
# SİBER GÜVENLİK OPERASYON MERKEZİ GEREKSİNİMLERİ

## UZMANLIK TEZİ

**HAZIRLAYAN: EMİNE ERÇAĞLAR**

**ANKARA-2017**


# SİBER GÜVENLİK OPERASYON MERKEZİ GEREKSİNİMLERİ

Tez Hazırlayanın Adı Soyadı: Emine ERÇAĞLAR
Tez Danışmanın Adı Soyadı: Mehmet Tamer ÇOBANOĞLU
Birim Amirinin Adı Soyadı: Ömer ALAN

Emine ERÇAĞLAR tarafından hazırlanan Siber Güvenlik Operasyon Merkezi Gereksinimleri adlı bu tezin Çevre ve Şehircilik Uzmanlık tezi olarak uygun olduğunu onaylarım.

Çevre ve Şehircilik Uzmanı, Mehmet Tamer, ÇOBANOĞLU
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Çevre ve Şehircilik Uzmanlık tezi olarak kabul edilmiştir.

Başkan : Genel Müdür V., Ömer, ALAN

Üye : Genel Müdür Yrd. V., M. Yavuz, TORUN

Üye : Daire Başkanı V., Bircan, TÜRKMENOĞLU

Üye : Daire Başkanı V., İskender, ERMİŞ

Üye : Çevre ve Şehircilik Uzmanı, M. Tamer, ÇOBANOĞLU

Bu tez, Çevre ve Şehircilik Uzmanlığı Tez Hazırlama Yönergesi'ne uygundur.

# İÇİNDEKİLER

# ÖZET


| ÇEVRE ve ŞEHİRCİLİK BAKANLIĞI | |
|---|---|
| Tezin Adı | Siber Güvenlik Operasyon Merkezi Gereksinimleri |
| Türü | Çevre ve Şehircilik Bakanlığı Uzmanlık Tezi |
| Yazar | Emine ERÇAĞLAR |
| Teslim Tarihi | 24.08.2017 |
| Anahtar Kelimeler | Bilgi, BGYS, Siber Güvenlik, SGOM |
| Tez Danışmanı | Mehmet Tamer ÇOBANOĞLU |
| Sayfa Adedi | 96 |

Bilginin önemi ve bilginin güvenliği kavramları son yıllarda giderek daha fazla önem kazanmaktadır. Günümüzde daha fazla bilgi temelli yaşam süren ve elektronik ortamda daha fazla bilgi kullanan insanoğlu, bilginin güvenliği için daha fazla çalışma yürütmektedir. Bu çerçevede, Bilgi Güvenliği Yönetim Sistemleri gündeme gelmektedir.

Buna ek olarak elektronik ortamda bilgi paylaşımının artması ile birlikte yaşanan bilgi güvenliği sorunları ve siber saldırılar nedeniyle siber güvenlik çalışmalarının önemini de artmıştır. Bu noktada özellikle de birçok kullanıcının bilgileri ile çalışmalar yürütürken kurum ve kuruluşların çeşitli siber güvenlik çalışmalarına ağırlık vermeleri gerekmektedir.

Bu çerçevede son yıllarda Ülkemizde de önemli mevzuat çalışmaları ve faaliyetler yürütülmektedir. Bu çalışmalar kapsamında Siber Güvenlik Operasyon Merkezlerinin kurulması ve yönetimi çalışmaları önemli bir adım olarak karşımıza çıkmaktadır.

Bu çalışma kapsamında Bilgi Güvenliği, Siber Güvenlik ve SGOM gibi temel kavramlar ile bu kapsamda yapılan ve yapılması gereken çalışmalar, değerlendirmeler ve öneriler belirtilecektir.

# ABSTRACT


| MINISTRY OF ENVIRONMENT AND URBANIZATION | |
|---|---|
| Thesis | Cyber Security Operation Center Requirements |
| Type | Ministry of Environment and Urbanization Expertise Thesis |
| Author | Emine ERÇAĞLAR |
| Submission Date | 24.08.2017 |
| Key Words | Information, Information Security Management System, Cybersecurity, Cyber Security Operation Center |
| Advisor | Mehmet Tamer ÇOBANOĞLU |
| Total Page | 96 |

Abstract

The importance of knowledge and the security of information have become increasingly important in recent years. Nowadays, as human beings use more information-based living and use more information in the digital environment, there is a need for further work on the security of information. In this context, information Security Management Systems are on the agenda.

In addition, studies on cyber security have become more and more common due to information security problems and cyber-attacks, which have been accompanied by increased information sharing in the digital environment. At this point, especially when working with the knowledge of many users, institutions and organizations need to focus on various cyber security studies.

In this framework, important legislation studies and activities are being carried out in our country in recent years about cyber security. As a part of these efforts, the establishment and management of Cyber Security Operations Centers is being carried out as one of the important step.

In this study, basic concepts such as Information Security, Cyber Security and SGOM will be mentioned and the studies, evaluations and suggestions are discussed.

# TEŞEKKÜR

Tez çalışması boyunca desteğini esirgemeyen başta Eşime, Aileme, Birim Amirlerime, yardım ve katkılarıyla beni yönlendiren tez danışmanıma ve çalışmaların süresince bana destek olan tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim.

Emine ERÇAĞLAR

# TABLO LİSTESİ

# ŞEKİL LİSTESİ

# KISALTMALAR

| | |
|---|---|
| ABD | : Amerika Birleşik Devletleri |
| API | : Uygulama Programlama Ara yüzü |
| BGYS | : Bilgi Güvenliği Yönetimi Sistemi |
| BSI | : İngiliz Standartları Enstitüsü |
| CBSGM | : Coğrafi Bilgi Sistemleri Genel Müdürlüğü |
| COBIT | : Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri |
| ÇŞB | : Çevre ve Şehircilik Bakanlığı |
| DDOS | : Dağınık Hizmet Engelleme Saldırısı |
| IDS | : Saldırı Tespit Sistemi |
| IP | : İnternet Protokol |
| IPS | : Saldırı Önleme Sistemi |
| IIS | : İnternet Bilgi Servisleri |
| IoT | : Nesnelerin İnterneti |
| ISO | : Uluslararası Standartlar Komitesi |
| NATO | : Kuzey Atlantik Antlaşması Örgütü |
| NIST | : Ulusal Standartlar ve Teknoloji Enstitüsü |
| OWASP | : Açık Web Uygulama Güvenliği Projesi |
| SGOM | : Siber Güvenlik Operasyon Merkezi |
| SIEM | : Olay İzleme ve Yönetim Sistemi |
| SNMP | : Basit Ağ Yönetim Protokolü |
| SOME | : Sektörel ve Kurumsal Siber Olaylara Müdahale Ekipleri |
| SSCB | : Sovyet Sosyalist Cumhuriyetler Birliği |
| TSE | : Türk Standartları Enstitüsü |
| TÜBİTAK | : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| UEKAE | : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü |
| USOM | : Ulusal Siber Olaylara Müdahale Merkezi |
| WAF | : Web Uygulama Güvenlik Duvarı |

# GİRİŞ

İnsanoğlu bugüne kadar dünya üzerinde geçirmiş olduğu tarihsel süreç boyunca üç önemli toplum anlayışı benimsemiştir. Bunlar beslenme ihtiyaçlarını sağlamak için tarım toplumu, ihtiyaçlarını daha hızlı ve kolay bir şekilde gerçekleştirebilme amacıyla sanayi toplumu ve son olarak teknolojinin ve gelişmelerin gerektirdikleri çerçevesinde de bilgi toplumu anlayışıdır.

Bilgi toplumu; temelinde bilginin var olduğu, teknolojik gelişmelerle beraber bilginin sayısallaştırılarak kolaylıkla iletilmesi, saklanması ve kullanılmasının mümkün olduğu bir toplum yapısıdır. Bu toplum yapısı ve teknolojik gelişmelerle birlikte insan yaşamı oldukça kolaylaşmıştır. Bankacılık işlemleri, fatura ödeme, başvuru işlemleri gibi birçok işlemin internet üzerinden gerçekleştirilebilmesi bu kolaylıklardan bazılarıdır.

Bu kolaylıkların yanında bilgi toplumunun getirdiği olumsuzluklar da mevcuttur. Bilginin ele geçirilmesi, bilginin yok edilmesi, sosyal mühendislik saldırılarıyla insanların kandırılması ve buna benzer birçok kötü niyetli eylemler bu olumsuzluklara örnek olarak verilebilir. Bu olumsuzlukların gerçekleşme ihtimallerini minimum seviyeye indirmek ya da olumsuzluğun farkında olarak, gerçekleştiğinde normale dönebilmek adına planlar hazırlamak için bilgi güvenliğini sağlamak gerekmektedir.

Bilgi güvenliği; bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumaktır. Kuruluşların itibar kaybı yaşamaması, maddi zararlara maruz kalmaması gibi önem arz eden olaylar yaşama ihtimalini minimum seviyede tutmak için bilgi güvenliğinin sağlanması gerekmektedir. Bilgi güvenliğini gerçekleştirebilmek için Bilgi Güvenliği Yönetimi Sistemi (BGYS) kurulmalı ve sürdürülmelidir.

BGYS başarıyla kurulduktan sonra siber güvenlik aşamasının ele alınması gerekmektedir. Bu gerekliliğin kaynağı ise, çoğu faaliyetlerin siber uzaya dâhil olarak gerçekleştirilmesidir. Siber güvenlik aşamasının neden uygulanması gerektiğinin daha iyi anlaşılması için birkaç örnek vermek gerekirse;

- Yahoo gibi milyonlarca kullanıcısı olan sosyal medya hesap bilgilerinin çalınması,
- Meksika'da yaşanan 87 milyon seçmenin verilerinin internet ortamında yayınlanması,
- Dropbox kullanıcı bilgilerinin internette yayınlanması,

gibi olaylar verilebilir.

Siber güvenlik genel anlamda, siber ortamdaki siber tehditlere karşı alınan güvenlik önlemleridir. Özellikle kuruluşların sahip olduğu kritik alt yapılar vasıtasıyla sundukları hizmetler ve bu uygulamalar için vatandaşlara ve tüzel kişilere ait bilgilerin kullanılması nedeniyle, bu kavramın önemi hızla artmıştır. Bu çerçevede, bilgilerin korunması, kuruluşların ve Türkiye'nin itibar ve güvenilirliğinin olumsuz şekilde etkilenmemesi için Siber Güvenlik konusunda gerekli işlemlerin yürütülmesi gerekmektedir.

Bu çalışma kapsamında, Mevzuat ve güncel Bakanlık çalışmaları ile bu alanda çalışmalar yürüten kurum ve kuruluş çalışmaları incelenmiştir. Buna ek olarak, güncel makaleler, bilimsel çalışmalar ve yayınlar incelenerek, çalışma tamamlanmıştır.

Bu çalışmamın birinci bölümde, bilgi ve bilgi güvenliği konusunda günümüze kadar ne gelişmeler yaşandığı, bilgi güvenliği ve kavramlarının açıklamaları ve BGYS'yi kuruluşlarda kurmak için nasıl bir yol izlenmesi gerektiği anlatılacaktır.

İkinci bölümde siber güvenlik kavramları tanımlanacak, geçmişten günümüze yaşanmış siber saldırılardan örnekler anlatılarak, Türkiye'nin siber güvenlik konusunda ne durumda olduğu ve bu konuda yaptığı çalışmalar hakkında bilgiler verilecektir.

Üçüncü bölümde ise siber güvenlik operasyon merkezinin (SGOM) ne olduğundan, kuruluşlarda neden kurulması gerektiğinden ve kurulması için yapılması gereken çalışmalardan bahsedilecek, Bakanlığımız SGOM kurulumu ile ilgili bilgiler verilecek ve ziyaret edilen kurumların SGOM yapısına değinilecektir.

Çalışmanın son bölümünde ise genel olarak açıklanan kavramların değerlendirmesinin yanında temel olarak Siber Güvenlik konusunda ülkemizin ve Bakanlığımızın yürüttüğü birçok önemli çalışmanın daha güvenli ve sağlıklı bir şekilde yürütülebilmesi için önemli bir adım olan Siber Güvenlik Operasyon Merkezinin (SGOM) kurulması ve daha etkin olarak çalıştırılabilmesi için neler yapılması gerektiği ve SGOM'un başarılı şekilde yönetilebilmesi için değerlendirmeler ve öneriler paylaşılacaktır.

# I. BİLGİ GÜVENLİĞİ KAVRAMI

## I.1 Bilgi Güvenliğinin Ortaya Çıkışı

İnsanlar varoluşlarından itibaren çeşitli toplum süreçlerinde yaşamışlar ve her dönemde bilgi, insanın hayatında yer alan barınma, yeme, içme gibi doğal bir ihtiyaç olmuştur.

Bu noktada doğal olarak bilgi güvenliği de insanların temel sorunlarından biri olmuştur. Bunun en güzel örneği, geçmişte yaşamış olan Julius Caesar'ın iletmek istediği mesajları o günün şartlarıyla hala kendi adı ile anılan *Caesar Şifrelemesi* ile şifreleyerek göndermesidir.

Bilgi güvenliği ve bilginin güvenliği ihlali konusunda bakacağımız ikinci örnek ise, Enigma Şifreleme Sisteminin kırılmasıdır.

Savaş sırasında şifreli haberleşme için Almanya tarafından kullanılan Enigma, bilginin şifrelenmesi ve şifrenin çözülmesi işlemlerini yapan ve bulunulan zaman dilimine göre kırılması nerede ise imkânsıza yakın bir sistemdi. Buna rağmen, İkinci Dünya Savaşı sırasında birkaç matematikçi tarafından kırılmış ve Almanların savaşı kaybetmesinde büyük rol oynamıştır.

Son yıllarda buna benzer birçok olay yaşandı. Teknolojinin gelişmesiyle birlikte bu olayların sayısı her geçen gün arttı ve kapsamı hızla büyüdü. Bunun en önemli nedenini, insanların bilgi toplumu yapısına geçmesi ve bilgiye sahip olan toplumların diğerleri karşısında daha güçlü hale gelmesi olarak ifade edebiliriz. Bilgi teknolojilerinde ileri ülkelerin daha büyük ekonomik güce sahip olduğunu örnek olarak verebiliriz.

Bilgi toplumuna geçişle birlikte bilgi, sayısallaştırılarak istenilen her yere rahatlıkla taşınma, sınır tanımadan istendiği her kişiye iletilme, defalarca çoğaltılabilme özelliklerini kazandı. Bu yapı da bilgi ve bilgi güvenliği kavramlarının önemini hızla arttırdı ve bu konuda kapsamlı çalışmaların yapılmasına olan ihtiyacı ortaya çıkardı.

Bu kapsamda yapılan çalışmaların ilki, İngiltere'de gündeme gelmiştir. 1990'lı yıllarda İngiltere'de bazı sanayi kuruluşlarının talepleri doğrultusunda, İngiliz Standartları Enstitüsü (BSI) tarafından Bilgi Güvenliği Standartları oluşturulması çalışmaları başlatılmış ve *BS7799* adlı standart 1995 yılında hazırlanarak, yayımlanmıştır. Bu standart daha sonra iki kısma ayrılarak, birinci kısım *BS7799-1:1999* ve ikinci kısım *BS7799-2:1998* olarak yayımlanmıştır.

Bu standardın birinci kısmı olan *BS7799-1:1999* Uluslararası Standartlar Komitesi (ISO) tarafından küçük düzeltme ve uyarlamalardan geçirilerek, kabul görmüş ve 2000 yılında *ISO/IEC 17799* olarak yayımlanmıştır.

Ülkemizde ise; *TSE ISO/IEC 17799*, 2002 yılında kabul edilerek piyasaya sunulmuştur. 2005 yılında *BS7799-2* standardının üzerine eklemeler ve düzeltmeler yapılmış ve dünyaca kabul görmüş olan *ISO/IEC 27001* standardı adıyla yayımlanmıştır.

2006 yılında Türk Standartları Enstitüsünün (TSE) *BS7799-2* standardını iptal etmesi üzerine *TS ISO/IEC 27001:2006* kabul görmüş ve "*TS ISO/IEC 27001* Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimleri" adıyla yayımlanmıştır. 2006 yılında yayımlanan sürümün üzerinde eklemeler ve düzeltmeler yapılarak 2013 yılında yayımlanan ve son hali olan *ISO/IEC 27001: 2013* kullanıma sunulmuştur.

*ISO/IEC 27001*, bilgi güvenliğini kurmak ve yönetmek için uygulanması gereken ilkelerin yer aldığı yol gösterici bir kılavuzdur. Daha sonraki yıllarda TSE tarafından *ISO/IEC 2700*1'de yer alan ilkelerin daha detaylı açıklandığı *ISO/IEC 27002* Uygulama Kılavuzu yayımlanmıştır.

> Bilgi güvenliği ile ilgili diğer bir İngiliz standardı Aralık 2005'te BS7799–3: 2005 Bilgi Güvenliği Yönetim Sistemleri Risk Yönetiminin Kuralları ismiyle hazırlanmıştır. Standart 2006 yılında tekrar gözden geçirilmiş ve BS7799–3: 2006 ismiyle yayımlanmıştır. Bu standardın yayımlanma amacı, BS7799–2 standardının uygulanması için destek sağlayarak standardın yaygınlaşmasına yardımcı olmaktır (http://dergipark.gov.tr).

Şekil 1.1 : Bilgi Güvenliği Yönetim Standartları Tarihçesi


Kaynak: http://www.simet.com.tr/index.cfm?fuseaction=objects2.detail_content&cid=740

Bu kapsamda Şekil 1.1'de bilgi güvenliği konusunda ilk yapılan çalışmaların tarihsel gelişimi gösterilmiştir. 2005 yılından sonra oluşturulan standartların dışında, ülkelerde bilgi güvenliği konusunda çeşitli çalışmalar, toplantılar yapılmış ve bu konuda çalışan kurum, kuruluş ya da birimler kurulmuştur. Türkiye'de bu konuda gelişmeleri yakından takip ederek, önemli çalışmalar yürütmüştür.

## I.2. Temel Bilgiler

Bilgi güvenliği temel olarak bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasıdır. Bu üç kavramın yanı sıra bilgi güvenliği; hesap verilebilirlik, inkâr edememe, güvenilirlik kavramlarını da kapsamaktadır. Bu kavramları daha iyi anlayabilmek için kısaca bahsetmek gerekirse;

*Gizlilik*, TS ISO/IEC 27000 standardına göre, bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğidir. Gizliliğin sağlanması için yetkisi olmayan üçüncü şahısların ağ dinleme gibi değişik yöntemlerle bilgiye erişiminin önlemesi gerekmektedir.

*Bütünlük*, TS ISO/IEC 27000 standardına göre varlıkların doğruluğunu ve tamlığını koruma özelliğidir. Bilgiye sahip olan kuruluşlar tarafından bilginin bütünlüğünü korumak için gerekli kişilere sorumluluklar tanımlanmaktadır.

*Erişilebilirlik*, TS ISO/IEC 27000 standardına göre yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir. Sistemlerin hizmet vermemesi sebebi

ile erişilebilirliğinin olmaması kullanıcılar tarafından olumsuz karşılanmaktadır. Bu da kuruluş için maddi kayıpların yanı sıra itibar kaybına da sebep olmaktadır.

Şekil 1.2: Bilgi Güvenliği Kavramları


Kaynak: https://www.cocc.edu/its/infosec/concepts/cia-triad/

*Hesap verilebilirlik*, bilgi güvenliği konusunda kişilere düşen sorumluklar çerçevesinde, herkesin sorumluluğunu bilmesi, yaptıkları ve yapmadıkları konusunda sorumlu olması olarak ifade edilmektedir.

> *İnkâr edememe*, bilgi alışverişinde gönderici ve alıcı olmak üzere iki taraf mevcutsa, iki tarafın karşılıklı olarak aldıklarını ve gönderdiklerini reddedememesidir. Diğer bir deyişle, herhangi bir iş ve işlemin gerçekleştirilmiş olduğunun ispatlanmasını ifade eder, hesap verilebilirlik ve izlenebilirlik kavramları ile ilişkilendirilebilir (https://www.btk.gov.tr).

*İzlenebilirlik*, bir sistemde yapılan veri tabanı tablosundan sorgulama, şifre ile sayfaya girme, veri transferi gerçekleştirme gibi bütün işlemlerin kayıt altına alınmasını ifade etmektedir. Bu kavram yapılan işlemlerin daha sonra kontrol edilebilmesi amacını taşımaktadır. Yapılan kontroller sonucu sistemde anormal davranışlar, hatalı giriş denemeleri gibi bir kayıt saptandığında bu olay hakkında yetkililerin uyarılması ve gerekli önlemlerin alınması hedeflenmektedir.

## I.3 Bilgi Güvenliği Yönetimi

Bilgi Güvenliği Yönetimi, kasıtlı/kasıtsız bilişim sisteminde bulunan çeşitli varlıkların sebep olduğu gizlilik, bütünlük ve erişilebilirlik ihlalleri için koruyucu, önleyici, düzeltici ve iyileştirici faaliyetlerin bütünüdür.

Bilgi Güvenliği Yönetimi sayesinde kuruluşun iş sürekliliğine katkıda bulunulması, kuruluş imajının bilgi güvenliği ihlali sebebi ile zedelenmesinin önlenmesi, bilgi güvenliği ihlali gerçekleşmesi halinde uygun yönetimin sağlanarak oluşabilecek zararı minimumda tutacak gerekli planların uygulanması sağlanabilecektir. Bu da kurum ve kuruluşlar için bilgi güvenliğinin sağlanmasının ne kadar önemli olduğunu belirtmektedir.

Bilgi güvenliğini sağlamak için TS/ISO IEC 27001 Bilgi Güvenliği Yönetim Sistemleri (BGYS), TS/ISO IEC 27002 Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri ve bu konuda uzman kuruluşların danışmanlığı referans alınarak BGYS'yi kurmak gerekmektedir.

BGYS kurmak için izlenecek süreçler sırasıyla açıklanırsa;

### I.3.1 Üst Yönetim Desteğinin Sağlanması

En temel ve kritik aşamadır. Bu aşama olmadan BGYS'nin kurulması ve sürdürülmesi mümkün değildir.

Bu aşamada üst yönetim tarafından aşağıdaki şartları;

- Kuruluşun amacına uygun,
- Bilgi güvenliği amaçlarını içeren veya bilgi güvenliği amaçlarını belirlemek için bir çerçeve sağlayan,
- Bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına dair bir taahhüt veren,
- Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi için bir taahhüt (TS ISO/IEC 27001:2013)

içeren bir bilgi güvenliği politikası oluşturulur.

Üst yönetim tarafından onaylanan bilgi güvenliği politikası yazılı hale getirilir ve kuruluştaki bütün çalışanlara duyurulur. Ayrıca üst yönetim, bilgi güvenliği ile ilgili roller

için sorumlulukları ve sorumlu kişileri belirleyerek gerekli çalışmaların yürütülmesini sağlamalıdır.

### I.3.2. BGYS Kapsamı Belirleme

BGYS kapsamı belirlenirken kuruluşun bilgi güvenliği konusundaki gelmek istedikleri aşama ve kuruluşun üst yönetiminin geleceğe yönelik hedefleri göz önüne alınır.

> BGYS kapsamını oluştururken; iş (aktiviteler), organizasyon (yönetimsel birimler), işin mekânı, varlıklar ve teknoloji karakteristikleri belirtilerek kapsam dışında kalacak olan her kontrolün sebepleri açıklanır. Hangi yönetimsel birimlerin ve aktivitelerin bilgi güvenliği yönetim kapsamı içerisinde yer alacağı belirtilir (Perendi, 2008, 6).

### I.3.3 BGYS Organizasyon Yapısının Oluşturulması ve Eğitimi

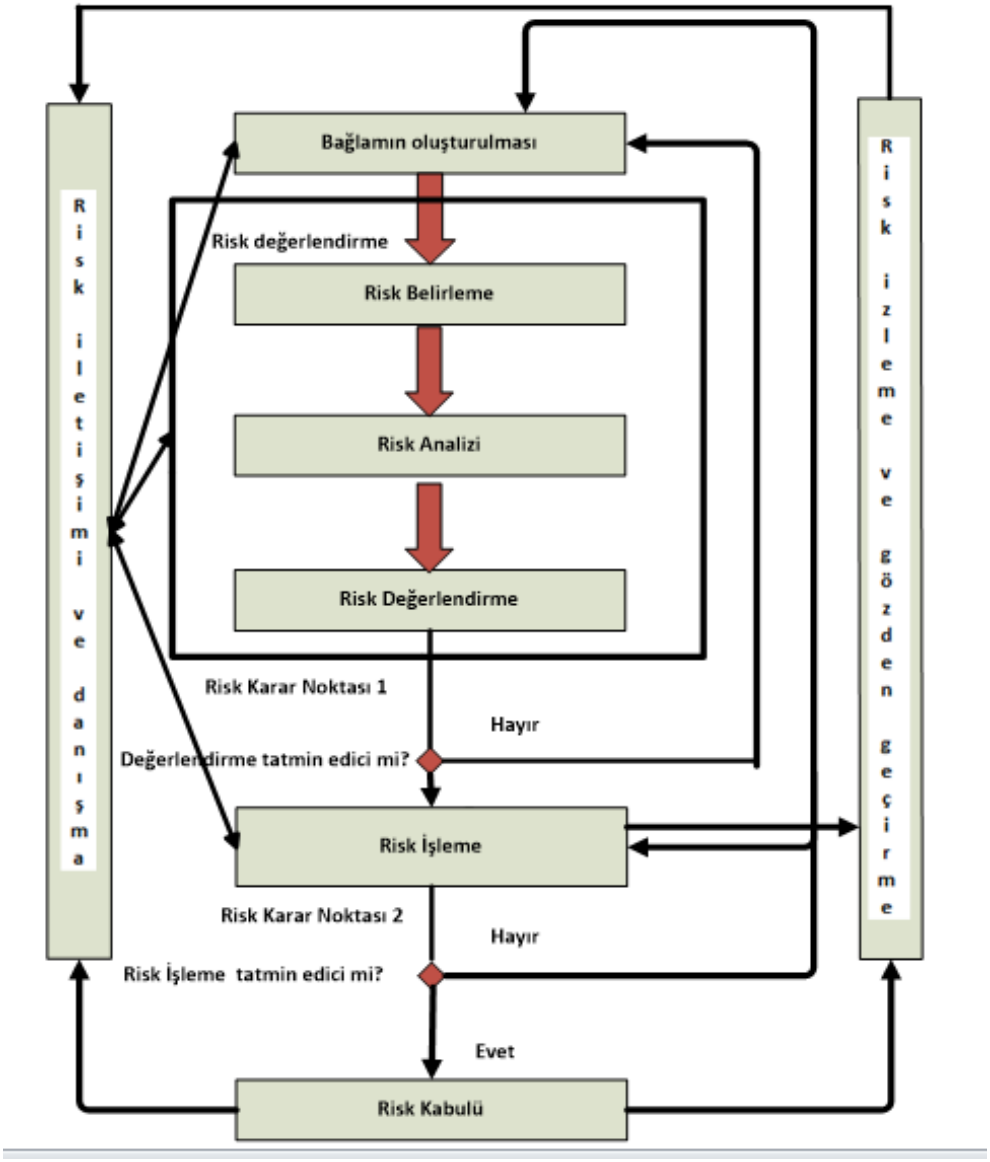
Kuruluş içerisinde BGYS'nin uygulanabilmesi ve sürdürülebilmesi için bir organizasyon yapısı kurulmalıdır. Bu yapıyı kurmak için, bilgi güvenliği sorumluları belirlenmeli, rol ve sorumlulukları atanmalıdır.

