Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi **23** (1-2) 1 - 12 (2007)
http://fbe.erciyes.edu.tr/
ISSN 1012-2354

BİLGİSAYAR SİSTEMLERİNE YAPILAN SALDIRILAR VE TÜRLERİ: BİR İNCELEME

Gürol CANBEK, Şeref SAĞIROĞLU*

Gazi Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara, TÜRKİYE

ÖZET

Günümüzde bilgisayar sistemlerinin güvenliği arttırılmasına rağmen, bu sistemlerine yapılan saldırılar da artmaktadır. Bu sistemlerin sahip olduğu güvenlik yapısını aşmaya çalışan saldırılar ile alınan karşı tedbirlerin sayısının da yükseldiği ve farklılıklar gösterdiği tespit edilmiştir. Bu tür saldırılardan korunmak için; yapılan tüm saldırıların takip edilmesi, gelişiminin izlenmesi, bilgisayar güvenliğinin yeterli ve etkin bir seviyede oluşturulmasında önemli bir gereksinimdir. Bu makalede; bilgisayar sistemlerine yapılan saldırılar incelenmiş; saldırı-saldırgan ilişkisi değerlendirilmiş; saldırıların ortak olarak sahip olduğu karakteristikler sunulmuş; yapılan saldırıların gelişimi irdelenmiş ve temel saldırı türleri gözden geçirilmiştir. Sonuçta; bilgisayar sistemlerine yapılan saldırılarda, kullanılan yöntemler ve metodolojiler iyi bilinmesinin, saldırganların hedefi olan sistemlerin güvenliği sıkılaştırılmasının, saldırı karakteristikleri izlenmesinin, saldırılarda hedef alınan korunmasızlıklar ile zayıflıkların giderilmesinin ve alınacak tedbirlerde saldırgan profillerinin de mutlaka dikkate alınmasının faydalı olacağı değerlendirilmektedir. Bunun yanında; bilgisayar sistemleri güvenliği, doğru ve etkili bir şekilde sağlanmak korumak için alınacak tedbirlerde güvenlik yaşam döngüsü mutlaka uygulanmalı ve bu çerçevede karşılaşılacak zayıflıklar ve eksiklikler giderilmelidir.

Anahtar Kelimeler: Saldırı, Bilgisayar güvenliği.

ATTACKS AGAINST COMPUTER SYSTEMS AND THEIR TYPES: A REVIEW STUDY

ABSTRACT

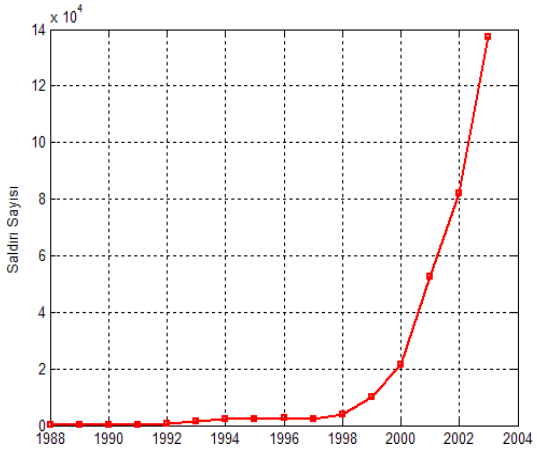
Although computer system security being upgraded day by day, the attacks against the systems have also increased. The attacks attempting to bypass the system increase in diversity and quantity. Monitoring and evaluating the attacks are essential requirements for building up a sufficient and efficient information and computer security system. In this study, we have reviewed the attacks conducted to computer system; evaluated attack-attacker relation; presented the common characteristics of attacks; inspected the tendency of the conducted attacks and fundamental attacks types. Consequently, the methods and methodology used in the attacks against computer systems must be studied. Targeted systems under attacks must be secured and upgraded. The characteristics of the attacks must be traced. The targeted vulnerabilities and weak points must be eliminated, and the attacker profile must be taken into account while determining the precautions. We can conclude that it is necessary to apply the security life cycle in securing the systems truly and efficiently to liminate the weaknesses and deficiencies faced in computer security systems to reduce the losses.

Keywords: Attack, Computer security.

***E-posta:** ss@gazi.edu.tr

1. GİRİŞ

Bilgisayar sistemlerine karşı yapılan saldırılar sıklık ve karmaşıklık bakımından gün geçtikçe artma eğilimi göstermektedir. İlk zamanlarda, bilgisayar korsanı (hacker) olarak adlandırılan saldırganların idealistlik ve dikkat çekme güdüleri ile kendilerini boy gösterdikleri bir yöntem olan saldırılar, günümüz bilgisayar ve bilgisayar ağı sistemlerinde var olan açıklar sebebi ile bir endüstri halini almıştır. 2005 yılında CERT/CC İstatistiklerinde rapor edildiği gibi, 2000 yılından beri var olan saldırı çeşidi 6 kat artarak 2005'de 4000'e kadar ulaşmış; yaklaşık 150000 saldırı olayı saptanmıştır [1]. 1988 ile 2003 yılları arasında bildirilen saldırı sayıları Şekil 1'de gösterilmektedir.



Şekil 1. 1988-2003 yılları arasında bilgisayar sistemlerine rapor edilen saldırıların sayısı [1].

Artan bu saldırılara karşı geliştirilmek istenen güvenlik süreçlerinin belirlenmesinde yapılan ön teorik çalışmalar dışında; var olan sistemlere yönelik gerçekleşmiş veya gerçekleşebilecek olan saldırıların birer sayıdan öte, çok incelenmesi ve analiz edilmesi gerekmektedir. Sonuçta; güvenlik süreçleri hayali saldırıları önlemekten çok; gerçekten karşılaşılabilecek saldırılara yönelik sistemin gözden geçirilmesi ve tasarlanmasıdır. Yani oluşturulacak güvenlik sistemine sadece kendi tarafımızdan değil; dışardan, saldırganın tarafından bakılması gereklidir. Adi Shamir tarafından bu konuda söylenen "Güvenlik atlatılır, saldırılmaz" sözü bu bakışı özetlemektir [2]. Böyle bir bakış açısı Şekil 2'de çok güzel bir şekilde tasvir edilmektedir. Otoparka izinsiz giriş yapmak isteyen araçlar, yol üzerinde bulunan kontrol noktasındaki engeli yıkmak veya aşmak yerine; bu engelin çevresinden dolanmaktadır. Aslında bilgisayar sistemlerine yapılan saldırılar, çoğunlukla doğrudan güvenlik sistemini hedef alacak şekilde değil; güvenlik sistemine fark etmeden istenileni elde edecek şekilde yapılmaktadır.

