görebilmesi ve gerekli tedbirleri alabilmesi için yapılan simülasyonudur.

1. Firma tarafından Müşteri'ye verilecek Hizmet'in ön hazırlıkları sırasında, saldırı simülasyonları öncesi ve saldırı simülasyonları sırasında eğer varsa tüzel ve/veya gerçek üçüncü kişileri, haberdar etmek, gerekiyorsa onlardan yazılı ve/veya sözlü olarak gerekli her türlü izni almak ve simülasyonlar sırasında gözlemlerini yaptırtmaktan Müşteri sorumludur. Bilgi verilmemiş, izin alınmamış veya gözlem yaptırılmamış tüzel ve/veya gerçek üçüncü kişilerle çıkacak anlaşmazlıklardan, bu üçüncü kişilerin taleplerinden ve bu sebeple doğabilecek doğrudan ve/veya dolaylı zararlardan dolayı firmanın sorumlu olmadığını Müşteri kabul eder. Müşteri firmayı bu anlaşmazlıklardan, taleplerden ve zararlardan ari tutacaktır.
2. Firmanın ağır kusuru ile sebep olduğu haller hariç olmak üzere, saldırı simülasyonları sırasında Müşteri'nin DoS, DDoS veya test sistemlerinin zarar görmesi ve bunun hizmet kesintisine sebep olması halinde firmanın sorumlu olmayacağını Müşteri kabul eder.
3. Saldırı simülasyonları sırasında oluşabilecek, hizmet kesintisi, sistem yüklenmeleri gibi durumlardan firmanın kesinlikle sorumlu olmayacağını Müşteri kabul eder.
4. İşbu Feragatname, Müşteri'nin yetkili kişileri tarafından imza edilmekle geçerli ve bağlayıcıdır.

İşbu Feragatname iki nüsha olarak <gg.aa.yy> tarihinde imzalanmış olup, 01.09.2013 <gg.aa.yy> tarihi itibarıyla geçerli ve bağlayıcı olmak üzere yürürlüğe girmiştir.

Firma	Müşteri Kuruluş

Kaynakça

[1] TS ISO/IEC 27001:2005, Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

[2] TS EN ISO/IEC 17025, Deney ve kalibrasyon laboratuvarlarının yeterliliği için genel şartlar

[3] Burlu, K. (2010). Bilişimin Karanlık Yüzü

[4] SAĞIROĞLU, Ş., VURAL, Y., Kurumsal Bilgi Güvenliğinde Güvenlik Testi ve Öneriler, Gazi Üniv. Müh. Mim. Fak. Der., Cilt 26, No 1, 89-103, 2011

[5] www.owasp.org

Ek-17.Geniş Kapsamlı Sızma Testi Kapsam Dokümanı

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
16. Yerinde ve uzaktan kırmızı takım testleri

Siber Güvenlik Faaliyet Raporu Formatı

1. Kuruluş Bilgileri

2. Kurumsal SOME

    a. Kurumsal SOME Personel Listesi

        i. Kurumsal SOME Yöneticisi

            1. Adı-Soyadı

            2. Unvanı

            3. İş Telefonu

            4. Cep Telefonu

            5. Kurumsal E-Posta Adresi

            6. Sorumlu Olduğu Kurumsal SOME Görev/Görevleri

        ii. Kurumsal SOME Personeli

            1. Adı-Soyadı

            2. Unvanı

            3. İş Telefonu

            4. Cep Telefonu

            5. Kurumsal E-Posta Adresi

            6. Sorumlu Olduğu Kurumsal SOME Görev/Görevleri

    b. 2021 Yılı İçerisinde Kurumsal SOME Çalışanlarına Aldırılan Siber Güvenlik Eğitimleri Hakkında Kapsamlı Bilgi

        i. Alınan Eğitim Adı

        ii. Eğitimin Süresi

        iii. Eğitimin Alındığı Kurum/Kuruluşun Adı

        iv. Varsa Eğitim İle İlgili Sertifika/Katılım Belgesi

    c. 2021 Yılı İçerisinde Kurumsal SOME Çalışanlarının Katılım Sağladığı Konferans ve Toplantı Listesi

3. Siber Güvenlik Risk Analizi

    a. Siber Güvenlik Risk Değerlendirme Raporu Yönetici Özeti

4. ISO 27001 Bilgi Güvenliği Sertifikasyon Çalışmaları

    a. Kurum/Kuruluşun Sahip Olduğu ISO 27001 Sertifikası

b. Diğer Çalışmalar

5. 2021 Yılı İçerisinde TSE Tarafından Akredite Edilmiş Kurum/Kuruluşlar Tarafından Yapılan Geniş Kapsamlı Sızma Testi

a. Test Kapsamı

b. Testin Süresi

c. Testin Yaptırıldığı Kurum/Kuruluş

d. Sızma Testi Yönetici Özeti

6. 2021 Yılı İçerisinde Gerçekleşen Siber Olaylar

a. Olay Türü

b. Olayın Gerçekleşme Tarihi

c. Olayın Kısa Tanımı

d. Olayın Sebep Olduğu Tahmini

e. Olayın Bir Daha Tekrarlanmaması Amacıyla Alınan Karşı Önlemler

7. Kurum İçi ve Dışı Paydaşlarla Yapılan Çalışmalar

8. 2021 Yılı İçerisinde Yapılması Planlanan Siber Güvenlik Eğitim Takvimi

a. Kurum/Kuruluş Çalışanlarının Siber Güvenlik Farkındalığını Arttırmaya Yönelik Olan Siber Güvenlik Eğitimleri

b. Kurumsal SOME Çalışanlarının Teknik Yeterliliklerini Arttırmaya Yönelik Olan Siber Güvenlik Eğitimleri

9. 2021 Yılı İçerisinde Yapılması Planlanan Siber Güvenlik Test Takvimi

a. Kurumsal SOME Çalışanları Tarafından Yapılması Planlanan Testler

b. TSE Tarafından Akredite Edilmiş Kurum/Kuruluşlara Yaptırılması Planlanan Testler

10. Varsa Siber Güvenlik Hakkında Yapılan İç Denetim Raporu

11. 2021 Yılı İçerisinde ISO 27001 Kapsamında Yapılmış İç Tetkik Raporları Yönetici Özeti

12. Diğer Faaliyetler

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

HAVACILIK SEKTÖRÜ İÇ KONTROL METODOLOJİSİ

HAVACILIK GÜVENLİĞİ DAİRE BAŞKANLIĞI-SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

1. GRUP HAVACILIK SEKTÖRÜ İŞLETMELERİ

HAVACILIK GÜVENLİĞİ DAİRE BAŞKANLIĞI-SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

Sıra	Kontrol Maddesi	Seviye 1	Seviye 2	Seviye 3	Seviye 4	Toplam
1	Erişim Yönetimi	5	7	5	4	21
2	Varlık Yönetimi	1	3	3	2	9
3	İz Kayıt	4	6	3	4	17
4	Farkındalık	3	5	3	2	13
5	Olay Yönetimi	2	3	1	2	8
6	Bakım	3	1	1	1	6
7	İnsan Kaynakları Güvenliği	3	2	1	0	6
8	Fiziksel Güvenlik	2	3	1	1	7
9	Yedekleme	2	1	1	2	6
10	Risk Yönetimi	3	3	3	3	12
11	Durumsal Farkındalık ve Sistem Test	3	4	3	4	14
12	Sistem ve Haberleşme Güvenliği	9	20	11	11	51
13	Siber Güvenlik Yapılanması	2	5	3	2	12
14	İş Sürekliliği	1	1	3	3	8
15	Tedarikçi Yönetimi	2	2	3	1	8
16	Yasal Uyum	1	1	1	1	4
17	İşletim Güvenliği	2	2	1	0	5
18	Sistem Temini, Geliştirme ve Bakım	2	3	1	1	7
19	Yerli Milli Ürün Kullanılması	1	1	1	1	4
20	İletişim	1	1	1	1	4

Seviye Toplam	**52**	**74**	**50**	**46**	**222**

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

No	1. Erişim Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını user behaviour inceleme teknikleri ile analiz et, yetkilerini kullanmıyorsa yetkiyi iptal et.
2	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması	Son kullanıcılara ait BT varlıklarına usb, harici harddisk vb. cihazlar ile erişimin engellenmesi
3	Son kullanıcı erişim hakları matrisinin oluşturulması	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personelin farklı olması	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını kullanıcı davranışları inceleme teknikleri ile analiz edilmesi, yetkilerin kullanılmaması durumunda yetkinin iptal edilmesi
4	Ayrıcalıklı erişim hakları matrisinin oluşturulması	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi	İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi	Tedarikçi firmalara verilen erişim yetkisinin ihtiyacın bitmesi sonucunda yetkinin ivedilikle sonlandırılması
5	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi	Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi	Tedarikçi firmalar işletme BT varlıllarına erişim sağlaması sürecinde çok faktörlü doğrulama kullanılması	
6		Kayıtlı olmayan cihazların networke erişiminin kısıtlanması		
7		Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi		

No	2. Varlık Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Varlık yönetimi prosedürünün hazırlanması	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi	Havacılık kritik data ve sistemlerin imha süreçlerin belirlenmesi
2		BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi,dokümante edilmesi ve ilgili paydaşların bilgisine sunulması	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi	Havacılık kritik data ve sistemlerin imha süreçlerinin denetlenmesi
3		Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi	