Rol ve sorumluluklar atanırken bilgi güvenliği politikaları ile uyumlu şekilde yapılmalıdır. Varlıkları korumak ve planlanan prosedürleri gerçekleştirmek için sorumluluklar açıkça tanımlanmalıdır.

### I.3.4 BGYS Risk Yönetim Süreci

Risk yönetim süreci birbirini takip eden süreçler olan bağlamın oluşturulması, risk belirleme, risk analizi, risk değerlendirme, risk işleme ve risk kabulü aşamalarından oluşur.

Şekil 1.3: Risk Yönetim Süreci




Kaynak: Çevre ve Şehircilik Bakanlığı (ÇŞB) Bilgi Güvenliği Risk Yönetimi Prosedürü

*Bağlamın oluşturulması***,** kuruluşun ve bilgi güvenliği yönetim sisteminin hedeflenen çıktılarını başarma kabiliyetini etkileyebilecek iç ve dış hususlar belirlenmelidir (ÇŞB Bilgi Güvenliği Risk Yönetimi Prosedürü).

*Risk belirleme işlemi*, varlıkların belirlenerek varlık envanteri oluşturulması aşaması ile başlar. Varlıklar belirlendikten sonra varlıkların zafiyetleri ve maruz kaldığı tehditler tespit edilir. Tehdidin gerçekleşmesi durumunda kuruluşun ne kadar zarar göreceği gizlilik,

bütünlük ve erişilebilirlik açısından değerlendirilir ve sonucunda oluşabilecek riskler ortaya çıkarılır.

*Risk analizi*, belirlenen sisteme yönelik risklerin gerçekleşmesi ihtimali gerçekçi bir şekilde değerlendirilir, ortaya çıkacak sonuçlar ve oluşacak risk seviyeleri belirlenir.

*Risk değerlendirme*, risk analizi sonuçlarının risk kriterleri ile karşılaştırılması ve analiz edilen risklerin risk işleme işlemi için önceliklendirilmesidir. Bu aşamada kabul edilebilir risk değeri belirlenir.

*Risk işleme*, risk değerlendirme sonucunda belirlenen kabul edilebilir risk değerine göre riskin indirgenmesi, riskin kabul edilmesi, riskin transferi veya riskten kaçınma şeklinde uygun kontroller seçilir.

### I.3.5. Yaygınlaştırma Faaliyetleri (Son Kullanıcı Farkındalık Eğitimleri)

Kurumsal bağlamda bilgi güvenliğini sağlamada en önemli faktör çalışanlar yani insanlardır. İnsanları bilinçlendirme, farkındalık oluşturma ve bilgilendirme konusunda nasıl bir süreç izleneceğini belirlemek için bu faaliyet oluşturulur.

Bu faaliyetler bilinçlendirme ve eğitim konularının seçilmesi, seçilen konular için materyallerin belirlenmesi, eğitim zamanlarının planlanması, verilen eğitimlerin değerlendirilmesi, değişen teknoloji ve kuruluş ihtiyaçları çerçevesinde güncellemelerin yapılması adımlarını içerir.

### I.3.6 Yazılı Bilgilerin Hazırlanması

Kuruluşun özel güvenlik ve iş amaçları göz önüne alınarak işlemlerin belli bir standartta ve uygun şekilde gerçekleştirilmesi amacıyla politika, süreç, prosedür, form, talimat gibi yazılı bilgilerin hazırlanmasıdır. Bu belgeler oluşturulduktan sonra mutlaka uygulanır, izlenir, gözden geçirilir ve iyileştirilir.

### I.3.7 Sistem Etkinliğini Ölçme

Sistem etkinliğini ölçme işleminin ne zaman ve ne sıklıkla yapılacağı, kimin tarafından gerçekleştirileceği, izleme ve ölçme sonuçlarının ne zaman analiz edilip değerlendirileceği ve kim tarafından analiz edilip değerlendirileceği konuları metrik değerlerle objektif olarak ölçülebilen ölçütlere göre belirlenir.

### I.3.8 İç Tetkik

Kuruluşun standardın şartlarını yerine getirdiğini, bilgi güvenliğinin etkin bir şekilde uygulandığı ve sürdürüldüğünü tespit etmek için planlanan aralıklarla gerçekleştirmesi gereken denetimler iç tetkik olarak adlandırılır.

Sıklıklar, yöntemler, sorumluluklar, gereksinim planları ve raporlama dâhil olmak üzere bir denetim programı planlanır, oluşturulur, uygulanır ve sürdürülür.

### I.3.9 Sürekli İyileştirme Faaliyetleri

TS/ISO IEC 27001 standardına göre kuruluşun, bilgi güvenliği yönetim sisteminin uygunluğunu, doğruluğunu ve etkinliğini sürekli olarak iyileştirmesi için bu adım yapılmalıdır.

Bu adımda ayrıca uygunsuzluk oluştuğunda alınması gereken düzeltici faaliyetlerde tespit edilir.

Kuruluş uygunsuzluk oluştuğunda şu faaliyetleri gerçekleştirir;

- Uygunsuzluğa tepki verilmesi ve mümkün olması durumunda
  - ✓ Kontrol edilmesi ve düzeltmek için eyleme geçilmesi ve
  - ✓ Sonuçları ile ilgilenilmesi,
- Aşağıdakilerin yerine getirilmesi yoluyla, uygunsuzluğun başka bir yerde tekrar etmemesi veya oluşmaması için nedenlerinin giderilmesi amacıyla eyleme geçme ihtiyacının değerlendirilmesi
  - ✓ Uygunsuzluğu gözden geçirerek,
  - ✓ Uygunsuzluğun nedenleri belirlenerek ve
  - ✓ Benzer uygunsuzlukların var olup olmadığını veya olasılıkla gerçekleşip gerçekleşmeyeceğini belirleyerek,
- Gerekli tüm faaliyetlerin uygulanması,
- Tüm düzeltici faaliyetlerin etkinliğinin gözden geçirilmesi ve
- Gerekli olan durumlarda bilgi güvenliği yönetim sisteminde değişikliklerin yapılması (TS ISO/IEC 27001:2013)

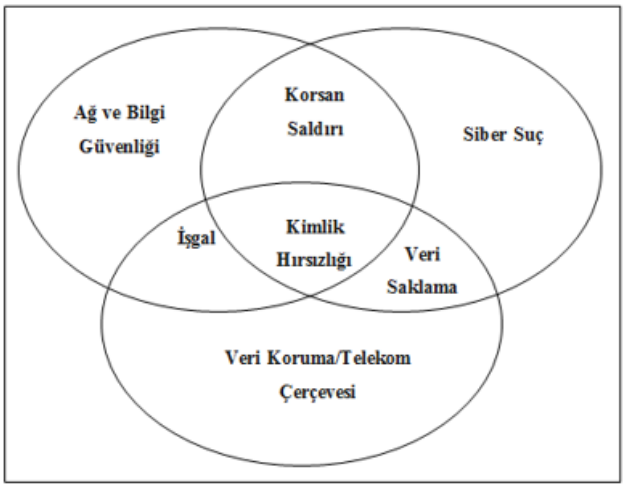
## I.4 BGYS Kapsamında Siber Güvenliğin Ele Alınması

Bilgi varlıklarının kasıtlı veya kasıtsız bir şekilde gizlilik, bütünlük ve erişilebilirliği unsurlarına bir zarar gelme ihtimaline karşı varlıkların korunmasıdır. Söz konusu bilgi varlıklarının, bilgisayar ve ağlarda kullanılması ağ güvenliği kavramını ortaya çıkarmıştır.

Ağ güvenliği; bir ağ üzerinde bulunan bilgisayarların haberleşmesi esnasında ağa ait yazılım ve donanımlara kötü niyetli insanlar tarafından yetkisiz erişim, ağ üzerinde alınan ve gönderilen verilerin değiştirilmesi, bozulması veya değiştirilmesine karşı alınan tedbirler olarak tanımlanmıştır.

Ağ güvenliği kritik alt yapılar, kişisel bilgisayarlar ve kurumsal bilgisayarlar olmak üzere birçok bilgi sisteminin korunmasını içermektedir. Ağın etkin bir şekilde kullanıldığı internet ortamının ortaya çıkması ve teknolojik gelişmelerle birlikte insan hayatında önemli bir yer alması ağ güvenliğini ön plana çıkarmış, bunun sonucunda bilgi güvenliğinden siber güvenlik kavramına geçilmiştir.

Şekil 1.4: Bilgi Güvenliği ve Siber Güvenlik




Kaynak: Avrupa Topluluğu Komisyonu, 2001

## I.5 Genel Değerlendirme

Teknolojik gelişmelerin ışığında bilgi, insan hayatında her geçen gün önemini arttırmaktadır. Bu nedenle varlıkların (*entity*) kasıtlı veya kasıtsız davranışları sonucu bilgileri

ihlal etme olasılığına karşı korunması gerekmektedir. Bilgi güvenliği kavramı, bu ihtiyaç sonunda çıkmıştır.

Bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak tanımlanmış olup, bunun sağlanması için kurum ve kuruluşlarda *TS/ISO IEC 27001, TS/ISO IEC 27002* gibi standartlar ve bu konuda faaliyetler yürüten uzman kuruluşların danışmanlık faaliyetlerinden yararlanılarak bilgi güvenliği yönetimi sisteminin kurulması ihtiyacı oluşmuştur.

Buna ek olarak da teknolojik gelişmelerle beraber internetin ortaya çıkması ve insan hayatında önemli bir yer alması sonucunda bilgilerin elektronik ortamda ve ağ üzerinde bilgisayarlar arasında iletilmesi, paylaşılması söz konusu olmuştur. Bilgi güvenliği kavramı bu konuda çok genel kalmış ve daha özel tedbirlerin alınması gerekliliği de yeni bir kavram olarak siber güvenlik kavramını ortaya çıkarmıştır.

# II. SİBER GÜVENLİK KAVRAMI VE SÜREÇLERİ

## II.1 Siber Güvenlik Kavramları

Siber güvenlik, elektronik ortamda gerçekleşen işlemler sırasında varlıkların bilinçsizliğinin sebep olduğu hatalardan veya kötü niyetli kişilerin saldırılarından kaynaklanan eylemler sonucunda zarar görmesini engellemek amacıyla alınan tedbirler şeklinde tanımlanır. Günümüzde önemi giderek artan bu kavramı daha iyi anlamak için siber uzay, siber saldırı ve siber güvenlik kavramlarının açıklanması faydalı olacaktır. Bu kapsamda;

### II.1.1. Siber Uzay

Siber uzay, dünyadaki insanların herhangi bir sınır tanımadan, bilgisayarlar ve telekomünikasyon sistemleri aracılılığıyla birbirleriyle iletişim halinde bulundukları elektronik ortam olarak tanımlanmıştır.

> Uluslararası Standartlar Örgütü ise siber uzayı, somut formda olmayan ağlar ve teknolojik cihazlardan oluşan İnternet üzerinde insanların yazılımların ve hizmetlerin birbirleriyle etkileşime girmesi sonucu ortaya çıkan karmaşık bir alan olarak tanımlamıştır. (Sarı, 2013, 15)

2016-2019 Ulusal Siber Güvenlik Stratejisinde ise Siber Uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı içermektedir.

Siber uzay başta internet olmak üzere uydu sistemleri, cep telefonları, ağ üzerinde birbirine bağlı bilgisayarlar, tabletler, elektromanyetik sistemler, robotlar, televizyonlar, yazılımlar ve donanımlar dâhil tüm bilgi sistemlerini kapsamaktadır.

Siber uzay ile beraber yer, mekân, sınır kavramları tamamen ortadan kalktığını belirtebilmekteyiz.

### II.1.2 Siber Saldırı

Siber saldırı; sistemler, yazılımlar ya da donanımlar üzerinde, bozma, değiştirme ya da çalışamaz hale getirme amaçlarıyla siber alanda uygulanan saldırılar olarak ifade edilir.

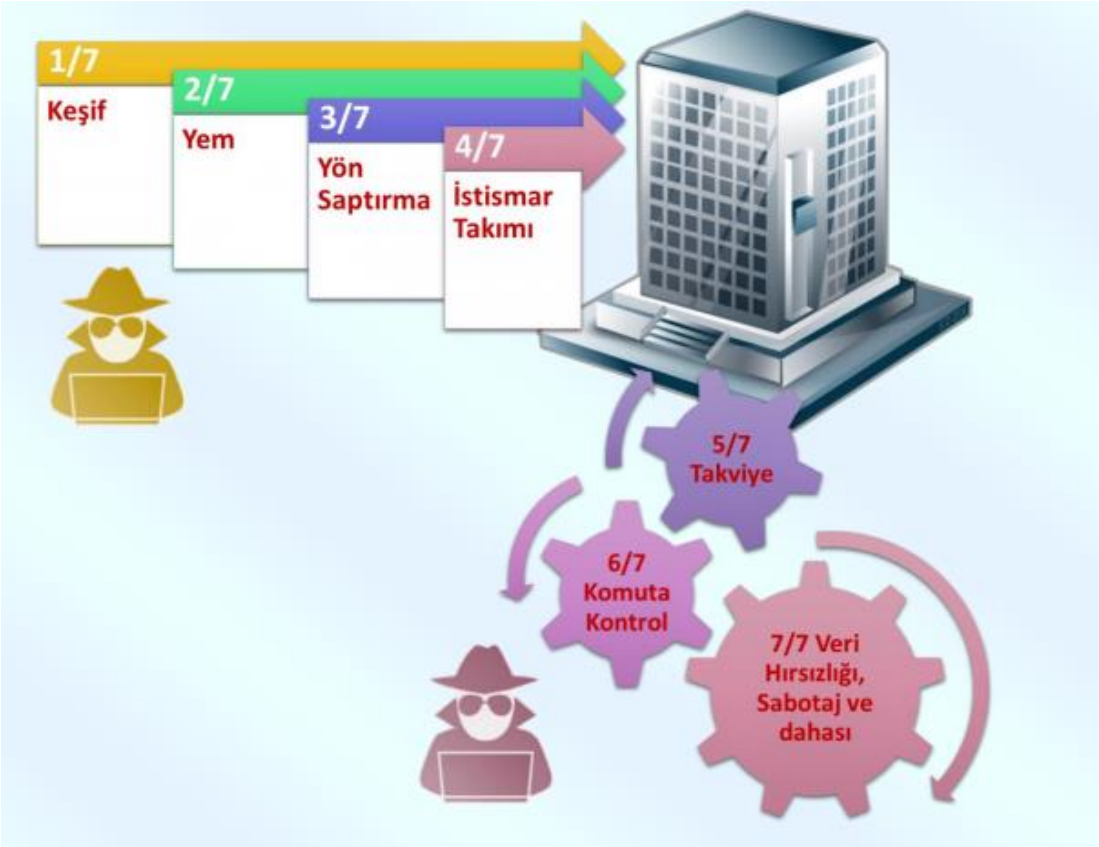
> Amerikan Ulusal Araştırma Meclisi, siber saldırıyı, bilgisayar sistemleri ile ağlarına yönelik veya bilgisayar sistemleri ile ağlarda iletilmekte olan veya içlerinde yer alan bilgi ve programlara yönelik kasten yapılan değiştirme, bozma, parçalara ayırma ve yok etme vb. fiilleri olarak tanımlamıştır (Sarı, 2013, 17).

Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından kurum ve kuruluşlarla işbirliği halinde hazırlanan ve yayınlanan 2016-2019 Ulusal Siber Güvenlik Stratejisinde; siber saldırı, ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler olarak tanımlanır.

Siber saldırılara çeşitli örnekler verilebilir. Bunlar, ağ trafiğini dinleyerek ağda bulunan verileri çalma, e-postalarda gönderilen linkler ya da zararlı eklentiler aracılığıyla sisteme virüs bulaştırma, sistemlere yetkisiz girişler sağlayarak kullanıcı bilgilerini çalma, kuruluşların web sitelerine kendi düşüncelerini içeren yazılar koyma şeklinde olabilir.

Bu örneklerin yanı sıra bilinçsiz kullanıcıların yaptığı hatalarda siber saldırılara sebep olabilir. Yapılan bu saldırılar sonucunda maddi ya da manevi kayıplar yaşanabilir, kuruluşların itibarları zedelenebilir, insanların özel bilgileri ifşa olabilir, ülkeler arasında savaşlara sebebiyet verilebilir veya kuruluşların kritik alt yapıları zarar görebilir.

Şekil 2.1: Siber Saldırı Örneği




Kaynak: http://havelsan.com.tr/files/files/folders/292201611322055_HAVELSAN_SiberGuvenlikBulteni_Sayi1.pdf

Şekil 2.1'de bir siber saldırının nasıl gerçekleştiği adım adım gösterilmektedir.

Birinci adımda, kötü niyetli saldırgan saldırı yapacağı kuruluş ile ilgili bilgi toplamaktadır.

İkinci adımda, kuruluşun çalışanlarına e-posta yoluyla gönderdiği virüs ya da herhangi bir zararlı yazılımla tuzak kurmaktadır.

Üçüncü adımda, kendisinin ifşa olmaması için önlemler alarak başka hedef göstermektedir.

Dördüncü adımda kurulan tuzağa düşen kullanıcılar vasıtasıyla ulaşmak istediği bilgiye erişmektedir.

Beşinci adımda diğer saldırganlardan takviye alarak, daha sonraki aşamada komuta kontrol sağlayarak son adımda hedefine ulaşmaktadır.

### II.1.3 Siber Güvenlik

Siber güvenlik, siber uzayda gerçekleştirilen siber saldırılara karşı önlem alınmasıdır. Diğer bir ifadeyle, siber uzayda kuruşların sahip oldukları kritik altyapıları, uygulamaları,

hizmetleri, varlıkları saldırılara karşı korumak amacıyla araç, politika, prosedür, eğitim gibi faaliyetlerin gerçekleştirilmesidir.

> Siber güvenlik kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, elektronik haberleşme sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır (www.btk.gov.tr).

Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında ise, "Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" şeklinde ifade edilmiştir.

## II.2 Siber Güvenlikte Yaşanan Örnek Olaylar ve Etkileri

Teknolojinin gelişmesiyle internet hayatımıza girmiş, insan hayatı oldukça kolaylaşmıştır. Bankacılık işlemleri, alışveriş, fatura ödemeleri zaman harcamadan bulunulan yerden kolaylıkla yapılabilmektedir. Bu kolaylıklar yanında bazı sıkıntıları da beraberinde getirmektedir.

İnsanların işlemleri kolaylıkla yapabilmesi gibi saldırganlarda teknolojinin avantajlarını kullanarak kolaylıkla varlıklarımıza ulaşabilmekte ve varlıklarımız üzerinde değiştirme ve yok etme gibi eylemler gerçekleştirebilmektedir. Geçmişten günümüze yapılan saldırılardan örnekler vermek gerekirse;

1982 yılında gerçekleşen ilk siber saldırı Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) ve Amerika arasında yaşanmıştır. SSCB, Trans Sibirya gaz boru hattının kontrolünü sağlamak için Amerika'dan yazılım satın almak istemiştir. Amerika'nın yazılımı satmak istememesi üzerine SSCB, kodlarının bir kısmını Kanadalı bir firmanın sistemine girerek gizlice ele geçirmiştir. Amerika, SSCB'nin niyetini öğrenmiş, durdurmak yerine yazılım içine Truva atı virüsü eklemeyi tercih etmiştir. Yerleştirilen virüs boru hatlarında gerçekleşen

normal akışı yüksek seviyelere çıkarmış ve dünyadaki en büyük patlamalardan birine sebep olmuştur.

1990 yılında Irak ve ABD arasında gerçekleşen Körfez Savaşı'nda Irak güçlü kara ordusuna sahip olmasına rağmen savaşı kaybetmiştir. Bu savaş sonunda anlaşılmıştır ki önemli olan ne kadar büyük ve güçlü bir orduya sahip olunduğu değil, siber saldırı konusunda hangi noktada olunduğudur. ABD bu savaşı kazanmak için öncelikle Irak'ın hava savunma radar ve füze üslerini etkisiz hale getirmiştir. İleriki aşamada telsiz konuşmalarına sızmış ve bütün haberleşmeyi dinlemiştir. Irak yedek telsiz hattını, daha sonra gönüllü telefon hatlarını denemiştir. ABD aynı yöntemle bu iletişim cihazlarına da sızmıştır. Irak'ın iletişim hattı tamamen ele geçirildiğinden savaş kaybedilmiştir.

1999 yılında Kuzey Atlantik Antlaşması Örgütü'ne (NATO) karşı yapılan siber saldırılar, uluslararası platformda kendisine güvenilen NATO'nun itibar kaybetmesine sebep olmuştur. 1999 yılında Kosova Kurtuluş Ordusuna karşı sürdürülen operasyonlarda, yetki NATO Genel Sekterine verilmiş; NATO Genel Sekreteri de Sırpları bombalama emri vermiştir. Bunun üzerine NATO'ya sistemi çalışamaz hale getiren Dağınık Hizmet Engelleme Saldırısı (DDOS) ve binlerce zararlı virüs içeren e-postalar gönderilmiştir. NATO'nun resmi sitesinde sürekli kesintiler yaşanmış ve NATO'nun e-posta hesabı günlerce kapalı kalmıştır.

2003 yılında ABD ve Irak arasında yaşanan ikinci savaşta ABD, Irak subaylarını psikolojik olarak çökerterek hiçbir çaba göstermeden savaşı kazanmıştır. Tek yapması gereken Irak e-posta sistemine girerek subaylara savaşmalarının gereksiz olduğunu, diğer savaşta olduğu gibi yine savaşı kazanacakları bilgisini içeren bir mesaj göndermesidir. Irak subayları bu mesajı gördükten sonra savaşmamışlardır.

2007 yılında Estonya bronz kızıl ordu askeri heykelini kaldırmak istemiş, Ruslar buna karşı çıkmışlardır. Bunun üzerine yapılan DDOS saldırısı üzerine Estonya'nın siteleri çökertilmiş, devletin internet sayfaları, gazetelerin web siteleri hizmet veremez hale gelmiştir. Saldırı daha da büyümüş, bankaların, devlet kuruluşlarının ve birçok önemli kritik alt yapının çalışamamasından dolayı iletişim ve ticaret durma noktasına gelmiştir. Sonucunda saldırıyı Rusya kabul etmemiş ve onlar tarafından yapıldığı kanıtlanamamıştır.

2014 yılında HSBC Türkiye'nin sistemine sızılmış ve milyonlarca müşterinin bilgileri çalınmıştır. HSBC müşterilerin herhangi bir finansal kayıp yaşamayacaklarını, sadece kredi kartlarının bağlı olduğu hesap bilgileri, kredi kartı son kullanma tarihlerinin çalındığını bildirmiştir. 2016 yılında Obama'nın eşi Michelle Obama'nın pasaport bilgileri hackerlar tarafından çalınmıştır. Aynı yıl Dropbox, Yahoo ve LinkedIn gibi milyonlarca kullanıcıya sahip uygulamalara düzenlenen siber saldırılar sonucunda kullanıcıların kişisel ve özel

bilgileri ele geçirilmiştir. Ayrıca 2016 Şubat ayında Bangladeş Bankası'ndan 81 milyon ABD doları (aktarılmaya çalışılan toplam para 951 milyon ABD doları) çalınmıştır.

Yukarıda bahsettiğimiz olaylarda görüldüğü üzere sistemlere zararlı yazılımlar aracılığıyla sızma sonucunda web sitelerini etkisiz duruma getirme, kişisel bilgileri çalma, itibar kaybına sebep olma durumları yaşanmıştır ve bu olaylar her geçen gün artmaya devam etmektedir.

Bu hızlı artış ileride oluşabilecek tehditlerin habercisidir. Bu tehditlerin ciddiyetini daha iyi anlamak için yapılan çalışmalardan sayısal örnekler vermek gerekirse;

- ✓ Cisco 2017 Yıllık Siber Güvenlik Raporu'na göre; güvenliği ihlal edilen kurumların yüzde 22'si müşteri kaybetti.
- ✓ STM'nin hazırlamış olduğu 2016 raporunda; Türkiye dâhil, dünya çapında 31 milyondan fazla Wi-Fi bağlantı noktasının analiz edilmesi sonucu her dört noktadan birinin (% 28) korumasız olduğu ve kullanıcıların kişisel bilgilerinin riske atıldığı belirtildi.
- ✓ Intel Security Tehdit Raporu'nda; 2016 yılı ikinci çeyreğinde, her bir dakikada 316, saniyede ise 5'ten fazla yeni tehdidin ortaya çıktığı belirtildi. Aynı rapora göre, 2016 yılı 3. çeyrek sonu itibariyle, 2016 yılında ortaya çıkan yeni fidye yazılımı örneklerinin toplam sayısı, yılın başından itibaren % 80 artış göstererek 3.860.603'e ulaştı.
- ✓ Cybersecurity Ventures'un 2016 yılı raporuna göre; 2015 yılında 3 trilyon dolar olan küresel siber suç maliyetlerinin 2021 yılına kadar 6 trilyona çıkacağı tahmin ediliyor. Ayrıca 2020 yılında dünyanın siber savunma yapabilmesi için bugünden 50 kat daha fazla veriye ihtiyacı olacağını, siber güvenlik iş açığının 2016 yılında bir milyon iken 2019 yılında 1,5 milyona çıkacağını ve 2020 yılında işletmelerde tespit edilen saldırıların % 25 inden fazlasının IoT (Nesnelerin İnterneti) içereceğini belirtiyor.

Tehditler sonucunda oluşan bu maddi ve manevi kayıpları önlemek için ülkeler siber güvenlik konusunda kendilerini sürekli geliştirmektedirler. Türkiye'de bu ülkeler birisidir.

## II.3. Türkiye'de Siber Güvenlik

Tablo 2.1: Türkiye'de Siber Güvenlik

| | |
|---|---|
| 2003 | 2003/10 sayılı Başbakanlık Genelgesinin yayımlanması |
| 2005 | Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmeliğin yürürlüğe girmesi |
| 2007 | 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun yürürlüğe girmesi |
| 2007 | İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğin yürürlüğe girmesi |
| 2010 | Siber Suçlar Sözleşmesine Ülkemiz tarafından imzalanması |
| 2012 | Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin, Bakanlar Kurulu Kararının yayımlanması |
| 2012 | Siber Güvenlik Enstitüsü Kurulması |
| 2012 | TSK Siber Savunma Merkezi Başkanlığı Kurulması |
| 2013 | UDHB Siber Güvenlik Dairesi Kurulması |
| 2013 | Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının yayımlanması |
| 2013 | Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ'in yayımlanması |
| 2013 | Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Bal küpü Sisteminin Telekomünikasyon İletişim Başkanlığı Tarafından Kurulması ve İşletilmesine Yönelik Kararın Resim Gazetede yayımlanarak yürürlüğe girmesi |
| 2014 | Siber Suçlar Sözleşmesinin TBMM tarafından onaylanması |
| 2016 | 2016 - 2019 Ulusal Siber Güvenlik Stratejisinin yayımlanması |

Tablo 2.1'de 2003'den bu yana Siber Güvenlik konusunda Ülkemizde yapılan önemli çalışmalar (mevzuat, ulusal ve uluslararası belgeler vb.) bir araya getirilerek son 1 yılda yapılan çalışmalar sunulmuştur. Bu çalışmalar Kamu ağırlıklı olup, özel sektör ve sivil toplum kuruluşları da bu çalışmalara önemli katkı sağlamıştır.

