1. BİLGİ GÜVENLİĞİ

1.1. BİLGİ GÜVENLİĞİ NEDİR?

Bilgi, bir organizasyonun diğer önemli ticari varlıkları gibi önemli bir varlığıdır, dolayısıyla iş ihtiyaçlarına uygun korunmuş olması gerekmektedir. Globalleşen dünyada, bilişim sektörünün artan gücünün bir sonucu olarak bilgiler, giderek artan sayıda ve çeşitlilikte tehditlere maruz kalmaktadır.

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmeli ve uygulanmalıdır. Bu politikalar, faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir. Bilgi güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan güvenlik mühendisliğinin bir alt alanı olarak görülmektedir.

Bilgi güvenliği, “bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak” tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise “kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır”.

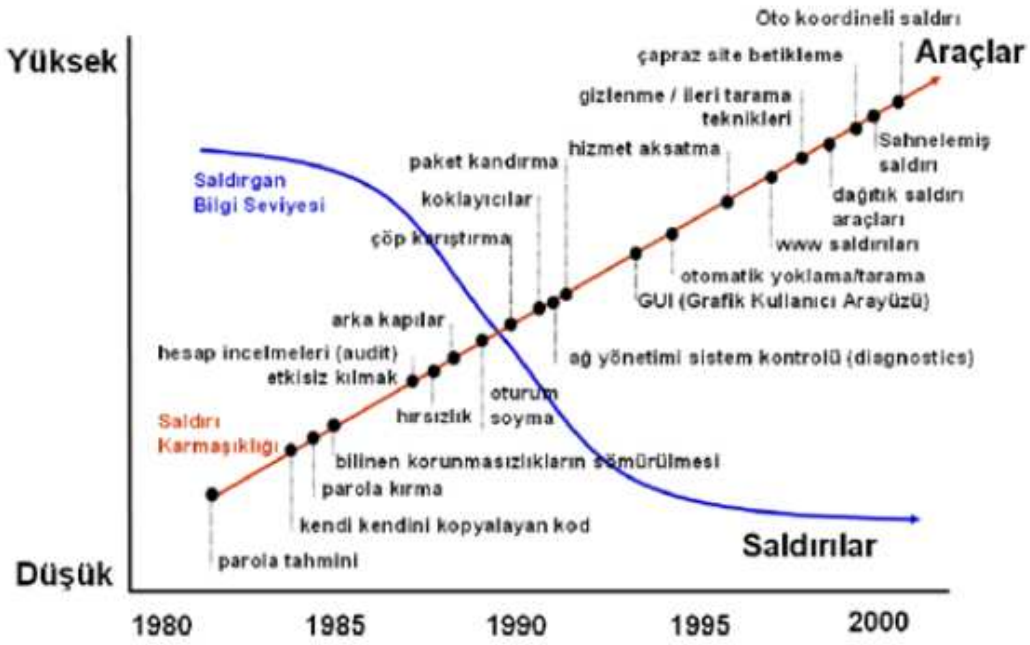
Özellikle ülkemizde, ne yazık ki, birçok kurum ve kuruluşun ve her seviyeden bilgisayar kullanıcısının çoğunlukla bilgi ve bilgisayar sistemlerine ve bilgi güvenliğine bakış açısının yeterli seviyede olmadığı tespit edilmiştir.

Bilgi güvenliği yönetimi, diğer yönetim sistemleri gibi, bir süreklilik gerektirir. Bu nedenle güvenlik yönetimi bir program yönetimi yaklaşımıyla gerçekleştirilmelidir. Program yönetiminden kasıt planlama, gerçekleştirme ve kontrol etme aktivitelerini içeren ve bu aktiviteleri periyodik olarak gerçekleştirmeyi öngören bir yönetim anlayışıdır. Yeni kurulan bir yönetim sistemi bir proje dahilinde kurulabilir. Proje, tanımı gereği bir başı ve bir sonu olan, bir kereye mahsus gerçekleştirilen, yani rutin operasyonları içermeyen bir çalışmadır. Yönetim sisteminin temel yapı taşları bir proje ile geliştirilebilir ancak sistemin devamlılığı ancak program yönetimiyle gerçekleştirilebilir.

1.2. BİLGİ GÜVENLİĞİ NEDEN GEREKLİDİR?

Bilgi ve destek süreçleri, sistemler ve ağlar gibi önemli iş süreçleridir. Bilginin güvenliği rekabet avantajı, nakit akışı, karlılık, yasal uyum ve ticari imaj için gereklidir. Kritik altyapıları korumak için bilgi güvenliği hem kamu sektörü hem de özel sektör için çok önemlidir.