No	3. İz Kayıt			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sekteye uğraması durumuna karşı bir alarm mekanizması oluşturulması	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması	İz kaydı yönetim sürecinde görevlerin ayrılığı ilkesine uygun bir şekilde görevlendirme yapılması
2	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması	Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi
3	NTP server kullanılması	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SGSYY'ye sunulması	Tehdit istihbarat verilerinden gelen bilgiler kapsamında iz kayıt korelasyon sürecinin geliştirilmesi
4	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması		Alarmların ve olayların incelenmesi sonucunda mevcut korelasyonların değerlendirilerek iyileştirilmesi
5		İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi		
6		Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi		

No	4. Farkındalık			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	İşletme üst yönetimine özelleştirilmiş bir siber güvenlik farkındalık eğitiminin verilmesi	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi	Verilen farkındalık eğitimleri sonrasında yapılan sınav sonuçlarının analiz edilmesi ve hedeflenen farkındalık artışını sağlamaması durumunda eğitim sürecinin(eğitim materyali, eğitmen, eğitim verilme şekli vb.) gözden geçirilerek iyileştirilmesi
2	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az 6 ayda bir sosyal mühendislik testlerinin yapılması	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması
3	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümante edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi	İşletme içi siber güvenlik kültürünün arttırılması için bülten, poster vb. materyallerin hazırlanması	
4		İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması		
5		İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi		

No	5. Olay Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması	Siber güvenlik ihlal olay yönetim süreçlerinde olay inceleme süreçlerinin etkin bir şekilde yürütülmesi	Siber güvenlik ihlal olay yönetim süreçlerinde tehdit istihbarat hizmetlerinin kullanılarak olası saldırgan gruplarının belirlenmesi, olağan saldırgan gruplarının davranış şekillerinin incelenerek olay yönetim sürecinin yürütülmesi
2	Dokümante edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması		Haberli veya habersiz olmak üzere periyodik olarak işletmenin siber güvenlik ihlal olaylarına karşı yanıt verme yetkinliğini test edilmesi
3		İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması		

No	6. Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümante edilmesi, izlenmesi ve bu sürelere uygun olarak bakım çalışmalarının gerçekleştirilmesi	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması	Bakım sürecinde yer alan sistemlerin operasyonel süreçlere dahil edilmeden önce güvenlik testlerinin yapılarak söz konusu sistemlerin gizlilik, bütünlük ve erişilebilirlik unsurlarının etkilenmediğinden emin olunması
2	Bakım süreçlerinde görev alacak personelin izlenmesi			
3	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			

No	7. İnsan Kaynakları Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümante edilmesi ve uygulanması	
2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi		
3	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			

No	8. Fiziksel Güvenlik			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi	Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi	İşletmenin ISO 27001 Ek.A.11 kapsamında senede en az 2 kere denetim faaliyeti gerçekleştirmesi
2	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi		
3		Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması		

No	9. Yedekleme			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin süreç kritikliğinide göz önüne alarak bir yedekleme politika veya prosedürü oluşturması	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi	Alınan yedeklerin farklı bir sunucuda yer alması	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması
2	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması.			Bilgi işleme olanaklarının, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmesi

No	10. Risk Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	Varlık envanteri kapsamında belirlenmiş varlıkları 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümante edilmesi	Siber Güvenlik sigortası bulunması
2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlenmesi ve dokümante edilmesi	Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümante edilmesi	Siber güvenlik risk değerlendirme çalışmasının tehdit istihbarat çalışmaları çıktıları sonucuna göre güncellenmesi ve iyileştirilmesi
3	Siber Güvenlik Risk Değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi	Siber Güvenlik Risk Değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

No	11. Durumsal Farkındalık ve Sistem Test			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması
2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi	Tehdit avcılığı mekanizmasının oluşturulması ve kullanılması
3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması	Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi	Siber güvenlik alanında icra edilen iç ve dış kaynaklı test,denetim, zafiyet taraması vb. çalışmalar sonucu tespit edilen bulguların ve risklerin giderilmesi amacıyla bir bulgu yönetim sürecinin tesis edilmesi ve uygulanması	Kırmızı takım çalışmalarının yapılması
4		Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi		Bug bounty çalışmalarının gerçekleştirilmesi
5		Periyodik zafiyet taraması yapılması		

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(1. Grup Havacılık İşletmeleri)

No	12. Sistem ve Haberleşme Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması	Birim bazında ağ segmentasyonunun yapılması	Görev ve kritiklik bazında ağ seğmentasyonunun yapılması	Risk teşkil eden BT varlıklarına yönelik disk şifreleme çözümlerinin kullanılması
2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi	Mevcut DNS filtreleme çalışmalarının KamuDNS projesi ile entegrasyonunun sağlanması
3	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması	İşletme mobil cihazlarının tek bir merkezden güvenlik operasyonlarının yürütülmesi amacıyla MDM kullanılması
4	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi	Kritik bilgi akışının şifreli bir şekilde yapılması	Network ve sunucu mimarisinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümante edilmesi ve iyileştirilmesi
5	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırması	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kripografik şifreler oluşturması ve bu şifrelerin kullanımınının yönetilmesi	Güvenlik sıkılaştırmalarının yeterliliğinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümante edilmesi ve iyileştirilmesi
6	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi	İşletme siber güvenlik kabiliyetinin arttırılması amacı ile siber istihbarat hizmetlerinin kullanılması	VOİP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması	Network güvenlik cihazlarının konumlandırılmasının ve konfigürasyonlarının görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümante edilmesi ve iyileştirilmesi
7	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin siber tehdit istihbarat hizmeti verilerine göre sıkılaştırması	İşletme bilgi teknolojileri altyapısını korumak için honeypot çözümlerinin kullanılması
8	Mobil cihazlar, sunucular ve son kullanılara ait BT varlıklarında antivirüs yazılımı kullanılması	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için özelleştirilmiş firewall çözümlerinin kullanılması
9	DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi	DNS filtreleme çalışmasının gerçekleştirilmesi	Sanallaştırma sistemlerinde kullanılacak olan imajların sıkışlaştırılmasının yapılması ve sürecin denetlenmesi	Veri aktarımı için diyot ürünlerinin kullanılması
10		URL filtreleme çalışmasının gerçekleştirilmesi	İşletme bünyesinde DLP çözümlerinin kullanılması	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için veri aktarımı şifreleme çözümlerinin kullanılması
11		Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması	İşletme bünyesnde bulunan sunucularda EDR çözümlerinin kullanılması
12		İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygunlanması		
13		Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması		
14		Network trafiğinde şüpheli hareket analizinin yapılması		
15		Kullanıcı bazında şüpheli hareket analizinin yapılması		
16		İşletme bünyesinde NAC çözümlerinin kullanılması		
17		İşletme bünyesinde load balancer çözümlerinin kullanılması		
18		İşletme bünyesinde WAF çözümlerinin kullanılması		
19		İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması		
20		İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması		

No	13. Siber Güvenlik Yapılanması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	SOME'nin kurulmuş olması	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması	SGSYY'nin SHT-Siber EK-5'de yer alan sertifikalara sahip olması	Siber Güvenlik Stratejik Planı'nın oluşturulması, gözden geçirilmesi ve güncellenmesi
2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması	İstihdam devam ederken rastgele güvenlik soruşturması araştırmalarının yapılması(adli sicil kaydı, şahıs güvenlik belgesi v.b.)	SOME personeli memnuniyetinin ölçülerek birim bazında personel değişiklik oranının düşürülmesi için faaliyetlerde bulunulması
3		SGSYY'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması	Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması	
4		Some personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)		
5		Some'de görev alan 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		

No	14. İş Sürekliliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması	İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi	BT süreçlerini etkileyen tüm varlıklara yönelik iş sürekliliği yedekliliğinin sağlanması
2			İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması	İş sürekliliği planlarınına yönelik tüm hususların tatbikatının senede en az bir kere yapılması
3			İş sürekliliği çalışmalarının, görevler ayrılığı ilkeside gözetilerek, objektif bir şekilde değerlendirilmesi	İş sürekliliği planı iyileştirme çalışmalarının gerçekleştirilmesi

No	15. Tedarikçi Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi	Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi
2	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi	Tedarikçi çıkış stratejilerinin oluşturulması	Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması	
3			Kritik tedarikçilerin denetim sonuçlarına göre ihtiyaç duyulması halinde çıkış stratejilerinin uygulanması	

No	16. Yasal Uyum			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin ISO 27001 Sertifika belgesine sahip olması	ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması	Yasal uyum süreci ile alakalı boşluk analizinin yapılması

No	17. İşletim Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Yama yönetiminin uygulanması	Değişiklik yönetiminin uygulanması	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi	
2	Lisanssız yazılımların kullanılmaması	Kapasite yönetiminin uygulanması		

No	18. Sistem Temini, Geliştirme ve Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi	Test verisinin kişisel veri veya operasyonel kritik veri içermemesi	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi
2	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi	İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi		
3		Test ve geliştirme ortamlarının ayrıştırılması		

No	19. Yerli Milli Ürün Kullanılması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %10'den fazla ve %20'dan az olması	Yerli ve milli ürünlerin işletme ürün envanterindeki oranının %20'den fazla olması