Bu çalışmaları kısaca açıklamak gerekirse;

2003/10 sayılı Başbakanlık Genelgesi, siber güvenlik konusunda atılan adımlardan ilkidir. Bu genelgenin amacı, güvenlik kültürünü oluşturmak ve bu konuda neler yapabileceği konusunda öneriler sunmaktır. Bu genelge ile siber güvenlik konusunda yapılan çalışmalar hız kazanmış ve bu konu ile ilgili toplantı, bilinçlendirme eğitimleri ve kuruluşların gerekliliği fark edilmiştir.

Bu farkındalık sonucunda atılan ciddi adımlardan biri, 10 Kasım 2005 tarihinde 25989 sayılı Resmi Gazete ’de “Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik” in yayımlanmasıdır.

Bu yönetmeliğin yayımlanmasından iki yıl sonra siber güvenlik konusunda hukuki anlamda yapılan çalışma, 23 Mayıs 2007 tarihinde 26530 sayılı Resmi Gazete ‘de yayımlanan “İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” dur. Bu kanun ile internet üzerinden zararlı içeriklerin yayımlanmasını önlemek, gerçekleştirilen siber suçların önüne geçmek ve saldırganları tespit etmek hedeflenmiştir.

Bu kanunda yer alan maddeler çerçevesinde 01 Kasım 2007 tarihinde 26687 sayılı Resmi Gazete‘de “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik” yayımlanmıştır.

Çıkarılan kanun ve yönetmelikler uygulanmakta, fakat teknoloji hızla gelişmeye devam ederken saldırganlarda aynı hızla kendilerini geliştirmektedir. Saldırganların bu gelişimi, saldırıların daha ciddi ve fark edilemez şekilde gerçekleştirilmesini tetiklemektedir. Bu nedenle hukuksal anlamda yapılan çalışmaların yanı sıra eylem planları ve politikalar hazırlamak, hazırlanan bu politika ve eylem planlarını uygulamak gerekmektedir.

Bu anlayış çerçevesinde 2009 yılında Ulusal Sanal Ortam Güvenlik Politikası, ülkemizi sanal ortamdaki saldırılara karşı hazır hale getirecek ve sanal ortamda yaşanacak sorunların ardından hızlı geri dönüşü sağlayacak sanal ortam güvenlik adımlarını belirlemek amacıyla hazırlanmış ve uygulanmaya başlamıştır.

Türkiye kendi içerisinde siber güvenlikle ilgili önlemler almaya devam ederken, siber saldırıların sınır tanımaması nedeniyle ülkeler arasında da yapılması gereken çalışmalar ihtiyaç halini almıştır.

Bu nedenle, 2010 yılında Avrupa Konseyi bünyesinde, 2001 yılında Budapeşte’de kabul edilen, Siber Suçlar Sözleşmesi (*Council Of Europe Convention on Cybercrime*) imzalanmıştır. Ağ üzerinden işlenen suçlara karşı uluslararası bağlayıcılığı olan ilk ve tek anlaşma niteliği taşıyan Sözleşme, 2014 yılında Türkiye Büyük Millet Meclisi tarafından onaylanmıştır.

Türkiye’de siber güvenlik konusunda atılan ciddi adımlardan biri de 20 Ekim 2012 tarihli ve 28447 sayılı Resmi Gazete ‘de yayımlanan “Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin, Bakanlar Kurulu Kararı”dır.

Bu karar ile Türkiye, siber güvenlik konusundaki çalışmalarına resmen başlamıştır. Karar kapsamında; Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.

Oluşturulan Siber Güvenlik Kurulu 4 defa toplanmış ve bu toplantılar sonucunda da siber güvenlik konusunda ciddi kararlar almıştır. Bu kararlardan biri 2013 yılında 2013/4890 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" dır. Bu eylem planı 25 Ekim 2013 tarihinde 28683 sayılı Resmi Gazete 'de yayımlanmıştır. Bu eylem planı ile özellikle elektrik, su gibi kritik alt yapılara sahip kuruluşlara yapılması muhtemel siber saldırıların önüne geçilmesi planlanmıştır.

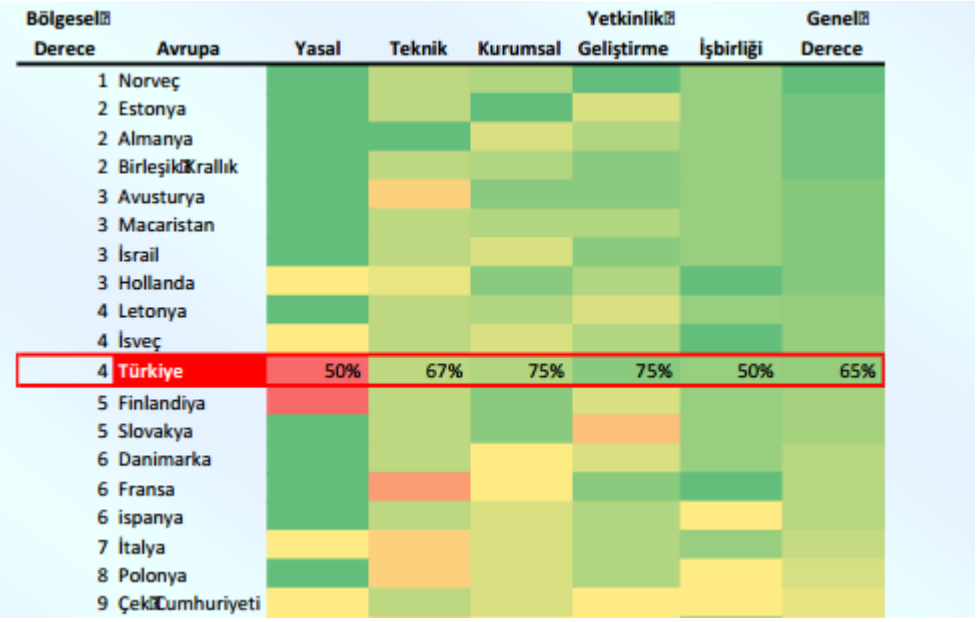
Bu eylem planı kapsamında "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" maddesi yer almıştır.

Bu madde kapsamında11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazetede, "Siber Olaylara Müdahale Ekiplerinin Kuruluş Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ"i yayımlanmıştır.

Bu tebliğ esas alınarak, "Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Bal küpü Sisteminin, Telekomünikasyon İletişim Başkanlığı Tarafından Kurulması ve İşletilmesine Yönelik Karar onaylanmış ve SOME Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar" yayımlanmıştır.

Türkiye'nin siber güvenlik konusunda son dönemde yaptığı çalışmalardan biri de, 2016 yılında yayımlanan "2016-2019 Ulusal Siber Güvenlik Stratejisi"dir.

Şekil 2.2: Türkiye'de Siber Güvenlik



| Bölgesel Derece | Avrupa | Yasal | Teknik | Kurumsal | Yetkinlik Geliştirme | İşbirliği | Genel Derece |
|---|---|---|---|---|---|---|---|
| 1 | Norveç | | | | | | |
| 2 | Estonya | | | | | | |
| 2 | Almanya | | | | | | |
| 2 | Birleşik Krallık | | | | | | |
| 3 | Avusturya | | | | | | |
| 3 | Macaristan | | | | | | |
| 3 | İsrail | | | | | | |
| 3 | Hollanda | | | | | | |
| 4 | Letonya | | | | | | |
| 4 | İsveç | | | | | | |
| 4 | Türkiye | 50% | 67% | 75% | 75% | 50% | 65% |
| 5 | Finlandiya | | | | | | |
| 5 | Slovakya | | | | | | |
| 6 | Danimarka | | | | | | |
| 6 | Fransa | | | | | | |
| 6 | ispanya | | | | | | |
| 7 | İtalya | | | | | | |
| 8 | Polonya | | | | | | |
| 9 | Çek Cumhuriyeti | | | | | | |

Kaynak: http://www.havelsan.com.tr/files/files/folders/17102016135850390_SiberGuvBulteni_Sayi7_Ekim2016.pdf

Şekil 2.2'de 2015 yılına kadar Türkiye'nin yaptığı yasal düzenlemeler, kurumsal yapılanmalar, kullanıcı farkındalığı geliştirme, diğer ülkelerle yapmış olduğu ortak çalışmalar ve siber güvenlik konusunda yaptığı teknik unsurlar değerlendirilerek 22 ülke arasındaki sıralaması gösterilmiştir. Yapılan bu değerlendirme ile ilgili detaylı bilgiler EK-1'de yer alan Küresel Siber Güvenlik Göstergesi ve Siber Memnuniyet Profilleri raporunda anlatılmaktadır.

### II.3.1 Siber Güvenlik Kapsamında Yürütülen Diğer Çalışmalar

Ülkemizde siber güvenlik çalışmaları son yıllarda özellikle de Siber Suçlar Sözleşmesinin imzalanmasından sonra giderek hızlanmıştır. Bu kapsamda yapılan hukuki çalışmalar, eylemler ve politika çalışmaları dışında, kurum ve kuruluşların siber güvenlik konusunda farkındalığını arttırmak ve mevcut durumu analiz etmek amacıyla siber güvenlik tatbikatları düzenlenmiştir.

Bu tatbikatlardan ilki, Bilgisayar Olayları Müdahale Ekibi 2008 Tatbikatıdır. 2008 yılında yapılan 8 adet kurum ve kuruluşun katıldığı bu tatbikat, kurumlara saldırı gerçekleşmesi durumunda işbirliği süreçlerinin nasıl uygulanacağını belirlemek amacıyla yapılmıştır.

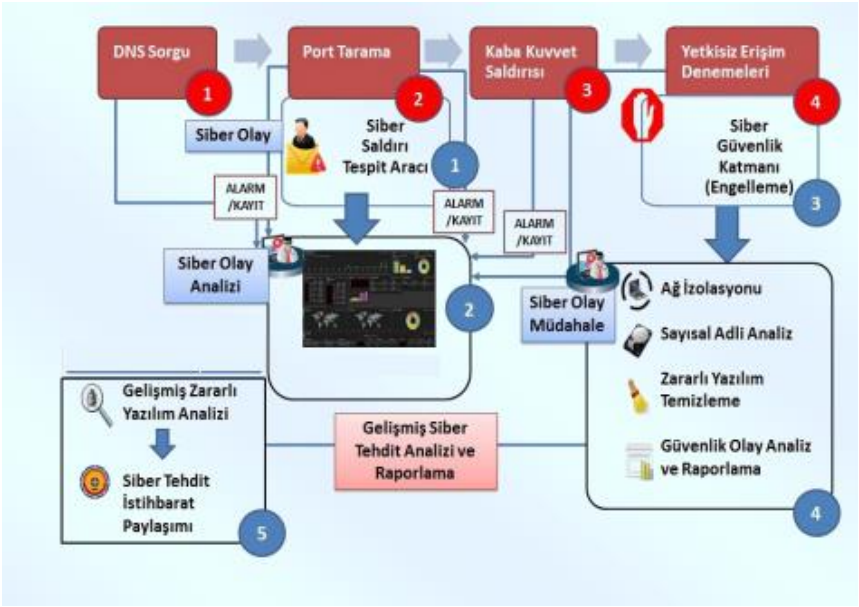
2011 yılında yapılan ikinci siber güvenlik tatbikatı, Ulusal Siber Güvenlik 2011 Tatbikatı, 41 kamu kuruluşu, özel sektör ve sivil toplum kuruluşunun katılımıyla

gerçekleşmiştir. Katılımcı kuruluşların bu konudaki yeterliliklerini tespit etmek ve olası saldırılara müdahale etme yeteneğini kazandırmak amacıyla hem gerçek hem de simülasyonların gerçekleştirildiği bir tatbikat olarak düzenlenmiştir.

Siber Kalkan 2012 Tatbikatı, 2012 yılında Türkiye'de internet erişim hizmeti sunan ve internete erişim sağlayan elektronik haberleşme sektörünün % 99,9'unu oluşturan 12 firmanın katılımıyla, siber saldırılara karşı önlem alma yeteneğinin kazandırılması amacıyla yapılmıştır.

> Ulusal Siber Güvenlik 2013 Tatbikatı, 2013 yılında 61 kurum ve kuruluşun katılımıyla, siber saldırılara önlem alınması, kurumların bilgi güvenliği sistemlerinin güçlendirilmesi ve kurumlar arası koordinasyonun artırılması amacıyla düzenlenen siber tatbikattır (Ercan, 2015, 33)

Şekil 2.3 Siber Güvenlik Tatbikat Senaryosu




Kaynak: http://www.havelsan.com.tr/files/files/folders/1562016093136381_SiberGuvBulteni_Say4_Haziran2016.pdf

# III. SİBER GÜVENLİK OPERASYON MERKEZİ (SGOM) VE ÖNEMİ

Çağımızın gereği olarak internet ve internet üzerinden gerçekleştirilen işlemler yaygındır ve insan hayatını kolaylaştırmaktadır. Bu kolaylık ve avantaj sadece iyi yönde değil kötü niyetli insanlar tarafından olumsuz şekilde de kullanılabilmektedir. Bu konuda geçmişten günümüze kadar sayısız örnek mevcuttur.

Yukarıda anlatılmış olan örneklerden bazıları; itibarların yok olmasına, savaşların kaybedilmesine, maddi ve manevi kayıplar yaşanmasına sebep olan yaşanmış binlerce siber saldırıdan sadece birkaç tanesidir.

Bu nedenle siber saldırılara karşı Türkiye'de çeşitli çalışmalar yürütülmektedir. Bu çalışmalar 2013 yılında 2013/4890 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı sonrasında giderek daha fazla gelişmektedir.

Bu eylem planında "Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması" başlığı altında "Kurum ve kuruluşlar bünyesinde de sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır." ifadesi yer almaktadır. SOME'lerin kurulmasından sonra siber güvenlik konusunda yapılacak bir diğer adım ise Siber Güvenlik Operasyon Merkezi (SGOM) kurulmasıdır.

Bu bölümde SGOM'un ne olduğu, neden kurulması gerektiği, özellikleri, görevleri ve çalışma sistemi ortaya konularak, ÇŞB bünyesinde kurulan SGOM'da yürütülen çalışmalar paylaşılacaktır.

## III.1. SGOM

SGOM; bilgi varlıklarını, bilgisayar ve iletişim altyapısını oluşabilecek ihlallere karşı 7/24 esasına göre izleyen ve gözlemleyen; oluşmuş veya oluşabilecek ihlalleri değerlendiren; bu ihlallere karşı kurum ve kuruluşu savunan, kurum ve kuruluşta yer alan özel bir alandır.

Bu merkezler, saldırı tespit ve kayıt yönetimi, izleme ve olay yönetimi, zafiyet analizi, zararlı yazılım analizi gibi siber güvenlik konularında uzman kişilerden oluşan bir ekip tarafından işletilmekte ve yönetilmektedir. Bu merkeze yetkisiz kişiler tarafından giriş yapılması mümkün olduğunca engellenmektedir.

Bu operasyon merkezinde siber olayların izlenmesi, analiz edilmesi, raporlanması ve alarm üretilmesi işlemleri gerçekleştirilmektedir.

Şekil 3.1: Örnek SGOM

http://www.havelsan.com.tr/a/Main/urun/780/siber-guvenlik-operasyon-merkezi-hizmeti

## III.2. SGOM Önemi

Günümüzde teknolojinin ulaştığı nokta göz önüne alındığında, bilgiyi üreten ve kullanan kurum ve kuruluşların güvenliği büyük önem taşımaktadır. Bu noktada kurum ve kuruluşların güvenliğini sağlamak için kurulacak SGOM'un önemini sıralamak gerekirse;

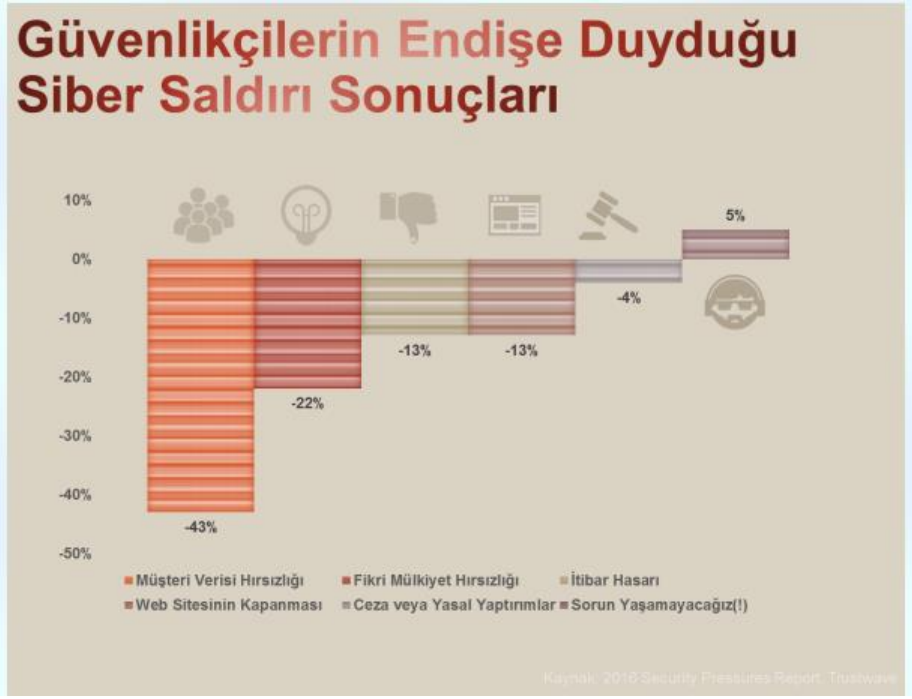
- ✓ Kurumsal itibarın sağlanması,
- ✓ Verilen hizmetin aksamaması,
- ✓ Varlıkların gizlilik, bütünlük ve erişilebilirliğin sağlanması,
- ✓ Tehdit ve risklerin önceden belirlenerek, gerekli önlemlerin alınması,
- ✓ Kurum çalışanlarında bilgi güvenliği farkındalığının oluşturulması,
- ✓ Yaşanan saldırılara karşı zamanında ve etkin müdahale edilmesi,
- ✓ Varlıkların kötü amaçlı kullanılmasını ve suistimal edilmesini engellemesi,

- ✓ İlgili taraflarla iletişim halinde bulunulması,
- ✓ Güncel tehdit ve saldırılardan en kısa sürede haberdar olunması,
- ✓ Yasal zorunlulukları uymakta kolaylık sağlanması
- ✓ Maddi kayıpların azaltılması,
- ✓ Ani durumlarda ortaya çıkan stresin en aza indirilmesi,
- ✓ Kritik olan sistemlerin sürekli izlenmesinin sağlanması,

olarak ifade edebiliriz.

Şekil 3.2'de görülen saldırganların gerçekleştirdiği ihlaller sonucu; müşteri verilerinin çalınması, web sitelerinin kapanması, kuruluşların itibar kaybetmesi, fikri mülkiyet hırsızlığının yüzdelik oranları SGOM'un ne kadar önemli olduğunu bir kez daha göstermektedir.

Şekil 3.2: SGOM Önemi



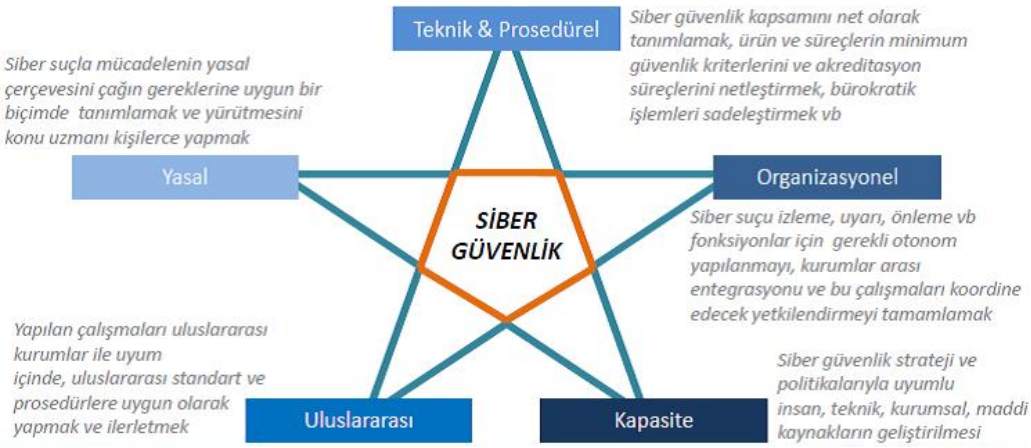

Kaynak: http://www.havelsan.com.tr/files/files/folders/292201611322055_HAVELSAN_SiberGuvenlikBulteni_Sayi1.pdf

## III.3. SGOM Gereksinimleri

Kurum ve kuruluşlarda SGOM kurulurken; kurum ve kuruluşun bütün varlıkları düşünülmeli, bu varlıkların zafiyetleri tespit edilmeli, zafiyetlerin oluşturduğu riskleri minimuma indirmek için gerekli önlemler alınmalı, insan faktörünün önemi unutulmamalı, yapılacak saldırılar hakkında bilgi sahibi olunmalı ve bu saldırılara karşı hazırlıklı olunmalıdır.

Bu adımlar tamamlandıktan sonra siber güvenliğin sağlanması için gereken önleme, tespit ve müdahale etme adımlarının uygulanması için insan, süreç ve teknoloji kategorileri yapılandırılmalıdır.

Şekil 3.3: SGOM Yapısı




Kaynak :http://www.cybermagonline.com/siber-guvenlik-ve-siber-savaslar-2/

SGOM kurulurken göz önüne alınması gereken kavramlar Şekil 3.3'de belirtilmiş olup, detaylı olarak açıklamak gerekirse;

### III.3.1. Üst Yönetim Desteği

SGOM yapısının etkin bir şekilde oluşturulması ve işletilmesi için kuruluşun üst düzey yöneticileri tarafından kuruluş içerisinde önemli bir rol oynayacak SGOM kurulumunun istenmesi; maddi, manevi destek verilmesi, belirli bir bütçe ve zaman ayrılması gerekmektedir.

Üst yönetimin SGOM konusunda destek vermesi için üst yönetime siber güvenliğin ne olduğu, ne kadar önemli olduğu, kurum ve kuruluşun bu yapıya neden ihtiyacı olduğu

konularının doğru bir şekilde aktarılması gerekmektedir. Ayrıca siber güvenlik için hangi aşamadan başlanacak ve ne kadar sürede ne konuma gelinecek bilgisinin iyi bir şekilde planlanarak üst yönetime doğru bir şekilde aktarılması konusu da çok önemlidir.

SGOM kurmak ilk adımda ciddi maliyetler gerektirdiğinden bütçe konusu önemli bir mevzudur. Aynı zamanda uygulanacak adımlar için belirli bir zamana ihtiyaç bulunmaktadır. Bu nedenle üst yönetimin desteği olmadan ilerlemek nerdeyse imkânsızdır.

### III.3.2. İhtiyaçların Belirlenmesi

Her kuruluşun kendine özgü bir iş gücü ve sahip olduğu belirli seviyede kritik alt yapısı mevcuttur. Örneğin; enerji üretimi ve dağıtımı yapan bir kuruluş ile kâğıt üretimi yapan bir kuruluşun sahip olduğu kritik alt yapı seviyesi aynı değildir.

Bu nedenle SGOM kurma kararı alındıktan sonra kuruluş içerisinde bazı analizler yapılması gerekmektedir. Bu analizler yapılırken şu adımlar izlenir.

- Kurum veya kuruluşa ait bilgi ya da varlıkların belirlenmesi,
- Bilgi varlıkların kurum veya kuruluş açısından ne kadar değerli olduğunun saptanması,
- Bu varlıklara gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması,
- Muhtemel kayıpların nasıl sonuçlar vereceğinin araştırılması,
- Her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması,
- Bu varlıklarda gerçekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi,
- İleriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların belirlenmesidir.

Bu adımlar gerçekleştiğinde kuruluş tarafından varlıklar belirlenmiş, varlıkların sahip olduğu zafiyetler ve varlıklara karşı olan tehditler saptanmış ve sonucunda kuruluşun sahip olduğu riskler ortaya çıkmış olur.

Yapılan çalışmalar sonunda belirlenen riskleri önlemek için kritik sistemleri sürekli olarak izlemek, bu sistemlerin zafiyetlerini tespit etmek, bu sistemlerden kayıt toplamak ve bu kayıtları değerlendirmek için uygulanması gereken planlar ve gerekli cihazlar belirlenir.

Teknolojinin değişmesiyle beraber yeni saldırı türleri ve yeni saldırı yöntemleri çıkması, kuruluşların yeni varlıklara sahip olması bahsedilen bu adımların belirli aralıklarla tekrarlanmasını gerektirir.

### III.3.3. SGOM'da Çalışacak Personel

SGOM'da çalışacak personelin bilgi güvenliği ve siber güvenlik konusunda uzmanlaşmış, en az iki yıl bilgi işlem tecrübesine sahip, belirli eğitimleri almış, otoriteler tarafından itibar gören uluslararası sertifikalara sahip olması siber güvenlik konusunda daha etkin olmasını sağlayacaktır. Bu personele kuruluş tarafından uygulama sınavları gerçekleştirilmeli ve personel bu sınavları başarıyla tamamlamalıdır.

SGOM'da çalışacak personele karar verilirken öncelikle kurum personeli değerlendirilmeli, kurum personelinin sayıca ihtiyacı karşılamaması sonucunda destek personeli alınmalıdır.

Destek personeli elde etmiş oldukları bilgiler dolayısıyla sır saklama yükümlülüğüne sahiptir. Bu nedenle destek personeline gizlilik sözleşmeleri mutlaka imzalatılmalıdır. Kuruluş tarafından destek personeli için güvenlik soruşturması yaptırılmalıdır. Destek personeli için hazırlanan sözleşmelerde kuruluşta personel istihdamını düzenleyen kanun maddeleri göz önüne alınmasına dikkat edilmelidir.

SGOM'un sağlıklı bir şekilde yürütülebilmesi için yeterli sayıda uzman personel bulunmalı, kritik rollerde çalışan personelin yedeği mutlaka sağlanmalıdır. Süreç bazlı bir çalışma yapılarak çalışan personelin rolleri, sorumlulukları, ilgili paydaşların görevleri ve alt süreçlerin işlem adımları açıkça tanımlanmalıdır.

Aşağıda görevleri belirtilen uzman personelin SGOM bünyesinde yer alması SGOM yapısının daha etkin bir şekilde sürdürülmesine katkı sağlayacaktır;

*Güvenlik direktörü*; SGOM yapısının ve tüm siber güvenlik faaliyetlerinin yönetim ve denetimini sürdürmektedir.

*Güvenlik mimarı*; kurum ve kuruluşun iş ihtiyaçları, güncel olaylar ve mevzuatın takibi, kurum veya kuruluşun SGOM yapısının analizi, değişen koşullara göre teknik iyileştirmelerin tavsiye edilmesi, planlanması ve uygulanmasından sorumludur.

*Güvenlik analisti*; güncel tehdit ve saldırılarının takip edilmesi, sistemlerden toplanan kayıtların analiz edilmesi ve gerçekleşebilecek saldırıların tespit edilmesi ve önlenmesinden sorumludur.