Bilgi ve bilgisayar güvenliğinde, karşı taraf, kötü niyetli olarak nitelendirilen kişiler (korsanlar veya saldırganlar) ve yaptıkları saldırılardır. Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler saldırı veya atak olarak adlandırılmaktadır. Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi, bilgi güvenliği için büyük bir önem arz etmektedir.



Şekil 1 : Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi

Şekilde gösterildiği gibi, saldırılar zamanla ve gelişen teknoloji ile oldukça farklılıklar göstermektedir. Parola tahmin etme ya da işyerlerinde kâğıt notların atıldığı çöpleri karıştırma gibi basit saldırılar, günümüzde artık yerini daha kapsamlı olan çapraz site betikleme (cross site scripting), oto koordineli (auto coordinated), dağıtık (distributed) ve sahnelenmiş (staged) saldırılara bırakmıştır. Saldırılar veya saldırılarda kullanılan araçlar, teknik açıdan gittikçe karmaşıklaşırken, bu saldırıyı yürütecek

saldırganın ihtiyaç duyduğu bilginin seviyesi de gittikçe azalmaktadır. Bu durum saldırı ve saldırgan sayısını, saldırılar sonucunda oluşacak zararları artırırken, saldırıyı önlemek için yapılması gerekenleri de zorlaştırmaktadır.

Son günlerde, bilgi sistemlerinde bilgi güvenliği konusunda zafiyet oluşturan, virüsler, solucanlar, truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımların yanında, reklâm, parazit, hırsız, püsküllü bela yazılım, tarayıcı yardımcı nesnesi, uzaktan yönetim aracı, ticari RAT, bot ağı, ağ taşkını, saldırgan ActiveX, Java ve betik, IRC ele geçirme savaşı, nuker, paketleyici, ciltçi, şifre yakalayıcılar-soyguncular, şifre kırıcılar, anahtar üreticiler, e-posta bombardımanı, kitle postacısı, web böcekleri, aldatmaca, sazan avlama, web sahtekârlığı-dolandırıcılığı, telefon kırma, port tarayıcılar, sondaj aracı, arama motoru soyguncusu, koklayıcı, kandırıcı, casus yazılım ve iz sürme çerezleri, turta, damlatıcı, savaş telefon çeviricileri ve tavşanlar adı altında ve her biri farklı amaçlara yönelik değişik yöntemler kullanan çok çeşitli kötücül yazılımın var olduğu da tespit edilmiştir.

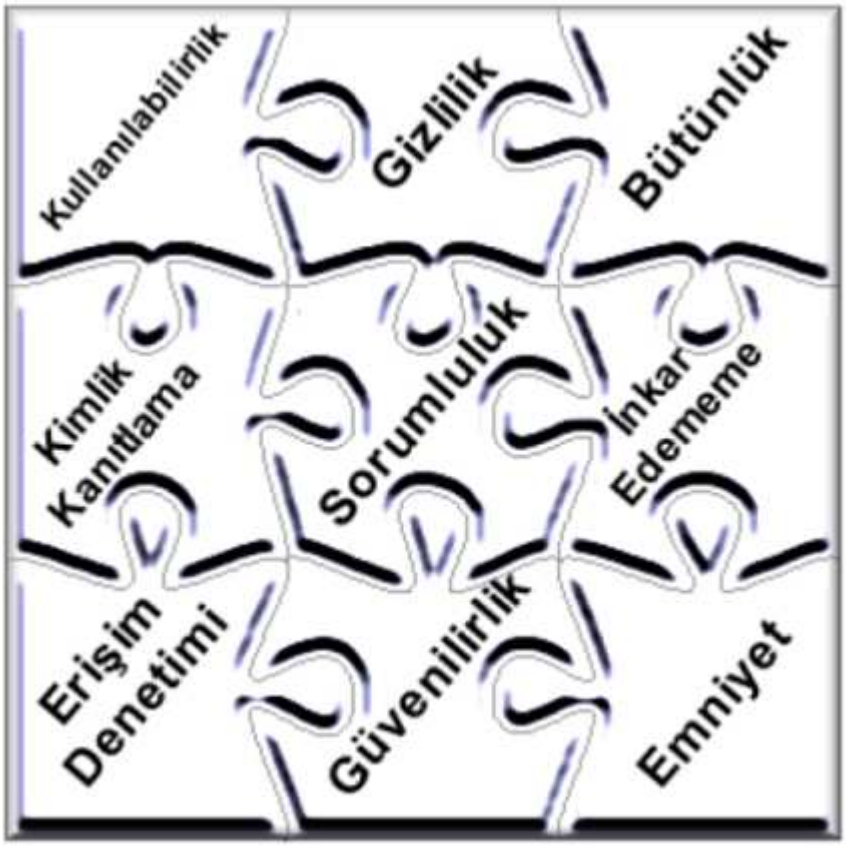
1.3. GÜVENLİK GEREKSİNİMLERİ NASIL SAPTANIR?

