Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi

Muhammet BAYKARA[1], Resul DAŞ[1], İsmail KARADOĞAN[2]

[1] Fırat Üniversitesi, Elazığ/Türkiye, resuldas@gmail.com, muhammetbaykara23@gmail.com
[2]Kahramanmaraş Sütçü İmam Üniversitesi, Kahramanmaraş, ikaradogan@gmail.com

***Abstract* – The importance of the security of information systems has been increasing for person, institution and organisations in parallel to extraordinary advancements in the IT world. Many studies has been done in order to provide security on information systems. The purpose of these studies is to provide the security in information and informatics system. For this purpose, used security software is very important to protect belong to person, institution or organizations. In this paper, prevalent used security tools were examined in detail and these tools were categorised according to functionality, usage area as 22 category. At the same time, various solutions are listed to ensure the security of information systems for person, institution and organizations. So, constructive security policies that are important for safety information system presented for fundemental of security strategics are needed for personal or institutional factors.**

***Keywords* – Computer Security, Information Security Tools, Information Security, Spyware.**

***Özet* – Bilişim dünyasındaki olağanüstü gelişmelere paralel olarak kişi, kurum ve kuruluşlar açısından bilgi sistemleri güvenliğinin öneminde büyük ölçüde artan bir süreç yaşanmaktadır. Bilgi sistemlerinde güvenliğin sağlanması için birçok farklı çalışmalar yapılmaktadır. Bu çalışmalar ile bilgi veya bilgisayar sistemlerinde güvenliğin sağlanması amaçlanmaktadır. Bu amaç doğrultusunda kullanılan güvenlik yazılımları kişi kurum ve kuruluşlara ait sistemlerin korunmasında büyük önem taşımaktadır. Bu makale çalışmasında, günümüzde yaygın olarak kullanılan güvenlik araçları detaylıca incelenmiş ve bu araçlar işlevleri, kullanım alanları gibi birçok özellikleri dikkate alınarak 22 farklı kategoride sunulmuştur. Bununla birlikte kişi, kurum ve kuruluşların bilgi sistemleri güvenliğinin sağlamasına yönelik çeşitli çözüm önerileri sıralanmıştır. Böylece bilgi sistemleri güvenliği konusunda önem arz eden sağlam güvenlik politikaları, yararlı güvenlik araçları ve çeşitli güvenlik önlemleri sunularak, kişisel veya kurumsal olarak ihtiyaç duyulan temel güvenlik stratejileri ortaya konulmuştur.**

***Anahtar Kelimeler* – Bilgisayar Güvenliği, Bilgi Güvenliği Araçları, Bilgi Güvenliği, Casus Yazılımlar**

I. GİRİŞ

Bilgi güvenliği, bilgilerin izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunma işlemidir. Bilgi güvenliği, bilgisayar güvenliği ve bilgi sigortası terimleri sıkça birbirinin yerine kullanılmaktadır. Bu alanlar birbirleri ile alakalıdırlar ve kişisel veya kurumsal mahremiyetin, bütünlüğün ve bilginin ulaşılabilirliğinin korunması hususunda ortak amaçlara sahiptirler.

İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte Bilişim sistemlerindeki güvenlik açıkları da artmaya başlamıştır. Bilişim sistemlerindeki gizlilik, bütünlük ve sürekliliğin sağlanması için birçok güvenlik ürünü ve projesi geliştirilmiştir ve hala geliştirilmektedir. Bu makalede son zamanlarda bilgi güvenliği araştırmalarında ön plana çıkmış olan güvenlik araçları üzerinde durulmuştur.