*Güvenlik operasyon* mühendisi; SGOM içerisinde yer alan güvenlik ürünlerinin bakım ve yönetiminden sorumludur.

*Olay müdahale uzmanı*; yaşanabilecek bir olayın öncesinde yapılması gerekenlerin planlanmasından, yaşanmış bir olay esnasında ve sonrasında uygulanması gereken adımların belirlenmesinden ve icra edilmesinden sorumludur.

Sızma testi uzmanı; kurum veya kuruluşun sahip olduğu bilgi sistemlerine sızma testlerinin yapılmasından ve yaptırılmasından sorumludur.

### III.3.4 Uygulanması Gereken Planlar

- Bir siber güvenlik olayı gerçekleşmesi sonucunda olay yönetim süreci devreye alınır, dijital delillerin bozulmaması için gerekli önlemler uygulanır. Ek 2'de yer alan Olay Müdahale Süreci işletilir.
- Uzman personel tarafından mevcut olan saldırıların terminolojileri hakkında detaylı bilgiye sahip olunması, sürekli güncel olayların takip edilerek yeni çıkan saldırılar hakkında bilgi toplanması gerekir.
- Kuruluş üzerinde gerçekleşmiş olan siber olaylar, tehditler tespit ve analiz edilir. Gerçekleşen siber olayları analiz aşamasında türleri, miktarları ve maliyetleri kabaca ölçülür ve izlenir. Yapılan bu analizin sonucunda önlemler ve aksiyonlar alınır; alınan önlemler ve aksiyonlar etkin bir şekilde takip edilir ve yönetilir.
- Siber uzayda gerçekleştirilen saldırıları takip etmek, analiz etmek ve bunlara karşı alınacak önlemleri ve aksiyonları belirleyebilmek adına güvenlik istihbarat servislerine üye olunarak takip edilebilir. Oluşturulan önlemler ve aksiyonlar etkin bir şekilde takip edilir ve yönetilir.
- Ulusal ve uluslararası boyutta yaşanan siber güvenlikle ilgili yapılan bütün çalışmalar (yasa, kanun, tebliğ, ulusal ve uluslararası standartlar, strateji belgeleri, eylem planları, ulusal ve uluslararası eğitim ve seminerler vb.) yakından takip edilir, edinilen bilgilerin SGOM'a uyarlanması için çalışmalar yapılır.
- Kuruluşun içerisinden gerçekleşen veri sızıntıları izlenir, tespit edilir ve önlenir.
- SGOM, operasyonlarını yürütürken kuruluşun ve kullanıcıların işlerinin devamlılığı konusunda aksaklıklara sebep olmaz, işlemler yürütülürken görünmez olur; fakat bir olay gerçekleştiğinde veya gerçekleşme ihtimali olduğunda devreye girer.
- Kritik olan sistemleri sürekli olarak gözetim altında tutar.
- SGOM merkezi izleme bölümünde ekranlarda aşağıdakiler takip edilmelidir;

- ✓ Kritik uygulamaların çalışıp çalışmadığı ve performansları,
- ✓ Sunucuların durumları,
- ✓ Ağ trafiği,
- ✓ Güvenlik ihlal olay bildirimleri,
- ✓ Bilişim sistemlerine ait klima ve soğutma sistemleri,
- ✓ Güvenlik ihlal olay müdahale aşamaları

- SGOM merkezinde kullanılmak üzere iletişim dokümanı oluşturulmalı ve düzenli aralıklarla kontrol edilmelidir.

  İletişim dokümanı en az aşağıdaki alanlardan oluşmalı;
  - ✓ İletişim konusu
  - ✓ İletişimden sorumlu kişi
  - ✓ Hangi durumda iletişim kurulacağı,
  - ✓ İletişim kurulacak taraf - İlgili kişi,
  - ✓ İletişim bilgileri

  İletişim dokümanı en az şu birimleri içermelidir;
  - ✓ İtfaiye (iş sürekliliği için)
  - ✓ Telekomünikasyon sağlayıcı (Erişilebilirliğin sağlanması için)
  - ✓ Su tedarikçileri (soğutma tesisleri için)
  - ✓ Elektrik tedarikçileri
  - ✓ USOM
  - ✓ Yetkili firma sorumlusu
  - ✓ Kurum ve kuruluştaki yetkili sistem sorumlusu

- Yılda en az bir kez yapılması gereken testler şunlardır;
  - ✓ İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması
  - ✓ Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması
  - ✓ Dışa açık web uygulamalarının sızma testleri
  - ✓ Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri
  - ✓ Veri tabanı yapılandırma testleri

- ✓ Kuruma özel geliştirilmiş yazılımlar
- ✓ DNS servisi testleri
- ✓ E-posta servisi testleri
- ✓ Sosyal mühendislik testleri
- ✓ Sadece kurum içinden erişilen web uygulamaları sızma testleri
- ✓ DDOS testleri
- ✓ Sanallaştırma sistemleri testleri
- ✓ Kablosuz ağ testleri
- ✓ Güvenlik duvarı testleri
- ✓ URL ve içerik filtreleme testleri (Kurumsal SOME Kuruluş ve Yönetim Rehberi)

- Kuruluşlarda çalışanlar için bilgi güvenliği ve siber güvenlik konusunda farkındalık oluşturulmalıdır. Bunun için;
  - ✓ Tatbikatlar yapılarak kullanıcılar güncel sosyal mühendislik saldırıları konusunda bilgilendirilmeli,
  - ✓ Siber güvenlikle ilgili düzenli aralıklarla kuruluş içi bülten yayınlanmalı,
  - ✓ Kuruluş çalışanlarına bilgi güvenliği ve siber güvenlik ile ilgili hatırlatma e-postaları veya eğitici videolar gönderilmeli,
  - ✓ Yıllık ya da periyodik olarak siber güvenlik seminerlerine davet edilmeli,
  - ✓ Sadece kuruluş personelinin erişim sağladığı kuruluş sayfasında siber güvenlik ile ilgili bir bölüm oluşturulmalı,
- Siber olay öncesi, siber olay sırasında ve siber olay sonrasında yapılacaklar belirlenmeli ve prosedür haline getirilmelidir.

  Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu hazırlanır ve kuruluşun üst düzey yetkililerine iletilir (ÇŞB için hazırlanan Siber Güvenlik Operasyon Merkezi Dokümanı).

- Uzman personelin siber olayları tespit etme ve siber olaylara müdahale etme kabiliyetlerini geliştirmek için en az yılda bir defa tatbikat yapmaları faydalı olacaktır.
- DDOS ataklarından korunmak amacıyla yük dengeleme yapılır.

- Güçlü bir siber güvenlik politikası oluşturulur.
- İşletim sistemleri, yazılımların servis paketleri ve cihazlar güncellenmelidir. Güncelleme ve yama aldıktan sonra yeni güvenlik açıklıkları oluşması ihtimallerine karşı testler yapılması gerekir.
- Kullanıcı hakları asgari seviyede tutulmalı; kullanılmayan servisler, protokoller ve bileşenler çalıştırılmamalıdır.
- Gizlilik seviyesi yüksek olan bilgiler ve dosyalar şifrelenerek muhafaza edilmelidir. Bilgilerin ağ üzerinde başka bir yere gönderilmesi gerektiğinde mümkünse yetkisiz kişilerce okunmasını engellemek amacıyla şifreleme işlemi yapıldıktan sonra gönderilmesi gerekir. Yüksek kritiklik seviyesine sahip bilgiler için şifreleme yetersiz kaldığında saldırganların bilginin önemli bir bilgi olduğunu fark edememeleri için bilgiyi başka bir bilgi içine saklama tekniği kullanılarak iletişim sağlanmalıdır. Açık anahtar yapısı ve elektronik-imza da bu yapılarla birlikte kullanılır.
- Olabilecek ani saldırı veya doğal afetlere karşı felaket kurtarma ve acil durum planları, müdahale planları hazırlanır, belli aralıklarla güncellenir.
- Bilişim alt yapısı içerisinde yer alan cihazların kullanılamaz hale gelmesi veya işlevini yitirmesi sonucunda içinde bulunan verilere ulaşılamayacak ve geri dönüşümü mümkün olmayacak şekilde imha edilir.
- ISO 27001 standardının gerektirdiği prosedürler, politikalar uygulanır.
- Bilgiler yedeklenir, yedeklerin güvenliği ile ilgili önlemler alınır, yedekleme ve yedekten dönme prosedürleri mevcut bulunur.

### III.3.5 SGOM İhtiyaçları

SGOM kurulabilmesi için üst yönetim desteği, personel ve planlar dışında SGOM'da çalışacak güvenlik cihazları da gerekmektedir.

Cihazlar temin edilirken, cihazların ortak niteliklere sahip olmasına, birbirlerini desteklemesine, bundan dolayı bütüncül bir yaklaşım sergilemesine dikkat edilmelidir. Bunun dışında SGOM içerisinde yapılandırılacak cihaz ve sistemlerin mümkünse yüzde yüz milli ürünlerden oluşturulması en büyük hedeflerden biridir. Mümkün olmadığı noktalarda ise otoriter kuruluşlar tarafından incelenmiş ve uygun bulunan cihaz ve sistemler kullanılmalıdır.

SGOM içerisinde bulunması gereken sistem, cihaz ve özelliklere bakacak olursak;

### *III.3.5.1 Testler*

***Sızma Testi***

Sızma testi TSE'nin onaylı sızma firmalarından ve TSE onaylı sızma testi uzmanları tarafından yapılır. Uluslararası TS/ISO IEC 27001, Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (COBIT), Açık Web Uygulama Güvenliği Projesi (OWASP) standartları gereği yılda en az bir defa yaptırılması gerekir.

Sızma testlerinde saldırgan mantığıyla kontrollü saldırılar gerçekleştirilerek saldırı simülasyonu yapılır, böylece güvenlik açıklıkları ortaya çıkmış olur. Sızma testleri sonunda saptanan zafiyetler SGOM personeli veya firma tarafından kapatılır. Zafiyetler kapandıktan sonra doğrulama testleri yapılır.

**Sızma testleri**

- ✓ Planlama,
- ✓ Bilgi Toplama,
- ✓ Zafiyet Analiz,
- ✓ Zafiyet Kullanım
- ✓ Rapor Aşaması olmak üzere 5 aşamadan oluşmaktadır.

Planlama aşamasında, kuruluşun varlıklarına ve varlıkların kritiklik seviyesine göre yapılacak sızma testi türü, testi yaparken kullanılacak araçlar belirlenir.

Bilgi toplama aşamasında, yapılacak testin türüne göre çeşitli kaynaklar ve saldırı yöntemleriyle sızma testi gerçekleştirilecek kuruluş hakkında bilgi toplanır.

Zafiyet analiz aşamasında, varlıkların sahip olduğu zafiyetler tespit edilerek tanımlanması ve sınıflandırılması işlemi gerçekleştirilir.

Zafiyet kullanım aşamasında, adından anlaşıldığı üzere tespit ve analiz edilen bilişim sistemleri üzerinde çalışan uygulama ve yazılımların zafiyetleri kullanılır.

Son aşama olan rapor aşamasında, sızma testi sonunda açığa çıkan sonuçları özetleyen ve kuruluşun üst düzey yetkililerine tavsiyelerde bulunan bir rapor hazırlanmaktadır.

Sızma testleri, kapalı kutu sızma testleri, açık kutu sızma testleri ve zafiyet değerlendirme testleri olmak üzere üç farklı şekilde uygulanabilir.

Kapalı kutu sızma testlerinde testi yapacak firmaya hiçbir bilgi verilmez. Açık kutu sızma testinde firmaya sistem hakkında maksimum seviyede bilgi verilir. Böylece daha önce firmada çalışmış ve sisteme zarar vermeye çalışan bir çalışanın zarar verebileceği seviye

ölçülmüş olur. Zafiyet değerlendirme testi ise konuya ilişkin özel testler kullanılarak tüm dikkat açıklıkları tespit etme üzerinedir. Firmada çalışan kısıtlı yetkilere sahip bir çalışanın sisteme ne gibi zararlar verebileceği üzerinde çalışılır.

Sızma testi yaptırılmasında dikkat edilmesi gereken bir nokta dış kaynaklı olarak gerçekleştiriliyorsa her sızma testinin farklı yetkili firmalara yaptırılması gerekmektedir. Bunun en önemli sebebi, firmalar ne kadar bu konuda yetkin olsalar da her firmanın farklı bir bakış açısı mevcuttur ve her firmanın kaçırdığı zafiyetler olacaktır.

Gelişmiş bir SGOM yapısı için sızma testlerinin SGOM personeli tarafından yapılması önem arz etmektedir. SGOM personeli tarafından yapılan testlerin doğrulanması ve tespit edilemeyen zafiyetler mevcut ise bunların tespit edilmesi amacıyla yılda bir defa dış kaynaklı olarak gerçekleştirilmesi yararlı olacaktır.

***Sosyal Mühendislik Testleri***

Sosyal mühendislik, kullanıcıların zafiyetlerini kullanarak bilgi elde etmek amacıyla yapılan çeşitli ikna etme veya kandırma yöntemleridir.

Sosyal mühendislik testleri, bazı kuruluş çalışanlarının hedef alınarak indirim içeren bir alışveriş sayfası linki gönderildiğinde ya da ilginç bir haber e-posta atıldığında güvenlik önlemlerine dikkat etmemesini, telefon ile yapılan görüşme sonucunda herhangi bir doğrulama yapmadan istenen işlemi gerçekleştirmesini sağlayacak farklı senaryolar üretir. Bu senaryolar sonucunda kuruluşun güvenlik politikalarının yeterliliği, çalışanların güvenlik farkındalığı, fiziksel güvenlik önlemlerinin aşılıp aşılamayacağı gibi kuruluş içerisinde yaşanabilecek zafiyetler test edilir.

Sosyal mühendislik testlerinde amaç, siber güvenliğinin bir varlığı olan insan faktörünün değerlendirilmesidir.

Yapılan sosyal mühendislik testlerinden sonra siber güvenlik konusunda bilinçlendirme eğitimleri verilir. Bu eğitimlerin tamamlanması ile birlikte belirli bir süre sonra sosyal mühendislik testi tekrar uygulanır. Bu işlem belirli aralıklarla tekrar edilerek kurum veya kuruluşun siber güvenlik farkındalığı konusunda ilerleme grafiği ortaya çıkarılır.

***DDOS Testi***

Bilgi güvenliği, bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasıdır. DDoS saldırısı bilginin erişilebilirlik bileşenini ihlal etmektedir.

DDoS saldırısı saldırganlar tarafından sıklıkla kullanılmaktadır. Bu nedenle DDoS testlerinin belirli sıklıklarla yaptırılarak kurum veya kuruluşun alt yapısının saldırılara karşı

dayanıklı olup olmadığı ölçülerek, herhangi bir problem ile karşılaşılması durumunda uzman gözetiminde ağ alt yapısını düzenlemek için gerekli önlemlerin zaman kaybetmeden alınması gerekmektedir.

SGOM yapısının bir önemi de iş sürekliliğinin sağlanmasıdır ve DDoS testleri yaptırılıp önlem alınmamasını takiben gerçekleşecek bir DDoS saldırısı sonucu sistemler uzun süre cevap veremez hale gelebilir. Bu durumda SGOM yapısından beklediğimiz performans sağlanmamış olur.

Bu testlerin dışında kırmızı takım tatbikatları ve kablosuz ağ testleri de kuruluşlarda siber güvenlik konusunda yapılan testlerdir.

### *III.3.5.2. Cihazlar*

***Güvenlik Duvarı***

İstenmeyen kaynaklara giden trafiğin engellenmesini sağlayan yazılım ve donanım parçasıdır. Genellikle paket filtreleme ve vekil sunucular ile birlikte kullanılır. Güvenlik duvarı sadece bilgisayardan internete giden trafiği değil, internetten bilgisayara gelen trafiği de izlemektedir. Bunun en önemli faydası, içeri sızan bir saldırganın dışarı veri kaçırmak istemesi durumunda internetten bilgisayara giden trafiğin izlenmesinden dolayı tespit edilebilmesidir.

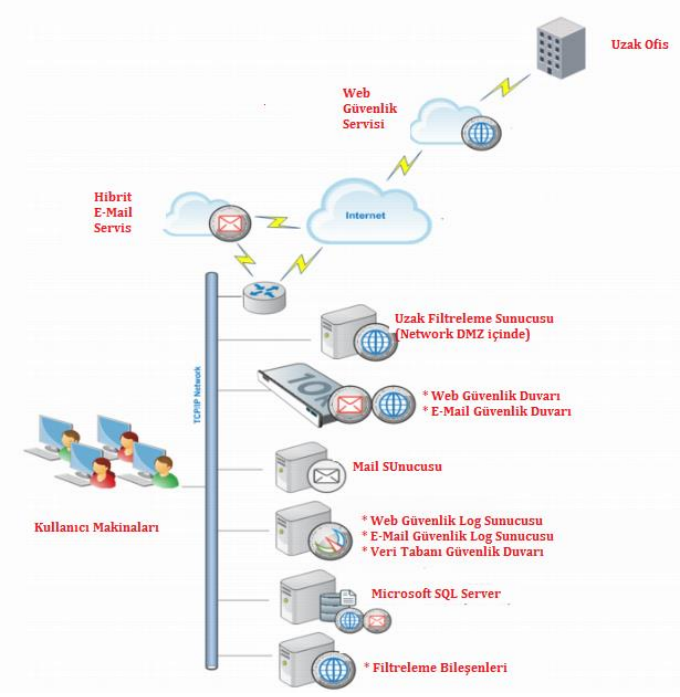
Güvenlik duvarının sahip olması gereken özellikler;

- ✓ Belirli kurallar yazılarak yapılandırılmalı,
- ✓ Güvenlik duvarının sahip olduğu dâhili servislerden gerekmeyenler kapatılmalı, erişim engellenmeli,
- ✓ Bilinen tehdit türlerini tanımalı ve güncel koruma özelliklerini desteklemeli,
- ✓ Yetkilendirme ve izinler, portlar ve IP üzerinden değil uygulama kimliği tanıma ve erişim kimlik doğrulaması üzerinden yapılmalıdır.
- ✓ Kullanıcıları ve cihazları belli özellikte gruplara ayırarak güvenlik politikalarını ve tanımlanan kuralları daha anlaşılır hale getirmeli,
- ✓ Uzun süreli DDOS atağı ve bozuk paket gönderen İnternet Protokolleri (IP) tanımalı ve engellemeli,
- ✓ İmza tabanlı sistem saldırılarını protokol ve port düzeyinde tanımalı, sahte yönlendirme adresleri içeren, belli ülkelerden gelen istenmeyen ve bilinen güvenlik riskleri taşıyan şüpheli erişimlere izin vermemeli,

- ✓ Üzerinden akan trafiği gözlemleyerek, uygulama ve port bazında kullanım raporu oluşturabilen yapıda olmalı,
- ✓ İzinsiz dosya ve veri aktarımlarına müdahale edilebilmeli,
- ✓ İnternet ve uygulama erişimi, kullanıcı ve saat bazında denetlenebilir olmalı,
- ✓ URL filtreleme ve web erişim denetimi özelliğine sahip olmalı,
- ✓ Güvenlik duvarının yönetim paneli zorunlu olmadıkça internet üzerinden erişime açılmamalı, içeriden yapılan bağlantı mutlaka SSH benzeri şifreli yapıda olmalıdır (Kurumsal SOME Kuruluş ve Yönetim Rehberi).

Güvenlik duvarı saldırıların önlenmesi için kullanılan katmanlardan sadece biridir. Sadece gönderici ve alıcı bilgilerine, paket başlıklarına ve porta bakar. Bu öğeler dışında gelen veri ile ilgilenmez. Yazılan kurallara göre inceleme yapar. Bu nedenle daha önce tespit edilmemiş bir saldırıyı ya da yazılmamış bir kural sonucunda gelen saldırıyı tespit etme olasılığı düşüktür.

Şekil 3.4 : SGOM İhtiyaçları




Kaynak : http://www.websense.com/content/support/library/deployctr/v76/WESG_v10k_ch.aspx

***Web Uygulama Güvenlik Duvarı (WAF)***

Web servisleri üzerinde detaylı paket inceleme yapan; URL, IP ve etki alanı kontrollerini sağlayan; zararlı istekleri engelleyen güvenlik sistemidir. Günümüzde siber saldırı ve tehditlerin web uygulamaları üzerinde yoğunlaşmasından dolayı WAF, güvenlik duvarıyla birlikte kullanılmalıdır.

WAF da beyaz liste modeli, kara liste modeli ve öğrenme tabanlı model olmak üzere çeşitli yaklaşımlar kullanılmaktadır.

Beyaz liste modelinde, izin verilen işlemler haricinde bütün işlemler engellenir. Kara liste modelinde, yasaklanmış işlemler haricinde bütün işlemlere izin verilir.

Öğrenme tabanlı modelde, gelen ve giden istekler takip edilerek, öğrenme sonrasında web sayfaları haritası çıkarılır. Öğrenilen istekler WAF'a gönderilir, yetkili uzman tarafından incelenerek kabul edilir ya da reddedilir. Sitenin zararlı olduğu kabul edildiyse, WAF o sitenin bulunduğu sunucudan gelen istekleri fark ederek engeller.

WAF sistemleri kendi üreticilerine ve uluslararası kabul görmüş kara liste veri tabanlarına gerçek zamanlı olarak bağlanarak veri tabanını güncel tutmaktadır. Sadece bu sistemlerden veri almamakta, USOM tarafından yayınlanan zararlı olarak bildirilen IP adresleri ve web sitelerinden de beslenmektedir.

***Veri Tabanı Güvenlik Duvarı***

Veri tabanında bulunan bilgilerin güvenliğini sağlamak için kullanılan güvenlik sistemleridir. Web uygulamaları gibi veri tabanını kullanan yazılımlar veri tabanı ile bütünleşmiş bir şekilde çalışmaktadır. Web uygulamasına erişen bir saldırganın veri tabanına erişememesi için alınması gereken bir önlemdir.

Veri tabanı güvenlik duvarı izleme ve bloklama, erişim kontrolü, denetim ve raporlama, veri maskeleme gibi birçok özelliği içermektedir. Böylece veriye kim, ne zaman ve ne kadar veriye ulaşmış gibi bütün bilgiler takip edilerek anormal bir hareket gözlendiğinde incelenerek gerekli işlemler zaman kaybetmeden yapılabilecektir.

***Saldırı Önleme Sistemi (IPS) ve Saldırı Tespit Sistemi (IDS)***

Ağ trafiğini sürekli izleyerek zararlı davranışları ve yazılımları tespit eden ve şüpheli paketleri belirleyen güvenlik sistemleridir. Düzgün bir şekilde yapılandırılması gerekir.

IDS sadece olay ihlallerini kaydeder ve kullanıcıya uyarı gönderir. IPS ise ağ üzerine herhangi bir şüpheli davranış tespit ederse güvenlik duvarını yeniden programlar ve ağ trafiğini ve saldırıyı engeller.

IPS de diğer çoğu güvenli duvarı gibi imza tabanlı olarak çalışır. İmza tabanlı çalışması sonucu daha önce tespit edilmiş bir saldırıyı tespit eder, fakat henüz tespit edilmemiş bir saldırıyı tanıyamaz ve geçmesine izin verir.

Donanım tabanlı bir saldırı engelleme sistemidir. SQL injection, ara bellek taşımı, şifre dosyası okuma saldırısı gibi birçok kritik imzayı tetiklemektedir.

***Ağ İzleme Cihazı***

Kuruluşlar tarafından ağ hizmetlerinin güvenilirliğini ve kalitesini sağlamak için sıklıkla kullanılır. Bu cihaz istisnai ağ trafiği aramak ve ağda ortaya çıkan kötü amaçlı faaliyetleri algılamak için kullanılır. Ağ üzerindeki trafiğin normal olup olmadığı hakkında bilgi verir.

Ağ izleme cihazının takip ettiği ağın görsel olarak ekranlarda SGOM izleme ekibi tarafından sürekli izlenmesi gerekmektedir. Herhangi bir anomali tespitinde gerekli incelemelerin başlatılması, ilgili birimlerle iletişime geçilmesi, koordineli bir şekilde çalışarak sorunun çözümlenmesi gerekmektedir.

***Zafiyet Tarama Sistemleri***

SGOM personeli tarafından siber olay gerçekleşmeden önce sistemde bulunan bilgisayar, ağ sistemleri, işletim sistemleri ve yazılım uygulamaları dâhil bütün bilişim sistemleri üzerindeki zafiyetlerin tespit edilebilmesini ve bunlar için karşı önlemler alabilmesini sağlar. Aynı zamanda yama eksikleri ve kurum politikasına aykırı yapılandırılmış sistemleri de tespit ederler.

***Kayıt Yönetim Sistemi***

SGOM personelinin sistemdeki kayıtları takip edebilmesine, izleyebilmesine, sistemlerde gerçekleşebilecek tehditlerin önceden fark edilmesine olanak sağlar. Belirli zaman aralıklarında kimler çalışıyordu, bu zaman aralığında kimler harici bellek kullandı, veri tabanı sunucusuna kimler erişti gibi birçok sorunun cevabı tutulan bu kayıtlar sayesinde kolaylıkla cevaplanabilmektedir.

Ayrıca 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, ISO/IEC 27001, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve bunun gibi birçok yasal mevzuata göre verilerin saklanması gerekmekte ve bu işlem de kayıt yönetimi sistemi tarafından

gerçekleştirilmektedir. Herhangi bir talep ya da yaşanan bir olay sonucunda istenen kayıtların yetkili kişilere ulaştırılması gerekmektedir.

Güvenlik cihazlarından, uygulamalardan, kurum veya kuruluşun sahip olduğu bütün sistemlerden kayıtlar alınmaktadır. Bu kayıtlar alınan sisteme göre syslog, Basit Ağ Yönetim Protokolü (SNMP), Apache, İnternet Bilgi Servisleri (IIS) ve bunun gibi farklı formatlarda alınmaktadır. Bu kayıtlar olay yönetimi Bilgi Güvenliği ve Olay Yönetimi (SIEM) tarafından tek bir formata dönüştürülerek incelenmektedir.

Kayıtlar büyüklüğüne ve sağlanan şartlara göre bulut sistemlerinde, büyük veri merkezlerinde, CD, DVD gibi ortamlarda tutulmaktadır.

Kayıt yönetim sisteminin oluşturduğu iz kayıtları olayların gerçekleştiği sistemden ayrı bir merkezde saklanır. Saklama merkezlerinde yer alan iz kayıtları yedeklenir, uygun bir şekilde muhafaza edilir, silinmesine veya değiştirilmesine izin verilmez. Saklama işlemi için gönderilen iz kayıtları, mümkünse kayıtların saklandığı merkeze şifreli olarak gönderilir.

Kritik olayların iz kayıtları saklama merkezlerine anlık, diğer iz kayıtları belirlenen aralıklarla gönderilir.

İz kayıtları saldırının hangi IP adresinden yapıldığı, ne zaman yapıldığı ve verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği zaman bilgilerini içeren zaman mührüne sahip olmalıdır.

Kayıt yönetim sistemi aracılığıyla iz kayıtları düzenli olarak takip edilir. İz kayıtları dönemsel (günlük, haftalık, aylık vb.) olarak analiz edilir ve birbirleriyle ilişkilendirilmeye çalışılır. Çalışma sonunda hazırlanan rapor kuruluşun üst yetkililerine sunulur.