Bir organizasyonun güvenlik gereksinimlerini tanımlamak önemlidir. Güvenlik ihtiyaçlarının üç ana kaynağı vardır;

- Birinci kaynak organizasyon için risklerin değerlendirilmesinden sağlanır. Risk değerlendirmesi ile varlıklar için riskler belirlenir ve tehditler tanımlanır.
- İkinci kaynak firmaların ve servis sağlayıcıların ticari ortakları ile yerine getirmesi gereken yasal, resmi, düzenleyici şartlar ve bir organizasyonun sözleşme şartlarıdır.
- Üçüncü kaynak bir organizasyonun faaliyetlerini desteklemek amacıyla bilgi işleme için hedefler, şartlar ve ilkelerin özelleştirilmesidir.

Saldırılar ve zafiyetler karşısında, bilgi güvenliğini sağlamak için bu güvenliği oluşturan unsurların belirlenmesi gereklidir. Bu unsurların yokluğu veya bu unsurlarda oluşabilecek zafiyetler, doğrudan oluşturulmak istenen güvenliğin etkinliğini belirleyecektir.

Bilgilerin, istenmeyen hasarlardan korunması için, en temel açıdan atılması gereken adımlar, güvenlik unsurlarının yerine getirilmesi ile sağlanmaktadır.



Şekil 2 : Güvenlik Unsurları

Gizlilik (confidentiality), bütünlük (integrity), kullanılabilirlik (availability), kimlik kanıtlama (authentication) ve inkâr edememe (non-repudiation) bilgi güvenliğinin en temel unsurlardır. Bunun dışında sorumluluk (accountability), erişim denetimi (access control), güvenilirlik (reliability) ve emniyet (safety) etkenleri de bilgi güvenliğini destekleyen unsurlardır. Bu unsurların tamamının gerçekleştirilmesiyle ancak bilgi güvenliği tam olarak sağlanabilecektir. Şekilden de görülebileceği gibi, bu unsurların bir veya birkaçının eksikliği, güvenlik boyutunda aksamalara sebebiyet verebilecektir. Bu unsurların birbirini tamamlayıcı unsurlar olduğu hiçbir zaman unutulmamalıdır.

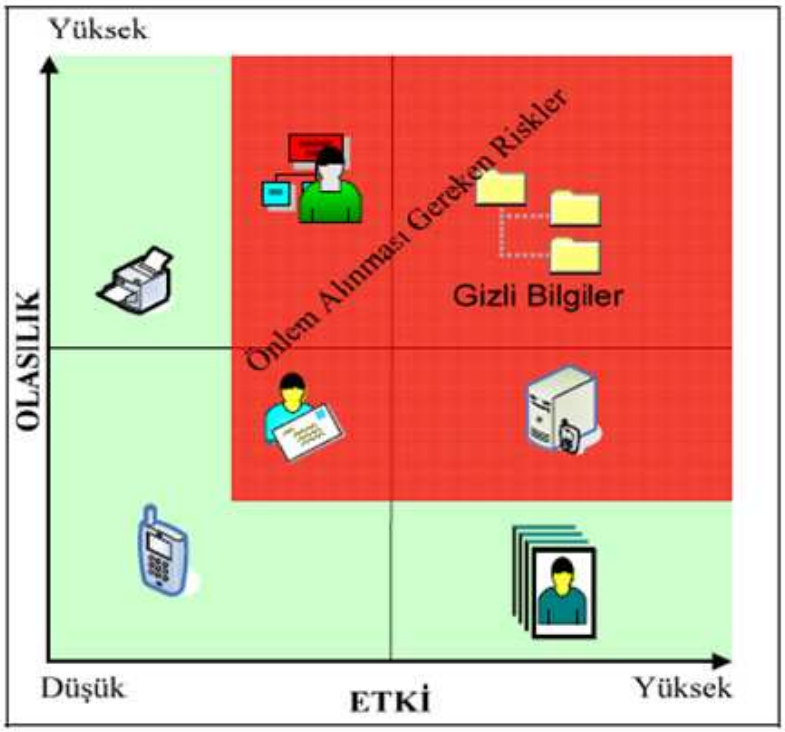
Sorumluluk, belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirleme yeteneğidir. Tipik olarak etkinliklerin kayıtlarını tutmak için bir kayıt tutma (logging) sistemine ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyar. **Erişim denetimi**, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir. **Güvenilirlik**, bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir. **Emniyet**, bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda,

kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları önleme tedbirlerini içermektedir.