No	20. İletişim			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi

Havacılık Sektörü İç Kontrol Metodolojisi 1. Grup Havacılık Sektörü İşletmeleri Kontrol Listesi						
Ana Kontrol Maddesi	**Seviye**	**Kontrol No.**	**Alt Kontrol Maddesi**	**U**	**UD**	**NA**
1. Erişim Yönetimi	1	*1.1.1*	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması			
		1.1.2	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi			
		1.1.3	Son kullanıcı erişim hakları matrisinin oluşturulması			
		1.1.4	Ayrıcalıklı erişim hakları matrisinin oluşturulması			
		1.1.5	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi			
	2	*1.2.1*	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi			
		1.2.2	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi			
		1.2.3	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması			
		1.2.4	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi			
		1.2.5	Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi			
		1.2.6	Kayıtlı olmayan cihazların networke erişiminin kısıtlanması			
		1.2.7	Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi			
	3	*1.3.1*	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması			
		1.3.2	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması			
		1.3.3	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personelin farklı olması			
		1.3.4	İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi			

		1.3.5	Tedarikçi firmalar işletme BT varlıllarına erişim sağlaması sürecinde çok faktörlü doğrulama kullanılması			
	4	***1.4.1***	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını user behaviour inceleme teknikleri ile analiz et, yetkilerini kullanmıyorsa yetkiyi iptal et.			
		1.4.2	Son kullanıcılara ait BT varlıklarına usb, harici harddisk vb. cihazlar ile erişimin engellenmesi			
		1.4.3	Son kullanıcı hakları ve ayrıcalıklı erişim hakları sahiplerinin, sahip oldukları yetkileri kullanımını kullanıcı davranışları inceleme teknikleri ile analiz edilmesi, yetkilerin kullanılmaması durumunda yetkinin iptal edilmesi			
		1.4.4	Tedarikçi firmalara verilen erişim yetkisinin ihtiyacın bitmesi sonucunda yetkinin ivedilikle sonlandırılması			
2. Varlık Yönetimi	**1**	***2.1.1***	Varlık yönetimi prosedürünün hazırlanması			
	2	***2.2.1***	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi			
		2.2.2	BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi,dokümante edilmesi ve ilgili paydaşların bilgisine sunulması			
		2.2.3	Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi			
	3	***2.3.1***	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		2.3.2	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi			
		2.3.3	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi			
	4	***2.4.1***	Havacılık kritik data ve sistemlerin imha süreçlerin belirlenmesi			
		2.4.2	Havacılık kritik data ve sistemlerin imha süreçlerinin denetlenmesi			
	1	***3.1.1***	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi			
		3.1.2	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması			
		3.1.3	NTP server kullanılması			

3. İz Kayıt		***3.1.4***	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması			
	2	***3.2.1***	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sekteye uğraması durumuna karşı bir alarm mekanizması oluşturulması			
		3.2.2	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması			
		3.2.3	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması			
		3.2.4	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması			
		3.2.5	İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi			
		3.2.6	Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi			
	3	***3.3.1***	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması			
		3.3.2	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması			
		3.3.3	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SGSYY'ye sunulması			
	4	***3.4.1***	İz kaydı yönetim sürecinde görevlerin ayrılığı ilkesine uygun bir şekilde görevlendirme yapılması			
		3.4.2	Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi			
		3.4.3	Tehdit istihbarat verilerinden gelen bilgiler kapsamında iz kayıt korelasyon sürecinin geliştirilmesi			
		3.4.4	Alarmların ve olayların incelenmesi sonucunda mevcut korelasyonların değerlendirilerek iyileştirilmesi			
	1	***4.1.1***	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.1.2	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.1.3	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümante edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi			

4. Farkındalık	**2**	***4.2.1***	İşletme üst yönetimine özelleştirilmiş bir siber güvenlik farkındalık eğitiminin verilmesi			
		4.2.2	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		4.2.3	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi			
		4.2.4	İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması			
		4.2.5	İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi			
	3	***4.3.1***	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi			
		4.3.2	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az 6 ayda bir sosyal mühendislik testlerinin yapılması			
		4.3.3	İşletme içi siber güvenlik kültürünün arttırılması için bülten, poster vb. materyallerin hazırlanması			
	4	***4.4.1***	Verilen farkındalık eğitimleri sonrasında yapılan sınav sonuçlarının analiz edilmesi ve hedeflenen farkındalık artışını sağlamaması durumunda eğitim sürecinin(eğitim materyali, eğitmen, eğitim verilme şekli vb.) gözden geçirilerek iyileştirilmesi			
		4.4.2	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması			
5. Olay Yönetimi	**1**	***5.1.1***	Siber güvenlik ihlal olay yönetim ve müdahale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması			
		5.1.2	Dokümante edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması			
	2	***5.2.1***	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması			
		5.2.2	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması			
		5.2.3	İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması			
	3	***5.3.1***	Siber güvenlik ihlal olay yönetim süreçlerinde olay inceleme süreçlerinin etkin bir şekilde yürütülmesi			
	4	***5.4.1***	Siber güvenlik ihlal olay yönetim süreçlerinde tehdit istihbarat hizmetlerinin kullanılarak olası saldırgan gruplarının belirlenmesi, olağan saldırgan gruplarının davranış şekillerinin incelenerek olay yönetim sürecinin yürütülmesi			

	4	5.4.2	Haberli veya habersiz olmak üzere periyodik olarak işletmenin siber güvenlik ihlal olaylarına karşı yanıt verme yetkinliğini test edilmesi			
6. Bakım	1	6.1.1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			
		6.1.2	Bakım süreçlerinde görev alacak personelin izlenmesi			
		6.1.3	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			
	2	6.2.1	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümante edilmesi, izlenmesi ve bu sürelere uygun olarak bakım çalışmalarının gerçekleştirilmesi			
	3	6.3.1	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması			
	4	6.4.1	Bakım sürecinde yer alan sistemlerin operasyonel süreçlere dahil edilmeden önce güvenlik testlerinin yapılarak söz konusu sistemlerin gizlilik, bütünlük ve erişilebilirlik unsurlarının etkilenmediğinden emin olunması			
7. İnsan Kaynakları Güvenliği	1	7.1.1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması			
		7.1.2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması			
		7.1.3	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			
	2	7.2.1	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi			
		7.2.2	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi			
	3	7.3.1	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümante edilmesi ve uygulanması			
8. Fiziksel Güvenlik	1	8.1.1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
		8.1.2	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması			
	2	8.2.1	Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması			
		8.2.2	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi			

		8.2.3	Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması			
	3	***8.3.1***	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi			
	4	***8.4.1***	İşletmenin ISO 27001 Ek.A.11 kapsamında senede en az 2 kere denetim faaliyeti gerçekleştirmesi			
9. Yedekleme	**1**	***9.1.1***	İşletmenin süreç kritikliğinide göz önüne alarak bir yedekleme politika veya prosedürü oluşturması			
		9.1.2	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması.			
	2	***9.2.1***	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi			
	3	***9.3.1***	Alınan yedeklerin farklı bir sunucuda yer alması			
	4	***9.4.1***	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması			
		9.4.2	Bilgi işleme olanaklarının, erişilebilirlik gereksinimlerini karşılamak için yeterli fazlalık ile gerçekleştirilmesi			
10. Risk Yönetimi	**1**	***10.1.1***	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi			
		10.1.2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi			
		10.1.3	Siber Güvenlik Risk Değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi			
	2	***10.2.1***	Varlık envanteri kapsamında belirlenmiş varlıkları 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi			
		10.2.2	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlenmesi ve dokümante edilmesi			
		10.2.3	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	3	***10.3.1***	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümante edilmesi			
		10.3.2	Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümante edilmesi			

		10.3.3	Siber Güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	4	***10.4.1***	Siber Güvenlik sigortası bulunması			
		10.4.2	Siber güvenlik risk değerlendirme çalışmasının tehdit istihbarat çalışmaları çıktıları sonucuna göre güncellenmesi ve iyileştirilmesi			
		10.4.3	Siber Güvenlik Risk Değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi			
11. Durumsal Farkındalık ve Sistem Test	**1**	***11.1.1***	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması			
		11.1.2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.1.3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması			
	2	***11.2.1***	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi			
		11.2.2	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.2.3	Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			
		11.2.4	Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			
		11.2.5	Periyodik zafiyet taraması yapılması			
	3	***11.3.1***	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi			
		11.3.2	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi			
		11.3.3	Siber güvenlik alanında icra edilen iç ve dış kaynaklı test,denetim, zafiyet taraması vb. çalışmalar sonucu tespit edilen bulguların ve risklerin giderilmesi amacıyla bir bulgu yönetim sürecinin tesis edilmesi ve uygulanması			
	4	***11.4.1***	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması			
		11.4.2	Tehdit avcılığı mekanizmasının oluşturulması ve kullanılması			

	4	***11.4.3***	Kırmızı takım çalışmalarının yapılması			
		11.4.4	Bug bounty çalışmalarının gerçekleştirilmesi			
	1	***12.1.1***	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması			
		12.1.2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması			
		12.1.3	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması			
		12.1.4	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi			
		12.1.5	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi			
		12.1.6	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi			
		12.1.7	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi			
		12.1.8	Mobil cihazlar, sunucular ve son kullanılara ait BT varlıklarında antivirüs yazılımı kullanılması			
		12.1.9	DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi			
		12.2.1	Birim bazında ağ segmentasyonunun yapılması			
		12.2.2	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması			
		12.2.3	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması			
		12.2.4	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi			
		12.2.5	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırması			
		12.2.6	İşletme siber güvenlik kabiliyetinin arttırılması amacı ile siber istihbarat hizmetlerinin kullanılması			