***E-posta Güvenlik Sistemi***

Posta sunucusu üzerinde aşırı bir trafik oluştuğunda uyarı veren sistemlerdir. Gelen e-postaları inceleyerek reklam amaçlı gönderilen veya sisteme zarar vermek amacıyla zararlı kaynak içeren e-postaları engeller. E-posta güvenlik sistemi örneğin bilinmeyen bir alandan belirli bir zaman içerisinde belli bir sayıdan fazla e-posta geldiğinde bu e-postaların yayılmasını durdurur ve riski azaltır.

E-posta güvenlik sistemi e-postaları incelerken güncel veri tabanında mevcut olan zararlı yazılımlar ile karşılaştırma yaparak tespit etmesi durumunda e-postanın gönderimini engeller. Spam e-posta kontrolü sağlar. Sistem kullanıcıları tarafından tanımlanmış zararlı veya aldatma e-postası olma ihtimali olan içerikleri ayrı bir alana alarak yetkili kişilerin kontrol etmesine olanak sağlar.

***Anti Virüs***

Solucan, virüs, Truva atı gibi kötü yazılımları sisteme girmeden yakalayan, girmesini engelleyen ve yok eden; sisteme girdiyse tespit edip, sistemi temizleyen, belirli aralıklarla güncellenmesi gereken yazılımlardır.

Kuruluşlarda kullanılacak anti virüs yazılımlarında olması gereken özellikler,

- ✓ Ağdaki kullanıcılar belirli özelliklere göre gruplanarak her gruba özel farklı güvenlik politikaları oluşturulmalıdır.
- ✓ Merkezi konsol aracılığıyla ağ üzerinde anti virüs programının çalışmadığı makinelerin tespit edilerek yazılım kullanıcıyla etkileşime girmeden kullanıcının sistemine kurulmalıdır.
- ✓ Kullanıcıların gerçekleştirdiği (ya da maruz kaldığı tehditler gibi) olaylar merkezdeki konsola gönderilmeli ve bu konsol tarafında bunlar tutularak istenen kriterlere göre raporlanmalıdır (Yaşar, 2014, 48).

Anti virüs çözümü seçerken üretici firmalarının; Türkiye'de bir ofisinin mevcut olması ve ofiste çalışan Türk yetkilerinin bulunması, web sayfasındaki bilgilerin gelişmiş düzeyde olması, kullanıcılarının sorunlarına çözüm üretebilmesi ve kolay erişilebilmesi güvenlik açısından öncelik sağlamaktadır.

***Veri Kaçağı Önleme Sistemi***

Sistemde mevcut olan verilerin ağ üzerinden izinsiz bir şekilde kuruluş dışına çıkarılması ya da sızdırılmasının önlenmesi için izleme ve önleme işlemlerini yapan donanım ve yazılımlardır.

***İçerik Filtreleme Sistemi***

Ağ üzerinde bütün trafiği izleyerek kuruluş tarafından karar verilen bazı kelimeler, içerikler, resimler ve buna benzer istenmeyen birçok içeriğe sahip trafiği eleyen sistemlerdir.

***Bal Küpü***

Bal küpleri (honeypot); bilgi sistemlerine yetkisiz erişen saldırganlar ya da kullanıcılar hakkında bilgi toplamaya yarayan tuzak sunuculardır. Bal küpleri genelde bir ağın parçasıymış gibi görünen bilgisayar veya veri barındıran herhangi bir sunucu olabilir. Aslında

saldırganlara göre, saldırmak için sebep olabilecek bilgi veya değer taşıyan bir hedef gibi duran, izole edilmiş ve hareketleri özellikle izlenen bir kaynaktır.

Ağ izleme ve erken uyarı sistemi özellikleri de mevcuttur. Ayrıca saldırganın kullandığı saldırı yöntemlerini tespit etme özelliği kullanılarak benzer saldırılara karşı sistem içerisinde önlemler alınır.

***Ağ Erişim Kontrol Sistemi***

> Ağ erişim kontrol sistemi, bir bilgisayarın ağa veya ağdaki çeşitli kaynaklara erişiminin gerçekleşmesinden önce bilgisayarın gerekli konfigürasyon ve güvenlik politikalarını sağlayıp, sağlamadığını kontrol eden eğer sağlıyorsa ağa bağlanmasına izin veren, sağlamıyorsa gerekli güncelleme ve ayarların yapılabilmesi için ilgili sunuculara yönlendiren sistemlerdir (Çeliktaş, 2016, 50).

***Bilgi Güvenliği ve Olay Yönetimi (SIEM)***

SIEM, kuruluşların bilgi alt yapısında bulunan ağ, sistem ve güvenlik cihazları tarafından üretilen ham verileri toplar ve korale eder. Aşırı veri, uzman personelin aradığını bulmasında zorluk yaratır ve bunun sonucunda aradığı veriyi gözden kaçırma riski artar. Ayrıca cihaz üzerinde fazla veriden dolayı yük oluşacağından veri kaybı yaşanabilir. Bu cihaz aldığı verileri işleyerek uzman personelinin rahatlıkla anlayabileceği ve analiz edebileceği hale getirir.

Normalde tespit edilemeyen saldırılar SIEM'e giriş verisi olarak verilerek değerlendirilmesi sonucunda saptanacaktır.

SIEM'in çalışma mantığı, belirtilen sistemlerden gelen kayıt ve saldırı verilerini toplar; bu kayıtları tek bir formata dönüştür; bu kayıtları ilişkilendirir ve ilişkilendirdiği bu kayıtları inceleyerek aynı içeriğe sahip kayıtları ortak noktada birleştirip tek bir kayıt haline getirir; oluşan bu kayıtlar arasında bir önceliklendirme gerçekleştirir, rapor ve alarm üreterek işlemini tamamlar.

SIEM üzerinden kaynak kullanım raporları, zararlı yazılım raporları, kritik hata raporları, ağ aktiviteleri raporları gibi birçok rapor temin edilebilir.

SIEM'in sistemler için avantajları, durumsal farkındalık yaratır, kayıtlardan anlamlı sonuçlar elde edilmesini sağlar, karmaşık saldırıların tespitini kolaylaştırır, merkezi izleme olanağı sağlar.

***Yük Dengeleyici***

Yük dengeleyici, erişilebilirliği en üst seviyede tutmak için yoğun istek gelen sunucular arasında yük paylaştırırlar.

***Yedekleme***

Kurum ve kuruluşun sahip olduğu sistemlerin yedeklerinin alınması herhangi bir problem yaşandığında anda sistemin aksamadan çalışması için kritik önem taşımaktadır. Yedeklerin merkezi bir şekilde alınması ve geri dönüş senaryolarının oluşturularak belirlenen aralıklarla geri dönüş testlerinin yapılması gerekmektedir.

### *III.3.6. SGOM Yapısı*

- SGOM sadece yetkili kişilerin giriş yapabilmesi için mutlaka avuç içi tarama, retina taraması, parmak izi tanıması gibi güçlü bir kimlik doğrulama sistemine sahip olmalıdır. Dışardan bir kişinin girmesi durumunda SGOM personeli tarafından kendisine eşlik edilir.
- SGOM diğer paydaşlarla ve servis sağlayıcılarla sürekli işbirliği içinde olmalıdır. Teknolojik gelişmeler, yeni çıkan saldırı ve saldırı yöntemleri, mevcut yaygın güvenlik riskleri paydaşlarla paylaşılır.
- SGOM fiziksel saldırılara karşı da güvenlik sağlayacak şekilde yer alır. SGOM herhangi bir fiziksel saldırıya maruz kalmayacak şekilde yalıtılır. Su baskını, elektrik kesintisi gibi fiziksel sorunlardan etkilenmeyecek şekilde yapılandırılır.
- SGOM içerisinde 7/24 kayıt alan kameralar bulunmalıdır. Sel, yangın gibi doğal afetler düşünülerek yangın söndürme sistemleri, uyarı sistemleri, ısı ve nem algılayıcı cihazların bulunması ve bu cihazlarla iletişim halinde bulunan merkezi cihazların farklı noktalarda konumlandırılması gerekmektedir.
- SGOM 7/24 esasına göre çalışmalıdır.

### *III.3.7. SGOM Genel Değerlendirme*

Tablo 3.1: SGOM Genel Değerlendirme

| **SGOM'da Olması Gerekenler** | **Açıklama** |
|---|---|
| Güvenlik Duvarı | En temel güvenlik cihazıdır. Gelen ve giden trafiğin kontrol edilmesi için gerekmektedir. |
| IPS/IDS | IPD/IDS güvenlik duvarından sonraki ikinci katmandır. Güvenlik duvarı tarafından tespit edilemeyen zararlı içerikleri tespit etmektedir. |
| E-posta Güvenlik Sistemi | Dış ağdan binlerce spam ve zararlı e-posta gelmektedir. E-posta yoluyla sosyal mühendislik saldırıları gerçekleştirilmektedir. Bu nedenle e-postalar ve e-posta içerisinde gelen eklerin kontrol altına alınması gerekmektedir. |
| Web Uygulama Güvenlik Duvarı | Uygulamalar web tabanlı olarak gerçekleştirilmektedir. Bu nedenle kurum ve kuruluşlar sayısız web uygulamasına sahiptir. Bu uygulamaların güvenliğini sağlamak için gereklidir. |
| Kayıt Toplama Sistemi | 5651 sayılı Kanun gereğince kayıtların tutulması ve kaydedilmesi gerekmektedir. |
| Bilgi Güvenliği ve Olay Yönetimi | Sistemlerden alınan kayıtlar kişiler tarafından yönetilemeyecek kadar fazladır. Kayıtların merkezi bir sistem tarafından analiz edilmesi ve olay içeren kayıtların bildiriminin yapılması gerekmektedir. |
| İçerik Filtreleme Sistemi | 5651 sayılı Kanun gereğince içerik filtreleme ve URL işleminin yapılması gerekmektedir. |
| Anti virüs | Bir günde tonlarca virüs ortaya çıkmaktadır. Bir sistem tarafından bu virüslerin tespit edilmesi ve önlem alınması gerekmektedir. |
| 7x24 izleme sistemi | 7x24 izleme sistemleri ile kurum ve kuruluşun sahip olduğu kritik uygulamaların, kritik sistemlerin izlenmesi gerekmektedir. |
| Sızma Testleri (En az yılda bir kez) | Kurum ve kuruluşlarda bir web uygulama ve bir sistem olmak üzere iki zafiyet tarama sistemi mevcuttur. Sızma testleri ile birlikte farklı araçlarla otomatik olarak ve uzman kişiler tarafından manuel olarak testler yapılarak açıklıklar tespit edilmektedir. |
| Kontrollü giriş-çıkış uygulaması | Sadece yetkili kişiler tarafından yetkili alanlara ulaşılması gerekmektedir. |
| Dışardan gözlemlenememesi | Güvenlik konusunda temel güvenlik önlemlerinin alınması gerekmektedir. Kurum ve kuruluşa ait ekranlara, bilgilere yetkisiz kişilerin ulaşımı engellenmelidir. |
| Yetki tanımlamaları ve düzenli kontroller | Yetkiye sahip kullanıcıların ayrılması, değişmesi durumda bu yetkileri kullanarak herhangi bir olaya sebebiyet vermemesi için yetkilerinin alınması gerekmektedir. |

| | |
|---|---|
| İletişim dokümanları | Herhangi bir olay anında doğru yetkili kişilere hızlı bir şekilde ulaşılması gerekmektedir. |
| Yazılı bilgi ve dokümanlar (Olay müdahale prosedürleri, cihazların çalışma talimatları vb.) | Hangi konuda nasıl bir yöntem uygulanacağının bilinmesi gerekmektedir. |
| Eksiksiz veri envanteri ve durumları | Hangi verileri koruyacağımızın bilinmesi ve durumlarının kontrol edilmesi gerekmektedir. |
| Kritik sistemlerin bulunduğu alanların kamera ile kayıt altına alınması | Yaşanabilecek herhangi bir olayın çözümlenebilmesi için ihtiyaç duyulan bazı verilere ulaşabilmesi ve sistemlerin takibinin yapılabilmesi gerekmektedir. |
| Yedekleme ve geri dönüş testlerinin uygulanması | Herhangi bir olay yaşanması anında sistemlerin erişebilirliğinin bozulmaması için yedeklerin alınması ve bu yedeklerin doğru alındığının kontrol edilmesi gerekmektedir. |
| Ekran izleme faaliyetleri | SGOM ekibi tarafından güvenlik açısından kritikliği olan sistemlerin izlenmesi gerekmektedir. |
| Farkındalık | Kurum ve kuruluş personelinin farkındalığı herhangi bir olayın yaşanması ihtimalini düşürmektedir. |

## III.4. Çevre ve Şehircilik Bakanlığı SGOM Çalışmaları

Bakanlığımızda sistem, ağ, donanım, yazılım gibi bilişim alt yapısını yönetmekten ve Bakanlığımızın sahip olduğu varlıklara karşı yapılabilecek herhangi bir ihlale karşı bilişim güvenliğinin sağlanmasından Bakanlığımızın Coğrafi Bilgi Sistemleri Genel Müdürlüğü (CBSGM) sorumludur.

Bu sorumluluk çerçevesinde CBSGM kurumsal bilgi güvenliğini sağlamak adına TS ISO/IEC 27001 gibi uluslararası kabul görmüş standartlardan ve deneyimli uzman firmaların danışmanlıklarından faydalanarak bu yönde çalışmalar başlatılmıştır.

Bu çalışmaların sebebi, teknolojinin gelişmesiyle beraber güvenlik olayı önemini hızla artmıştır. Saldırı teknikleri sürekli gelişmekte, hiçbir bilgisi olmayan kişiler bile bilerek ya da bilmeyerek sistemlere zarar vermektedir. Bakanlığımız ortofoto verileri, doküman yönetim sisteminde yer alan veriler, yapı denetim sistemi verileri gibi çok ciddi iş ve işlemler yürütme ve bunların güvenliği sağlamak zorundadır.

Bu nedenle yapılan bu çalışmalardan ilki, “BGYS Kurulumu Projesi”dir. Bu proje kapsamında, ilgili şube müdürlükleriyle görüşmeler yapılmış, sahip oldukları varlıklar, varlıkların sahip olduğu zafiyetler, varlıklara karşı tehditler, tehditler sonucunda çıkan riskler belirlenmiştir.

Riskler değerlendirilerek, risklere karşı alınabilecek önlemler konusunda çalışmalar yapılmış ve sonucunda Kurumsal Bilgi Güvenliği Politikası ve Prosedürleri oluşturularak

30.12.2014 tarihli 90743779/010.06/4476 sayılı "Bilgi Güvenliği Politikaları" konulu Genelge yürürlüğe girmiştir.

Bu genelge ile Bakanlığımızın bilgi güvenliği konusunda yapması gereken adımlar, rol ve sorumluluklar belirlenmiştir.

Yapılan bu çalışmalar sonucunda Bilişim Proje Koordinasyon Şube Müdürlüğü'nün altında BGYS yapısı oluşturulmuştur. 2015 yılında 01.10.2015 tarihli 24173523-907.01-E.4102 sayılı Bakanlık Olur'u ile BGYS yapısı Bilişim Proje Koordinasyon Şube Müdürlüğü'nün bünyesinden ayrılarak, Bilgi Güvenliği Şube Müdürlüğü adıyla yeni bir birim olarak kurulmuştur.

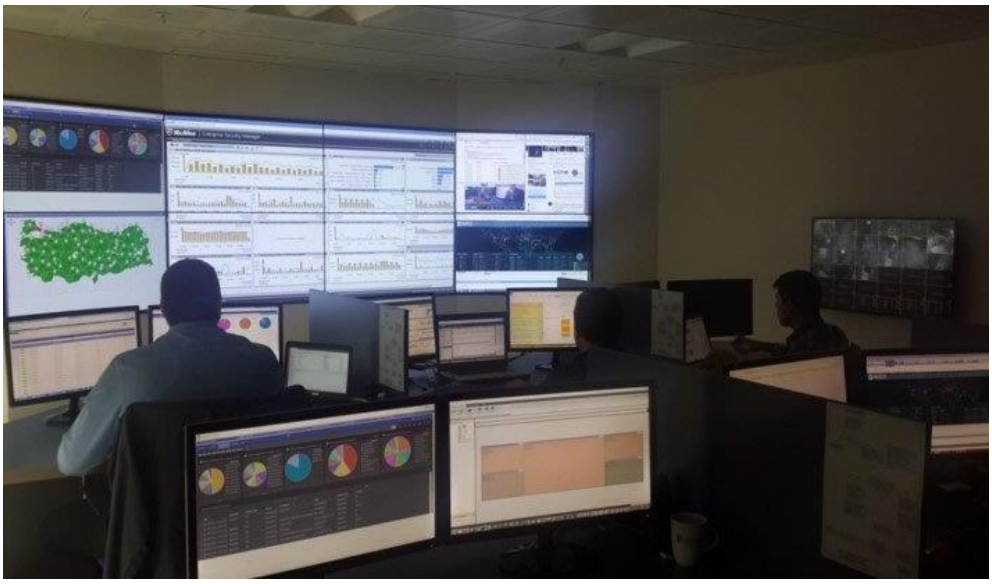
Bilgi Güvenliği Şube Müdürlüğü'nün kurulmasıyla beraber bilgi güvenliği konusunda yapılan çalışmalar hız kazanmış, her yıl bilgi güvenliği farkındalığını artırmak amacıyla BGYS sorumlularına ve İl Bilgi İşlem sorumlularına eğitimler verilmiştir.

Bakanlığımızda bilgi güvenliği konusunda yapılan çalışmalar devam ederken teknolojiyle beraber aynı zamanda siber güvenlik konusunda da çalışmalar yapılmaya başlanmıştır. Bunun en önemli sebepleri;

- Bakanlığımızın CBSGM Bilişim Ağları ve Sistem Yönetimi Daire Başkanlığı ile Yazılım Teknolojileri Dairesi Başkanlığı'nın yönettiği, Merkez ve Taşra Teşkilatının da dahil olduğu bilişim sistemlerinde önemli işlemler yürütülmekte olması,
- Kullanıcı ve çalışanların yapılacak iş ve işlemler için Bakanlık ağ yapısını kullanıyor olması,
- Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda yer alan "Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması" stratejik eylem planı başlığı altındaki "Kurum ve kuruluşlar bünyesinde de sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır" maddesidir.

Bu sebepler dâhilinde siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi, yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesi ve paylaşılması amaçlanmıştır.

Şekil 3.5: ÇŞB SGOM



Hedeflenen bu amaçlar doğrultusunda Bakanlığımızda siber güvenlik konusunda danışmanlık hizmetleri alınmakta; personel ve cihaz ihtiyaçlarını karşılamak, eksiklikleri tespit etmek amacıyla projeler yürütülmektedir.

Yürütülen projelerden ilki, "Bakanlık CBS Altyapısının Kurulması ve Geliştirilmesi Projesi"dir. Bu proje ile siber güvenlik konusunda kurulum ve mevcut altyapı entegrasyonu için hizmet adımları gerçekleştirilmiştir. Bu hizmet adımlarının gerçekleştirilmesi sonunda kurulacak olan yönetim sisteminde güvenlik cihazlarının birbirleriyle uyumlu olması, risk analizi yapabilmesi ve bir siber tehdit oluşması durumunda mevcut güvenlik ürünlerine manuel ve otomatik aksiyon aldırabilmesi hedeflenmektedir.

Network IPS Sistemi, Log Yazılımı Güncelleme Hizmeti, danışmanlık alınan konularla ilgili analiz raporları, SGOM'da çalışan personel için eğitim bu proje kapsamında temin edilen diğer hizmetlerdir.

Log Yazılımı Güncelleme Hizmeti ile birlikte Bakanlık merkez ve taşra teşkilatlarının logları alınmakta ve merkezden uzak bir konumda saklanmaktadır. Saklama işlemi esnasında indeks yapısı kullanılması sonucunda aranan herhangi bir log kısa sürede bulunabilmektedir. Bakanlığımız logları günlük olarak zaman damgası ile mühürlenmektedir. Loglar üzerinde tam metin arama yapılabilmektedir.

"Bakanlık CBS Altyapısının Kurulması ve Geliştirilmesi Projesi" ile yapılan analiz çalışmaları incelenip, değerlendirildikten sonra tespit edilen ihtiyaçlar doğrultusunda siber

güvenlik konusunda yapılan ikinci proje ise “Bakanlık Siber Güvenlik Altyapısı Kurulum Hizmetleri II. Faz Projesi”dir.

Bu proje ile birinci olgunluk seviyesinden ikinci olgunluk seviyesine geçilmesi hedeflenmiştir. Bakanlık olgunluk seviyesi tespit edilirken CoBIT Olgunluk modelinden ziyade danışman firmanın birçok uluslararası doküman sonucunda oluşturduğu kendine özel bir model kullanılmıştır.

Bu proje içerisinde gerçekleştirilen “SGOM İş Gücü Geliştirme Hizmeti” ile beraber SGOM’da çalışan personel sayısının arttırılması hedefi için bir adım atılmıştır. Bu hizmetin gerçekleştirilmesi sonucunda SGOM’da çalışan iki güvenlik operasyon mühendisi ve bir tane güvenlik analisti rollerine ek olarak bir tane baş güvenlik uzmanı (güvenlik mimarı), iki tane güvenlik operasyon mühendisi ve bir tane güvenlik analisti SGOM’da çalışmaya başlamıştır.

Ayrıca bu hizmet karşılığında kurum personelinin SGOM konusunda yetkinliğini arttırmak amacıyla görevlendirilen iki personele eğitim verilmiştir.

Bu çalışmaların devamında Bakanlığımızda güvenlik izleme destek hizmeti için 5 (beş) gün x 8 (sekiz) saat esasına göre güvenlik izleme faaliyeti gerçekleştirildiğinden, bu proje kapsamında yapı 7 (yedi) gün x 24 (yirmi dört) saat izleme gerçekleştirilmektedir. Bu hizmet ile Bakanlığımız izlenmekte, herhangi bir olay yaşanması ya da yaşanma ihtimali olması halinde yetkili SGOM personeli bilgilendirilmektedir. Bu iş ve işlemler rapor halinde hazırlanmakta ve yetkili üst birimlere iletilmektedir. Yetkili SGOM personeli tarafından çözülemeyecek bir olay yaşanması halinde Bakanlığın onayı ile en fazla dört kez olaya müdahale hizmet alınan yetkin firma tarafından sağlanmaktadır.

Bu proje kapsamında her hafta bir gün olmak üzere danışman firmadan gelen uzman kişilerden teknik destek alınmakta, sistemlerle ilgili rutin kontroller gerçekleştirilerek olası bir sorun önlenmektedir.

Bunların dışında, risk analizi yazılımı, ağ ve ağ güvenliği cihazları yedekleme ve konfigürasyon izleme sistemi, olay müdahale ve istihbarat paylaşımı yazılımı, veri tabanı güvenlik duvarı, sınır güvenliği etkinlik analiz sistemi bu proje kapsamında temin edilen sistemlerdir. Bu sistemlerin Bakanlık içerisinde kullanım amaçları aşağıda anlatılmaktadır.

*İz kayıtlarının yapay zekâ ile analizi ve raporlanması* hizmeti yetkin personel tarafından seçilen algoritma ile çalışmaktadır. Ürünün kabulü aşamasında bir kez anomali tespiti gerçekleşmiştir. Anomali gerçekleşmeden en az beş dakika öncesine kadar tespit yeteneği mevcuttur. Bakanlığın SGOM işletilmesi ve yürütülmesi çalışmaları kapsamında ilerleyen aşamalarda bu sürenin yetkili firma tarafından bir dakikaya düşürülmesi hedeflenmektedir. Bu yazılım, istenen cihaz ya da ürünlerden toplanan logları belirtilen

algoritma ile inceleme; incelenen logların belirli bir eşik değerinin üzerine çıkması sonucunda anomali olarak belirleme; en son adımda da saldırı olma ihtimalini değerlendiriyor. Bu sistem geliştirme aşamasında olduğu ve yatırım amaçlı olarak temin edildiği için Bakanlık SGOM'da etkin bir şekilde kullanılmamaktadır.

*Risk analizi yazılımı*, cihazlar üzerinde yazılı olan mevcut kuralları inceleyerek, kurallar üzerinde iyileştirmeler önermektedir. Ayrıca güvenlik cihazlarının konfigürasyonlarında mevcut olan bozuklukları da düzeltmektedir. Bakanlıkta kullanılmaya başlamasıyla beraber sayısız güvenlik duvarı kuralında iyileştirme gerçekleştirmiştir. Böylece konfigürasyon uyumluluğu artmıştır.

*Ağ ve ağ güvenliği cihazları yedekleme ve konfigürasyon izleme sistemi* ile Bakanlığın sahip olduğu güvenlik cihazlarının konfigürasyonları merkezi olarak yedeklenmektedir. Yedekten geri dönüş testleri mevcut olup, Bakanlıkta alınan cihaz konfigürasyonları için yedekten geri dönme işlemi yapılmamaktadır. Yapılan araştırmalar sonucunda küçük bir ihtimalde olsa alınan yedeklerden geri dönülememe işlemleri yaşanmıştır. Bu durumda geri dönüş testleri uygulanması önem arz etmektedir.

*Olay müdahale ve istihbarat paylaşımı yazılımı*, gelişmiş saldırı savunma sistemi ile entegre bir şekilde çalışmaktadır. Olay müdahale ve istihbarat paylaşımı yazılımı sistemde tarama işlemi yapar, herhangi bir zararlı tespiti yaparsa bunu gelişmiş saldırı savunma sistemine gönderir ve inceleme yaptırır. Eğer bu sistem zararlı olarak kabul etmezse yetkili SGOM personeli tarafından incelenir. Bu işlemlerin herhangi birinde zararlı olduğu kabul edilirse Bakanlık merkez ve taşra teşkilatı olmak üzere bütün bilgisayarlarda bu zararlıyı engeller. Bu yazılım henüz bütün Bakanlık bilgisayarlarına uygulanamamaktadır. Yaygınlaştırma işlemleri için çalışmalar devam etmektedir.

*Veri tabanı güvenlik duvarı*, veri tabanı sorguları, şifrelenmiş trafik analizi, çevrimiçi ağ dinleme, sorgu trafiği, anomali tespiti gibi işlemler yapabilmektedir. 2017 yılının ikinci yarısı faaliyete geçmiştir. Henüz gerçek faaliyetini gerçekleştirememekte, dinleme modunda çalışmaktadır.

*Sınır güvenliği etkinlik analiz sistemi*, zafiyet tarama ve penetrasyon testlerini destekler nitelikte bir yazılımdır. Dış sunucudan Bakanlık altyapısına saldırı yaparak Bakanlık altyapısında herhangi bir açıklık olup olmadığını tespit etmekte ve yetkili kişilere raporlamaktadır. 900 farklı atak imzası kullanmaktadır.

Bu proje kapsamında SGOM Test ve Denetim Hizmetleri çerçevesinde sızma testi, DDoS testi, kablosuz ağ testi ve sosyal mühendislik testini içeren güvenlik testleri, kırmızı takım tatbikatları gerçekleştirilecektir.