Şekil 2. Saldırı yerine atlatmanın tercih edilmesi.

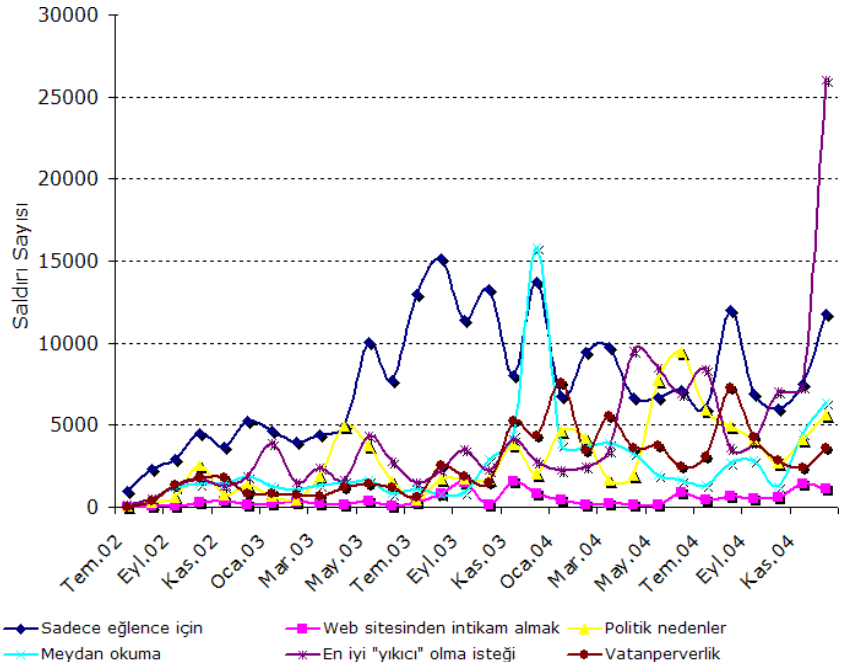
Bunun için saldırgan, sistemin korunmasızlıklarını araştırır ve ona göre hareket eder. Korunmasızlık (vulnerability), ilgili sistem, ağ, uygulama veya protokolün güvenliğini tehlikeye atan; beklenmeyen ve istenmeyen bir olaya sebep olabilecek bir zayıflığın varlığı, tasarım veya gerçekleme hatası olarak tanımlanmaktadır [3]. Bilgisayar sistemlerinin güvenliği ile ilgili geliştirilen yöntemlerin anlaşılması için bu korunmasızlıkları hedefleyen saldırı (atak) türlerinin belirlenmesi ve bu saldırılara karşı alınabilecek önlemlerin geliştirilmesi gerekmektedir.

Bu çalışmada, Bölüm 2'de saldırı olgusu tanımlanmış, saldırıların zamanla ulaştığı nokta ile saldırıyı yürüten saldırganları bunu yapmaya iten sebepler irdelenmiş, saldırıların zamanla gelişimi incelenmiş ve yapılan tüm saldırıların ortak olarak sahip olduğu temel karakteristikler ele alınmıştır. Bölüm 3'de saldırıların ne gibi etkenlere göre sınıflandırılabileceği incelenmiştir. Bölüm 4'de ise en temel saldırı türleri ele alınmıştır. Bölüm 5'de, sunulan bu çalışma genel olarak değerlendirilmiş ve elde edilen bulgular tartışılmıştır.

2. BİLGİSAYAR SİSTEMLERİNE YAPILAN SALDIRILAR

Bilgi ve bilgisayar güvenliğinde; karşı taraf, genel olarak kötü niyetli olarak nitelendirilen kişiler (korsanlar) 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 [4]. 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.

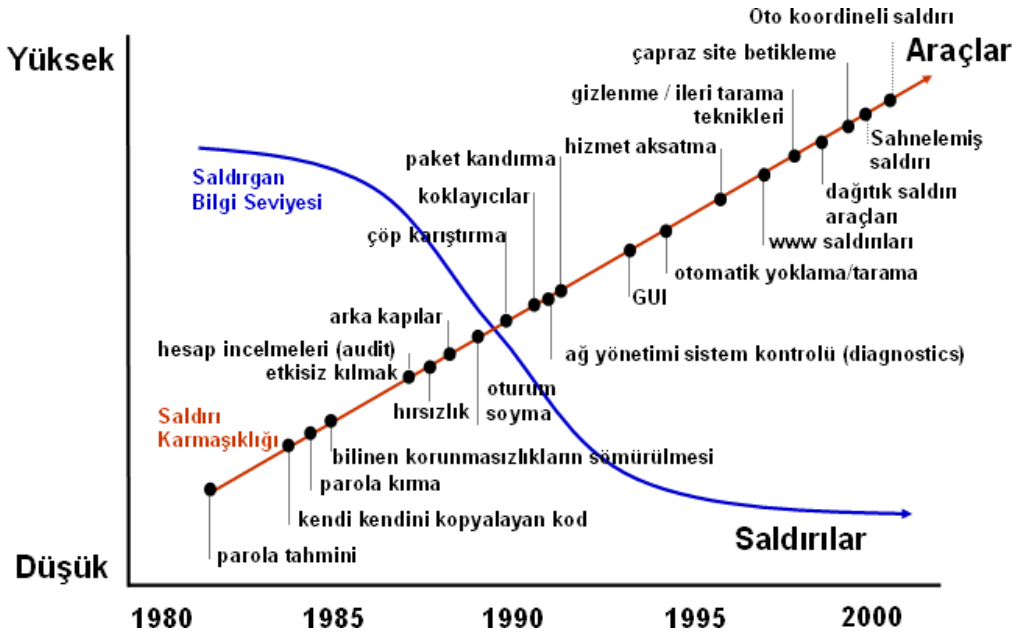
Bilgisayar sistemlerine yapılan saldırıların neden gerçekleştirildiğini anlamak, saldırıların ve alınabilecek önlemlerin belirlenmesinde önemli bir veri sağlayacaktır. Genel olarak bir saldırganı bu yola iten sebepler takip edilmelidir. Bu konuda İnternet web sunucularına yapılan saldırılara ait bilgileri, doğruladıktan sonra sınıflayıp, tutan Zone-H oluşumunun, yaklaşık bir milyon sunucuya ait, geçmiş yıllara dayanan istatistikleri saldırganın saldırı yapmaya iten sebepleri de göstermektedir [5]. 2002-2004 yılları arasında saldırı sebepleri; "sadece eğlence için", "web sitesinden intikam almak için", "politik sebepler", "meydan okuma", "en iyi yıkıcı olmak için" ve "vatanperverlik" olarak sınıflandırılmıştır. Bu nedenlere göre yapılan saldırıların 2002-2004 yılları arasında dağılımı Şekil 3'de gösterilmektedir.