12. Sistem ve Haberleşme Güvenliği	**2**	***12.2.7***	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması			
		12.2.8	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi			
		12.2.9	DNS filtreleme çalışmasının gerçekleştirilmesi			
		12.2.10	URL filtreleme çalışmasının gerçekleştirilmesi			
		12.2.11	Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması			
		12.2.12	İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygunlanması			
		12.2.13	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması			
		12.2.14	Network trafiğinde şüpheli hareket analizinin yapılması			
		12.2.15	Kullanıcı bazında şüpheli hareket analizinin yapılması			
		12.2.16	İşletme bünyesinde NAC çözümlerinin kullanılması			
		12.2.17	İşletme bünyesinde load balancer çözümlerinin kullanılması			
		12.2.18	İşletme bünyesinde WAF çözümlerinin kullanılması			
		12.2.19	İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması			
		12.2.20	İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması			
		12.3.1	Görev ve kritiklik bazında ağ seğmentasyonunun yapılması			
		12.3.2	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi			
		12.3.3	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması			

	3	***12.3.4***	Kritik bilgi akışının şifreli bir şekilde yapılması			
		12.3.5	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kripografik şifreler oluşturması ve bu şifrelerin kullanımınının yönetilmesi			
		12.3.6	VOİP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması			
		12.3.7	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin siber tehdit istihbarat hizmeti verilerine göre sıkılaştırması			
		12.3.8	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi			
		12.3.9	Sanallaştırma sistemlerinde kullanılacak olan imajların sıkışlaştırılmasının yapılması ve sürecin denetlenmesi			
		12.3.10	İşletme bünyesinde DLP çözümlerinin kullanılması			
		12.3.11	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması			
	4	***12.4.1***	Risk teşkil eden BT varlıklarına yönelik disk şifreleme çözümlerinin kullanılması			
		12.4.2	Mevcut DNS filtreleme çalışmalarının KamuDNS projesi ile entegrasyonunun sağlanması			
		12.4.3	İşletme mobil cihazlarının tek bir merkezden güvenlik operasyonlarının yürütülmesi amacıyla MDM kullanılması			
		12.4.4	Network ve sunucu mimarisinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümante edilmesi ve iyileştirilmesi			
		12.4.5	Güvenlik sıkılaştırmalarının yeterliliğinin görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümante edilmesi ve iyileştirilmesi			
		12.4.6	Network güvenlik cihazlarının konumlandırılmasının ve konfigürasyonlarının görevler ayrılığı ilkesi gözetilerek değerlendirilmesi, dokümante edilmesi ve iyileştirilmesi			
		12.4.7	İşletme bilgi teknolojileri altyapısını korumak için honeypot çözümlerinin kullanılması			
		12.4.8	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için özelleştirilmiş firewall çözümlerinin kullanılması			
		12.4.9	Veri aktarımı için diyot ürünlerinin kullanılması			

		12.4.10	İşletme bünyesinde kullanılan EKS,SCADA ve IOT teknolojileri için veri aktarımı şifreleme çözümlerinin kullanılması			
		12.4.11	İşletme bünyesnde bulunan sunucularda EDR çözümlerinin kullanılması			
13. Siber Güvenlik Yapılanması	**1**	***13.1.1***	SOME'nin kurulmuş olması			
		13.1.2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması			
	2	***13.2.1***	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması			
		13.2.2	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması			
		13.2.3	SGSYY'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması			
		13.2.4	Some personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)			
		13.2.5	Some'de görev alan 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			
	3	***13.3.1***	SGSYY'nin SHT-Siber EK-5'de yer alan sertifikalara sahip olması			
		13.3.2	İstihdam devam ederken rastgele güvenlik soruşturması araştırmalarının yapılması(adli sicil kaydı, şahıs güvenlik belgesi v.b.)			
		13.3.3	Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması			
	4	***13.4.1***	Siber Güvenlik Stratejik Planı'nın oluşturulması, gözden geçirilmesi ve güncellenmesi			
		13.4.2	SOME personeli memnuniyetinin ölçülerek birim bazında personel değişiklik oranının düşürülmesi için faaliyetlerde bulunulması			
	1	***14.1.1***	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması			
	2	***14.2.1***	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması			
		14.3.1	İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			

14. İş Sürekliliği	**3**	***14.3.2***	İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması			
		14.3.3	İş sürekliliği çalışmalarının, görevler ayrılığı ilkeside gözetilerek, objektif bir şekilde değerlendirilmesi			
	4	***14.4.1***	BT süreçlerini etkileyen tüm varlıklara yönelik iş sürekliliği yedekliliğinin sağlanması			
		14.4.2	İş sürekliliği planlarınına yönelik tüm hususların tatbikatının senede en az bir kere yapılması			
		14.4.3	İş sürekliliği planı iyileştirme çalışmalarının gerçekleştirilmesi			
15. Tedarikçi Yönetimi	**1**	***15.1.1***	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması			
		15.1.2	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi			
	2	***15.2.1***	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi			
		15.2.2	Tedarikçi çıkış stratejilerinin oluşturulması			
	3	***15.3.1***	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi			
		15.3.2	Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması			
		15.3.3	Kritik tedarikçilerin denetim sonuçlarına göre ihtiyaç duyulması halinde çıkış stratejilerinin uygulanması			
	4	***15.4.1***	Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi			
16. Yasal Uyum	**1**	***16.1.1***	İşletmenin ISO 27001 Sertifika belgesine sahip olması			
	2	***16.2.1***	ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması			
	3	***16.3.1***	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması			
	4	***16.4.1***	Yasal uyum süreci ile alakalı boşluk analizinin yapılması			

17. İşletim Güvenliği	1	17.1.1	Yama yönetiminin uygulanması			
		17.1.2	Lisanssız yazılımların kullanılmaması			
	2	17.2.1	Değişiklik yönetiminin uygulanması			
		17.2.2	Kapasite yönetiminin uygulanması			
	3	17.3.1	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi			
18. Sistem Temini, Geliştirme ve Bakım	1	18.1.1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması			
		18.1.2	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi			
	2	18.2.1	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi			
		18.2.2	İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi			
		18.2.3	Test ve geliştirme ortamlarının ayrıştırılması			
	3	18.3.1	Test verisinin kişisel veri veya operasyonel kritik veri içermemesi			
	4	18.4.1	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi			
19. Yerli Milli Ürün Kullanılması	1	19.1.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması			
	2	19.2.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması			
	3	19.3.1	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %10'den fazla ve %20'dan az olması			
	4	19.4.1	Yerli ve milli ürünlerin işletme ürün envanterindeki oranının %20'den fazla olması			
	1	20.1.1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

20. İletişim	**2**	***20.2.1***	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	3	***20.3.1***	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	4	***20.4.1***	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

U: Uygun
UD:Uygun Değil
NA:Uygulanamaz

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

2. GRUP HAVACILIK SEKTÖRÜ İŞLETMELERİ

HAVACILIK GÜVENLİĞİ DAİRE BAŞKANLIĞI-SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

Sıra	Kontrol Maddesi	Seviye 1	Seviye 2	Seviye 3	Seviye 4	Toplam
1	Erişim Yönetimi	2	4	8	2	16
2	Varlık Yönetimi	1	1	2	3	7
3	İz Kayıt	3	6	2	3	14
4	Farkındalık	2	3	3	2	10
5	Olay Yönetimi	1	2	2	1	6
6	Bakım	2	1	1	1	5
7	İnsan Kaynakları Güvenliği	2	3	1	0	6
8	Fiziksel Güvenlik	1	2	1	2	6
9	Yedekleme	1	1	2	1	5
10	Risk Yönetimi	2	2	4	2	10
11	Durumsal Farkındalık ve Sistem Test	3	2	5	1	11
12	Sistem ve Haberleşme Güvenliği	6	13	11	7	37
13	Siber Güvenlik Yapılanması	2	3	1	2	8
14	İş Sürekliliği	1	1	0	3	5
15	Tedarikçi Yönetimi	1	1	1	3	6
16	Yasal Uyum	1	0	1	1	3
17	İşletim Güvenliği	1	1	2	1	5
18	Sistem Temini, Geliştirme ve Bakım	1	1	4	1	7
19	Yerli Milli Ürün Kullanıması	0	0	1	1	2
20	İletişim	1	1	1	1	4

Seviye Toplam	**34**	**48**	**53**	**38**	**173**

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(2. Grup Havacılık İşletmeleri)

No	1. Erişim Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması
2	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personel/personellerin farklı olması
3		Son kullanıcı erişim hakları matrisinin oluşturulması	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması	
4		Ayrıcalıklı erişim hakları matrisinin oluşturulması	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi	
5			Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi	
6			Kayıtlı olmayan cihazların networke erişiminin kısıtlanması	
7			İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi	
8			Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi	

No	2. Varlık Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Varlık yönetimi prosedürünün hazırlanması	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi	BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi,dokümante edilmesi ve ilgili paydaşların bilgisine sunması	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi
2			Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi
3				Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi

No	3. İz Kayıt			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması
2	NTP server kullanılması	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sekteye uğraması durumuna karşı bir alarm mekanizması oluşturulması	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SOME birimi yöneticisine sunulması	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması
3	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması		Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi
4		Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması		
5		İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi		
6		Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi		

No	4. Farkındalık			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az senede bir sosyal mühendislik testlerinin yapılması
2	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümante edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması
3		İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması	İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi	

No	5. Olay Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik ihlal olay yönetim ve müdehale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması	Dokümante edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması	Siber güvenlik ihlal olay yönetim süreçlerinde adli bilişim süreçlerinin etkin bir şekilde yürütülmesi
2		İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması	