Sızma testleri 15 kritik Bakanlık uygulaması için gerçekleştirilmiş olup testler sonucunda hazırlanan raporlar ilgili birimlerle paylaşılmış ve gerekli önlemlerin alınması için çalışmalar başlatılmıştır. Bu test yapılırken hizmet alınan firmanın kendine özel geliştirmiş olduğu test metodolojisi kullanılmıştır. Bu testlerin sonucunda SQL injection zafiyeti, güncel olmayan jQuery versiyonu, güncel olmayan sunucu yazılımları gibi açıklıklar tespit edilmiştir.

Sosyal mühendislik testi, 300'ü Merkez Teşkilatı Personeli ve 300'ü de Taşra Teşkilatı Personeli olmak üzere 600 kişi üzerinde gerçekleştirilmiştir. Kırmızı takım tatbikatları çerçevesinde yapılacak sosyal mühendislik testi de bu altı yüz kişiden farklı olan yüz kişi üzerinde farklı bir senaryo üzerinden gerçekleştirilecektir. Kırmızı takım tatbikatlarının yapılması için ise çalışmalar devam etmektedir.

Bu proje içerisinde yer alan eğitimlerden Siber Güvenlik Yetiştirme Programı, Siber Güvenlik Rol Bazlı Eğitimlerin bir kısmı, Bakanlık SGOM personeline verilmiş olup eğitimler devam etmektedir. Yöneticiler için Siber Güvenlik Farkındalık Çalışmaları konusunda eğitim ise üst düzey yirmi yöneticiye bir günlük bilinçlendirme eğitimi olarak verilmiştir.

SGOM yapısı içerisinde birçok iş ve işlemde rutin bir şekilde devam etmektedir. Bu iş ve işlemler, SGOM yapısında bulunan diğer sistemler ve Bakanlık içerisindeki işlevleri aşağıda anlatılmaktadır.

Bakanlık SGOM içerisinde yapılandırılan SIEM güvenlik, network ve sistem cihazları, Bakanlık uygulamaları olmak üzere 101 farklı varlıktan log almaktadır

SIEM ile 109 adet özel ve 25 adet Bakanlığımıza özel korelasyon oluşturulmuş olup; uluslararası kurum ve kuruluşlar, hizmet alınan firmalar ile danışman firmanın ARGE ekibi gibi kaynaklardan alınan 400'den fazla korelasyon ile çalışmaktadır.

Bakanlığımıza özel korelasyonlardan bazıları, mesai saatleri dışında yapılan uzaktan bağlantılar, aynı web adresine fazla istekte bulunulması, bir bilgisayardan birden fazla oturum açılması, yetkili bir kullanıcının hesabının kilitlenmesi, herhangi bir kullanıcının "domain admin" grubuna eklenmesi veya benzeri yetki gruptan çıkartılmasıdır. Oluşan bu korelasyonlarla ilgili yetkili kişilere e-postalar gelmektedir.

SIEM ile sızılmış uygulamalar, güvenlik açıklıkları, tespit edilmemiş virüsler ve birçok varsayılan parola içeren sistem tespit edilmiştir.

Zafiyet tarama sistemi Bakanlığımızda 2017 yılı itibariyle etkin bir şekilde kullanılmaktadır. Yaklaşık 8.000 zafiyet tespit edilmiştir. Bu zafiyetler ilgili Bakanlık Birimlerine bildirilmiş olup, kapatılması ile ilgili gerekli çalışmalar devam etmektedir.

Zafiyet tarama sistemi hafta sonu gece yarısı çalışacak şekilde iki farklı tarama görevi ile çalışmaktadır. Bakanlığımızda mevcut olan zafiyet tarama sistemi sunucu bazında tarama işlemi gerçekleştirmektedir. Web uygulamaların tarama işlemi ise Bakanlık tarafından yapılamamaktadır. Bu eksikliğin giderilmesi için çalışmalar yapılması gerekmektedir.

Gelişmiş tehdit savunma sistemi, e-posta güvenlik sistemi, WAF, olay müdahale ve istihbarat paylaşımı yazılımı ile birlikte çalışmaktadır. E-posta güvenlik sistemine gelen eklerin zararlı yazılım içerip içermediğini kontrol etmektedir.

Anti virüs ve son kullanıcı yönetimi merkezi olarak gerçekleştirilmekte olup, son kullanıcıların anti virüs ile ilgili işlemlere müdahale etmesi mümkün değildir. Acil durumlarda, yetki verilen Kurum personeli ile Bakanlık Merkez Binasının bulunduğu ilin dışında bulunan yerlerde Bakanlığın hizmet aldığı firmaların sisteme uzaktan bağlanmasını sağlayan bir yazılım kullanılmaktadır.

Envanter Belirleme Sistemi ile Bakanlık ağında yer alan sistemlerin tespiti yapılmaktadır. 176 sistemin sahiplik kaydına ulaşılmış olup, 297 adet sistemin sahiplik bilgisine henüz ulaşılamamıştır. Bu sistemler, Bakanlık sunucu ağlarında çalışmakta ve hizmet vermekte olup ancak ne iş yaptıkları ve sahipleri tam olarak bilinmemektedir. Aynı şekilde ağ cihazlarının aktif olup olmadığını ve envanter takibini yapan bir sistem daha SGOM içerisinde yapılandırılmıştır. Bu sistem Bakanlıkta bulunan birçok sistemden performans ve erişilebilirlik verileri toplamaktadır.

Bakanlık WAF sisteminde *Beyaz Liste Modeli* kullanılmaktadır. Böylece sadece engellenmek istenen sistemler için kurallar yazılmış olup, engellenen siteler hariç bütün sitelere erişim sağlanabilmektedir.

Bakanlık e-posta güvenlik sistemi, e-posta adreslerine gelen e-postalarda zararlı yazılım kontrol taraması yaparak; zararlı yazılım içeren ekler, program parçacıkları ve şifrelenerek sıkıştırılan ekleri engellemekte ve son kullanıcılara göndermemektedir. Spam e-postaların geldikleri adres tespit edilerek bu sitelerden e-posta gelmesi de engellenmektedir.

Bakanlığımızda e-posta güvenlik sistemimiz yedekli bir şekilde çalışmaktadır.

Güvenlik cihazları ile yapılan koruma dışında SGOM yapısının gerektirdiği iyileştirmeler yapılarak da Bakanlığın dış dünyaya karşı güvenliği artırılmaya çalışılmaktadır.

Bu iyileştirmelerden biri, 2017 yılında yapılmaya başlanan ve tamamlanan segmentasyon çalışmasıdır. Bu işlem sonunda backbone da sona eren trafik güvenlik duvarında sonlandırılarak iç ağı izleme imkânı sağlanmıştır. Böylece iç ağda gerçekleşen anormal hareket ve olaylardan haberdar olunacaktır. Aynı zamanda TS/ISO IEC 27001 standardı tarafından istenilen ağların ayrımı, ağlar arası kontrol ve kayıt altına alma işlemleri

de gerçekleşmiş olacaktır. Bu çalışma makro düzeyinde bir segmentasyon olup mikro düzeyinde bir segmentasyon yapılması gerekmektedir.

TS/ISO IEC 27001 Bilgi Güvenliği Yönetim Sistemi faaliyetleri çerçevesinde standardın kurulması, idame ettirilmesi ve izlenmesi faaliyetleri gerçekleştirilmiş; Bakanlık çalışanlarının bilgi güvenliği ve siber güvenlik konularında bilgilendirilmesi ve farkındalığın artırılması hususlarında gerekli çalışmalar yapılmış; Üst yönetim desteğinin önemi göz önüne alınarak yöneticiler içinde farkındalık eğitimleri verilmiş ve denetim aşaması sonucunda TS/ISO IEC 27001 sertifikası kapsam dâhilindeki Yazılım Teknolojileri Daire Başkanlığı ve Bilişim Ağları ve Sistem Dairesi Başkanlığı olmak üzere iki Başkanlık için alınmıştır.

USOM tarafından bildirilen 200 IP, SIEM üzerinden kara listeye alınmıştır. USOM'dan gelen bütün bildirimler ve uyarılar dikkatle incelenerek hemen uygulama aşamasına geçilmiştir.

Hizmet alımı ile gerçekleşen yazılımlar için şartnamede mutlaka güvenlik testlerinin yapılması istenmekte, Bakanlık tarafından uygulama için yapılan testler sonucunda tespit edilen açıklıkların firma tarafından kapatılması istenmektedir. Bakanlık kendi geliştirdiği yazılımlar içinde gerçek ortama almadan önce testler yapmakta veya yaptırmaktadır.

Bakanlığımız SGOM yapısının kurulmasıyla beraber olayları daha etkin bir şekilde gözlenmeye başlamıştır. Bu olaylardan bazıları;

2017 yılı içerisinde iki kez Bakanlığımıza DDoS atağı gerçekleşmiştir. Alınan DDoS hizmeti sayesinde ataklar zamanında önlenmiş olup, herhangi bir olumsuz durum yaşanmamıştır. DDoS atakları dışında 4 kez SQL injection, 2 kez yetkisiz elektronik mektup kullanımı, flash belleğin bilgisayara takılması sonucu bilgisayarlara zararlı yazılımın bulaşması ve sayısız sömürü atak girişimi gerçekleşmiştir. Bu IP ler kara listeye alınarak engellenmektedir. Bazı cihazların bilgi güvenliği ve siber güvenlik farkındalığı eksikliğinden dolayı bazı cihazlarda varsayılan (default) parola bırakıldığı ve sonucunda açıklıklar oluşturduğu tespit edilmiştir.

Güvenlik ihlal olayları gerçekleştiğinde Bilgi Güvenliği Yönetim Sistemi çalışmaları kapsamında oluşturulan dokümanlardan biri olan CSB.BGYS.SR.01_OlayYönetimiSüreci prosedür adımları takip edilerek müdahale edilir. Ayrıca ihlal olayları dışında özel durumları işlemek maksadıyla politika, prosedür, form, talimat yine Bilgi Güvenliği Yönetim Sistemi çalışmaları kapsamında hazırlanmıştır.

Tablo 3.2: ÇŞB SGOM Değerlendirme

| SGOM'da Olması Gerekenler | ÇŞB Mevcut Durum |
|---|---|
| Güvenlik Duvarı | Var |
| IPS/IDS | Var |
| E-posta Güvenlik Sistemi | Var |
| Web Uygulama Güvenlik Duvarı | Var |
| Kayıt Toplama Sistemi | Var |
| Bilgi Güvenliği ve Olay Yönetimi | Var |
| İçerik Filtreleme Sistemi | Var |
| Anti virüs | Var |
| Sızma Testleri (En az yılda bir kez) | Yapıldı |
| İletişim dokümanları | Var |
| Yazılı bilgi ve dokümanlar (Prosedürler, cihazların çalışma talimatları vb.) | Var |
| Kontrollü giriş-çıkış uygulaması | Personel tarafından parmak izi kullanılmaktadır. Ziyaretçiler refakatçi eşliğinde girmekte olup, ziyaretçi defterine kaydı yapılmaktadır |
| Dışardan gözlemlenememesi | Bakanlığımızda kritik sistemlerin bulunduğu alanlar dışardan izlenebilmektedir |
| Kritik sistemlerin bulunduğu alanların kamera ile kayıt altına alınması | Kritik sistemlerin bulunduğu alanlarda kameraların sayısı ve görüş açıları uygundur |
| Farkındalık | Eğitim, broşür, afiş gibi materyallerle farkındalık yaratılmıştır |
| 7x24 izleme sistemi | Firma aracılığıyla sağlanmaktadır |
| Eksiksiz veri envanteri ve durumları | Veri envanteri mevcut olup, eksiklikler kapatılmaya devam etmektedir |
| Yetki tanımlamaları ve düzenli kontroller | Yetki tanımları mevcuttur. Düzenli kontrollerle ilgili yapılan işlemler devam etmektedir |
| Yedekleme ve geri dönüş testlerinin uygulanması | SGOM cihazlarının yedekleri alınmakta, geri dönüş testlerinin nasıl yapılacağına dair bir doküman mevcut bulunmakta; fakat geri dönüş testleri yapılmamaktadır |
| Ekran izleme faaliyetleri | Olması gereken düzeyde değildir |

## III.5. Örnek İki Kurumun SGOM Çalışmaları

Bu çalışma kapsamında 2 farklı kurumun SGOM'u ziyaret edilmiş olup, kurumların isimleri güvenlik dolayısıyla paylaşılmamaktadır.

Birinci Kurumu ziyaret edilmiş, siber güvenlik hakkındaki görüşleri, yaptıkları çalışmalar üzerine bilgiler edinilmiştir. Bu ziyaret sonucunda kurumun SGOM yapısı hakkında alınan bilgiler aşağıda yer almaktadır.

Ziyarette bulunduğum kurum, SGOM yapısının efektif bir şekilde çalışması için bilgi güvenliği ve siber güvenlik farkındalığının en üst düzeyde olması gerektiğine dair farkındalığa sahiptir. Bu nedenle farkındalık çalışmalarına aşırı önem ve öncelik vermektedir. Farkındalığı arttırmak içinde her ay siber güvenlik bülteni çıkartmaktadır. En son 9. sayılarını çıkartmıştır. Siber güvenlik bülteni son kullanıcılara e-posta ile gönderilmekte ve intranet sayfalarında yayımlamaktadır.

Siber güvenlik ekipleri iki haftada bir toplanarak genel değerlendirme gerçekleştirmektedir. Bu toplantıda kurumda hangi olaylar gerçekleşmiş, bu konuda ne gibi çalışmalar yapılabilir gibi konular görüşülmekte, USOM ve benzer kuruluşlardan gelen belgeler incelenmekte ve ortak bir karar alınmaktadır.

Usb gibi cihazlarla veri kaçırmayı önlemek ve kurum bilgisayarlarına zararlı yazılım bulaştırmayı engellemek için özel bir yazılım kullanmaktadırlar. Böylece bilinçsiz bir kullanıcının kurum bilgisayarlarına herhangi bir zararlı yazılım yüklenmesinin önüne geçilmektedir.

Veri tabanı güvenlik duvarını aktif bir şekilde kullanmakta ve temel bir siber güvenlik yapısı için veri tabanı güvenlik duvarının mutlaka kullanılması gerektiğini savunmaktadır.

Ekran izleme işlemi ile 81 il dâhil olmak üzere 500 adet noktayı takip edilmektedir. Bu izleme ile ağ bağlantılarını kontrol etmekte; yazılımların performansları, çalışıp çalışmadıkları, yazılımın sorguya ne kadar sürede cevap verdiği gibi bilgiler ve SIEM çıktıları gözlemlemektedir. 7 gün x 24 saat sistemi kurum personeli ile sağlanmakta olup üç vardiyalı olarak çalışmaktadır. Her vardiyada üç personel yer almaktadır. Kurum tarafından dış kaynaklı personele olumlu bakılmamaktadır.

Bütün bilişim kadrosu tamamen kadrolu personelden oluşmakta, firma personeli yer almamaktadır.

Siber güvenlikle ilgili yaptığı çalışmalara başlarken danışmanlık hizmetine başvurulmamış olup, kadronun bilgi ve becerisinden yararlanılmıştır.

Sistemlerde yer alan admin kullanıcılarının ekran görüntülerinin 7x24 kaydedildiği bir yazılım kullanmaktadırlar. Siber güvenlik konusunda herkes suçlu olabilir ya da herhangi bir hata yaşanma olasılığı her zaman mevcuttur. Bu nedenle üst düzey yetkilere sahip kullanıcıların yaptıkları işlemler mutlaka kayıt altına alınmalı, gerekli durumlarda incelenmelidir.

Güvenlik testleri yılda 2 defa yapılmaktadır. İki ayrı firmaya yaptırılarak testlerin doğruluğu kontrol edilmektedir. Ayrıca yazılıma ait kaynak kodlarının statik ve dinamik testleri kurum personeli tarafından yapılmaktadır. Yazılan bütün uygulamalar için yük testi, performans testi, güvenlik testleri siber güvenlik ekibi tarafından yapılmaktadır.

Yapılan ve yaptırılan güvenlik testleri sonucunda çıkan zafiyetler için eylem planı oluşturulmaktadır. Bu eylem planı Genel Müdüre onaylatılmakta ve bütün birimlere gönderilmektedir. Herkes belirlenen zaman aralığında kendi üzerine düşen işlemi gerçekleştirmektedir.

Segmentasyon mikro düzeyde gerçekleştirilmektedir. Tek bir sunucu önünde firewall yer almaktadır. Böylece sunucunun herhangi birini ele geçiren saldırgan diğer sunuculara geçememektedir.

Kamu.net'e geçen ilk kurumlardan biridir.

Organizasyon yapısı, üst düzey yetkililerin desteği kurumda oluşmuş durumdadır. Personel çalışma şartlarının iyileştirilmesiyle ilgili imkânlar (örneğin Sosyal faaliyetler, her kişiye 10 metrekare olmak üzere hobi bahçeleri vb.) üst düzeydedir.

Kurum personelinin gelişme ve yetişmesine önem vermekte ve eğitimler, seminerler, toplantılar ve güvenlik ile ilgili organizasyonlara kurum personelinin katılımını sağlamaktadırlar.

Sistemi efektif bir şekilde yürütebilmek için yeterli personel sayısına sahiptir.

SGOM konusunda küçük ve emin adımlarla giderek zaman içerisinde etkin bir SGOM olmayı hedeflemektedir.

İkinci kurum ile yapılan görüşme sonunda alınan bilgiler;

7 gün x 24 saat izleme sistemi kurumun kendi personeli tarafından iki vardiyalı olarak gerçekleştirilmektedir. İzleme sisteminde e-devlette mevcut olan uygulamaları, klima ve soğutma sistemlerini, taşra teşkilatı ile yapılan uzaktan erişimleri ve ethernet bağlantılarını izlemektedirler. Herhangi bir sorunla karşılaşılması durumunda ilk müdahale izleme ekibi tarafından yapılmakta, sorun çözülemiyorsa ilgili birime gönderilmektedir.

Olay müdahale yapısı bir sistemle izlenmekte, olaya müdahale edilip edilmediği, kimin bu olayı tetiklediği takip edilmektedir.

SGOM yapısı izleme ekibi, güvenlik test ekibi, güvenlik ürünleri ekibi, bilgi güvenliği ekibi ve ağ ekibinden oluşmaktadır.

Kurumda personel eğitimine önem verilmekte, ekiplere uzmanlıklarına göre eğitimler sağlanmaktadır. Güvenlik test ekibindeki personele TSE sızma testi uzmanı, OWASP gibi eğitimler; bilgi güvenliği ekibine baş tetkikçi, sertifika eğitimleri; güvenlik ürünleri ekibine ürün yönetim eğitimleri verilmektedir.

Son kullanıcılar için farkındalık eğitimleri periyodik olarak verilmekte, bunun dışında afiş, e-posta bilgilendirme ve bilgisayar oturum açma ekranı bilgilendirme gibi çalışmalarda sürdürülmektedir.

SGOM yapısı içerisinde yedekli ayrıştırılmış güvenlik duvarları, IPS-IDS sistemleri, DDOS önleme hizmeti ve ürünleri, end-point protection ürünleri, siber istihbarat ürünleri, kaynak kod analiz ürünleri, güvenlik testi ürünleri, risk yönetim yazılımı, monitoring ürünleri, olay yönetim ürünleri, e-posta güvenlik ürünleri ve malware yönetim ürünleri mevcuttur.

Güvenlik testlerinin de güvenlik ürünlerinin kullanımı kadar kritik olduğu düşünülmektedir. Bu nedenle kritik uygulamalar devreye alınmadan önce güvenlik testi kurum personeline yaptırılmaktadır. Ayrıca kurum dışından yılda bir periyodik güvenlik testi hizmeti alınmaktadır. Kurum içi personele de periyodik kritik uygulamaları test etmektedir. Sorumlu birime rapor teslim edilmekte ve onlar tarafından kapatma işlemini koordine etmektedir.

Veri tabanı güvenlik duvarı henüz kullanılmamakta olup, kullanılması için gerekli çalışmalar sürdürülmektedir.

Tablo 3.3: Kurumlar ve Bakanlık Karşılaştırma

| Kurum 1 | Kurum 2 | Bakanlık |
|---|---|---|
| Kurum personeli eğitimlere gönderilerek yetiştirilmektedir. | Kurum personeli eğitimlere gönderilerek yetiştirilmektedir. | Firma personeli ve kurum personeli yetiştirme eğitimlerine gönderilmektedir. |
| Bilgisayarlara zararlı yazılım bulaştırmamak ve veri sızıntısını önlemek amacıyla özel bir yazılım kullanmaktadır. | Bu konuda bir önlem bulunmamaktadır. | Bu konuda bir önlem bulunmamaktadır. |
| Veri tabanı güvenlik duvarı aktif bir şekilde kullanılmaktadır. | Veri tabanı güvenlik duvarı mevcut değildir. | Veri tabanı güvenlik duvarı dinleme modunda çalışmaktadır. |
| Ekran izleme işlemi performanslı bir şekilde yapılmaktadır. | Ekran izleme işlemi performanslı bir şekilde yapılmaktadır. | Ekran izleme işlemi efektif bir şekilde yapılmamaktadır. |
| 7 gün x 24 saat hizmeti kurum personeli ile sağlanmaktadır. | 7 gün x 24 saat hizmeti kurum personeli ile sağlanmaktadır. | 7 gün x 24 saat hizmeti hizmet alımı yöntemiyle sürdürülmektedir. |
| Bütün bilişim kadrosu tamamen kadrolu personelden oluşmaktadır. | Bütün bilişim kadrosu tamamen kadrolu personelden oluşmaktadır. | Firma personeli ve danışman firma ağırlıklıdır. |
| Admin rolüne sahip kullanıcılarının ekran görüntülerinin 7 gün x 24 saat kaydedildiği bir yazılım mevcuttur. | Buna benzer özel bir yazılım kullanılmamaktadır. | Buna benzer özel bir yazılım yoktur. |
| Güvenlik testleri yılda 2 kez yaptırılmaktadır. | Güvenlik testleri yılda bir kez yaptırılmaktadır. | Güvenlik testleri yılda bir kez yaptırılmaktadır. |
| Yeterli personel sayısına sahiptir. | Personel alınacaktır. | Personel alınacaktır. |
| Farkındalık çalışmaları yapılmaktadır. | Farkındalık çalışmaları yapılmaktadır. | Farkındalık çalışmaları yapılmaktadır. |

# V. GENEL DEĞERLENDİRME, SONUÇ VE ÖNERİLER

İnsanoğlunun dünya üzerindeki yaşamı bilgiyi keşfetmesi ve onu kullanması ile doğru orantılı olarak gelişmiştir. Örnek olarak, doğa olayları hakkında bilgisi arttıkça ona karşı önlem alması, doğal kaynakları kendi ihtiyaçları doğrultusunda değerlendirmesi ve kendi refahı için nasıl kullanacağını öğrenmesi verilebilir.

Bu noktada, Francis Bacon "bilgi tek başına güçtür (Latincesi: ipsa scientia potestas est) ve bilmek doğaya egemen olmaktır." diyerek bu gelişimi özetlemiştir. Francis Bacon'un söylediği sözden anlaşılacağı üzere bilginin insan hayatı için önemli bir kavram olduğu söylenebilir.

Fakat teknolojinin gelişmesiyle beraber bilgi toplumuna geçen insanoğlu için bilginin erişiminin kolaylaşması, kullanımının toplumun tüm kesimlerine yaygınlaşması ile birlikte önemi gittikçe daha fazla artmaya başlamıştır. Böylece kolay erişilen ve kullanılan bilginin önemi arttıkça buna bağlı olarak bilgi güvenliğinin de günlük hayatımızda öneminin arttığı ifade edilebilir.

Bilgi Güvenliği kısaca bilginin sahip olduğu değerlerin korunması olarak kabul edilirse, bilginin güvenliği noktasında en temel husus olan, bilgi güvenliğini sağlamanın yolunun yine bilgi ile olabileceği söylenebilir.

Bu çerçevede, bilgi güvenliğinin sağlanması için bilginin tam olarak tanımlaması ve buna göre adım atılması gerektiği belirtilebilir.

Bilgi güvenliğini sağlamak isteyen ilgili kurum ve kuruluşlarda, bilgi güvenliğinin tüm hususlarını içeren bir BGYS yapısını kurulmalıdır.

Bu yapıyı oluşturmak için atılacak ilk adım, üst yönetim desteğidir. Üst yönetimin, kuruluşun hedefleri arasına bilgi güvenliğini sağlama prensibi doğrultusunda bu konuda bütçe ve zaman ayırması da önemli bir husustur.

İlerleyen aşamalarda bilgi güvenliği konusunda kullanıcı farkındalığı oluşturma, varlıkları belirleme, varlıkların sahip olduğu zafiyetleri ve varlıklara karşı tehditleri tespit etme, riskleri ortaya çıkarma işlemleri yapılır. Riskleri belirledikten sonra ne konuda önlem almamız gerektiği ve alınacak önlemler konusunda yapılması gereken planlar belirlenir. Bu planlar çerçevesinde kullanıcıların destek alması ve kullanması için dokümanlar hazırlanabilir.

Günümüzde yalnız bilgi güvenliğini uygulamak, bilginin korunması için yeterli değildir. Elektronik ortamın hayatımıza girmesiyle birlikte bilgi farklı bir ortama taşınmış ve bu yapı da siber güvenlik kavramının ortaya çıkmasına sebep olmuştur.

Siber güvenlik, siber uzayda meydana gelen kullanıcı hatasına ya da kötü niyetli kişilerin hedefleri doğrultusunda gerçekleşen siber saldırılara yönelik yürütülen çalışmalar (değerlendirme, test, danışmanlık, eğitim vb.) olarak tanımlanabilir.

Bilgi güvenliği ve siber güvenlik birbirine bağlı iki kavramdır. İki kavram da bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasını amaçlamaktadır. Buna karşın daha geniş bir kavram olarak bilgi güvenliği, kâğıt ortamında yer alan bilginin güvenliğinden de sorumlu iken, siber güvenlik ise sadece ağda gerçekleşen ihlal olaylarını kapsadığı belirtilebilir.

Siber güvenliğin önemini daha iyi anlamak için geçmişten günümüze gerçekleşen siber olaylara bakmak yeterli olacaktır. Yapılan siber saldırılar sonucunda milyonlarca kullanıcı bilgisi çalınmış, ülkelerin devlet sistemleri hizmet veremez duruma gelmiş, ülkeler arası savaşlar bir tek silah bile kullanmadan siber güce sahip devletlerin zaferiyle sonuçlandığı hatırlanabilir.

Gerçekleşen bu olaylarda sadece maddi kayıplar oluşmamış, itibar zedelenmesi, insanların güvenlerinin yitirilmesi gibi birçok manevi kayıpta yaşanmıştır. Bu nedenle ülkeler bu konuda ciddi çalışmalar yapmaya başlamıştır. Türkiye'de bu ülkeler arasında yerini almaya çalıştığı yapılan çalışmalar kapsamında vurgulanabilir.

Türkiye'de bu konuda atılan ilk adım 2003/10 sayılı Başbakanlık Genelgesidir. Bu genelgeyi ilgili kuruluşların oluşturulması, toplantılar, siber güvenlik tatbikatları, hukuki alanda yapılan çalışmalar, ülkeler arası imzalanan sözleşmeler, eylem planlarını takip ettiği söylenebilir.

Bu çalışmalar arasında yer alan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda yer alan "Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması" stratejik eylem planı başlığı altındaki "Kurum ve kuruluşlar bünyesinde de sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır" ibaresi kuruluşlarda SGOM kurulmasını gerektiği ve bu kapsamda gerekli çalışmaların hızlandığı belirtilebilir.