Bilgi güvenliği çerçevesinde kurulacak güvenlik sistemi altyapısının ve politikasının doğru bir şekilde belirlenebilmesi için, korunmak istenen bilginin değerlendirilmesi ve güvenlik yönetiminin doğru ve eksiksiz bir şekilde yapılması gerekir. Güvenlik yönetimi, bilgi ve bilgisayar güvenliğini olumsuz yönde etkileyecek faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir.

1.4. GÜVENLİK RİSKLERİNİ DEĞERLENDİRMEK

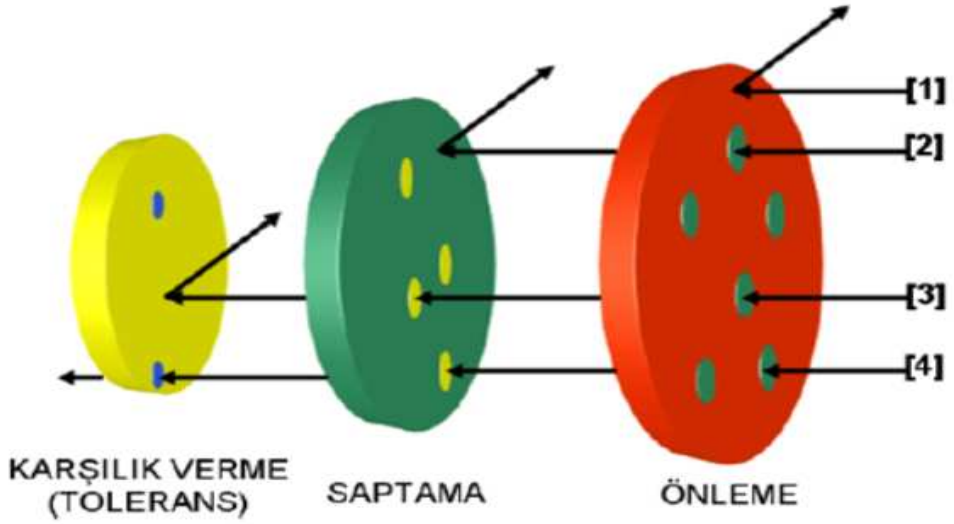
Risk Değerlendirme, hangi bilgi varlıklarının korunacağı belirlendikten sonra kuruluşa uygun risk değerlendirme yönteminin seçilerek risklerin tanımlanması yapılır. Seçilen risk değerlendirme yöntemine göre bilgi varlıkları şekilde örneği gösterilen risk haritasında konumlandırılır. Değerlendirilme yapıldıktan sonra risk değerlendirme haritasında, etkisi ve olasılığı yüksek olan tehditler için risklerin iyileştirilerek kontrol altına alınması işlemlerini kapsar. Risk haritasında bilgi varlıklarının yeri değişebileceğinden risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.



Şekil 3 : Risk Değerlendirme Haritası

Risk, bir olayın ve bu olayın sonucunun olasılıklarının birleşimi olarak tanımlanmaktadır. Risk yönetiminin bir adımı olan risk değerlendirmesi, risklerin tanımlandığı ve tanımlanan bu risklerin etkilerinin ve önceliklerinin belirlendiği bir süreçtir. Risk yönetimi, kabul edilebilir düzeyde bir riskin belirlenmesi, hali hazırdaki riskin değerlendirilmesi, bu riskin kabul edilebilir düzeye indirilebilmesi için gerekli görülen adımların atılması ve bu risk düzeyinin sürdürülmesidir. Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, var olan sistemde bulunan korunmasızlıklar ve güvenlik sistem denetimleri, mevcut riski tayin eden bileşenlerdir. Korunması gereken bilgi ya da varlıkların belirlenmesi; bu varlıkların kuruluşlar açısından ne kadar değerli olduğunun saptanması; bu varlıkların başına gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması; muhtemel kayıpların nasıl cereyan edebileceğinin araştırılması; her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması; bu varlıklarda ger-çekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi ve ileriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların planlanması, risk değerlendirmesinin belli başlı safhalarındandır.