No	6. Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması	Bakım süreçlerinde görev alacak personelin izlenmesi	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümante edilmesi, izlenmesi ve bu sürelere uygun olarak bakım çalışmalarının gerçekleştirilmesi	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması
2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			

No	7. İnsan Kaynakları Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümante edilmesi ve uygulanması	
2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması		
3		Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi		

No	8. Fiziksel Güvenlik			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi
2		Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması		Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması

No	9. Yedekleme			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin süreç kritikliğinide göz önüne alarak bir yedekleme politika veya prosedürü oluşturması	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması
2			Backupların farklı bir sunucuda yer alması	

No	10. Risk Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi	Varlık envanteri kapsamında belirlenmiş varlıkları ISO 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümante edilmesi
2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlemesi ve dokümante etmesi	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi
3			Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümante edilmesi	
4			Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi	

No	11. Durumsal Farkındalık ve Sistem Test			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması
2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	Periyodik zafiyet taraması yapılması	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması	
3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması		Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi	
4			Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi	
5			TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi	

No	12. Sistem ve Haberleşme Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması	Birim bazında ağ segmentasyonunun yapılması	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması	Görev ve kritiklik bazında ağ seğmentasyonunun yapılması
2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması
3	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi	İşletme siber güvenlik kabiliyetinin arttırılması amacı ile siber istihbarat hizmetlerinin kullanılması
4	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırması	Kritik bilgi akışının şifreli bir şekilde yapılması	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi
5	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kripografik şifreler oluşturması ve bu şifrelerin kullanımınının yönetilmesi	İşletme bünyesinde load balancer çözümlerinin kullanılması
6	Mobil cihazlar, sunucular ve son kullanılara ait BT varlıklarında antivirüs yazılımı kullanılması	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi	İşletme bünyesinde WAF çözümlerinin kullanılması
7		DNS filtreleme çalışmasının gerçekleştirilmesi	VOİP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması
8		URL filtreleme çalışmasının gerçekleştirilmesi	Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması	
9		İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygunlanması	Kullanıcı bazında şüpheli hareket analizinin yapılması	
10		Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması	İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması	
11		DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi	İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması	
12		Network trafiğinde şüpheli hareket analizinin yapılması		
13		İşletme bünyesinde NAC çözümlerinin kullanılması		

No	13. Siber Güvenlik Yapılanması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	SOME'nin kurulmuş olması	SOME Yöneticisi'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması
2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması	SOME personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)		Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması
3		Some'de görev alan 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		

No	14. İş Sürekliliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması		İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi
2				İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması
3				İş sürekliliği çalışmalarının, görevler ayrılığı ilkeside gözetilerek, objektif bir şekilde değerlendirilmesi

No	15. Tedarikçi Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi
2				Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması
3				Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi

No	16. Yasal Uyum			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletmenin ISO 27001 Sertifika belgesine sahip olması		ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması

No	17. İşletim Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Lisanssız yazılımların kullanılmaması	Yama yönetiminin uygulanması	Değişiklik yönetiminin uygulanması	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi
2			Kapasite yönetiminin uygulanması	

No	18. Sistem Temini, Geliştirme ve Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi
2			İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi	
3			Test ve geliştirme ortamlarının ayrıştırılması	
4			Test verisinin kişisel veri veya operasyonel kritik veri içermemesi	

No	19. Yerli Milli Ürün Kullanılması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması

No	20. İletişim			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi

Havacılık Sektörü İç Kontrol Metodolojisi 2. Grup Havacılık Sektörü İşletmeleri Kontrol Listesi						
Kontrol Başlığı	**Seviye**	**Kontrol No.**	**Kontrol Maddesi**	**U**	**UD**	**NA**
1. Erişim Yönetimi	**1**	***1.1.1***	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması			
		1.1.2	Varlıkların kritiklik seviyesine uygun bir parola yönetim süreci tesis edilmesi, uygulanması ve denetlenmesi			
	2	***1.2.1***	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi			
		1.2.2	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi			
		1.2.3	Son kullanıcı erişim hakları matrisinin oluşturulması			
		1.2.4	Ayrıcalıklı erişim hakları matrisinin oluşturulması			
	3	***1.3.1***	Çalışan grupları dışında kalan kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi			
		1.3.2	Son kullanıcılara ait bt varlıklarına usb, harici harddisk vb. cihazlar ile erişimin yönetilmesi			
		1.3.3	Ayrıcalıklı erişim hakkına sahip kullanıcılarda en az yetki prensibinin uygulanması			
		1.3.4	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi			
		1.3.5	Ayrıcalıklı kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden geçirilmesi			
		1.3.6	Kayıtlı olmayan cihazların networke erişiminin kısıtlanması			
		1.3.7	İşletme BT varlıklarına erişim sağlaması gereken tedarikçiler için erişim yöntemi ve kontrol mekanizmasının oluşturulması ve yürütülmesi			
		1.3.8	Tedarikçi firmalara verilen erişim haklarının ilgili süreç bazında ihtiyaç duyulan minimum süre ve minimum yetki bazında verilmesi			
	4	***1.4.1***	Kritik varlıklara usb, harici harddisk vb. cihazlar ile erişimin kısıtlanması			
		1.4.2	Erişim yetki tanımlaması yapan personel ve erişim yetki gözden geçirmesini yapan personel/personellerin farklı olması			
	1	***2.1.1***	Varlık yönetimi prosedürünün hazırlanması			
	2	***2.2.1***	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi			

2. Varlık Yönetimi	**3**	***2.3.1***	BT varlıklarının kabul edilebilir kullanımlarının belirlenmesi,dokümante edilmesi ve ilgili paydaşların bilgisine sunması			
		2.3.2	Varlık gruplarının puan ve etki analizinin periyodik olarak gözden geçirilmesi			
	4	***2.4.1***	Varlık gruplarının puan ve etki analizinin ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		2.4.2	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin belirlenmesi			
		2.4.3	Kritik BT süreçlerine yönelik varlıkların imha süreçlerinin denetlenmesi			
3. İz Kayıt	**1**	***3.1.1***	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi			
		3.1.2	NTP server kullanılması			
		3.1.3	İşletme tarafından alınan iz kayıtları kapsamında toplanan kayıtların nitelik bakımından inkar edilemez olmasının sağlanması			
	2	***3.2.1***	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması			
		3.2.2	İz kayıt toplama sürecinin herhangi bir sebepten ötürü sekteye uğraması durumuna karşı bir alarm mekanizması oluşturulması			
		3.2.3	İz kayıtlarına erişimin yönetilmesi ve kayıt altına alınması			
		3.2.4	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması			
		3.2.5	İz kayıtlarına yönelik periyodik analiz raporlarının oluşturulması ve gözden geçirilmesi			
		3.2.6	Korelasyonlar sonucunda oluşan alarmların incelenerek ihtiyaç duyulması halinde diğer güvenlik süreçlerinin tetiklenmesi			
	3	***3.3.1***	Herhangi bir sebepten dolayı iz kayıt sağlayamayan sistemlerin tespit edilmesi için bir tespit mekanizmasının oluşturulması			
		3.3.2	İz kayıtları alarmlarına yönelik yapılan çalışmalar hakkında periyodik olarak analiz yapılması ve söz konusu bu analiz raporunun SOME birimi yöneticisine sunulması			
	4	***3.4.1***	Toplanan iz kayıtlarının söz konusu uygulama veya sistemlerden farklı bir serverda tutulması			
		3.4.2	İşletme veya sektör paydaşlarının karşılaştığı siber güvenlik olaylarına yönelik korelasyonların oluşturulması			
		3.4.3	Mevcut korelasyon setlerinin periyodik olarak gözden geçirilmesi ve iyileştirilmesi			

4. Farkındalık	1	4.1.1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.1.2	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümante edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi			
	2	4.2.1	İşletme tesislerinde görev alan tedarikçi personele için etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
		4.2.2	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		4.2.3	İşletme personeline verilen siber güvenlik farkındalık eğitimlerinin sonrasında eğitimin yarattığı farkındalık seviyesinin ölçülmesi amacı ile sınavların yapılması			
	3	4.3.1	Siber güvenlik farkındalığı eğitiminin ve sıklığının eğitimi alan personelin icra ettiği görevin kritikliğine uygun olarak verilmesi			
		4.3.2	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi			
		4.3.3	İhtiyaç duyulması halinde işletme paydaşlarının söz konusu siber risk ve tehditler kapsamında bilgilendirilmesi			
	4	4.4.1	İşletme çalışanlarının siber güvenlik farkındalığı seviyesinin ölçülmesi için işletme çalışanlarının tümünü kapsayacak şekilde en az senede bir sosyal mühendislik testlerinin yapılması			
		4.4.2	Yapılan farkındalık sınav ve testlerinde hedeflenen başarı oranının altında kalan personelin farkındalık seviyesini arttırmak amacıyla faaliyetlerde bulunulması			
5. Olay Yönetimi	1	5.1.1	Siber güvenlik ihlal olay yönetim ve müdehale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması			
	2	5.2.1	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması			
		5.2.2	İşletmenin yaşadığı siber güvenlik ihlal olaylarının nedenlerini alınan dersleri ve bir daha yaşanmaması için alınacak önlemleri kayıt altına alması ve ilgili otoriteler ile paylaşması			
	3	5.3.1	Dokümante edilmiş bir siber güvenlik ihlal olay müdahale sürecinin oluşturulması			
		5.3.2	İşletmenin yaşadığı siber güvenlik ihlal olaylarını analiz etmesi, kayıt altına alması ve bir daha benzer bir siber güvenlik ihlal olayının yaşanmaması için gerekli önlemleri alması			
	4	5.4.1	Siber güvenlik ihlal olay yönetim süreçlerinde adli bilişim süreçlerinin etkin bir şekilde yürütülmesi			
6. Bakım	1	6.1.1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			
		6.1.2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			
	2	6.2.1	Bakım süreçlerinde görev alacak personelin izlenmesi			