SGOM, 7 gün x 24 saat izleme ve müdahale prensibine göre çalışan, konusunda uzman personelden oluşan, bilişim alt yapısının oluşabilecek ihlallere karşı korunması amacıyla kurulan, kuruluş bünyesinde yer alan özel bir alan olarak tanımlanabilir.

SGOM kurulurken ilk adım bilgi güvenliği yapısını oluşturmada da olduğu gibi üst yönetim desteğidir. Kuruluşun amaçları içerisinde siber saldırılara karşı önlem almak, kullanıcı farkındalığı yaratmak, siber güvenlik kültürü oluşturmak düşüncesi yer alıyorsa; üst

yönetim tarafından bütçe ve zaman ayrılarak bu konuda çalışmalara başlanmasının büyük önem arz ettiği tekrarlanabilir.

SGOM yapısı için önemli olan konular, SGOM'da çalışacak personel, kullanılacak cihazlar, yapılacak testler ve uygulanması gereken planlardır. Bunların hepsinin uyum içerisinde olması ve birbirini tamamlaması uygun olabilir.

SGOM'da çalışacak personelin, siber güvenlik konusunda bilgi sahibi olan, bu konuda ulusal ve uluslararası güncel olayları takip ederek kendini sürekli geliştiren, uzman kuruluşlar tarafından onaylı sertifikalara sahip olan, uygulamalı sınavlarda başarılı olan kişilerden oluşması SGOM'un sürdürülebilmesi için daha uygun olur.

SGOM içerisinde kullanılacak cihazlar, kuruluşun sahip olduğu varlıklar, kullanıcılar, çalışan personel, kritik alt yapı seviyesi gibi faktörler göz önüne alınarak değerlendirilir, ihtiyaçlar doğrultusunda gerekli cihazların temin edilmesi uygun olacaktır.

SGOM içerinde kullanılması gerekli cihazlara örnek olarak ihtiyaçlar dâhilinde güvenlik cihazı, WAF, veri tabanı güvenlik duvarı, IPS ve IDS, ağ izleme cihazı, zafiyet tarama sistemleri, kayıt yönetim sistemi, anti virüs, e-posta güvenlik sistemi, veri kaçağı önleme sistemi, içerik filtreleme sistemi, bal küpü, SIEM, yük dengeleyici, ağ erişim kontrol sistemi, yedekleme sistemi verilebilir.

SGOM'un sağlıklı bir şekilde yürütülmesi için gerekli olan planlar şu şekilde belirtilebilir. Siber güvenlik konusunda yapılan ulusal ve uluslararası bütün çalışmaların izlenmesi, güncel siber saldırıları ve yöntemlerinin takibi, yılda en az bir kere güvenlik testlerin yapılması, kuruluş içerisinde gerçekleşen siber olayların incelenip analiz edilmesi, kullanıcı farkındalığının oluşturulmasıdır.

Bakanlığımız 2014 yılında bilgi güvenliği çalışmalarının devamında siber güvenlik konusunda da çalışmalara başlamıştır. Kullanıcı farkındalığı oluşturmak adına her yıl BGYS sorumlularına ve İl Bilgi İşlem Sorumlularına eğitimler verilmektedir. Bilgi güvenliği ve siber güvenlik konusunda danışmanlık hizmetleri alınmakta; personel ve cihaz ihtiyaçlarını karşılamak, eksiklikleri tespit etmek amacıyla projeler yürütülmektedir.

Yürütülen "Bakanlık CBS Altyapısının Kurulması Ve Geliştirilmesi Projesi" ve "Bakanlık Siber Güvenlik Altyapısı Kurulum Hizmetleri II. Faz Projesi" kapsamında yapılan analiz çalışmalarının değerlendirilmeleri sonucunda ortaya çıkan eksiklikler giderilmeye çalışılmalıdır.

# ÖNERİLER

Bakanlığımız tarafından siber güvenlik konusunda yapılması gereken çalışmalara devam edilmektedir.

Bu çalışmalar kapsamında, yapılması gereken faaliyetlerden biri, Bakanlığımız çalışanlarında bilgi güvenliği ve siber güvenlik konularında farkındalık oluşturmaktır. Farkındalık oluşturma eylemine üst yönetimden başlamak doğru bir karar olacaktır. Üst yönetimin bu konularda bilgisi arttıkça personelini de bu konuda yönlendirecek, Bakanlıktaki farkındalık konusundaki eksiklikler daha hızlı bir şekilde giderilecektir.

Buna ek olarak, Bakanlık SGOM'un daha efektif bir şekilde yürütülebilmesi için nitelikli personel sayısının arttırılmasının sağlanmasıdır. Sürekli gelişen ve değişen siber güvenlik alanında konusunda uzman personelin varlığı Bakanlığın bu konudaki çalışmalarına katkı sağlayacaktır.

Bakanlık içerisinde çoğu sistem ve uygulama için test ortamı mevcut değildir. Test ortamları yapılacak herhangi bir değişikliğin canlı sistemde yapılmasının önüne geçmekte ve yaşanabilecek herhangi bir sorun sonucunda iş sürekliliğinde kesinti yaşanmasını engellemektedir. Bu nedenle Bakanlık içerisinde gerçekleşen iş ve işlemlerde kesinti yaşanma ihtimalini en aza indirmek için test ortamlarının kurulması yarar sağlayacaktır.

Logların taşra teşkilattan toplanması ve Bakanlık Merkez Teşkilattan log merkezine gitmesi işlemleri sırasında loglar text metin olarak karşıya gönderilmelidir. Bu işlem sırasında saldırganın akan verilere ulaşması sonucunda Bakanlık ile ilgili birçok veriye sahip olma ihtimali mevcuttur. Bu nedenle gönderilen logların şifreli bir şekilde iletilmesi güvenliği artıracaktır.

Bilinçsiz kullanıcılar tarafından takılan ve zararlı yazılım içeren harici bellekler kurum bilgisayarlarına ve hatta bazen kurum ağına zarar vermektedirler. Bakanlık içerisinde kullanılacak olan harici belleklerin kurum bilgisayarlarında kullanılmasını engelleyecek bir sistem bu sorunun yaşanma ihtimalinin önüne geçecektir.

Süreç ve sistemlerde içerisinde yer alan kritik işlemlerin tek bir personel ya da destek hizmeti kuruluşu tarafından yönetilmemesi herhangi bir problem ile karşılaşıldığında yedek personelin desteğiyle de sistemin yürütülmesine olanak sağlayacaktır.

Ayrıcalıklı erişim haklarına sahip kullanıcı ve sistem hesapları tarafından gerçekleştirilen işlemlerin kayıtlarının alınması ve saklanması yetkili kişilerin işlemlerinin kontrol altına alınmasını sağlayacaktır.

Log toplama sisteminde sadece tek kullanıcı mevcuttur. Log toplama sistemi ile ilgili bir problem olduğunda herhangi bir müdahale söz konusu değildir. Ayrıca USOM a göre sistem ile sistemi işleten kişi arasında herhangi bir bağlantı bulunmaması gerekmektedir. Bakanlığın USOM un bildirdiği uyarıya uyması güvenliğin artması konusuna katkı sağlayacaktır.

Bakanlık için yeni bir bilgi sistemi temini aşamasında ihtiyaçların doğru analiz edilmesi ve bu bilgi sistemlerini etkileyen diğer ilgili birimlerle koordinasyon sağlanması temin edilen sistemin Bakanlık içerisinde etkin bir şekilde kullanılmasını sağlayacaktır.

Bakanlığa ait bir veri herhangi bir sisteme iletilirken Bakanlık verisinin şifreli bir şekilde gönderilmesi saldırgan tarafından ele geçirilmesi durumunda Bakanlığın bu durumdan en az seviyede etkilenmesini sağlayacaktır.

Yedekleri alınan sistemlerin yedeklerinin geri dönüş testleri ile düzenli aralıklarla kontrol edilmesi yedeklerin sağlıklı bir şekilde alınmış olduğu bilgisi sağlayacaktır. Böylece herhangi acil bir durumda yedekten geri dönme işleminde bir sorun yaşanmama olasılığı artacaktır.

SGOM kurulmasına karar verilmesi aşamasında kurum ve kuruluşların siber güvenlik stratejilerini belirlemeleri, politika ve yol haritalarını oluşturmaları doğru bir SGOM için önemlidir. Böylece kurum ve kuruluşun ne aşamada olduğu ve hangi aşamadan hangi aşamaya ne kadar sürede gideceği adımlarının belirli olmasına bağlı olarak doğru bir ilerleme kaydedilecektir.

Kurum ve kuruluşların temin ettiği sistemler, mevcut bulunan veya yeni kullanımına açılan uygulamaların parolaları hiçbir zaman varsayılan olarak bırakılmamalıdır. Bunun en kritik sebebi saldırganların herhangi bir saldırı sırasında ilk işlem olarak varsayılan parolaları deneme yöntemine gitmeleridir.

SGOM için ekran izleme faaliyeti de güvenlik cihazlarının yaptığı iş ve işlemler kadar önemlidir. Ekran izleme işlemi sayesinde ağ trafiğinde herhangi bir anomali tespiti, cihazlar üzerinde herhangi bir olumsuz durum yaşanması gibi konular bütün SGOM personeli tarafından takip edilebilmelidir.

Sadece güvenlik sistemlerinin işletiliyor olması etkin bir SGOM için yeterli olmayabilir, bu nedenle güvenlik testlerinin de kurum tarafından yapılabilmesi büyük önem arz etmektedir. Güvenlik testlerinin kurum tarafından gerçekleştirilebilmesi için de bu konuda eğitimler verilerek uzman personelin yetiştirilmesi faydalı olacaktır.

Güvenlik sistemlerinin kullanımlarının yazılı hale getirilmesi bu sistemleri yeni kullanacak SGOM personelinin daha kısa zamanda ve efektif bir şekilde sistemi kullanmasına olanak sağlayacaktır.

SGOM çalışmaları kapsamında görevlendirilecek personele eğitim, çalıştay gibi faaliyetlerle destek olunarak, gelişimlerine katkı sağlamak ve desteklemek faydalı olacaktır.

Bakanlık çalışmalarının sağlıklı ve güvenli şekilde yürütülmesi için bu konuda çalışmalar yürüten kurum ve kuruluşlar ile işbirliğinin geliştirilmesi ciddi katkılar sağlayacaktır. Buna ek olarak uluslararası çalışmaların uzman personel tarafından güncel olarak takip edilmesi sağlanmalıdır.

Bilgi Güvenliği temelinde Bakanlıkta yürütülecek çalışmalarda bütüncül bir bakış açısı ortaya konulmalıdır. Bu kapsamda atılacak adımlar, alınacak malzemeler gibi unsurlar CBSGM koordinasyonunda belirli bir planlama doğrultusunda yapılmalıdır. Örnek olarak, başka birimleri de ilgilendiren hususlarla ilgili SGOM'a alınacak cihazlar için ilgili birimlerle koordineli bir şekilde çalışılarak, gereksinimler doğrultusunda uygun cihaz alımı yapılmalıdır.

SGOM çalışmaları kapsamında araç, gereç ve ekipman alımları noktasında güncel süreçlerin takibi yapılarak, uygun bütçelerin sağlanması ve etkin olarak kullanımı sağlanmalıdır.

SGOM kapsamında sağlanan sistemlerin tam ve efektif bir şekilde kullanılması gerekmektedir.

# KAYNAKLAR


1) 2015, Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu, TBMM No: 204, Türkiye
2) 2016 – 2019 Ulusal Siber Güvenlik Stratejisi
3) AKAY İsmayil Gökhan, 2014, Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları, Bilecik Şeyh Edebali Üniversitesi Yüksek Lisans Tezi, Bilecik
4) AKYILDIZ Muhammed Alparslan, 2013, Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar İle Değerlendirilmesi, Süleyman Demirel Üniversitesi Yüksek Lisans Tezi, Isparta
5) ALTUN Ramazan, 2014, Belirli Kısıtlara Göre Bilgi Güvenliği İhlallerinin Tespiti, Beykent Üniversitesi Yüksek Lisans Tezi, İstanbul
6) andacmesut.trakya.edu.tr/bmg/Ders13.ppt (Erişim Tarihi : 23.12.2016)
7) AYTEKİN Akın, 2015, Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi, Gazi Üniversitesi Yüksek Lisans Tezi, Ankara
8) Bakanlık Cbs Altyapısının Kurulması Ve Geliştirilmesi Projesi Teknik Şartnamesi, Çevre ve Şehircilik Bakanlığı Coğrafi Bilgi Sistemleri Genel Müdürlüğü, 2015
9) Barikat, 2016, ÇŞB için hazırlanan İstila Emareleri Değerlendirme Raporu, Ankara
10) Barikat, 2016, ÇŞB için hazırlanan Siber Güvenlik İş Gücünün İyileştirilmesi Değerlendirme Raporu, Ankara
11) Barikat, 2016, ÇŞB için hazırlanan Siber Güvenlik Operasyon Merkezi, Ankara
12) Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun (23.05.2007 tarihli ve 26530 sayılı Resmi Gazete)
13) CISCO, 2017, CISCO 2017 Annual Cybersecurity Report
14) ÇELİKTAŞ Barış, 2016, Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme, Karadeniz Teknik Üniversitesi Yüksek Lisans Tezi, Trabzon
15) Çevre ve Şehircilik Bakanlığı (ÇŞB) Bilgi Güvenliği Risk Yönetimi Prosedürü
16) Çifci, H. 2013), Her Yönüyle Siber Savaş(Birinci Baskı). Ankara: TUBİTAK Popüler Bilim Kitapları, 3-184.
17) ERCAN Mehmet, 2015, Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri, Gebze Üniversitesi Yüksek Lisans Tezi, Gebze

18) GANBAT Otgonjargal, 2013, Bilgi Güvenliği Yönetim Sistemi Iso/Iec 27001 ve Bilgi Güvenliği Risk Yönetimi Iso/Iec 27005 Standartlarının Uygulanması, Ege Üniversitesi Yüksek Lisans Tezi, İzmir
19) HAVELSAN, 2016, Siber Güvenlik Bülteni Sayı 1, http://www.havelsan.com.tr/files/files/folders/292201611322055_HAVELSAN_SiberGuvenlikBulteni_Sayi1.pdf (Erişim Tarihi: 23.01.2017)
20) HAVELSAN, 2016, Siber Güvenlik Bülteni Sayı 3, http://www.havelsan.com.tr/files/files/folders/952016105911735_SiberGuvBulteni_Say3_Mayis2016.pdf (Erişim Tarihi: 23.01.2017)
21) http://dergipark.gov.tr/download/article-file/75726 (Erişim Tarihi: 14.11.2016)
22) http://umut-simsek.blogspot.com.tr/2012/11/bt-guvenlik-operasyon-merkezi-it.html (Erişim Tarihi: 10.11.2016)
23) http://www.armabelgelendirme.com/hizmetlerimiz/icerik/2/iso-27001-bilgi-guvenligi-yonetim-sistemi (Erişim Tarihi: 24.12.2016)
24) http://www.bilgitoplumu.gov.tr/bilgi-toplumu/bilgi-toplumu-dairesi-hakkinda/ (Erişim Tarihi: 10.10.2016)
25) http://www.milliyet.com.tr/hsbc-turkiye-ye-siber-saldiri-bilisim-1969049/?PAGE=2 (Erişim Tarihi: 11.11.2016)
26) http://www.resuldas.com/pubs/bg.pdf (Erişim Tarihi: 23.12.2016)
27) https://seminer.linux.org.tr/wp-content/uploads/bgtk-210902.pdf (Erişim Tarihi: 12.12.2016)
28) https://www.academia.edu/9599660/Ulusal_Sanal_Ortam_G%C3%BCvenlik_Politikas%C4%B1 (Erişim Tarihi: 07.12.2016)
29) https://www.bilgiguvenligi.gov.tr/hakkimizda.html(Erişim Tarihi: 01.10.2016)
30) https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/neden-bgys-3.html (Erişim Tarihi: 06.01.2017)
31) https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/ornek-varlik-envanteri-olusturma-metodolojisi.html (Erişim Tarihi: 11.01.2017)
32) https://www.bilgiguvenligi.gov.tr/risk-analizi/bilgi-guvenliginde-risk-in-bes-hali-kargasayi-onleme-cabasi-3.html (Erişim Tarihi: 15.12.2016)
33) https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf (Erişim Tarihi: 16.12.2016)
34) Intel Security, 2016, McAfee Labs Threats Report

35) KARA Mahruze, 2013, Siber Saldırılar - Siber Savaşlar Ve Etkileri, İstanbul Bilgi Üniversitesi Yüksek Lisans Tezi, İstanbul
36) Kurumsal SOME Kurulum ve Yönetim Rehberi, Sürüm 1, 2014
37) North Atlantic Treaty Organization, 2011, NATO Cyber Defense Concept, NATO, 3-45.
38) PERENDİ Ünal, 2008, Bgys Kapsamı Belirleme Kılavuzu, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Sürüm 1.00 TÜBİTAK'a bağlı
39) SARI Onur, 2013, Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar, İstanbul
40) Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ (11.11.2013 tarihli ve 28818 sayılı Resmi Gazete)
41) STM, 2016, 2016 Türkiye Siber Tehdit Durum Raporu
42) TS ISO/IEC 27001 Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler
43) TS ISO/IEC 27002 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri
44) Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar (20.10.2012 tarihli ve 28447 sayılı Resmi Gazete)
45) Ulusal Siber Güvenlik Stratejisi ve 2013-2015 Eylem Planı (20.10.2012 tarihli 28447 sayılı Resmi Gazete)
46) United States Department of Defense, 2010, Department of Depense Dictionary of Military And Associated Terms, DoD, 13-71
47) YAŞAR Hakan, 2014, Kurumsal Siber Güvenliğe Yönelik Tehditler ve Mücadele Yöntemleri: Eylem Planı Örneği, Gazi Üniversitesi Yüksek Lisans Tezi, Ankara
48) YILDIZ Mithat, 2014, Siber Suçlar ve Kurum Güvenliği, Ulaştırma Denizcilik ve Haberleşme Bakanlığı Uzmanlık Tezi, Ankara

# EKLER

# EK 1 - KÜRESEL SİBER GÜVENLİK GÖSTERGESİ & SİBER MEMNUNİYET PROFİLLERİ RAPORU

GCI projesi ile ülkelerin siber güvenlik konusunda yapmış olduğu hazırlıklar değerlendirilmiş ve bu değerlendirme sonucunda küresel bir sıralama elde edilmiştir. Bu sıralamanın amacı belirli bir önlemin etkinliğini ve başarısını vurgulamak değil sadece siber güvenliği uygulamak ve geliştirmek için ülkelerin neler yaptığını belirlemektir. Bu proje siber güvenlik kültürü oluşturmanın yanı sıra farklı seviyelerde olan devletlerin siber güvenlik konusunda bilgi paylaşımında bulunmalarını da sağlayacaktır.

Bu proje, Uluslararası Telekomünikasyon Birliği (ITU) ve özel sektör şirketi ABI Research tarafından iki aşamada gerçekleştirilmiştir. Aşağıda yer alan tabloda verilen sorular ülkelere gönderilmiş olup, bu sorulara verilen cevaplar ışığında değerlendirmeler yapılmıştır. Bu sorular ile ülkelerin siber güvenlik konusunda çıkarmış olduğu yasalar, yönetmelikler; hazırlamış olduğu politikalar, ulusal stratejiler, standartlar; almış olduğu sertifikalar; düzenlemiş olduğu mesleki eğitimlerin olup olmadığı tespit edilmiştir.

Bu projeye 193 ülkeden katılım sağlanmıştır. Bu sıralamada ülkemiz 7. Sırada yer almaktadır. Bu sıralama yapılırken kullanılan ana göstergeler yasal önlemler, teknik önlemler, organizasyonel önlemler, kapasite geliştirme ve uluslararası işbirliğidir. Bu beş gösterge, ulusal bir kültürün doğal yapı taşlarını oluşturmaları nedeniyle, siber güvenlikteki ulusal yeteneklerin ölçülmesi için kritik önem taşır.

Bu çalışma boyunca ITU ve ABI Research sorulara verilen cevapları değerlendirdi, performans metriklerini belirledi, küresel bir sıralama mekanizması geliştirdi, ulus devletlerin siber güvenlik yetenekleri üzerine veriler araştırdı ve topladı, ulus devletler ve ilgili organizasyonlar ile irtibat kurdu ve küresel bir siber güvenlik endeksi yayınladı.

Çıkan sonuç bir dizi bireysel göstergeyi bir araya getiren birleşik bir göstergenin sonucudur. Siber güvenlik gelişimi süreci beş önemli geniş kategoride analiz edildi. Aşağıdaki göstergeler ve alt gruplar belirlendi ve ülkeler her göstergenin sağladığı karşılaştırma ölçütlerine göre sıralandı.

**Yasal Önlemler**

Mevzuat, belirli cezai davranışların yasaklanması veya asgari düzenleyici gerekliliklerin uygulanması, kurum ve kuruluşların uyumlu bir çerçeve sağlayan ortak bir düzenleyicide birleşmesi için kritik bir önlemdir. Sonuçta amaç, tüm ulus devletlerin

uygulamalarını uluslararası düzeyde uyumlu hale getirmek, birlikte çalışabilir önlemler için bir ortam sunmak ve uluslararası mücadeleyi kolaylaştırmak için siber suçlara karşı uygun yasaları uygulamalarını sağlamaktır.

Hukuki ortam, siber güvenlik ve siber suçlarla mücadele eden yasal kurumların ve çerçevelerin varlığı ve sayısı temel alınarak ölçülebilir. Alt grup, aşağıdaki performans göstergelerinden oluşur:

a. Ceza yasası

   Siber suç yasaları yetkisiz erişim yapılması; bilgisayar, sistem gibi cihazların kötü amaçlar için kullanılması gibi durumlarda uygulanması gereken işlemleri belirtir. Değerlendirme aşamasında siber suç yasası üç seviyede belirlenir. Yasanın hiç bulunmaması, kısmi bulunması ya da kapsamlı bir şekilde bulunmasıdır. Kısmi bulunma durumunda, var olan diğer yasalar içerisinde basit bir şekilde bilgisayarla ilgili ifadelere değinilmesidir. Kapsamlı yasalar, bilgisayar suçlarının çok özel yönleriyle (ör. Birleşik Krallık Bilgisayarında Kötüye Kullanım Yasası 1990) ilgili özel bir yasanın veya eylemin yürürlüğe konması anlamına gelir.

b. Düzenleme ve uyumluluk

   Siber güvenlik düzenlemesi, veri koruma, ihlal bildirimi ve sertifikasyon/standardizasyon gereksinimleri ile ilgili yasaları belirtir. Siber güvenlik düzenlemesi de ceza yasası ile aynı şekilde üç sınıflandırmada belirlenir. Değer hesaplaması yapılırken ülkede siber güvenlik düzenlemesinin bulunmaması; mevcut veya yeni yönetmelik, standart ya da belgede bilgisayarla ilgili ifadelere yer verilip verilmediği (Kişisel verilerin işlenmesine ve bu verilerin serbest dolaşımına ilişkin olarak kişilerin korunması hakkında 95/46 / EC sayılı AB Yönergesi), siyasal güvenliğe uyumu gerektiren özel bir yasanın, eylemin veya talimatın (ör. ABD Federal Bilgi Güvenliği Yönetim Yasası 2002) yürürlükte olması dikkate alınır.

**Teknik Önlemler**

Teknoloji, siber tehditlere ve kötü amaçlı davranışlara karşı ilk savunma hattıdır. Yeterli teknik önlemler, siber saldırıları tespit etme ve bunlara tepki verme yetenekleri olmadan ulus devletler ve ilgili birimleri siber tehditlere karşı savunmasız kalmaktadır. Bilişim teknolojileri güvenli bir ortamda gelişebilir ve başarılı olabilir. Bu nedenle ulus devletleri, yazılım uygulamaları ve sistemleri için kabul edilmiş minimum güvenlik ölçütlerini oluşturmak için stratejiler geliştirebilmelidir. Bu çabalara, ulusal düzeyde siber olaylarla

uğraşmaya odaklanan bir ulusal varlığın oluşturulması, en azından sorumlu bir devlet kurumuyla birlikte izleme, uyarı ve olay yanıtı için eşlik eden bir ulusal çerçeve eşlik etmelidir.

Teknik önlemler, ulus devletin onayladığı veya oluşturduğu siber güvenlikle ilgilenen teknik kurumların ve çerçevelerin varlığına ve sayısına dayanarak ölçülebilir. Alt grup aşağıdaki performans göstergelerinden oluşur:

a. CERT/CIRT /CSIRT

Siber tehditleri belirlemek, bunlara karşı savunma oluşturmak, siber güvenlikle ilgili soruları yanıtlamak ve bütün kurum ve kuruluşları merkezi olarak yönetmek için ulusal bir CIRT (Bilgisayar Olay Müdahale Ekibi), CERT (Bilgisayar Acil Müdahale Ekibi) veya CSIRT (Bilgisayar Güvenliği Olay Müdahale Ekibi) bulunmalıdır. Bu ekipler başka kaynaklar aracılığıyla değil kendi istihbaratları ile bilgileri toplamalıdır. Değerlendirme aşamasında, ülkelerin bünyelerinde herhangi bir ulusal ekip olup olmadığı ve yasal olarak zorunlu olup olmadığı temel alınacaktır.

b. Standartlar

Bu gösterge, kamu sektöründe uluslararası kabul görmüş (Devlet kurumları) ve kritik altyapı içindeki (özel sektör tarafından işletilse bile) siber güvenlik standartlarının uygulanması için hükümet tarafından onaylanmış (veya onaylanmış) bir çerçevenin (veya çerçevelerin) varlığını ölçmektedir. Bu standartlar, bunlarla sınırlı olmamak üzere, aşağıdaki ajanslar tarafından geliştirilen standartları içerir: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, vb.

c. Sertifikasyon

Bu gösterge Ulusal kuruluşlarının ve kamu sektörü profesyonellerinin uluslararası kabul görmüş siber güvenlik standartlarına göre belgelendirilmesi ve akreditasyonu için hükümet tarafından onaylanmış (veya onaylanmış) bir çerçevenin (veya çerçevelerin) varlığını ölçer. Bu sertifikalar, akreditasyonlar ve standartlardan bazıları şunlardır: Bulut Güvenliği Bilgisi, CISSP, Siber Güvenlik Şerifi Analisti ($ISC^2$), GIAC, GIAC GSSP (SANS), OSSTMM (ISECOM), PCIP / CCISP (Kritik Altyapı Enstitüsü), CERT-Sertifikalı Bilgisayar Güvenliği Olayı İşleyicisi (SEI), CITRMS (Tüketici Enstitüsü Finansal Eğitim), CSFA (Siber Güvenlik Kurumu), CCSA (İç Denetim Enstitüsü), (Profesyonel Risk Yöneticileri Uluslararası Birliği), PMP (Proje Yönetim Enstitüsü) vb.

**Organizasyonel Önlemler**

Organizasyonel önlemler, her tür ulusal girişimin düzgün bir şekilde uygulanması için gereklidir. Geniş bir stratejik hedef, uygulama, teslimat ve ölçme konusunda kapsamlı bir plan ulus devlet tarafından belirlenmelidir. Ulusal bir strateji ve denetim organı olmaksızın, farklı sektörlerdeki ve endüstrilerdeki çabalar, birbirinden ayrı ve birbiriyle bağlantısız hale gelir ve böylece, siber güvenlik alanındaki gelişme konusunda ulusal uyumlaştırmaya yönelik çabalar engellenir.