Risk yönetimi sonucunda kurulacak ve yürütülecek güvenlik sisteminin maliyeti, dikkate alınması gereken bir başka önemli husustur. Güvenlik sisteminin maliyeti, korunan bilginin değeri ve olası tehditlerin incelenmesiyle belirlenen risk ile sınırlı olmalıdır. %100 güvenliğin olmayacağı ilkesi ile beraber, bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir. Bu süreçler, önleme (prevention), saptama (detection) ve karşılık vermedir (response ya da reaction).



Şekil 4 : Güvenlik süreçleri ve Saldırılara Tepkileri

Şekil 4’ de güvenlik süreçlerine bir örnek verilmiştir. Bu şekilde, 4 farklı saldırı [1]-[4] ile gösterilmiştir. Şekilden de açıkça görülebileceği gibi, [1] numaralı saldırı, hemen önleme safhasında engellenirken; [2], [3] ve [4] numaralı saldırılar bu safhada önlenememiştir. Önleme sürecini atlatan bu saldırılardan [2] numaralı saldırı, saptama aşamasında tespit edilip, bertaraf edilirken; [3] ve [4] numaralı saldırılar, saptama aşamasından da geçebilmiştir. Belirlenen tolerans ile tasarlanmış son aşama olan karşılık verme safhasında, [3] numaralı saldırı önlenirken; bütün aşamaları atlatıp geçen [4] numaralı saldırı, bütün güvenlik süreçlerini geçip, sisteme zarar vermiştir. Takip eden kısımda güvenlik süreçlerinin her biri, temel özellikleri ile açıklanmaktadır.

Önleme; güvenlik sistemlerinin en çok üzerinde durduğu ve çalıştığı süreçtir. Bir evin bahçesine çit çekmek, çelik kapı kullanmak gibi güncel hayatta kullanılan emniyet önlemleri gibi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karşı, sistemin yalıtılmış olması için çeşitli önlemler geliştirilmektedir. Kişisel bilgisayar güvenliği ile ilgili, virüs tarama programlarının kurulu olması, bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması, bilgisayarda şifre korumalı ekran koruyucu kullanılması, bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması, kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi, disk paylaşımlarında dikkatli olunması, İnternet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi, önemli belgelerin parola ile korunması veya şifreli olarak saklanması, gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi, kullanılmadığı zaman İnternet erişiminin kapatılması, önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır.

Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önleme adımları daha geniş ve karmaşıktır. Güvenlik ile ilgili uzmanlaşmış kişilerin çalıştığı bu tür sistemlerde, önleme ile ilgili yapılanlardan bazıları:

- İşletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi,
- Kullanıcı haklarının asgari seviyede tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması,
- Veri iletişiminde şifreleme tekniklerinin, korunmasızlık tarayıcıları, Sanal Özel Ağ (Virtual Private Network) kullanılması,
- Açık Anahtar Altyapısı (Public Key Infrastructure) ve e-imza kullanımı ile,

- Biometrik tabanlı sistemlerin kullanımı olarak sıralanabilirler.

Aslında önleme sürecinde belirlenen işleyiş mükemmel olabilseydi, daha sonraki süreçlere hiç ihtiyaç duyulmazdı. Yapılan bütün saldırılar en baştan önlenmiş olurdu. Fakat hiç bir güvenlik ürünü kusursuz veya eksiksiz değildir. Ayrıca, hemen hemen her gün, işletim sistemleri, İnternet servisleri, web teknolojileri ve güvenlik uygulamalarında çeşitli açıklar tespit edilmektedir. Bu açıdan bakıldığında saptama ve karşılık verme süreçlerini kullanmak şarttır.