Şekil 3. Korsanlık nedenleri.

Şekil 3'den de görülebileceği gibi, sanal dünyada sayısal vandalizm, saldırganları güdüleyen en büyük etken olarak karşımıza çıkmaktadır [6]. Korsanların İnternet sitelerine daha çok, en iyi yıkıcı (defacer) olmak için ve sadece eğlence için saldırdıkları görülmektedir.

Saldırganların sahip olduğu veya olması gereken teknik bilgi seviyesi ve yaptıkları saldırıların boyutları da zamanla değişim göstermektedir. Şekil 4'de gösterildiği gibi, saldırılar zamanla ve gelişen teknoloji ile oldukça farklılıklar göstermektedir. Parola tahmin etme ya da işyerlerinde kağıt notların atıldığı çöpleri karıştırma gibi basit saldırılar, günümüzde artık yerini daha kapsamlı olan çapraz site betikleme (cross site scripting) [7], oto koordineli (auto coordinated), dağıtık (distributed) ve sahnelenmiş (staged) saldırılara bırakmıştır. Saldırılar veya saldırılarda kullanılan araçlar teknik açıdan gittikçe karmaşıklaşırken, saldırıları 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.

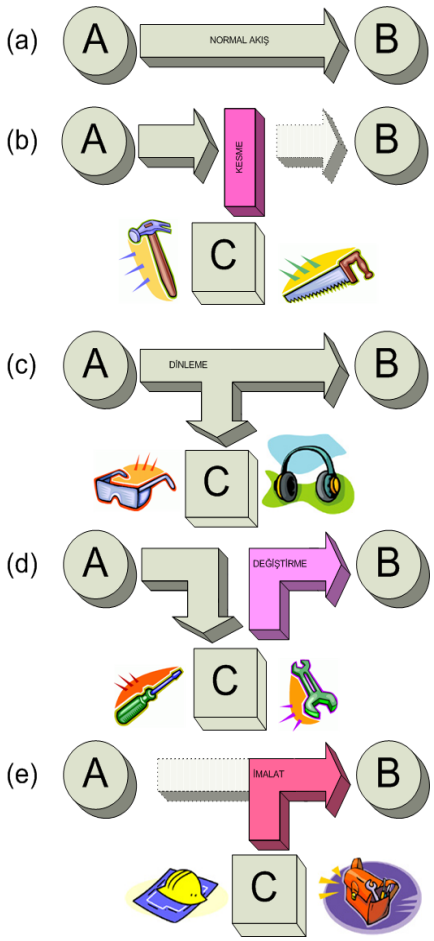


Şekil 4. Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi [8].

Normal ve sistem tarafından olması istenilen bilgi akışına yapılan saldırılar dört değişik karakteristik sergileyebilmektedir. Bunlar yarıda kesme (interruption), gizli dinleme (intercept), değiştirme (modification) ve imalat veya üretim (fabrication) olarak adlandırılmaktadır [9]. Şekil 5'de bu saldırı ve tehdit karakteristikleri gösterilmektedir.

Şekil 5'den de görülebileceği gibi, A ile B arasındaki iletişimde; C bu iletişime farklı şekillerde dahil olabilir. Bu şekillerden;

- **yarıda kesmede**, kaynak ve hedef arasındaki bilgi akışına engel olunarak iletişim koparılır. Burada sistemin değerli bir varlığı (yazılım, belge, veri, bilgi, vb.) yok edilir, erişilemez veya elde edilemez hale getirilir.
- **gizli dinlemede**, kaynak ve hedef arasındaki bilgi, saldırgan tarafından çeşitli şekillerde elde edilerek bilgi okunur. Burada yetkisiz taraf sistemin değerli bir varlığına erişim kazanmaktadır. Pasif saldırı olarak da tanımlanır. Gizli dinle dışındaki diğer tüm karakteristikler aktif olarak sınıflanmaktadır.
- **değiştirmede**, kaynak tarafından hedefe gönderilmek istenen bilgi, araya girilerek elde edilir ve bu bilgi üzerinde değişiklik yapılarak, hedefe kaynaktan geliyormuş gibi gönderilir. Burada, yetkisiz taraf sisteme erişim hakkını kazanmakla kalmaz, ayrıca sistemin değerli bir varlığını değiştirir.
- **imalat veya üretimde** ise, saldırgan tarafından üretilen suni bir bilgi, sanki kaynaktan geliyormuş gibi hedefe gönderilmesidir. Burada yetkisiz taraf, sisteme sahte nesneler ekler.



Şekil 5. Saldırı tehdit karakteristikleri: (a) Normal bilgi akışı. (b) kesme (c) dinleme (d) değiştirme (e) imalat veya üretim.