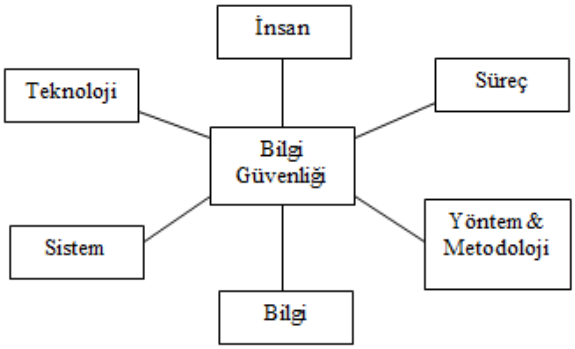
Bilgisayar ağ sistemlerinin yaygın olarak kullanılmaya başlanmasıyla birlikte ağ üzerinden yapılan saldırılarda da artışlar yaşanmaya başlanmıştır. Saldırı olaylarının bir kısmına bilinçsiz kullanıcılar neden olurken bir kısmına da bilerek sisteme zarar vermek isteyen kötü niyetli kişiler neden olmaktadır. 1980'li yıllarda bilgisayar haberleşmelerinde TCP/IP protokol ailesi dünya çapında kabul görmüş ve internet bu protokol aracılığı ile yaygınlaşmıştır. İnternetin yaygınlaşması ile bilgisayar haberleşmelerindeki atakların sayısı ve çeşidi de artmıştır [1]. Bu ataklar karşısında kimlik doğrulama, yetkilendirme, antivirüs programları gibi güvenlik çözümleri geliştirilmeye çalışılmıştır. İlk çıkan ataklar daha çok basit kod yürütme, parola tahminleri gibi etkisi ve olasılığı düşük ataklar olmasına karşın süreç içerisinde atakların karmaşıklığı ve etkileri artmıştır [2]. Buna karşın bu atakları kullanabilmek için gereken bilgi düzeyi düşmüştür. Çünkü bu bilgiler çoğunlukla internet üzerinden kontrolsüz olarak yayılmıştır. Şekil 1'de atakların zamana göre değişimleri, etkileri ve onları kullanabilmek için gerekli bilgi düzeyi görülmektedir [3].

Şekil 1: Atakların Zamana Göre Değişimleri [4]

Bilgi güvenliği tehditleri arasında, organizasyon bünyesinde çalışan kişilerin oluşturabileceği bilinçli veya bilinçsiz tehditler olarak tanımlayabileceğimiz iç tehditler çok önemli bir yer tutmaktadır. Bilinçli tehditler iki kategoride ele alınabilir. Birinci kategori, organizasyonda çalışan kötü niyetli bir kişinin kendisine verilen erişim haklarını kötüye kullanmasını içerir. İkinci kategori ise bir kişinin başka birine ait erişim bilgilerini elde ederek normalde erişmemesi gereken bilgilere erişerek kötü niyetli bir aktivite gerçekleştirmesini kapsar. Veri tabanı yöneticisinin, eriştiği verileri çıkar amacıyla başka bir firmaya satması ilk kategoriye verilecek örnektir. Veri tabanı yöneticisi olmayan ve normalde veri tabanına erişim hakkı bulunmayan birisinin erişim bilgilerini bir şekilde elde ederek verileri elde etmesi ve bunu çıkarı için kullanması ikinci kategoriye örnektir. CSI (Computer Security Institute) tarafından yapılan ankete göre katılımcıların %44'ü 2008 yılı içerisinde iç suiistimal yaşamışlardır [5]. Söz konusu oran, iç suistimallerin %50'lik virüs tehdidinden sonra ikinci büyük tehdit olduğunu göstermektedir. Bu tür suistimallerin tespitinin zor olduğu ve çoğunlukla organizasyon dışına bu konuda çok bilgi verilmek istenemeyebileceği de düşünülürse aslında %44'lük oranın daha büyük olduğu düşünülebilir. Anket çalışmasında, suistimal tabiri ile sadece bilinçli oluşan iç tehditlerin kastedildiği anlaşılmaktadır.

II. BİLGİ SİSTEMLERİ GÜVENLİĞİ

Bilgi güvenliği, bilgiyi yetkisiz erişimlerden koruyarak gizliliğini (confidentiality) sağlamak, bilginin bozulmadan tamlığını(bütünlük) ve doğruluğunu (integrity) sağlamak ve istenildiği zaman erişilebilirliğini (availability) garanti etmektir [6]. Bilgi güvenliği, içerisinde teknoloji (yazılım ve donanım), insan, süreç, yöntem ve metodoloji gibi bir çok kavramı barındıran ve bilişim dünyası için oldukça yüksek öneme haiz bir olgudur. Bu durum Şekil 2'de gösterilmiştir.



Şekil 2: Bilgi Güvenliği Kavramları

Bilgi güvenliği denilince gizlilik, bütünlük ve erişilebilirlik kavramları ön plana çıkmaktadır. Bilginin gizliliği kavramı ile kastedilen, bilgiye sadece o bilgiye erişmesi gereken kişi yada kişilerin erişimine izin verilmesidir. Bilginin bütünlüğü kavramı ile kastedilen, bilginin tahrif edilmeden, orijinal yapısı bozulmadan olduğu gibi korunmasının sağlanmasıdır. Bilginin erişilebilirliği kavramı ile kastedilen ise, bilgiye istenilen ve makul olan bir zamanda erişilmesi ve bilginin kullanılmasıdır.