Saptama; güvenlik, sadece önleme ile sağlanabilecek bir mesele değildir. Örneğin bir müzede iyi bir korunmanın sağlanmış olması, müzenin çevresinin çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri bekçi kullanılmamasını gerektirmez. Aynı şekilde bilgisayar sistemlerinde de saldırı girişimlerini saptayacak yöntemlerin de kullanılması şarttır. Önleme, saldırıları güçleştiren (ama imkânsız kılmayan) veya saldırganların cesaretini kıran (ama yok etmeyen) bir engel inşa etmeyi sağlar. Saptama ve karşılık verme olmadan önlemenin ancak sınırlı bir faydası olabilir. Sadece önleme ile yetinilseydi, yapılan çoğu saldırıdan haberdar bile olunamazdı. Saptama ile daha önce bilinen veya yeni ortaya çıkmış saldırılar, rapor edilip, uygun cevaplar verebilir. Saptamada ilk ve en temel basamak, sistemin bütün durumunun ve hareketinin izlenmesi ve bu bilgilerin kayıtlarının tutulmasıdır. Bu şekilde ayrıca, saldırı sonrası analiz için veri ve delil toplanmış olur. Güvenlik duvarları, saldırı tespit sistemleri (intrusion detection system), ağ trafiği izleyiciler, kapı (port) tarayıcılar, bal çanağı (honeypot) kullanımı, gerçek zamanlı koruma sağlayan karşı virüs ve casus yazılım araçları, dosya sağlama toplamı (checksum) kontrol programları ve ağ yoklayıcı (sniffer) algılayıcıları, saptama sürecinde kullanılan en başta gelen yöntemlerden bazılarıdır.

Karşılık verme; bekçiler, köpekler, güvenlik kameraları, algılayıcılarla donatılmış bir yerin, hırsızların dikkatini çekmesi gibi, gerçek zamanlı saptama sistemlerine sahip bilgisayar sistemleri de bilişim korsanları ve saldırganlara cazip gelir. Hızlı karşılık verme, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan esaslı bir öğe olarak ortaya çıkmaktadır. Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırı girişimlerini, mümkünse anında veya en kısa zamanda cevap verecek eylemlerin ifa edilmesi olarak tanımlanabilir. Saldırı tespit sistemleri, bu tespite cevap verecek birilerinin veya bir sistemin olması ile anlam kazanabilir. Aksi takdirde bu durum, hiç kimsenin duyup da önemsemediği bir araba alarmının getireceği faydadan öteye gitmez. Bu açıdan karşılık verme güvenlik sürecini tamamlayan önemli bir halkadır. Saldırı tam olarak önlenmese bile; sistemin normal

durumuna dönmesine, saldırıya sebep olan nedenlerin belirlenmesine, gerektiği durumlarda saldırganın yakalanmasına, güvenlik sistemi açıklarının belirlenmesine ve önleme, saptama ve karşılık verme süreçlerinin yeniden düzenlenmesine olanak verir. Saldırı tespit edilince yapılması gereken işlerin, daha önceden iyi bir şekilde planlanması, bu sürecin etkin bir şekilde işlemesini ve zaman ve para kaybetmemeyi sağlayacaktır. Yıkım onarımı (disaster recovery), bu aşama için gerçekleştirilen ve en kötü durumu ele alan esaslı planların başında gelir.

1.5. BİLGİ GÜVENLİĞİ BAŞLANGIÇ NOKTASI

Güvenlik, içinde birçok unsuru barındıran komple bir çözüm gerektirir. Güvenlik gereksinimlerinin başında veri ve sistemlerin bulunduğu fiziksel ortamın güvenliği yer almaktadır. İyi bir fiziksel güvenlik için önemli veri ve bilgilerin tutulduğu ortamlar güvenlik kameraları ile 24 saat izlenmelidir. Aynı zamanda bu ortamların tanımı yapılmalı ve güvenliğin sağlanması için yapılacak işlemler belirlenmelidir. Hangi personelin bu alanlara girebileceğine dair yetki tanımlamaları ve sınıflamalar yapılmalıdır. Stratejik ve kritik alanlara giriş/çıkış yapacak personelin, malzemenin veya ziyaretçinin nereye girdiğinin ve nereden çıktığının ayrıntılı olarak kayıtları tutulmalıdır.

Kuruluşlar için güvenlik çözümleri, uçtan uca tüm ağı kapsamalı, yazılım ve donanım alt yapısı olarak bir bütün şeklinde değerlendirilmelidir. Dolayısıyla, Güvenlik Duvarı (Firewall) ve antivirüs sistemlerini tek başına kullanmak komple bir güvenlik sağlamak için yeterli değildir. Ayrıca, kurum ve kuruluşların kendi içlerinde bir güvenlik politikasına sahip olmaları ve çalışanlarını bu konuda bilinçlendirmeleri gerekmektedir.