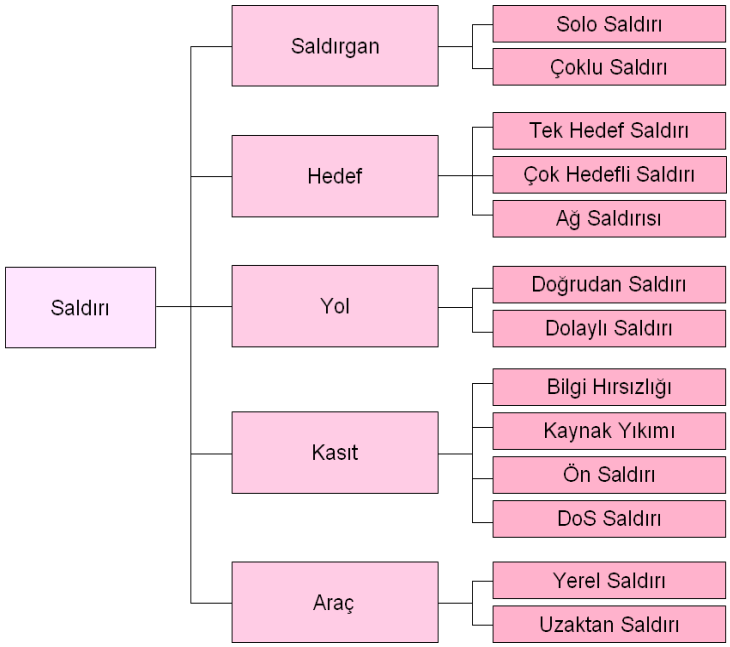
Tablo 1'de her bir saldırı karakteristiğin hangi güvenlik unsuruna karşı yapıldığı, bu saldırıda kullanılan yaklaşımlara örnekler ve her bir saldırı karakteristiğine karşı geliştirilen genel çözüm önerileri gösterilmektedir.

Tablo 1. Güvenlik unsurlarına yapılan saldırılar, kullanılan yaklaşımlar ve bu saldırılara önerilen çözümler.

Saldırı	Hedef Güvenlik Unsuru	Yaklaşımlar	Çözüm
Yarıda kesme (interruption)	kullanılabilirlik (availability)	• Donanım yıkımı • İletişim hatlarına fiziksel hasar verme • Gürültü yayma • Rota (routing) şaşırtma • Program ve dosya silimi • DoS (hizmet aksattırma) saldırıları	Etkin bir çözüm yok.
Gizli dinleme (intercept)	gizlilik (confidentiality) ve kişisel gizlilik (privacy)	• Gizli dinleme (Eavesdropping) • Hat izleme • Paket yakalama • Sistemle uzlaşma	Şifreleme/şifre çözme
Değiştirme (modification)	bütünlük (integrity)	• Veritabanı kayıtlarını değiştirme • İletişimde gecikmelerden yararlanma • Donanımda değişiklik yapma	Her bir mesaj paketi için sayısal imza kullanımı
İmalat veya üretim (fabrication)	asıllık (authenticity)	• Veritabanına yeni kayıt ekleme • IP kandırma ile yeni ağ paketi ekleme • Sahte e-posta veya bölge adları kullanma	Kimlik kanıtlama (authentication)

3. SALDIRILARIN SINIFLANDIRILMASI

Saldırılar çeşitli şekillerde sınıflandırılarak incelenebilir. Saldırgan sayısına, hedef türüne, kullanılan yola, kasıt ve araçlara göre saldırılar,
Şekil 6'da gösterildiği gibi sınıflanmaktadır.



Şekil 6. Saldırıların sınıflandırılması.

Tek bir saldırgan tarafından yürütülen solo saldırı, en genel türde saldırıların başında gelir ve saptanması daha kolaydır. Sistem korunmasızlık saldırıları ve yetkisiz erişim, solo saldırı türündedir. Birden fazla saldırganın karıştığı saldırılar, çoklu saldırı olarak adlandırılır. IP kandırma (spoofing) [10], e-posta bombardımanı [11] ve ağ taşkını (flooding) [12] bu tür saldırılardır. "Back Orifice" ve Winnuke saldırıları gibi saldırılar, tek hedefe yönelik saldırılardır. Anormal paket yayınlama saldırısı, tarama saldırısı ve anonim FTP saldırısı çok hedefli saldırılardır. DNS kandırma (DNS Spoofing) [13], yönlendirici (router) saldırısı ve ağ DoS (Denial of Service, hizmet aksattırma) saldırısı, ağ saldırı türüdür. Doğrudan saldırılar arasında arabellek taşması, ölümüne ping (ping of death) saldırılarını saymak mümkündür. Yerel saldırılar sisteme giriş (login) yapıldıktan sonra gerçekleştirilmektedir.

4. SALDIRI TÜRLERİ

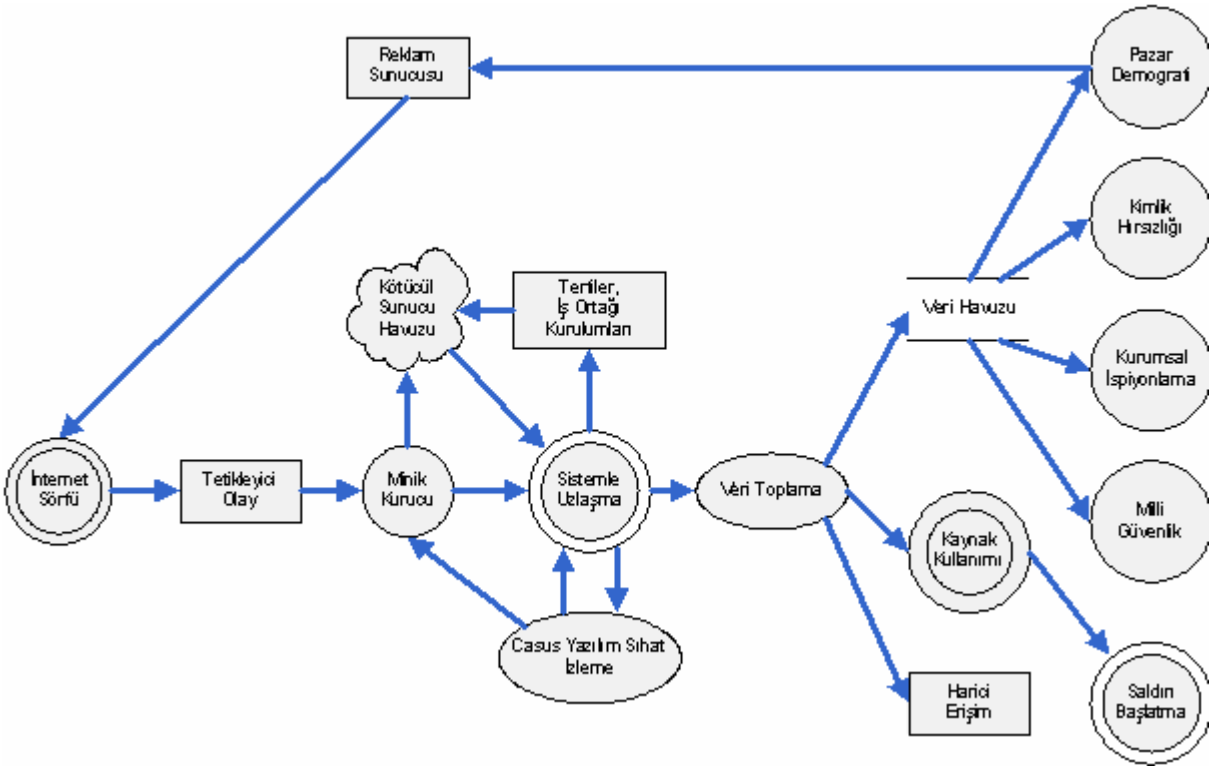
Başlıca saldırı türleri arasında, kaynak kod istismarı (code exploit), gizli dinleme (eavesdropping), hizmet aksattırma saldırıları (DoS), dolaylı saldırılar, arka kapılar (backdoor), doğrudan erişim saldırıları, sosyal veya toplum mühendisliği ve kriptografik saldırıları saymak mümkündür. Bu saldırılar aşağıda sırasıyla açıklanmaktadır.