	3	6.3.1	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümante edilmesi, izlenmesi ve bu sürelere uygun olarak bakım çalışmalarının gerçekleştirilmesi			
	4	6.4.1	Bakım verilerin kayıt altında tutulması ve gizliliğinin sağlanması			
7. İnsan Kaynakları Güvenliği	1	7.1.1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması			
		7.1.2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması			
	2	7.2.1	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi			
		7.2.2	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			
		7.2.3	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi			
	3	7.3.1	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümante edilmesi ve uygulanması			
8. Fiziksel Güvenlik	1	8.1.1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
	2	8.2.1	Kritik BT varlıklarını etkileyen fiziksel ortam ve unsurların envanterinin oluşturulması			
		8.2.2	Kritik BT varlıklarına fiziksel erişimin yetki kapsamında kısıtlanması			
	3	8.3.1	Kritik BT varlıklarına fiziksel erişimi izlenmesi ve yetkisiz erişimlerin tespit edilmesi			
	4	8.4.1	Kritik BT varlıklarının bulunduğu alanlara erişim yetkisine sahip olmayan iç ve dış kaynaklı çalışanlara ve ziyaretçilere söz konusu kritik bu alanlara erişimlerinde eşlik edilmesi, bu kişilerin aktivitelerinin izlenmesi			
		8.4.2	Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması			
9. Yedekleme	1	9.1.1	İşletmenin süreç kritikliğinide göz önüne alarak bir yedekleme politika veya prosedürü oluşturması			
	2	9.2.1	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması.			
	3	9.3.1	Periyodik olarak yedekten geri dönme test çalışmalarının gerçekleştirilmesi			
		9.3.2	Backupların farklı bir sunucuda yer alması			
	4	9.4.1	Farklı bir risk bölgesinde işletme kritik dataların hepsini içerecek bir FKM yapısının kurulması			

10. Risk Yönetimi	**1**	***10.1.1***	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi			
		10.1.2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi			
	2	***10.2.1***	Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi			
		10.2.2	Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan sızma testi, zafiyet taraması, kırmızı takım vb. çalışmaların sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	3	***10.3.1***	Varlık envanteri kapsamında belirlenmiş varlıkları ISO 27001 Ek.A maddeleri kapsamında her bir madde ayrı ayrı olacak şekilde değerlendirilmesi			
		10.3.2	İşletmenin üretici veya tedarikçi bağımlılığı kapsamında siber güvenlik risklerinin belirlemesi ve dokümante etmesi			
		10.3.3	Risk kabulü ile ilgili sürecin aktif bir şekilde yürütülmesi ve dokümante edilmesi			
		10.3.4	Siber güvenlik risk değerlendirme çalışmasının işletme iç ve dış kaynaklar tarafından yapılan denetim faaliyetlerinin sonuçlarına göre güncellenmesi ve iyileştirilmesi			
	4	***10.4.1***	Risk indirgeme çalışmalarının ilgili birimler ile koordine edilerek yürütülmesi, takip edilmesi ve dokümante edilmesi			
		10.4.2	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi			
11. Durumsal Farkındalık	**1**	***11.1.1***	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması			
		11.1.2	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.1.3	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması			
	2	***11.2.1***	Havacılık Sektörü İç Kontrol Metodolojisine uygun olarak en üst seviyeye erişmek için gerekli olan aksiyonların belirlenmesi			
		11.2.2	Periyodik zafiyet taraması yapılması			
	3	***11.3.1***	İşletmenin tabi olduğu yasal düzenlemelere uygun hale gelmek için gerekli aksiyonların belirlenmesi			
		11.3.2	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.3.3	Siber tehdit veya siber güvenlik ihlal olayı tespit yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			
		11.3.4	Siber olay müdahale yapılanmasının yeterliliğinin ölçülmesi ve iyileştirilmesi			

		11.3.5	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi			
	4	***11.4.1***	7x24 prensibine göre siber tehdit veya siber güvenlik ihlal olayı müdahale görevini icra edecek bir mekanizmanın kurulması			
	1	***12.1.1***	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması			
		12.1.2	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması			
		12.1.3	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi			
		12.1.4	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi			
		12.1.5	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi			
		12.1.6	Mobil cihazlar, sunucular ve son kullanılara ait BT varlıklarında antivirüs yazılımı kullanılması			
	2	***12.2.1***	Birim bazında ağ segmentasyonunun yapılması			
		12.2.2	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması			
		12.2.3	Firewall kurallarının periyodik olarak gözden geçirilmesi ve iyileştirilmesi			
		12.2.4	Ağ güvenlik cihazlarının ve sunucu güvenlik konfigürasyon setlerinin USOM,SHGM gibi üst kuruluşlardan gelen talimatlara göre sıkılaştırması			
		12.2.5	Network cihazlarının yönetiminde şifrelenmiş oturumlar kullanılması			
		12.2.6	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi			
		12.2.7	DNS filtreleme çalışmasının gerçekleştirilmesi			
		12.2.8	URL filtreleme çalışmasının gerçekleştirilmesi			
		12.2.9	İhtiyaç duyulduğu kadar yetki prensibine bağlı kalarak güvenlik kontrollerinin uygunlanması			
		12.2.10	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması			
		12.2.11	DDoS saldırılarına karşı önlem alınması ve alınan bu önlemlerin yeterliliğini periyodik olarak test edilmesi			

12. Sistem ve Haberleşme Güvenliği		***12.2.12***	Network trafiğinde şüpheli hareket analizinin yapılması			
		12.2.13	İşletme bünyesinde NAC çözümlerinin kullanılması			
	3	***12.3.1***	Her bir ağ segmentasyonu için ayrı ayrı güvenlik duvarı yapılanmasının oluşturulması			
		12.3.2	Dıştan içe veya içten içe iletilen medyanın taranması için sandbox uygulamalarının kullanılması			
		12.3.3	Firewall trafiğinin izlenmesi, analiz edilmesi ve yapılan analiz sonucunda riskli görülen trafiğin engellenmesi			
		12.3.4	Kritik bilgi akışının şifreli bir şekilde yapılması			
		12.3.5	Kritik operasyonlarda erişim yönetim süreçlerinde kullanılmak üzere kripografik şifreler oluşturması ve bu şifrelerin kullanımınının yönetilmesi			
		12.3.6	802.1x metodu ile kayıtdışı cihazların veya kullanıcıların networke erişiminin engellenmesi			
		12.3.7	VOİP teknolojileri kullanılıyorsa, söz konusu bu teknolojiye yönelik sıkılaştırmaların yapılması			
		12.3.8	Son kullanıcılar tarafından ziyaret edilen web sitelerinin zararlı bir bileşen(exploit kit vb.) içermediğinin doğrulanması			
		12.3.9	Kullanıcı bazında şüpheli hareket analizinin yapılması			
		12.3.10	İşletme bünyesinde IDS ve IPS çözümlerinin kullanılması			
		12.3.11	İşletme iç paydaşlarının kullanımına yönelik olan sistemlerin uzaktan erişiminin ipsec vpn üzerinden olması			
	4	***12.4.1***	Görev ve kritiklik bazında ağ seğmentasyonunun yapılması			
		12.4.2	DMZ yapılanmasının oluşturulması ve efektif bir şekilde kullanımının sağlanması			
		12.4.3	İşletme siber güvenlik kabiliyetinin arttırılması amacı ile siber istihbarat hizmetlerinin kullanılması			
		12.4.4	Tüm son kullanıcı gruplarının yükleme izni olan uygulamaların belirlenmesi amacıyla whitelist ve blacklist uygulanması ve söz konusu sistemin 7x24 izlenmesi			
		12.4.5	İşletme bünyesinde load balancer çözümlerinin kullanılması			
		12.4.6	İşletme bünyesinde WAF çözümlerinin kullanılması			

		12.4.7	Son kullanıcılara yönelik cihazlarda EDR çözümlerinin kullanılması			
13. Siber Güvenlik Yapılanması	1	13.1.1	SOME'nin kurulmuş olması			
		13.1.2	SOME birimi personelinin kapsam ve görev tanımlarının belirlenmiş ve dokümante edilmiş olması			
	2	13.2.1	SOME Yöneticisi'nin en az lisans derecesine sahip olması ve siber güvenlik konusunda uzmanlaşmış olması			
		13.2.2	SOME personeli işe alım sürecinden önce güvenlik soruşturmasının yapılması (adli sicil kaydı, şahıs güvenlik belgesi v.b.)			
		13.2.3	Some'de görev alan 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			
	3	13.3.1	SOME biriminin en az Genel Müdür Yrd. seviyesine bağlanması			
	4	13.4.1	SOME'nin BT birim ve süreçlerinden görevlerin ayrılığı ilkesi kapsamında ayrılması			
		13.4.2	Görevlendirilecek personelin some kapsamındaki görev ve sorumluluklarını yerine getirebilmesi için sorumlu olduğu konuda uzman olması			
14. İş Sürekliliği	1	14.1.1	BT varlıklarının iş sürekliliğine yönelik bir politika veya prosedürün oluşturulması			
	2	14.2.1	BT varlıklarına yönelik iş sürekliliği etki analizinin yapılması			
	4	14.4.1	İş sürekliliği risk ve etki analizinin periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
		14.4.2	İş sürekliliği planlarının oluşturulması, gözden geçirilmesi ve güncel tutulması			
		14.4.3	İş sürekliliği çalışmalarının, görevler ayrılığı ilkeside gözetilerek, objektif bir şekilde değerlendirilmesi			
15. Tedarikçi Yönetimi	1	15.1.1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması			
	2	15.2.1	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi			
	3	15.3.1	Tedarik ihtiyacı olan süreçle ilgili tedarikçi bilgi güvenliği gereksinim seviyelerinin belirlenmesi			
	4	15.4.1	Tedarikçi yönetim sürecinin değerlendirilmesi ve iyileştirilmesi			
		15.4.2	Kritik tedarikçilerin sözleşmelerinde bilgi güvenliği unsurlarının yer alması			