Bilgi güvenliğinin sağlanması için bilgi varlıklarının korunması gerekmektedir. Bir kurum veya kuruluşun kar etmek, katma değer sağlamak, rekabet oluşturmak ve kurumsal sürdürülebilirliğini sağlamak amacıyla sahip olduğu veya sahip olması gereken ürün, pazar, teknoloji ve organizasyona ait bilgilerin tümü bilgi varlıkları olarak tanımlanabilir. Bu bilgi varlıklarının fiziksel olarak korunması için, fiziksel güvenliğin, transfer edilmesi gereken bilgilerin sağlanması için iletişim güvenliğinin, bilgisayar sistemlerine erişimlerin kontrol edilmesi için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir. Bilgi güvenliğinin yüksek seviyede sağlanabilmesi için bu farklı güvenlik türlerinin tamamının organize bir şekilde sağlanması gerekmektedir [7]. Bilgi güvenliği ile ilgili literatürde çeşitli tanımlamalar mevcuttur.

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 önlemek " olarak tanımlanır [8]. Bilgi güvenliği, bilginin bir varlık olarak ele alınması ve olası hasarlardan korunması olarak tanımlanır [9].

Bilgi güvenliği, bilgi varlıklarına yetkisiz erişim ve onları kullanım, açığa çıkarma, yok etme, değiştirme, bozma gibi saldırı tehditlerinden verilerin korunması sürecidir [9-13].

Bilgi güvenliği, bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etme, bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etme ve yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etme olarak tanımlanmaktadır [14].

Bilgi güvenliği, kurumsal bilgi teknolojileri kaynaklarının erişilebilirlik, bütünlük ve gizliliği üzerindeki risk etkilerinin azaltılarak disipline edilmesidir [15].

BS 7799 bilgiyi, diğer bütün önemli iş varlıkları gibi bir kurum açısından değeri olan ve bu yüzden korunması gereken bir varlık olarak tanımlamaktadır. Bilgi güvenliği; iş sürekliliğini sağlamak, iş hasar zararlarını asgari düzeye indirgemek, yatırım geri dönüşü, getirilerini ve iş fırsatlarını azami düzeye çıkartmak amacıyla bilgiyi çok çeşitli tehditlere karşı korur [16].

Literatürdeki bu tanımlara bakıldığı zaman bilgi güvenliği kavramına çeşitli açılardan bakıldığı görülebilir. Bilgiye sürekli olarak erişimin sağlanması gereken bir ortamda, bilginin kaynağından hedefine kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden iletilmesi süreci ve işlemleri bilgi güvenliği olarak tanımlanır.

A. Kişisel Güvenlik Önlemleri ve Uygulamaları

Bilgi sistemlerindeki teknolojik gelişmeler, insan refahına olumlu katkılar sağlamışsa da suç kavramı ve suçluların izlediği yöntemlerde de bir takım değişimin yaşanmasına sebep olmuştur. Çünkü bilgi sistemleri ortamları birçok yeni suç çeşidinin ortaya çıktığı bir alan haline gelmiştir. Bu sebeple bilgi güvenliği kavramının önemi de artan bir seyir izlemektedir. Özellikle internetin, küreselleşmenin hızlanmasına olan katkısı, rekabetin küresel boyutlara erişmesi ve artması, kar marjlarının düşmesi ve müşteri memnuniyetinin daha önemli hale gelmesi gibi nedenlerle doğru karar ve strateji geliştirmek isteyen kişi, kurum ve kuruluşlar mümkün olduğunca fazla veriyi depolamak istemektedirler. Kişisel bilgilerin daha ziyade sayısal ortam kullanılarak depolanması ve işlenmesi ise bu verilerin kötüye kullanılma riskini artırmaktadır. Kişisel verilerin türlü şekillerde kötüye kullanılması sadece teknolojinin bir sonucu değildir. Bilgisayarlar ve internetin ağ etkisi, mahremiyetin ihlalinde ve kişilere ait veriler kullanılarak suç işlenmesinde hızlandıran etkiye sahiptir. Biyometrik karakterlerle tanımlama yapılmasını sağlayan teknolojiler, DNA bankaları, gözetim araçlarındaki artış, sokakları bile gözlemleyen kameralar, veri madenciliği, RFID vb. araçlar bu bilgilerin manipülasyonu ve kötüye kullanılması risklerini de beraberinde getirmiştir. Günümüzde yaygın olarak kullanılan sosyal paylaşım siteleri kişisel verilerin elektronik ortam kullanılmak suretiyle tutulmasını sağlayarak, küresel ölçekte kişilerin iletişimini kolaylaştıran bir hizmet olmakla beraber, büyük bir iktisadi faaliyetin de kaynağı durumundadır. Bu sosyal siteler, barındırdıkları kişisel verilerin çalındığı, satıldığı, fotoğrafların kötüye kullanıldığı, yani kişiye ait bilgilerin kontrol edilemez olduğu bir ortam halini almaya başlamıştır [17].