4.1. Kaynak Kod İstismarı (Code Exploit)

Sistemde kullanılan (işletim sistemi için hazırlanan sistem programları dahil) tüm yazılımlarda var olabilecek arabellek taşması (buffer overflow), CGI betikleme (scripting) hataları ve şifreleme hataları gibi yazılım kusurları, bir bilgisayar sisteminin kontrolünün ele geçirilmesine veyahut o bilgisayarın beklenmedik bir şekilde çalışmasına neden olabilir. Bu, son yıllara kadar gözden kaçırılan bir konu olarak, bir çok saldırıya açık kapı bırakmış bir korunmasızlıktır. Bazı yazılım firmalarının rekabet, karlılık gibi sebeplerle geliştirdikleri yazılım paketlerinde saptadıkları kimi hatalar için hata ayıklaması ve düzeltmesi yapmadan ürünü bir an önce piyasaya çıkarttığı bile

belirtilmektedir [14]. Özellikle işletim sistemi yazılımları tasarlanırken, geliştirilirken ve test edilirken, güvenliği hiç bir şekilde göz ardı etmeyecek çalışmalara ihtiyaç vardır. En çok kullanılan işletim sistemi olarak belirtilen Microsoft Windows işletim sisteminde, bu tür kaynak kod kusurları, hazırlanan güvenlik bültenleri ile kullanıcılara duyurulmakta, çok önemli düzeltmeler ("hot-fix") ve belirli aralıklarda çıkan hizmet paketleri, kullanıcılara gerek çevrimiçi gerekse CD gibi ortamlarda sunulmaktadır. Bu düzeltmelerin çokluğu, işletim sistemi geliştirilmesi sırasında öngörülmeyen veya dikkat edilmeyen yazılım kusurlarının çokluğuna işaret etmektedir. Bu konuda Microsoft firması, piyasaya çıkardığı işletim sistemi yazılımları için güvenliği merkeze alan çalışmalara hız vermiştir. "Güvenlik Geliştirme Yaşam Döngüsü" (SDL, Security Development Lifecycle) yaklaşımı ile geliştirilen Windows Server 2003'ün, Windows 2000'e göre çok daha az güvenlik bülteni ile piyasaya sürüldüğü belirtilmektedir [15]. Microsoft, güvenliğin önemini algılamış ve bu konudaki yatırımlarını ve çalışmalarını artırmaya başlamıştır [16].

Şekil 7'de İnternet tarayıcısı güvenlik ayarlarının yeterli seviyede verilmediği veya güncel sürümünün kullanılmadığı bir durumda yararlanılan "kaçak indirme" (drive-by download) kaynak kod istismarı ile yapılan bir casus yazılım saldırısı ve bu saldırının sonucunda sisteme karşı yürütebileceği faaliyetler gösterilmektedir [17]. Bu tür saldırılar, İnternet tarayıcılarında bulunan kaynak kod korunmasızlıkları bir bilgisayar sistemini ele geçirmek için sıklıkla kullanılmaktadır.



Şekil 7. Kaynak kod istismarı ile hedef sisteme yerleşen casus yazılımın yaşam döngüsü.

Buna göre İnternet üzerinde web sayfalarında gezinirken kötücül sitelere ait sayfalarda yer alan betik kodları istemcinin tarayıcısında saptadığı uygun bir korumasızlıktan yararlanarak minik bir kurucu programını çalıştırtmayı başarır. Bu program sistemle uzlaşarak faaliyetlerini başlatır. Burada istenilen casus yazılımlar sunucu tarafına kullanıcının haberi olmadan aktarılabilir. Bu çerçevede; çalışmakta olan casus yazılımın işlerliliğini sürekli olarak izleyen bir yapı da bulunabilir. Bu yapı, casus yazılımı silmeye veya parçalarını atmaya yönelik girişimleri saptadığında casus yazılımı çeşitli tekniklerle yeniden ayağa kaldırabilir. Sistemde sorunsuz bir şekilde çalışan casus yazılım için amaç, bilgi toplamaktır. Bu bilgiler; pazar araştırması, kimlik hırsızlığı, kurumsal ispiyonlama ve hatta milli güvenlik için kullanılabilir. Bu tür bir casus yazılım, konakladığı bilgisayara harici bir erişim imkanını da

sağlayabilir ya da sistem kaynaklarını, kullanıcının haberi olmadan başka saldırıları koordine etmek için kullanabilir.

4.2. Gizli Dinleme

Bir ağ veya kanal üzerinden iletilen verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasıdır. Bu saldırı tipinde, hatta kaynaktan hedefe giden verinin arada elde edilip, değiştirilerek hedefe gönderilmesi bile mümkündür. İngilizce "eavesdropping" (saçak damlası) olarak adlandırılan bu saldırının, sanıldığının aksine çok farklı uygulama alanı bulunmaktadır. Hiç bir bilgisayarla etkileşimi olmayan tek başına çalışan bir bilgisayar bile, mikroçip, ekran veya yazıcı gibi elektronik parçalarından yayılan elektrik veya elektromanyetik yayılım takip edilerek gizlice dinlenebilir. Bu cihazların bu tür dinlemelere olanak vermemesi için, Amerikan hükümeti 1950'li yılların ortasından başlayarak TEMPEST adında bir standart geliştirmiştir.