		15.4.3	Kritik tedarikçilerin bilgi güvenliği kapsamında denetlenmesi			
16. Yasal Uyum	**1**	***16.1.1***	İşletmenin ISO 27001 Sertifika belgesine sahip olması			
	3	***16.3.1***	ISO 27001 Ek.A.18.2.1 kapsamında yasal uyum süreci envanterinin oluşturulması			
	4	***16.4.1***	İşletmenin yasal sorumluluğunun olduğu alanlarda yeni çıkan regülasyonlar ile ilgili takip mekanizması oluşturması			
17. İşletim Güvenliği	**1**	***17.1.1***	Lisanssız yazılımların kullanılmaması			
	2	***17.2.1***	Yama yönetiminin uygulanması			
	3	***17.3.1***	Değişiklik yönetiminin uygulanması			
		17.3.2	Kapasite yönetiminin uygulanması			
	4	***17.4.1***	Kullanıcının yükleme izni olan uygulamalar için whitelist ve blacklist uygulanması ve sürecin izlenmesi			
18. Sistem Temini, Geliştirme ve Bakım	**1**	***18.1.1***	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması			
	2	***18.2.1***	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla analizin yapılması ve siber güvenlik gereksinimlerinin belirlenmesi			
	3	***18.3.1***	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi			
		18.3.2	İç veya dış kaynaklı sistem temini, geliştirme veya güncelleme süreçlerinde değişiklik yönetimi süreçlerinin etkin bir şekilde yürütülmesi			
		18.3.3	Test ve geliştirme ortamlarının ayrıştırılması			
		18.3.4	Test verisinin kişisel veri veya operasyonel kritik veri içermemesi			
	4	***18.4.1***	Temin edilecek, geliştirilecek veya güncellenecek sistemlerin güvenliğini sağlamak amacıyla SHT-Siber Ek-10'da yer alan Havacılık Sektörü Güvenli Yazılım Yazılım Geliştirme Rehberi içerisinde bulunan kontrol listesinin kullanılması ve bu sürecin SOME tarafından denetlenmesi			
19. Yerli Milli Ürün Kullanılması	**3**	***19.3.1***	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den az olması			
	4	***19.4.1***	Yerli ve milli ürünlerin işletme BT ürün envanterindeki oranının %5'den fazla ve %10'dan az olması			
	1	***20.1.1***	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

20. İletişim	**2**	***20.2.1***	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	3	***20.3.1***	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	4	***20.4.1***	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

U: Uygun
UD:Uygun Değil
NA:Uygulanamaz

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI
SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

3. GRUP HAVACILIK SEKTÖRÜ İŞLETMELERİ

HAVACILIK GÜVENLİĞİ DAİRE BAŞKANLIĞI-SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

Sıra	Kontrol Maddesi	Seviye 1	Seviye 2	Seviye 3	Seviye 4	Toplam
1	Erişim Yönetimi	0	1	1	2	4
2	Varlık Yönetimi	0	0	1	1	2
3	İz Kayıt	1	1	1	1	4
4	Farkındalık	1	0	1	2	4
5	Olay Yönetimi	0	1	0	1	2
6	Bakım	2	0	0	1	3
7	İnsan Kaynakları Güvenliği	1	2	2	1	6
8	Fiziksel Güvenlik	0	1	0	1	2
9	Yedekleme	0	0	1	1	2
10	Risk Yönetimi	0	0	3	1	4
11	Durumsal Farkındalık ve Sistem Test	0	0	2	3	5
12	Sistem ve Haberleşme Güvenliği	1	2	7	3	13
13	Siber Güvenlik Yapılanması	0	1	0	0	1
14	İş Sürekliliği	0	0	0	0	0
15	Tedarikçi Yönetimi	0	0	1	1	2
16	Yasal Uyum	0	0	0	1	1
17	İşletim Güvenliği	1	0	0	0	1
18	Sistem Temini, Geliştirme ve Bakım	0	1	0	1	2
19	Yerli Milli Ürün Kullanıması	0	0	0	0	0
20	İletişim	1	1	1	1	4

Seviye Toplam	8	11	21	22	62

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	1. Erişim Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Erişim Yönetimi Kontrol Prosedürünün Oluşturulması	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi
2				Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	2. Varlık Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Varlık yönetimi prosedürünün hazırlanması	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	3. İz Kayıt			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	NTP server kullanılması	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	4. Farkındalık			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması		Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümante edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi
2				İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	5. Olay Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Siber güvenlik ihlal olay yönetim ve müdehale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması		Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	6. Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümante edilmesi, izlenmesi ve bu sürelere uygun olarak bakım çalışmalarının gerçekleştirilmesi
2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	7. İnsan Kaynakları Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümante edilmesi ve uygulanması
2		İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi	

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	8. Fiziksel Güvenlik			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi		Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması

No	9. Yedekleme			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			İşletmenin süreç kritikliğinide göz önüne alarak bir yedekleme politika veya prosedürü oluşturması	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	10. Risk Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi
2			Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi	
3			Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi	

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	11. Durumsal Farkındalık ve Sistem Test			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması
2			Periyodik zafiyet taraması yapılması	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması
3				TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi

No	12. Sistem ve Haberleşme Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Mobil cihazlar, sunucular ve son kullanılara ait BT varlıklarında antivirüs yazılımı kullanılması	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması	Birim bazında ağ segmentasyonunun yapılması
2		Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması
3			İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması
4			DNS filtreleme çalışmasının gerçekleştirilmesi	
5			URL filtreleme çalışmasının gerçekleştirilmesi	
6			İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi	
7			Network trafiğinde şüpheli hareket analizinin yapılması	

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	13. Siber Güvenlik Yapılanması			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		İşletmenin siber güvenliğini sağlamak için en az 1 adet görevlendirilmiş uzman personelin olması		

14. İş Sürekliliği			
Seviye 1	**Seviye 2**	**Seviye 3**	**Seviye 4**
Kontrol maddesi ile alakalı bu grup işletmeler için alınması gereken tedbir yoktur.			

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	15. Tedarikçi Yönetimi			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1			Tedarikçi yönetimi politikası veya prosedürünün oluşturulması	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi

No	16. Yasal Uyum			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1				İşletmenin ISO 27001 Sertifika belgesine sahip olması

SİVİL HAVACILIK
GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	17. İşletim Güvenliği			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Lisanssız yazılımların kullanılmaması			

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	18. Sistem Temini, Geliştirme ve Bakım			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1		Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması		Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi

19. Yerli Milli Ürün Kullanılması			
Seviye 1	**Seviye 2**	**Seviye 3**	**Seviye 4**
Kontrol maddesi ile alakalı bu grup işletmeler için alınması gereken tedbir yoktur.			

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ

Havacılık Sektörü İç Kontrol Metodolojisi
(3. Grup Havacılık İşletmeleri)

No	20. İletişim			
	Seviye 1	Seviye 2	Seviye 3	Seviye 4
1	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi

Havacılık Sektörü İç Kontrol Metodolojisi 3. Grup Havacılık Sektörü İşletmeleri Kontrol Listesi						
Kontrol Başlığı	**Seviye**	**Kontrol No.**	**Kontrol Maddesi**	**U**	**UD**	**NA**
1. Erişim Yönetimi	2	*1.2.1*	Erişim Yönetimi Kontrol Prosedürünün Oluşturulması			
	3	*1.3.1*	Son kullanıcılara verilecek yetkilerin en az yetki prensibine göre verilmesi			
	4	*1.4.1*	Ayrıcalıklı erişim hakkının belirlenmesi ve yönetilmesi			
		1.4.2	Son kullanıcı erişim haklarının ilgili birim yöneticileri ile gözden gözden geçirilmesi			
2. Varlık Yönetimi	3	*2.3.1*	Varlık yönetimi prosedürünün hazırlanması			
	4	*2.4.1*	İşletme BT varlıklarının ve varlık gruplarının gizlilik,bütünlük ve erişilebilirlik kapsamında değerlerinin alan uzmanları ile birlikte belirlenmesi			
3. İz Kayıt	1	*3.1.1*	NTP server kullanılması			
	2	*3.2.1*	İz kayıt alınması gereken varlıkların belirlenmesi ve söz konusu bu varlıklardan toplanacak iz kayıt niteliğinin tespit edilip dokümante edilmesi			
	3	*3.3.1*	Belirlenen varlıklardan ihtiyaç duyulan iz kayıtlarının alınması			
	4	*3.4.1*	Olası bir siber güvenlik olayına karşı iz kayıtlarının korale edilerek, istenmeyen durumların tespiti için bir süreç oluşturulması			
4. Farkındalık	1	*4.1.1*	İşletme personellerine etkin bir siber güvenlik farkındalığı eğitiminin sağlanması			
	3	*4.3.1*	Son kullanıcıların siber olay yönetimindeki rollerinin açık bir şekilde dokümante edilmesi ve son kullanıcıların bu süreçteki rollerinin içselleştirilmesi			
	4	*4.4.1*	İşletme tarafından hazırlanan siber güvenlik eğitim materyallerinin periyodik olarak gözden geçirilmesi ve ihtiyaçlar ve güncel siber tehditler kapsamında güncellenmesi			
		4.4.2	İşletme personeline en az senede bir siber güvenlik farkındalığı tazeleme eğitimi verilmesi			
5. Olay Yönetimi	2	*5.2.1*	Siber güvenlik ihlal olay yönetim ve müdehale süreçlerini kapsayacak politika veya prosedürlerin oluşturulması			
	4	*5.4.1*	Son kullanıcılar ve ilgili paydaşların kullanımına sunulmuş bir siber olay raporlama mekanizmasının oluşturulması			
6. Bakım	1	*6.1.1*	Bakım amacıyla işletme dışına çıkarılacak sistemlerin içerisinde hiçbir data barındırmamasının sağlanması			
		6.1.2	BT ve OT süreçlerini etkileyecek varlıkların bakımlarının yetkili işletmeler tarafından görevlendirilen yetkili personel tarafından yapılması			