Kişisel bilgi güvenliği önlemi olarak aşağıda maddeler halinde verilen siber saldırı türlerine karşı çeşitli güvenlik önlemlerinin alınması tavsiye edilebilir;

- Program manipülasyonu,
- Sahtekârlık ve taklit,
- Erişim araçlarının çalınması,
- Kimlik çalma,
- Ticari bilgi çalma,
- İstihbarat amaçlı faaliyetler,
- Takip ve gözetleme,
- "Hack" leme,
- Virüsler, solucanlar(worms), truva atları (Slammer, MsBlaster, Sobig vb.),
- Ajan yazılım (spyware),
- Spam,
- Hizmeti durduran saldırılar.

Tüm bu siber saldırı türleri bilinmeli, kişisel farkındalık ve bilgi güvenliği bilinci geliştirilmeli ve bu gibi saldırılar için gerekli korumayı sağlayan yazılımsal ve donanımsal destek üniteleriyle kişisel bilgi güvenliği sağlanmalıdır.

B. Kurumsal Güvenlik Önlemleri ve Uygulamaları

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel güvenlik te sağlanamaz [18, 19].

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 tanımlanabilir [18]. 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.

Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bu süreçlerin yönetilmesi, güvenlik sistemlerinin uluslararası standartlarda yapılandırılması ve yüksek seviyede bilgi güvenliğinin sağlanması amacıyla tüm dünyada kurumsal bilgi güvenliğinin yönetiminde standartlaşma çalışmaları hızla sürmektedir. Standartlaşma konusuna önderlik eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799, sonrasında ise ISO–27001:2005 adıyla

dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir [19]. Ülkemizde Avrupa Birliği Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar yetersiz olup bu standardı uygulayan kurum ve kuruluşların sayısı yok denecek kadar azdır. ISO–27001:2005 standardı ülkemizde Türk Standartları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 "Bilgi Güvenliği Yönetim Sistemi" standardı adı altında yayınlanmış ve belgeleme çalışmaları başlatılmıştır. Bu standart kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde sağlanabilmesi amacıyla; gizlilik, bütünlük ve erişilebilirlik gibi güvenlik unsurlarının kurumlar tarafından sağlanması gerekmektedir [19]. ISO 27001'in öngördüğü bir BGYS kurmak kurumlara birçok yarar sağlayacaktır. BGYS kurma adımlarının izlenmesi sonucunda kurum her şeyden önce bilgi varlıklarının farkına varacaktır. Hangi varlıklara sahip olduğunu ve bu varlıkların önemini anlayacaktır. Risklerini belirleyip yöneterek en önemli unsur olan iş sürekliliğini sağlayabilecektir. İş sürekliliğinin sağlanması kurumun faaliyetlerine devam edebilmesi anlamına gelmektedir. Bilgiler korunacağından, bu durum kurumun iç ve dış paydaşlarında bir güven duygusu oluşturur, motivasyon sağlar. Daha iyi bir çalışma ortamı yaratılmasına katkı sağlar.

Kurum, kuruluş ve işletmelerin belirli güvenlik standartları çerçevesinde bilgi güvenliğini sağlayarak iç ve dış tehditler karşısında zarar görmeden veya en az zararla iş sürekliliklerini devam ettirebilmeleri için bilgi güvenliği standartlarını kendi kuruluşlarında uygulamaları artık neredeyse bir zorunluluk haline gelmiştir [20].