4.3. Hizmet Aksattırma Saldırıları (DoS, Denial of Service)

Hizmet aksattırma saldırıları, yetkisiz erişim veya sistem kontrolünü ele geçirmeye yarayan saldırılardan farklı bir amaç için gerçekleştirilen saldırılardır. Bu saldırının tek amacı, bir bilgisayar, sunucu veya ağın kaldırabileceğinden daha fazla yük bindirilmesi sağlanarak; sistemin kullanılmaz hale getirilmesidir. Bu tip saldırılar genelde bant genişliği, boş disk alanı veya CPU zamanı gibi bilgi işlem kaynaklarının tüketilmesi; yönlendirme (routing) bilgileri gibi yapılandırma bilgilerinin bozulması ve fiziksel ağ bileşenlerinin bozulması şeklinde yapılmaktadır. Ağ üzerinde kilit önem taşıyan bir sunucuya yapılan bu tip bir saldırı, tüm ağın işlemez hale gelmesine yol açabilir. Bu saldırıları önlemek için tüm ağın analizi gerektiğinden, saldırıların önüne geçilmesi çok zordur. Dağıtık hizmet aksattırma saldırıları (DDoS, Distributed Denial of Service), tek bir kaynaktan değil de birden fazla ele geçirilmiş konak bilgisayardan, tek bir hedefe doğru yapılan hizmet aksattırma saldırısıdır. Yeterli sayıda saldırgan bilgisayar kullanarak, çok büyük ve iyi ağ bağlantılı web sitelerinin hizmetleri bile aksattırılabilir.

4.4. Dolaylı Saldırılar

Bu tür saldırılar, uzaktan erişilerek devralınmış üçüncü parti bir bilgisayardan başlatılan değişik türde saldırıları kapsamaktadır. Hayalet bilgisayar (zombie computer) olarak adı geçen başka bir bilgisayarın saldırıda kullanılması, saldırıyı gerçekleştiren asıl kaynağın belirlenmesini güçleştirir.

4.5. Arka kapılar

Bilgisayar üzerinde sıradan incelemeler ile bulunamayacak şekilde, normal kimlik kanıtlama süreçlerini atlatan veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler, arka kapı olarak adlandırılmaktadır. Arka kapı, kurulu bir program şeklinde (örneğin Back Orifice) olabileceği gibi; var olan meşru bir programın bizzat kendisinde, o programı yazan kişi tarafından belgelendirilmemiş bir biçimde, kasten bırakılmış olabilir. Bu tür saldırılarda özellikle Truva atı (Trojan horse) programları yoğun bir şekilde kullanılmaktadır.

4.6. Doğrudan Erişim Saldırıları

Bir bilgisayar sistemine doğrudan fiziksel erişime sahip olan bir kişinin yaptığı saldırılar bu grupta toplanmaktadır. Bilgisayara fiziksel erişim sağlayan kişi, işletim sistemlerinde kendisi için bir kullanıcı belirlemek gibi ileride kullanılabilecek çeşitli değişiklikler yapabilir; yazılım solucanları, klavye dinleme sistemleri ve gizli dinleme cihazlarını sisteme kurabilir. Doğrudan erişime sahip olan saldırgan ayrıca, CD-ROM, DVD-ROM, disket gibi yedekleme ünitelerini, bellek kartları, sayısal kameralar, sayısal ses sistemleri, cep telefonu ve kablosuz/kızılötesi bağlantılı cihazları kullanarak, büyük miktarda bilgiyi kendi tarafına kopyalayabilir. Bu açıdan, bir bilgisayar sistemi üçüncü şahısların kullanımına kısa süreliğine bile olsa bırakılmamalıdır.

4.7. Sosyal veya Toplum Mühendisliği

İnsan faktörü, her işte olduğu gibi bilgisayar sistemleri güvenliğinde de, en önemli etken olarak karşımıza çıkmaktadır. Albert Einstein "Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı, aslında evrenin sonsuzluğundan da o kadar emin değilim." sözü, sosyal mühendisliğin her zaman gündemde olacağını belirtmiştir.

Bilgisayar sistemlerinde karşılaşılan güvenlik ile ilgili bir çok olay, insan faktörünün kasten veya bilerek devreye girmesiyle meydana gelmektedir. Bilgisayar güvenliğinde sosyal mühendislik, bir bilgisayar korsanının, ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel addır. Özellikle telefon ile kullanıcı ve şifre bilgilerini elde etme, buna en tipik örnektir. Korsan sıradan bir şirket kullanıcısı gibi sistem yöneticilerinden bu tür bilgileri edinebilir. Bu konuda bir çok taktik düşünülebilir ve tüm bu taktiklerden yara almadan çıkmak için yapılması gereken en önemli şey; kullanıcıların düzenli olarak eğitilmesi ve sistem yöneticileri dahil tüm kullanıcıların istisnasız güvenlik politikalarını uygulamasıdır [18].

Bilgisayar sistemlerinde gerçekleşen bir çok hasar insan hatasından kaynaklanmaktadır. Kurum içi kullanıcıların aslında bizzat kendileri, kullandıkları sisteme en çok hasar veren kişilerdir. Bir diğer dikkat edilmesi gereken husus, bir şirketten ayrılan veya çıkartılan kişinin, daha sonradan çalışmış olduğu bu şirkete zarar vermesi veya saldırması olasılığıdır. Bunun için şirketten ayrılan kişiler için çeşitli güvenlik politikaları oluşturulmalıdır. Sosyal mühendislikte kullanılan ilginç yöntemler, risk alanı, korsanın uyguladığı taktik ve bunlara karşı mücadelede yapılması gerekenler Tablo 2'de listelenmektedir. Listeden de görülebileceği gibi sosyal mühendislik, bir bilgisayar kullanıcısını, bilgisayarını kullanırken arkasından hissettirmeden gözetlemekten, iş yerinde kağıt atıkları arasında işe yarar belge aramaya kadar, akla gelmeyecek çeşitli yöntemleri kullanmaktadır.