	4	6.4.1	BT süreçlerini etkileyecek varlıkların bakım sürelerinin dokümante edilmesi, izlenmesi ve bu sürelere uygun olarak bakım çalışmalarının gerçekleştirilmesi			
7. İnsan Kaynakları Güvenliği	1	7.1.1	İşletme kritik BT varlıklarına erişim sağlayacak personelin işe alım sürecinden önce güvenlik soruşturmalarının yapılması			
	2	7.2.1	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik mekanizmanın oluşturulması			
		7.2.2	İş sonlandırma süreçlerinde ilgili personelin yetki ve hesap iptaline yönelik oluşturulan mekanizmanın uygulanmasının denetlenmesi			
	3	7.3.1	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmanın oluşturulması			
		7.3.2	Görev değişikliği süreçlerinde ilgili personelin eski görevine yönelik yetki ve hesap iptali mekanizmasının denetlenmesi			
	4	7.4.1	İşletme siber güvenlik politika ve prosedürleri ile belirlenmiş kural setlerine uyulmaması durumunda uygulanmak üzere bir disiplin sürecinin oluşturulması, dokümante edilmesi ve uygulanması			
8. Fiziksel Güvenlik	2	8.2.1	Fiziksel güvenlik prosedürünün oluşturulması, periyodik olarak gözden geçirilmesi ve ihtiyaç duyulması halinde güncellenmesi			
	4	8.4.1	Kritik BT varlıklarının bulunduğu alanlarda, yaka kartı takılmasının zorunlu olması ve kritik BT varlıklarına erişimde kişi yaka kartı eşleştirmesinin yapılması			
9. Yedekleme	3	9.3.1	İşletmenin süreç kritikliğinide göz önüne alarak bir yedekleme politika veya prosedürü oluşturması			
	4	9.4.1	İşletme yedekleme politika ve prosedürüne uygun şekilde düzenli olarak backup alınması			
10. Risk Yönetimi	3	10.3.1	Siber Güvenlik Risk Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi			
		10.3.2	Siber Güvenlik Etki Değerlendirme Metodolojisinin belirlenmesi, dokümante edilmesi			
		10.3.3	Siber güvenlik risk değerlendirme çalışmasının periyodik olarak gözden geçirilmesi ve güncellenmesi			
	4	10.4.1	Siber güvenlik risk değerlendirme faaliyetlerinin yeterliliğinin ölçülmesi ve iyileştirilmesi			
11. Durumsal Farkındalık ve Sistem Test	3	11.3.1	Mevcut güvenlik mimarisinin güncelliğinin ve işletme ihtiyaçlarını karşılayıp karşılamadığının değerlendirmesinin yapılması			
		11.3.2	Periyodik zafiyet taraması yapılması			
	4	11.4.1	Mesai saatleri içerisinde siber tehdit veya siber güvenlik ihlal olayı tespit görevini icra edecek bir mekanizmanın kurulması			
		11.4.2	Mesai saatleri içerisinde siber olay müdahale görevini icra edecek bir mekanizma kurulması			
		11.4.3	TSE akredite firmalar tarafından en az senede bir geniş kapsamlı sızma testi faaliyetinin gerçekleştirilmesi			

12. Sistem ve Haberleşme Güvenliği	1	12.1.1	Mobil cihazlar, sunucular ve son kullanılara ait BT varlıklarında antivirüs yazılımı kullanılması			
	2	12.2.1	İşletme iç ağında internete çıkış noktasına yerleştirilmiş bir güvenlik duvarı cihazının bulunması			
		12.2.2	Network cihazlarının fiziksel güvenliğinin sağlanarak yetkisiz erişiminin engellenmesi			
	3	12.3.1	Genel Müdürlük ve taşra teşkilatı bazında ağ segmentasyonun yapılması			
		12.3.2	Mac filtreleme metodu ile kayıtdışı cihazların işletme iç ağına erişiminin engellenmesi			
		12.3.3	İnaktif oturumların belirli bir süre sonrasında otomatik kilitlenmesi			
		12.3.4	DNS filtreleme çalışmasının gerçekleştirilmesi			
		12.3.5	URL filtreleme çalışmasının gerçekleştirilmesi			
		12.3.6	İşletme BT sistemleri ile ilgili konfigürasyon envanterlerinin ve temel konfigürasyon setlerinin oluşturulması ve dokümante edilmesi			
		12.3.7	Network trafiğinde şüpheli hareket analizinin yapılması			
	4	12.4.1	Birim bazında ağ segmentasyonunun yapılması			
		12.4.2	Port, protokol ve servis kısıtlamasının minimum yetki prensibine uygun olarak uygulanması			
		12.4.3	Eposta hizmetlerinin güvenliğini sağlamak üzere spam koruma ve email gateway kullanılması			
13. Siber Güvenlik Yapılanması	2	13.2.1	İşletmenin siber güvenliğini sağlamak için en az 1 adet görevlendirilmiş uzman personelin olması			
15. Tedarikçi Yönetimi	3	15.3.1	Tedarikçi yönetimi politikası veya prosedürünün oluşturulması			
	4	15.4.1	Dış kaynaklı olarak alınan hizmet ve ürünlerin işletmeye olan etkisine göre kritik tedarikçilerinin belirlenmesi			
16. Yasal Uyum	4	16.4.1	İşletmenin ISO 27001 Sertifika belgesine sahip olması			
17. İşletim Güvenliği	1	17.1.1	Lisanssız yazılımların kullanılmaması			
18. Sistem Temini, Geliştirme ve Bakım	2	18.2.1	Sistem temini geliştirme ve bakımı süreçlerini ele alan bir politika veya prosedürün oluşturulması			
	4	18.4.1	Geliştirilecek veya temin edilecek sistemin güvenliğini sağlamak amacıyla siber güvenlik test süreçlerinin gerçekleştirilmesi			

20. İletişim	**1**	***20.1.1***	Siber güvenlik yapılanması dahilinde sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	2	***20.2.1***	Tüm işletme kapsamında sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	3	***20.3.1***	Kritik BT varlıkları tedarikçi firmaları ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			
	4	***20.4.1***	İşletme siber güvenlik faaliyetlerini etkileyen tüm iç ve dış paydaşlar ile sağlıklı bir iletişim mekanizmasının oluşturulması ve yürütülmesi			

U: Uygun
UD:Uygun Değil
NA:Uygulanamaz

Ek-20.Trafik Işığı Protokolü

Trafik ışığı protokolü hassas bilgilerin uygun hedef kitle ile paylaşılmasını sağlamak amacı ile oluşturulmuş ve dünya çapında yaygın olarak kullanılan bir bilgi paylaşım metodolojisidir.

Bilgi paylaşımında bulunacak taraf paylaşımda bulunacağı belgenin görünür bir yerine sınıflandırmaya ilişkin rengi belirtir. Trafik ışığı protokolünde kırmızı, sarı, yeşil ve beyaz olmak üzere 4 renk vardır. Her renk sınıfı paylaşımı yapılacak belgeye ait paylaşım sınırlarını belirtir.

Renk	**Açıklama**
Kırmızı	Paylaşım yapılamaz, yalnızca paylaşılan taraflarla sınırlıdır.
Koyu Sarı	Sınırlı paylaşım yapılabilir, paylaşılan kişilerin bağlı bulundukları kuruluşlarıyla sınırlıdır.
Yeşil	Sınırlı paylaşım yapılabilir, belirli bir toplulukla sınırlıdır.
Beyaz	Paylaşım sınırı yoktur.

Ek-21.Bulgu Önem Seviyesi

Bulgu Seviyesi	Önem Seviyesi	Açıklama
4	Kritik	Faaliyetin yürütülmesini veya istenilen çıktı, ürün ya da hizmetin sunulmasını engelleyecek tüm bulgular bu grupta değerlendirilir. 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 bulgulardır.
3	Yüksek	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 bulgulardır.
2	Orta	Faaliyetin çıktılarının kalitesini etkileyen, yürütülmesinde gecikmelere ve sorunlara neden olabilecek bulgular bu grupta değerlendirilir.
1	Düşük	Faaliyetin genel işleyişini etkilemeyen ancak daha iyi bir hizmet sunulmasını engelleyebilecek bulgular bu grupta değerlendirilir.