Bir kurumun en büyük hedefi, her türlü ortam (kâğıt, cd, teyp, bilgisayar, ağ, internet vb.) üzerinde bulunan veri ve bilgilerin güvenliğini sağlamak, veri bütünlüğünü korumak ve veriye erişimi denetleyerek gizliliği ve sistem devamlılığını sağlamaktır. Bunun yapılabilmesi için bütün güvenlik çözümlerinin bir arada değerlendirilmesi ve uygulanacak politika doğrultusunda güvenlik önlemlerinin alınması gerekmektedir.

1.6. KRİTİK BAŞARI FAKTÖRLERİ

Günümüzde bilişim teknolojilerinin yaygınlaşması ve günlük hayatımızda yapmış olduğumuz iş ve işlemlerin elektronik ortamlarda hızla yapılmaya başlanması, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir. Bilgi güvenliğini sağlanabilmesi için, bilginin değerinin bilinmesi, yapılan iş ve işlemlerde bu çalışmada incelenen güvenlik unsurlarını, politikalarını ve süreçlerini uygulamak, büyük oranda karşılaşılacak sıkıntıları ve tehlikeleri azaltacak, işgücü, zaman ve parasal kayıpları

önleyecek, Internet üzerinden gelebilecek zararlı yazılımları veya program parçacıklarına karşı kişisel ve kurumsal bilgi güvenliğinin sağlanmasında büyük katkılar sağlayacaktır.

Bilgi güvenliği konusunda zafiyetlerle karşılaşılmaması için, kişilerin ve kurumların alması gereken ve basitten en karmaşık yöntemlere kadar bir dizi önlemler vardır. Ancak, tüm önlemler alınmış dahi olsa, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş kendini %100 güvende hissetmemelidir. Saldırıların elektronik ortamlardan kötü niyetli kişilerden gelebilmesinin yanı sıra, arkadaşlarımızdan ve tanıdığımız kişilerden de gelebilecek sosyal mühendislik altında incelenen tehditler de bulunmaktadır.

Genel olarak, bilgi ve bilgisayar sistemleri konusunda ne kadar önlem alınırsa alınsın, riskleri sıfıra indirgemenin çokta mümkün olmadığının farkında olunmasında fayda vardır. Alınması gereken en temel önlemler, risklere karşı sürekli uyanık olmak, bu çalışmada açıklanan süreçlerin meydana getirildiği güvenlik politikalarını etkin bir şekilde oluşturup kullanmak, oluşturulan süreçlerin başarımını sürekli olarak izlemek ve elde edilen sonuçlar ve yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirgemek olarak sıralanabilir.

İnceleme sonucunda, bilginin ve teknolojinin iç içe olduğu ve teknolojinin baş döndürücü bir hızla gelişen ve yayılan elektronik ortamları desteklemesi, her zaman yanı başımızda olacak bilgisayar korsanı gibi kötü niyetli kişilerin veya bu tür kişilerin yazdığı casus yazılımların, sistemlerin açığını bulma da, bu açıkları kullanıp sistemlere izinsiz erişmede ve sistemlere ve sistemi kullanan kişilere, kişisel veya kurumsal zarar vermede hemen hemen her yolu denemeye çalıştıkları tespit edilmiştir. Bu saldırı ve tehditlere karşı tedbir alınabilmesi için, bu tür yazılımların ve kullanılan yöntemlerin sürekli olarak incelenmesi gerektiği elde edilen bulgular arasındadır.

Dünyada ve ülkemizde bilgi güvenliğine yönelik en önemli tehditlerden olan kötücül ve casus yazılımların, yaygın olarak kullanımda olduğu fakat kullanıcıların bu tür saldırı ve tehditlerinden çoğunlukla haberdar olmadığı anlaşılmıştır. Her hangi bir zararla karşılaşıl-maması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, hassasiyet gösterilmesi ve gereken önlemlerin alınması ve farkındalık oluşturulması gerekmektedir.

2. KAPSAM

Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmanın ilk aşaması, kapsamın belirlenmesidir. Bilgi varlıklarının belirlenmesi, sahiplerin atanması, güvenlik seviyelerinin sorgulanması, risklerin ve mevcut durumun ortaya konması kapsam tarafından yönlendirilir. Özellikle ISO 27001 sertifikasını amaçlayan bir yönetim sistemi kuruluyorsa, hangi süreçlerin, departmanların, şehirlerin kapsam içine alınıp, hangilerinin dışarıda bırakılacağı daha da büyük önem kazanır.

Ancak burada bazı sorularla karşı karşıya kalırız: Bilgi güvenliği kapsamını dilediğimiz gibi seçebilir miyiz? Hangi seçim yolu izlendiğinde daha kolay ve başarılı sistemler kurulabilir? Kapsamın seçimi sadece yönetimin isteğine mi bağlıdır? Kurumu herhangi bir yerinden dilimleyip, istediğimiz gibi bir kapsam belirleyebilir miyiz?