Tablo 2. Yaygın sosyal mühendislik taktikleri ve önlemler [19].

Risk Alanı	Korsan Taktiği	Mücadele Stratejisi
Telefon (Yardım Masası)	Taklit ve inandırma	Çalışanların ve yardım masasının telefonla hiç bir şekilde şifre veya diğer gizli bilgilerin verilmemesi için eğitilmesi
Binaya giriş	Yetkisiz fiziksel erişim	Sıkı kimlik kartı güvenliği, çalışanların eğitilmesi ve güvenlik görevlilerin çalıştırılması
Ofis	Omuz sörfü (Klavye ile yazı yazarken çevredeki birinin sizi gözetlemesi)	Sizden başka birinin ortamda bulunduğu durumlarda şifrenizi girmeyin. Zaruri durumlarda hızlı bir şekilde tuşlara basınız.
Telefon (Yardım Masası)	Yardım masası aramalarında taklit etme	Bütün çalışanlara yardım masası desteği alabilmesi için tekil bir PIN numarası atanması.
Ofis	Kimsenin olmadığı açık odalar bulabilmek için koridorlarda dolaşma	Bütün misafirlere işyerinden bir refakatçi sağlanması
Posta odası	Sahte notların sokulması	Posta odasını kilitle ve izlemeye tabi tut
Makine odası – Santral	Erişmeye teşebbüs, cihazların kaldırılması ve gizli bilgileri elde edebilmek için bir protokol analizcisi eklenmesi	Santral, sunucu odaları v.s. her zaman kilitli tut ve cihazların güncel envanterini tut
Telefon ve PBX	Telefon görüşme ücreti erişimi çalma	Şehirlerarası, milletlerarası ve cep telefonu aramalarını kontrol et, konuşmaları izle, aktarmaları reddet
İş yeri atık deposu (dumpster)	Çöplük karıştırma	Bütün çöp kutularını güvenli ve izlenen alanlarda tut. Önemli belgeleri kesme makinesiyle yok et, manyetik ortamdaki verileri sil.
İntranet - İnternet	Şifre araklamak için İntranet veya İnternet üzerinde sahte yazılımların oluşturulması ve konulması	Sistem ve ağ değişikliklerinden sürekli haberdar olma, şifre kullanımı eğitimi
Ofis	Hassas belgelerin çalınması	Belgelere gizlilik derecesi ver ve bu belgeleri kilitli yerlerde sakla
Genel - Psikolojik	Taklit ve ikna	Bütün çalışanları sürekli uyanık tutarak ve eğitim programlarına tabi tutarak bilinçlendirme

4.8. Kriptografik Saldırılar

Şifrelenmiş bilgilerin şifresini kırmak veya çözmek için yapılan saldırılardır. Bu saldırılar, kriptoanaliz yöntemleri ile gerçekleştirilmektedir. Bunlar arasında kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack), sadece şifreli metin (chipertext only), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin (adaptive chosen plaintext) ve ilişkili anahtar (related key attack) saldırılarını saymak mümkündür [9,20,21,22].

5. SONUÇ VE DEĞERLENDİRMELER

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;

- Korunacak bilginin değerinin bilinmesi ve ona göre korunması,
- bu çalışmada incelenen saldırılar, türleri ve saldırgan davranışlarının karşı tedbirlerde dikkate alınması ve
- bu çerçeve belirlenecek olan politikaların uygulanması

karşılaşılacak sıkıntı ve tehlikeler büyük oranda azaltacak, işgücü, zaman ve maddi 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 basitten en karmaşığa bir dizi önlemler alması gereklidir. Ancak, tüm önlemler alınmış dahi olsa, sürekli gelişen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluş, sistemlerin %100 güvenli olduğunu düşünmemelidir. Saldırıların elektronik ortamlardan gelebilmesinin yanı sıra, arkadaşlarımızdan ve tanıdığımız kişilerden de gelebileceği unutulmamalıdır.

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 yani saldırılara karşı sürekli uyanık olmak, bu çalışmada açıklanan saldırıları ve türlerini bertaraf edecek güvenlik politikalarının etkin bir şekilde oluşturup uygulanması ve yeni gelişmeler ışığında gerekli güncellemeleri yaparak saldırılardan etkilenme olasılığını en aza indirgemek olarak sıralanabilir.

Yüksek seviyede bir güvenlik için yukarıda bahsedilen hususların yanında; somut olarak kurumsal bilgi güvenliği standardı olan TSE 17799'de belirtilen politikaların bilinmesi ve uygulanması ile ancak yüksek seviyede bir korumanın sağlanabileceği değerlendirilmektedir.

Literatür incelendiğinde, konuyla ilgili bir çok çalışma mevcut olsa da "bilgi ve bilişim sistemleri güvenliğinin" akademik ortamlarda yeterince tartışılmadığı ve konuya gereken önemin fazlaca verilmediği tespit edilmiştir. Böyle bir çalışmanın; konunun akademik gündeme taşınması açısından da önemli olacağı mütalaa edilmektedir.

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 saldırıların ve kullanılan yöntemlerin sürekli olarak incelenmesi gerektiği elde edilen bulgular arasındadır.

Dünyada ve ülkemizde bilgi güvenliğine yönelik en önemli tehditlerden olan kötücül ve casus yazılımlarla yapılan saldırıların, yaygın olarak kullanıldığı fakat kullanıcıların bu tür saldırı ve tehditlerinden çoğunlukla haberdar olmadığı tespit edilmiştir. Her hangi bir zararla karşılaşılmaması için, konuya gereken önemin verilmesi, bilgi birikiminin arttırılması, gereken önlemlerin alınması ve kısaca farkındalık oluşturulması gerekmektedir.