III. BİLGİ SİSTEMLERİNDE KULLANILAN GÜVENLİK ARAÇLARI

Bilgisayar sistemlerinin güvenliklerini sağlama amacıyla birçok çalışma yapılır. Bu çalışmalar genelde sisteme; güvenlik duvarları kurmak, saldırı tespit sistemleri kurmak, güvenli iletişim protokolleri sağlamak, zarar verici kodlara karşı yazılımlar kullanmak gibi çözümler olabilir. Fakat tüm bu yapılan çalışmalardan sonra bile sistemde saldırganların faydalanabileceği açıklar olabilir. Bu açıklar çeşitli güvenlik araçları kullanılarak tespit edilebilir ve gerekli önlemler alınabilir. Güvenlik araçları ayrıca sistemi izleme olanağı da sunarlar. Var olan güvenlik araçları genelde bilgisayar sistemlerine saldırı amacıyla geliştirilmiştir. Buradaki temel düşünce sistemin açıklarını saldırganlardan önce ortaya çıkarmak ve gerekli önlemleri almaktır [11].

Bilgisayar 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 duruma uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir. Bu politikalar;

- Etkinliklerin sorgulanması,
- Erişimlerin izlenmesi,
- Değişikliklerin kayıtlarının tutulup değerlendirilmesi,
- Silme işlemlerinin sınırlandırılması,

gibi bazı kullanım şekillerine indirgenebilmektedir.

Bilgisayar teknolojilerinde yer alan bilgisayar güvenliğinin amacı ise: "Kişi ve kurumların bu teknolojileri kullanırken karşılaşabilecekleri tehdit ve tehlikelerin incelemelerinin yapılarak gerekli önlemlerin önceden alınmasıdır". Bilgi ve bilgisayar güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan "Güvenlik Mühendisliği"nin bir alt alanı olarak görülmektedir. Bilgisayar güvenliği geniş anlamda bir koruyucu mekanizma olarak düşünüldüğünde, kişisel veya kurumsal bilgisayarlar için genel olarak aşağıdaki maddelerin hepsinin veya bazılarının uygulanması gerekmektedir:

- Kötücül yazılım (virüs, backdoors vb.) koruma yazılımlarının kurulu olması,
- Bu yazılımların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması,
- Bilgisayarda şifre korumalı ekran koruyucu kullanılması
- Kurmuş olduğunuz yazılımların paylaşıma açık olup olmadığının kontrol edilmesi,
- 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 internet erişiminin kapatılması
- Önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması
- İşletim sistemi güncelleştirmelerinin yapılması [10].

gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır.

Bu bölümde bilgi güvenliği sistemlerinde yaygın olarak kullanılan güvenlik araçları genel özellikleri ile tanıtılacaktır. Tablo 1'de bazı güvenlik araçları yeteneklerine göre kategoriler halinde gösterilmiştir [22].

Tablo 1: Bilgisayar Sistemlerinde Sıklıkla Kullanılan Bazı Güvenlik Araçları [22]

Genel Amaçlı Araçlar	Kötücül Yazılım Temizleyici	Rootkit Tarayıcıları	Böcek Bulma Araçları	Uygulamaya Özel Tarayıcılar	Web Tarayıcı Araçları	Web Proxy Araçları	Web Güvenlik Açığı Tarayıcıları	Şifre Kırıcılar	Şifreleme Araçları	Hata Ayıklayıcılar	Adli Bilişim Araçları	Paket İşçiliği Araçları	Paket Koklayıcıları	Port Tarayıcılar	Saldırı Tespit Sistemleri	Güvenlik Odaklı İşletim Sistemleri	Güvenlik Duvarları	Güvenlik Açığı Sömürü Araçları	Güvenlik Açığı Tarayıcıları	Ağ Trafiği İzleme Araçları	Kablosuz Ağ Araçları
Netcat	ClamAV	Sys internals	w3af	iks-scan	Firefox	Paros proxy	Burp Suite	Aircrack	OpenSSH /PuTTY /SSH	IDA Pro	Maltego	Netcat	WireShark	Angry IP Scanner	Snort	Knoppix	Netfilter	Meta sploit	Nessus	Ettercap	Air crack
Ping/telnet/dig traceroute/ whois/netstat	Virus Total	Tripwire	Wfuzz	NBTScan	Firebug	Sslstrip	W3af	Cain and Abel	TrueCrypt	Immunity Debugger	The Sleuth Kit	Hping	Ettercap	Super Scan	OSSEC HIDS	SELinux	Norton	W3af	Core Impact	Ngrep	Kismet
Perl/Python/R uby	Malwarebytes/ Anti-Malware	DumpSec	Wapiti	THC Amap	Tamper Data	Fiddler	Nikto	John the Ripper	GnuPG/PGP	WinDbg	EnCase	Scapy	Cain&Abel	NetScan Tools	OSSIM	Helix	Zone Alarm	Core Impact	Open VAS	Ntop	Net Stumbler
VMware		Hijack This	Skip fish		NoScript	ratproxy	Web Scarab	THC Hydra	OpenVPN	OllyDbg	Helix	Yersinia	TCP dump	Unicorn Scan	Sguil	Back track	Open BSD PF	Sqlmap	Nexpose	Etherape	inSSI DER
Google		AIDE					SQL map	ophcrack	KeePass	GDB		Nemesis	Kismet		ArcSight SIEM platform			Canvas	GFI Lan Guard	Solar Winds	Kis MAC
Firefox							Skip fish	Medusa	Stunnel			Socat	Network Miner		Honeyd			Web Goat	Retina	Splunk	
cURL							App Scan	fgdump	OpenSSL				Dsniff					Dradis	MBSA	Nagios	
Socat							Fire Bug	L0phtCrack	Tor				Ntop					BeEf	Qualys Guard	Argus	
							Samurai WTF	SolarWinds					Ngrep					Sql ninja	Nipper	P0f	
							Net Sparker	RainbowCrack					Etherape						SAINT		
								Wfuzz					P0f						Secunia		
								Brutus					inSSIDer						PSI		