Organizasyonel yapılar, ulusal düzeyde siber güvenlik gelişmesini organize eden kurumların ve stratejilerin sayısına dayalı olarak ölçülebilir. Alt grup, aşağıdaki performans göstergelerinden oluşur:

a. Politika

   Siber güvenliği artırmak için bir politika geliştirilmesi bir öncelik olarak kabul edilmektedir. Bu politika, esnek ve güvenilir bilgi altyapısını korumalı ve vatandaşların güvenliğini sağlamayı amaçlamalıdır. Bu politikanın amacı, vatandaşların, organizasyonların ve devletin maddi ve manevi varlıklarını korumak; kritik altyapılara karşı siber saldırıları önlemek ve siber saldırılardan kaynaklanan hasarı ve kurtarma sürelerini en aza indirmek olmalıdır. Bu politika içerisinde açıkça tanımlanmış roller ve sorumluluklar; siber güvenlik konusunda devlet tarafından yönetilen girişimlerde özel sektör katılımını ve ortaklığını teşvik etmek gibi konularda yer almalıdır.

b. Yönetim için yol haritası

   Siber güvenlik alanında bir yol haritası belirlemek için genellikle siber güvenlik konusunda ulusal strateji/politika belirlenir ve kilit paydaşlar tanımlanır. Bir ulusal politika çerçevesinin geliştirilmesi, siber güvenlik için üst düzey yönetim geliştirmede birincil önceliğe sahiptir. Ulusal politika çerçevesi, ulusal kritik bilgi altyapısının korunması ihtiyaçlarını hesaba katmalıdır. Aynı zamanda, kamu sektöründe ve ayrıca kamu ve özel sektör arasında bilgi paylaşımını teşvik etmeyi amaçlamalıdır.

   Bu politika içerisinde siber güvenlik yönetimi, zorlukları, diğer bilgi güvenliği ve ağ güvenliği konuları ulusal düzeyde değerlendirmeli; güvenlik yasalarını ağa ve çevrimiçi çevrelere aktaran yasal temeller belirlenmeli; tüm menfaat sahiplerinin katılımı gerçekleştirilmeli; siber güvenlik için bir kültür geliştirilmesi

sağlanmalı; güvenlik ihlallerine ve olaylarla mücadeleye yönelik prosedürler (raporlama, bilgi paylaşımı, uyarı yönetimi, adalet ve polis işbirliği) oluşturulmalı; ulusal siber güvenlik politikasının etkili bir şekilde uygulanması için yapılması gerekenler tespit edilmelidir.

c. Sorumlu kurum

Ulusal bir siber güvenlik stratejisi/politikası uygulayan sorumlu bir kuruluş, daimi komiteler, resmi çalışma grupları, danışma konseyleri veya disiplinler arası merkezleri içerebilir. Bu sorumlu kurum, gözlem ve uyarı sistemlerinden ve olay tepkisinden doğrudan sorumlu olacak; siber saldırılara yanıtların koordinasyonunda ihtiyaç duyulan örgütsel yapıların geliştirilmesi için çalışmalar yürütecektir.

d. Ulusal kıyaslama

Bu gösterge, siber güvenlik gelişimini ölçmek için kullanılan, resmi olarak kabul edilmiş herhangi bir ulusal veya sektörel kıyaslama egzersizinin veya referansın varlığını ölçer. Örneğin, ISO / IEC 27002- 2005'e dayanan bir ulusal siber güvenlik standardı (NCSec Referanslı) ulus devletlerin siber güvenlik gereksinimlerini belirtmesine yardımcı olabilir. Bu referans, beş alana ayrılmıştır: NCSec Stratejisi ve Politikaları; NCSec Organizasyonel Yapılar; NCSec Uygulaması; Ulusal Koordinasyon; Siber Güvenlik Bilinçlendirme Faaliyetleri.

**Kapasite Geliştirme**

Kapasite geliştirme ilk üç önlemin (yasal, teknik ve organizasyonel) temelinde yer almaktadır. İnsan ve kurumsal kapasite geliştirme, sektörler arasındaki bilgi ve tecrübeyi arttırmak, en uygun çözümleri uygulamak ve en yetkili profesyonellerin gelişimini teşvik etmek için gereklidir.

Siber güvenliğin geliştirilmesi için bir kapasite geliştirme çalışması gerçekleştirmek için, farkındalık yaratma ve kaynakları temin etme konuları ele alınmalıdır. Kapasite geliştirme, araştırma ve geliştirme, eğitim ve öğretim programları, sertifikalı profesyoneller ve kamu sektörü ajanslarının varlığına ve sayısına göre ölçülebilir. Alt grup, aşağıdaki performans göstergelerinden oluşur:

a. Standardizasyon geliştirme

Standardizasyon, bir teknolojinin olgunluk seviyesinin iyi bir göstergesidir ve kilit alanlarda yeni standartların ortaya çıkması, standartların vazgeçilmez önemini vurgular. Siber güvenlik her zaman ulusal güvenlik için bir konudur ve farklı ülkelerde farklı muamele görmekle birlikte, genel yaklaşımlar yaygın olarak kabul gören standartlar tarafından desteklenmektedir. ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC vb. bu standartlardan bazılardır.

b. İşgücü geliştirme

İnsan gücü geliştirme, ulus devletlerin mümkün olduğu kadar çok insana ulaşması olarak ifade edilmektedir. Bu kapsamda kurumlar, kuruluşlardan, kütüphanelerden, yerel ticaret örgütlerinden, toplum merkezlerinden, bilgisayar mağazalarından ve yetişkinlerden faydalanmak için yaygın tanıtım kampanyaları başlatmalıdır. Eğitim programları, okullar ve organizasyonlar siber davranışlarla ilgili bilgilendirmek için kullanılmalıdır. Farkındalık yaratmak için portallar ve web siteleri kurma, eğitimciler için destek materyali dağıtma ve mesleki eğitim kursları ve eğitim programlarını oluşturma (veya teşvik etme) gibi eylemler siber davranışlarla ilgili bilgilendirme için yapılacak diğer çalışmalardandır.

c. Profesyonel Sertifikasyon

Bu performans göstergesi, aşağıdakileri içeren ancak bunlarla sınırlı olmayan, uluslararası kabul görmüş sertifika programları standartlarına göre sertifikalı kamu sektörü profesyonellerinin sayısına göre ölçülebilir: Bulut Güvenliği Bilgisi (Bulut Güvenliği Birliği), CISSP, Siyaset Güvenliği Adli Analisti ( ISC²), GIS, CISO, Yazılım Güvenlik Mühendisliği Sertifikası, CFE (Sertifikalı Dolandırıcılık Denetçileri Derneği), CERT Onaylı Bilgisayar Güvenliği Olayı İşleyicisi (SEI), CITRMS (Tüketici Mali Eğitimi Enstitüsü), CIA, CCSA (İç Denetim Enstitüsü) vb.

d. Kamu sertifikası

Bu performans göstergesi, uluslararası kabul görmüş standartlar çerçevesinde belgelenmiş devlet kurumları ve kamu sektörü kuruluşlarının sayısı ile ölçülebilir. ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC vb.

**İşbirliği**

Siber güvenlik, tüm sektörlerden ve disiplinlerden gelen girdileri gerektirir ve bu nedenle çok paydaşlı bir yaklaşımla ele alınması gerekir. İşbirliği diyalog ve koordinasyonu arttırarak daha kapsamlı bir siber güvenlik alanının oluşturulmasını sağlar.

Siber suç meselesi küresel bir özellik taşıdığından dolayı işbirliği önemli bir noktadır. Bu işbirliği ile tehdit bilgisinin, saldırı senaryolarının, yanıt ve savunmada en iyi uygulamaların paylaşılması sağlanacaktır. Ülkeler, kurum ve kuruluşlar arasındaki işbirliği ne kadar güçlü ve yaygın olursa o derecede daha güçlü siber güvenlik özelliklerinin geliştirilmesine, tekrarlanan ve sürekli çevrimiçi tehditlerin engellenmesine ve kötücül ajanların daha iyi soruşturma, endişe ve kovuşturma yapılmasına yardımcı olabilir.

Ulusal ve uluslararası işbirliği, ortaklıkların varlığı ve sayısına, işbirliği çerçevelerine ve bilgi paylaşım ağlarına dayanılarak ölçülebilir. Alt grup, aşağıdaki performans göstergelerinden oluşur:

a. Devletlerarası işbirliği

   Devletlerarası işbirliği, diğer ulus devletlerle sınırlar ötesi siber güvenlik varlıklarını paylaşmak için yapılmış resmi ulusal veya sektörel ortaklıklar anlamına gelir. (örneğin, bilgi, uzmanlık, teknoloji ve / veya bilgi paylaşımı veya değişimi için imzalanmış iki taraflı veya çok taraflı ortaklıklar). Avrupa Birliği, Avrupa Konseyi, G8 Devlet Topluluğu, Asya Pasifik Ekonomik İşbirliği (APEC), Amerikan Devletleri Örgütü (OAS) ve Avrupa Ekonomik İşbirliği Örgütü (APEC) tarafından uygulanan bölgesel düzeydeki girişimler.

b. Kurumlar arası işbirliği

   Kurumlar arası işbirliği, kamu sektöründe siber güvenlik varlıklarını (insanlar, süreçler, araçlar) paylaşmak için resmi olarak tanınan ulusal veya sektörlere özgü programları ifade eder.

c. Kamu-Özel Sektör Ortaklıkları

   Kamu-özel ortaklıkları, kamu ve özel sektör arasındaki girişimlere atıfta bulunmaktadır. Bu performans göstergesi, kamu ve özel sektör arasında siber güvenlik varlıklarını (kişi, süreçler, araçlar) paylaşmak için resmi olarak tanınan ulusal ya da sektörel ortaklıkların sayısına göre ölçülebilir.

d. Uluslararası işbirliği

Bu performans göstergesi, uluslararası siber güvenlik platformlarına ve forumlara resmi olarak bir katılım sağlamayı ifade eder. Bu gibi işbirliğine dayalı girişimler şunları içerir: Birleşmiş Milletler Genel Kurulu; Uluslararası Telekomünikasyon Birliği (ITU); Interpol / Europol; Ekonomik İşbirliği ve Kalkınma Örgütü (OECD); BM Uyuşturucu ve Suç Sorunları Kuruluşları (UNODC); BM Bölgeler Arası Suç ve Adalet Araştırmaları Enstitüsü (UNICRI); Atanmış İsimler ve Sayılar için Internet Corporation (ICANN); Uluslararası Standartlar Organizasyonu (ISO); Uluslararası Elektroteknik Komisyonu (IEC); İnternet Mühendisliği Görev Gücü; İLK (Olay Yanıtlama ve Güvenlik Ekipleri Forumu).

## METODOLOJİ

Kullanılan istatistiksel modelde Çok Kriterli Analiz (MCA) temel alınacaktır. MCA performans matrisi seçenekleri tanımlar ve her sütun her kritere göre seçeneklerin performansını açıklar. Bireysel performans değerlendirmesi sayısaldır.

Kriter puanlaması, aşağıdaki göstergeler temel alınarak hazırlanacak ve her biri ağırlıkça eşit olarak puanlanacaktır (bazıları daha fazla alt grup içerdiğinden, alt kategoriler için puanlama diğerlerinden daha yüksek olacaktır). Hiçbir faaliyetin olmadığı yerlerde 0 puan; kısmi eylem için 1 puan ve daha kapsamlı eylem için 2 puan olarak değerlendirme yapılır. Her kategori için ayrılan toplam puan:

A. Yasal Önlemler 4
a. Ceza yasası 2
b. Düzenleme ve uyumluluk 2

B. Teknik Önlemler 6
a. CERT/CIRT /CSIRT 2
b. Standartlar 2
c. Sertifikasyon 2

C. Organizasyonel Önlemler 8
a. Politika 2
b. Yönetim için yol haritası 2

c. Sorumlu Kurum 2
d. Ulusal Kıyaslama 2

D. Kapasite Geliştirme 8
a. Standardizasyon geliştirme 2
b. İşgücü geliştirme 2
c. Profesyonel Sertifikasyon 2
d. Kamu sertifikası 2

E. İşbirliği 8
a. Devletlerarası işbirliği 2
b. Kurumlar arası işbirliği 2
c. Kamu-Özel Sektör Ortaklıkları 2
d. Uluslararası işbirliği 2

Gösterim:

$xqc$ q=1,…,Q ve c=1,…,M ile birlikte ülke c için bireysel gösterge q nın değeri
$Iqc$ Ülke c için bireysel göstergenin normalleştirilmiş değeri
$CIc$ Ülke c için bileşik göstergenin değeri

Kullanılan kıyaslamada, genel hazır olma durumunu en üst düzeye çıkaran tahmini ülkenin skoru 34 puan olacak. Ortaya çıkan bileşik endeks, sıfır (mümkün olan en kötü hazırlık) ile 1 (karşılaştırma ölçütü) arasında değişecektir:

$CIc = Iqc/34$

Normalleştirme tekniği, bir sıralama yöntemine dayanılacaktır:

$Iqc = Rank\ (xqc)$

## SONUÇ

GCI'nin uzun vadeli hedefi, siber güvenlik alanlarının küresel ölçekte benimsenmesi ve entegrasyonu için daha fazla çaba gösterilmesidir. Ulusal siber güvenlik stratejilerinin karşılaştırılması, belirli alanlarda yüksek sıralamaya sahip olan devletleri açığa çıkaracak ve sonuç olarak daha az bilinen fakat başarılı siber güvenlik stratejilerini ortaya koyacaktır. Bu durum, farklı gelişme seviyelerine sahip olan devletler için de siber güvenlik açığı konusunda artan bilgi paylaşımına neden olacaktır. Çeşitli alanlardaki siber güvenlik önlemlerinin düzeyini ölçerek devletlerin, nerede bir gelişme ölçeğinde olduklarını, daha fazla ilerleme kaydetmeleri için neler yapması gerektiğini ve kabul edilebilir düzeyde bir siber güvenlik uygulamaktan ne kadar uzakta olduklarını değerlendirmesine izin verecek.

## TÜRKİYE'YE AİT DEĞERLER

### Yasal Önlemler

a. Ceza yasası
   - Türk Ceza Kanunu
   - İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

b. Düzenleme ve uyumluluk
   - Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik
   - Elektronik Haberleşme Güvenliği Yönetmeliği

### Teknik Önlemler

a. CERT/CIRT /CSIRT
   - Türkiye resmen tanınmış bir ulusal CIRT'ye (TR-CERT) sahiptir.

b. Standartlar
   - Türkiye, 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile Elektronik Haberleşme Güvenliği Yasası vasıtasıyla uluslararası kabul görmüş siber güvenlik standartlarını uygulamak için ulusal (ve sektörel) siber güvenlik çerçevelerini resmi olarak tanıdı.

c. Sertifikasyon
   - Türk Standartları Enstitüsü, ISO IEC 27001, ISO IEC 15408, ISO IEC 12207 gibi birçok uluslararası standarda göre sistem, personel ve ürün belgelendirme hizmetleri sunmaktadır.

### Organizasyonel Önlemler

a. Politika
   - Türkiye, resmi olarak kabul edilmiş bir ulusal siber güvenlik stratejisine (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014) sahiptir. Strateji, kritik altyapılarda kullanılan bilgi sistemlerinin güvence altına alınması ve ulusal siber güvenlik sağlamak için gerekli önlemlerin alınması esasına dayanmaktadır.

b. Yönetim için yol haritası
   - Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 29 ana eylem ve 95 alt eylemi içermektedir. Mevzuat, kapasite geliştirme, teknik altyapının geliştirilmesi konularında sorumluluklar atar. Bu da Türkiye'de siber güvenlik konusunda ulusal bir yönetim yol haritası sunmaktadır.

c. Sorumlu Kurum
   - Siber Güvenlik Kurulu, ulusal bir siber güvenlik stratejisi, politikası ve yol haritası uygulamakla sorumlu resmi olarak tanınmış bir kuruluştur. Siber güvenlikle ilgili önlemleri belirlemek, hazırlanan plan, program, rapor, usul, ilke ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla kurulmuştur.

d. Ulusal Kıyaslama
    - Son üç yılda Türkiye, ulusal düzeyde üç siber güvenlik tatbikat düzenlemiştir. Hem kamu hem de özel sektörün katılımıyla gerçek siber saldırılar ve hazırlanmış senaryolar uygulanmıştır. Bu egzersizler, siber güvenlik bilincinin artırılmasında büyük rol oynadı ve aynı zamanda siber güvenlik gelişimini ölçmek için mükemmel bir araçtı. Ek olarak, Elektronik Haberleşme Güvenliği Yönetmeliği, elektronik iletişim servis sağlayıcılarının ISO IEC 27001'e uymasını şart koşmaktadır. BTK tarafından yapılan denetimler, elektronik iletişim sektörünün siber güvenlik düzeyinin ölçülmesinde büyük rol oynamaktadır.

**Kapasite Geliştirme**

a. Standardizasyon geliştirme
    - Standardizasyon faaliyetlerinden sorumlu olan kurum, Türk Standartları Enstitüsüdür. Uluslararası alanda kabul edilen siber güvenlik standartları, uyum sürecinin bir parçası olarak Türk standartları olarak benimsenmiştir. Kurum, ülke ve sektörün özel ihtiyaçlarını göz önüne alarak standartlaştırma hizmetleri de sunmaktadır.

b. İşgücü geliştirme
    - Türk Bilimsel ve Teknolojik Araştırma Kurumu ile Türk Standartları Enstitüsü, CEH, ISO IEC 27001 baş denetçisi, internet yönetimi gibi siber güvenlik eğitim programları vermektedir. Ayrıca, Bahçeşehir Üniversitesi ve Şehir Üniversitesi gibi çeşitli üniversitelerde bilgi güvenliği mühendisliği, siber güvenlik gibi lisansüstü programlar bulunmaktadır. Lisansüstü programlar, siber güvenlik alanının teknik ve yasal yönlerini kapsar. Ayrıca, halk arasında farkındalık yaratmak için www.bilgiguvenligi.gov.tr, www.bilgimikoruyorum.org.tr, www.guvenliweb.org.tr gibi çeşitli web siteleri kurulmuştur.

c. Profesyonel Sertifikasyon
    - Türkiye'de, siber güvenlik alanında uluslararası alanda kabul görmüş sertifikasyon programları kapsamında sertifikalandırılmış yaklaşık 400 kamu personeli bulunmaktadır.

d. Kamu sertifikası
    - ISO IEC 27001 sertifikasına sahip 106 elektronik iletişim servis sağlayıcı bulunmaktadır. Sertifikasyon kuruluşları hem akredite edilmiş ulusal (Türk Standartları Enstitüsü, Kalitest gibi) hem de uluslararası sertifikasyon kuruluşlarını (BSI, Bureau Veritas ve DAS gibi) içerir. ISO IEC 27001, ISO IEC 17025, ISO / IEC 18045 gibi belgelere sahip yaklaşık 15 kamu ve kamu kuruluşu bulunmaktadır. Sertifikasyon kuruluşları genellikle akredite ulusal sertifikasyon kuruluşlarıdır (örneğin Türk Standartları Enstitüsü, Kalitest vb.).

**İşbirliği**

a. Devletlerarası işbirliği
   - Siber güvenlik varlıklarının sınırlar ötesi veya diğer ulus devletlerle paylaşımını kolaylaştırmak için Türkiye, aşağıdaki ülkeler ve kuruluşlarla resmi olarak ortaklıklar tanımıştır:
     Arnavutluk, Azerbaycan, Bosna Hersek, Bulgaristan, Kosova, Kırgızistan, Makedonya, Fas, Nijer, Sudan Cumhuriyeti, Senegal, Sırbistan, Tunus, İran, Tayland, Mısır ve Ukrayna

b. Kurumlar arası işbirliği
   - 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, siber güvenlikle ilgili faaliyetlerde kamu kurumları arasında kaynakların verimli kullanılması ve paylaşılmasını teşvik eder.

c. Kamu-Özel Sektör Ortaklıkları
   - 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, siber güvenlikle ilgili faaliyetlerde kamu kurumları arasında kaynakların verimli kullanılması ve paylaşılmasını teşvik eder.

d. Uluslararası işbirliği
   - Türkiye ITU-IMPACT girişiminin bir üyesidir ve ilgili siber güvenlik hizmetlerine erişime sahiptir. Türkiye aynı zamanda ITU-T içindeki siber güvenlikle ilgili standardizasyon çalışmalarına da aktif olarak katılmaktadır. TR-CERT (USOM), FIRST and Trusted Introducer Membership için de adaydır. Uluslararası Siber Güvenlik Çalışması 2014 (ICSE 2014), Türkiye IMPACT ve ITU işbirliği ile Mayıs 2014'te İstanbul'da düzenlendi. Türkiye, Ekim 2012'de Bulgaristan'da yapılmış olan ITU Avrupa ve BDT Siber Güvenliği Bölgesel Forumu'nda Acil Müdahale Ekibi Uygulamalı Öğrenme Ekibi (ALERT) 2012'ye katıldı.

Tablo 1: Ülkelerin 5 gösterge için değerleri

| Europe | Legal | Technical | Organizational | Capacity Building | Cooperation | Index |
|---|---|---|---|---|---|---|
| Norway* | 1.0000 | 0.6667 | 0.7500 | 0.8750 | 0.5000 | 0.7353 |
| Estonia* | 1.0000 | 0.6667 | 1.0000 | 0.5000 | 0.5000 | 0.7059 |
| Germany* | 1.0000 | 1.0000 | 0.6250 | 0.6250 | 0.5000 | 0.7059 |
| United Kingdom | 1.0000 | 0.6667 | 0.7500 | 0.7500 | 0.5000 | 0.7059 |
| Austria* | 1.0000 | 0.3333 | 0.8750 | 0.7500 | 0.5000 | 0.6765 |
| Hungary* | 1.0000 | 0.6667 | 0.7500 | 0.6250 | 0.5000 | 0.6765 |
| Israel* | 1.0000 | 0.6667 | 0.6250 | 0.7500 | 0.5000 | 0.6765 |
| Netherlands* | 0.7500 | 0.5000 | 0.8750 | 0.6250 | 0.6250 | 0.6765 |
| Latvia* | 1.0000 | 0.6667 | 0.7500 | 0.5000 | 0.5000 | 0.6471 |
| Sweden* | 0.7500 | 0.6667 | 0.6250 | 0.6250 | 0.6250 | 0.6471 |
| Turkey | 0.5000 | 0.6667 | 0.7500 | 0.7500 | 0.5000 | 0.6471 |

# EK 2 – OLAY MÜDAHALE SÜRECİ

Kullanıcılar bilgisayar sistemlerinde herhangi bir olay tespit ettiklerinde ya da bilmedikleri bir adresten e-posta alıp şüpheli bulduğunda kısacası güvenlik ihlali gerçekleşme ihtimali durumunda veya olay vuku bulduysa kurum ya da kuruluş tarafından kullanılan yardım masası gibi bir uygulama üzerinden, e-posta veya telefon yoluyla bildirim yapar. Bunun üzerine yetkili kişiler tarafından gerçek bir olay olup olmadığı kontrol edilerek ilgili olay kayıt dokümanları hazırlanır.

İzlenen sistemler üzerinden bir olay gerçekleşme ihtimali oluştuğunda ya da olay gerçekleştiğinde kayıt altına alınması amacıyla ilgili dokümanlar hazırlanır.

İzleme esnasında SGOM personeli tarafından tespit edilen normal olmayan iş ve işlemler için ilgili olay kayıt dokümanları hazırlanır.

Hazırlanan dokümanlar kurum ve kuruluş tarafından belirlenen ilk seviye olay müdahale ekibi tarafından incelenir. İlk seviye müdahale ekibi tarafından müdahale edilemeyecek olaylar için uzman personelden oluşan ikinci seviyeye olay müdahale ekibi tarafından işlemler başlatılır. İkincxi seviye tarafından müdahale edilemeyen olaylarda da bir üst aşamaya (dışardan hizmet alımı, yetkili kurum ve kuruluşlar vb.) bildirilir.

İlk seviye veya ikinci seviye olay müdahale ekibi tarafından incelen olay için analiz çalışmaları yapılır, gerekli durumlarda deliller toplanır. Olaya sebep olan açıklıklar kapatılır ve gerekli önlemler alınır.

Olay kayıt dokümanında en az kaydın açılma zamanı, kaydı açan kullanıcı olayın kategorisi, etkisi, aciliyet seviyesi, olay açıklaması bilgileri yer almalıdır.

Aciliyet; olaya ne kadar zamanda cevap verilmesi gerektiğini anlatmaktadır.

Tablo 1: Aciliyet Tablosu Örneği

| Kategori | Tanımlar |
|---|---|
| 1 - Yüksek | • Kurum ve kuruluşun sistemlerine sızılması<br>• Kurum ve kuruluş dışına kritik veri sızdırılması<br>• … |
| 2 - Orta | • Saldırganın varlığından şüphe edilmesi<br>• Gelişmiş bir korelasyon kuralı tetiklenmesi<br>• … |
| 3 - Düşük | • Sistemde çalışmayı engellemeyecek hataların mevcudiyeti<br>• Temel bir korelasyonun tetiklenmesi<br>• … |

Etki; olayın kurum ve kuruluşu ne derece etkilediği ve çözülememesi durumunda ortaya çıkabilecek olası hasarın boyutunu simgelemektedir.

Tablo 2: Etki Tablosu Örneği

| Kategori | Tanımlar |
|---|---|
| 1 - Yüksek | • Kurum veya kuruluşun hizmet verdiği çoğu müşteri etkileniyor<br>• Mali hasarı çok yüksek<br>• … |
| 2 - Orta | • Kurum ve kuruluşun çalışması kısmen etkileniyor<br>• Belirli sayıda müşteri etkileniyor<br>• … |
| 3 - Düşük | • Bakanlık itibarı etkilenmiyor<br>• Kurum ve kuruluşun genel çalışmaları devam ediyor<br>• … |

Olaylara müdahale aşamasında etki ve aciliyet durumuna göre olayın önceliğine ve öncelik seviyesine göre olaya müdahale süresine karar verilmektedir. Olaya müdahale aşamasından sonra olayla ilgili yaşanılan deneyimler, çözüm yöntemleri raporlanmalı ve olaydan ders çıkarılmalıdır.

# ETİK KURALLARA UYGUNLUK BEYANI

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Çevre ve Şehircilik Uzmanlığı Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Çevre ve Şehircilik Bakanlığı tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Emine ERÇAĞLAR

# ÖZGEÇMİŞ

1987 yılında Ankara'da doğdu. İlk, orta ve lise öğrenimini Ankara'da tamamladı. 2010 yılında Gazi Üniversitesi Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü'nden mezun oldu. 2010 yılında bir yıl süre ile Hacettepe Üniversitesi içerisinde yer alan Teknokent'te çalıştı. 2011 yılında İşkur bünyesinde dış kaynaklı personel olarak göreve başladı ve üç yıl boyunca İşkur yazılımına destek verdi.2014 yılında Çevre ve Şehircilik Bakanlığı'nda Çevre ve Şehircilik Uzman Yardımcısı olarak göreve başladı.