Bölüm 3 ve 4'de de açıklandığı gibi; sistemlere yapılabilecek saldırıların boyutlarının hızla arttığı günümüzde, teknolojik olarak korunma teknikleri artarken tehditlerde de artış olduğu, kötücül yazılımlarla yapılan saldırıların

teknolojik yeniliklere göre şekil değiştirdiği, insanların zaaflarından çoğunlukla faydalanıldığı, kullanıcıların akıllarına bile gelmeyecek bir çok masumane yaklaşımların kullanıldığı, bilgisayar teknolojilerinde var olan açıklardan faydalanmanın yanında genelde göz ardı edilen sosyal mühendislik yaklaşımlarına da çok sık başvurulduğu, web teknolojilerinin, bu yazılımların çok kısa sürede ve kolayca yayılmasına ve yaygınlaşmasına olanak verdiği, kullanıcıların bilgisayar kullanma alışkanlıklarından, İnternet gezinme geçmişini incelemeye, mevcut port açıklarını tespit etmeye, işletim sistemi ve program korunmasızlık açıklarından yararlanmaya, önemli kritik ve kişisel bilgileri kötü niyetli kişilere göndermeye, bilgisayar sisteminde fark edilmeden ve iz bırakmadan çalışmaya, kullanıcı bilgisizlik ve zaaflarından faydalanmaya, kullanılan şifrelerin kırılmasına ve yakalanmasına, kendilerini farklı yazılımlar içerisinde saklayarak kötücül ve casus yazılım tarayıcıları ve koruma programlarını atlatmaya, hatta bu yazılımları devre dışı bırakmaya, bant genişliği ve işlemci gibi sistem kaynaklarını fark ettirmeden dışarının kullanımına açmaya kadar bir çok yöntem kullandıkları ve bilgi ve bilgisayar güvenliği konusunda güvenilir sistemler oluşturmak için büyük çabalar harcanması gerektiği değerlendirilmektedir.

Carnegie Mellon Üniversitesi tarafından 2001 yılında literatüre tanıtılmış ve "güvenlik yaşam döngüsü" olarak bilinen yaklaşımın dikkate alınarak, güvenliğin;

- statik değil dinamik bir sürece sahip olduğu,
- koruma ve sağlamlaştırma ile başladığını,
- bir hazırlık işlemine ihtiyaç duyulduğu,
- saldırıların tespit edilmesinden sonra hızlıca müdahale edilmesi gerektiği ve
- sistemde her zaman iyileştirme yapılması gerektiği

unutulmamalıdır.

Sonuç olarak yüksek seviyede bir bilgi ve bilgisayar sistemleri güvenliği için; Bruce Schneier'in "Güvenlik bir ürün değil bir süreçtir." ve Kevin Mitnick'in "güvenlik bir teknoloji sorunu değildir, bir insan ve yönetim sorunudur." cümleleri sürekli olarak dikkate alınmalıdır. bilgisayar sistemlerine yapılan saldırılar ve saldırılarda kullanılan yöntemler, saldırıların hedeflediği güvenlik unsurları, sergiledikleri karakteristik özellikler, saldırıların hedef aldığı korunmasızlık ve zayıflıklar, saldırgan profili, saldırganı saldırı yapmaya iten etkenler daima dikkate alınmalı, yukarıda da üzerinde durulduğu gibi sistematik yaklaşımlar uygulanarak önleyici karşı tedbirler alınmalıdır.

6. TEŞEKKÜR

Bu çalışma 06/2005-44 nolu BAP projesi kapsamında yapılmıştır. Yazarlar, Gazi Üniversitesine desteklerinden dolayı teşekkür eder.

7. KAYNAKLAR

1. CERT/CC Statistics 1988-2005, Mellon Software Engineering Institute, CERT Coordination Center, http://www.cert.org/stats/cert_stats.html.
2. Shamir, A., Turing Lecture on Cryptology: A Status Report, ACM, 2002 A.M. Turing Award Winners, 8, 2002.ss
3. Guttman, E., Leong, L., Malkin, G., Request for Comments: 2504, Users' Security Handbook, ISOC, RFC 2504, 31, 1999.
4. Canbek, G., Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2005.
5. 2004 Web Server Intrusion Statistics, Zone-H, http://www.zone-
6. h.org/files/82/ZoneHorg2004statisticsfinal.pdf, 2004.
7. Hamelink, C. H., The Ethics of Cyberspace, Sage Publications Inc, 32-34, 2001.
8. Klein, A., Cross Site Scripting Explained, Sanctum Security Group, http://crypto.stanford.edu/cs155/CSS.pdf, 2002.
9. Allen, J., The CERT® Guide to System and Network Security Practices, Addison-Wesley, 2001.
10. Stallings, W., Cryptography and Network Security: Principles and Practice, Prentice-Hall, Second Edition, 1999.

11. CERT® Advisory CA-1995-01, IP Spoofing Attacks and Hijacked Terminal Connections, http://www.cert.org/advisories/CA-1995-01.html, 1995.
12. Bass, T., Freyre, A., Gruber, D., and Watt., G., E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity, IEEE Network, 10-17, March/April 1998.
13. Wang, H., Zhang, D., and Shin, K. G., Detecting SYN flooding attacks, in Proc. IEEE INFOCOM, New York, NY, 1530 –1539, Jun. 2002.
14. DNS Spoofing, Men&Mice, http://www.menandmice.com/9000/9211_dns_spoofing.html.
15. Oram, A, New security attack identified: Denial of Responsibility (DoR), http://www.oreillynet.com/pub/wlg/1500?wlg=yes, 2002.
16. Lipner S. B., The Trustworthy Computing Security Development Lifecycle, ACSAC, 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, 2-13, 2004.
17. Microsoft to invest more in security: Bill Gates, April 15, Hindustan Times, 2005.
18. Barwinski, M. A., Taxonomy of Spyware and Empirical Study of Network Drive-By-Downloads, Thesis, Naval Postgraduate School, Monterey, California, 37, September 2005.
19. Granger S., Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus Infocus, Article No: 1527. 2001.
20. Granger S., Social Engineering Fundamentals, Part II: Combat Strategies, SecurityFocus Infocus, Article No: 1533. 2002.
21. Canbek, G., Sağıroğlu, Ş., Şifre Bilimi Tarihine Genel Bakış – I, Mayıs, Telekom Dünyası, 34-42, 2005.
22. Canbek, G., Sağıroğlu, Ş., Şifre Bilimi Tarihine Genel Bakış – II, Haziran, Telekom Dünyası, 36-44, 2005.
23. Canbek, G., Sağıroğlu, Ş., Şifre Bilimi Tarihine Genel Bakış – III, Temmuz, Telekom Dünyası, 56-58, 2005.