Bu soruların cevabını önce TS/ISO 27001 standardını inceleyerek bulmaya çalışalım. Standartta yer alan, "Bu standartta, 'iş' terimi geniş anlamda kuruluşun varlık amaçlarının temeli olan etkinlikler anlamına gelmektedir."(*) açıklaması, kapsamın mutlaka kuruluşun varlık amaçlarının temeli olan etkinlikleri içermesi gerektiğini söylemektedir. Ayrıca, aynı standardın 4.2.1.a maddesi de "... kapsamdan herhangi bir dışarıda bırakmanın ayrıntıları ve açıklamasını da ekleyerek, BGYS kapsamını ve sınırlarını tanımlama" zorunluluğunu ortaya koymaktadır.

Standart maddelerinden de anlaşıldığı gibi, BGYS kapsamının, tüm şirket olma zorunluluğu yoktur, ama şirket varlık amaçlarını içermesi gerekmektedir. Örneğin, bir finans kuruluşu, kendi finansal işlerinden ya da süreçlerinden sadece bir kısmını kapsam olarak tanımlayabilir, ancak kapsamı sadece "çalışanların izin bilgileri" olarak vermesi çok işe yarar olmayacaktır. Burada çalışan izinleri, kurumun varlık amaçları içinde yer almamaktadır. Oysa bir holdingin insan kaynakları firması için izin bilgileri en kritik bilgiler arasında yer alabilir ve kapsam olarak seçilebilir.

Kapsam seçerken, kurum için kritik bir bilgi/bilgi grubu seçilebileceği gibi, bir ya da birden fazla iş süreci ya da bir departmandaki tüm süreçler kullanılabilir. BGYS kurulması genellikle süreçler üzerinden devam ettiğinden, kapsamın süreçlere bağlı olarak seçilmesi çok daha yararlıdır. Kurumun BGYS kapsamının, bilgi güvenliği açısından en gelişmiş süreçlerinden/departmanlarından başlaması da bir başka avantajdır. Böylece BGYS kurma çalışmaları sırasında güvenlik seviyesinden çok, sistem kurmaya ağırlık vermek mümkün olacaktır.

Kapsam yazılı hale getirilirken içinde yer alan süreç, önemli varlıklar, ofisler, bağlantılar, ilişkiler ve anlaşmalar tanımlanmalıdır. Kapsam içine almanın ve dışında bırakmanın nedenlerinin de yazılı hale getirilmesi, bu kapsamla çalışacak tüm proje

ekibinin istekleri daha iyi anlamasına ve daha doğru kararlar vermesine yardımcı olacaktır. Ayrıca, kapsam tanımı ne kadar ayrıntılı yapılırsa, kapsam içi ile kapsam dışı arasındaki gri alanlar ne kadar ince bir çizgi haline getirilip yazılı hale sokulursa, proje başlangıcı o kadar kolaylaşır ve başarı olasılığı o kadar artar.

Kapsam seçimi sırasında kullanılabilecek bir yöntem de, şekilde görüldüğü gibi, bir şema (görsel kapsam) hazırlanmasıdır. Görsel kapsama, kapsam içindeki departman ve süreçler, bunların ilişkili olduğu diğer şirket içi (ama kapsam dışı bırakılan) departman/süreçler ve son olarak şirket dışı kapsamla ilişkili kurumlar yerleştirilir. Daha sonra, kapsam ile dışındakiler arasındaki veri akışları oklarla belirtilir. Bu okların (şekilde kalın çizgiyle gösterilmiştir) kapsam sınırlarını kestiği yerler ise, bize, anlaşmanın ya da mutabakatın zorunlu olduğu noktaları işaret eder. Tüm bu işaretli yerleri tanımlayan en az bir yazılı dokümanın bulunması ilişkilerin anlaşılmasını da kolaylaştıracaktır.

Kapsam belirlemek kadar önemli olan bir diğer konu, bilgi güvenliği yönetim sistemini kurmaya başladıktan sonra ilk döngü tamamlanana kadar kapsamı değiştirmemektir. Kapsam, beraberinde hemen tüm BGYS süreçlerini, varlıklarını, ilişkilerini ve anlaşmalarını tanımlar. Bu yüzden kapsamın değişmesi, tüm bu ilişkilerin yeniden değerlendirilmesini gerektirir.