1. Kötücül yazılım temizleyici (Antimalware)
2. Uygulamaya özel tarayıcılar (Application-specific scanners)
3. Web tarayıcı araçları (Web Browser-Related)
4. Şifre kırıcılar (Password crackers)
5. Şifreleme araçları (Encryption tools)
6. Hata ayıklayıcılar (Debuggers)
7. Güvenlik duvarları (Firewalls)
8. Adli bilişim araçları (Forensics)
9. Otomatik böcek bulma programları (Fuzzers)
10. Genel amaçlı araçlar (General purpose tools)
11. Saldırı tespit sistemleri (Intrusion detection systems)
12. Paket işçiliği araçları (Packet crafting tools)
13. Port tarayıcılar (Port scanners)
14. Rootkit dedektörleri (Rootkit Detectors)
15. Güvenlik odaklı işletim sistemleri (Security-oriented operating systems)
16. Paket koklayıcıları (Packet sniffers)
17. Güvenlik açığı sömürü araçları (Vulnerability exploitation tools)
18. Ağ trafiği izleme araçları (Traffic monitoring tools)
19. Güvenlik açığı tarayıcıları (Vulnerability scanners)
20. Web proxy araçları (Web proxies)
21. Web güvenlik açığı tarayıcıları (Web vulnerability scanners)
22. Kablosuz ağ araçları (Wireless tools)

A. NMAP

NMap (Network mapper) ağ araştırmasında ve güvenlik denetlemelerinde kullanılan açık kaynak kodlu bir programdır. Geniş ölçekli ağları tarama amacıyla tasarlanmasının yanında tek bir konak üzerinde de verimli bir şekilde çalışabilir. IP paketleri göndererek ağ üzerinde aktif olan bilgisayarları gösterir. Ayrıca bu bilgisayarlar üzerindeki ağa sunulan uygulamaları tespit edebilir, bu bilgisayarların kullandığı işletim sistemleri ve güvenlik duvarlarını bulabilir. Nmap birçok işletim sistemi üzerinde çalışabilir ve GNU GPL lisansıyla dağıtılır. NMAP yazılımı Matrix Reloaded, Die Hard 4, The Bourne Ultimatum gibi birçok filmde hackerların bilgisayarlarında kullandıkları yazılımdır [11].

B. NESSUS

Güçlü ve güncel bir uzaktan tarama aracıdır. Birçok UNIX türevi üzerinde ve Windows'ta çalışabilme özelliğine sahiptir. Nessus uyumlu ek yazılımları, arayüzleri ile çok kullanışlı bir güvenlik aracıdır. 1200'ün üzerinde güvenlik açığını yakalayabilir ve bunlar hakkında çeşitli biçimlerde raporlar sunabilir (HTML, LaTeX, ASCII, vs.) [11]. Nessus'un önemli özelliklerinden biri olarak bilinen, kurallara bağlı olmadan tarama yapabilmesidir. Örneğin 1234 numaralı portta çalışan bir web sunucusunu tespit edebilir ve güvenlik taramasından geçirebilir. Bulduğu açıklar için kullanıcıya güvenlik çözümleri önerebilir.

C. WIRESHARK

UNIX ve Windows platformları için ücretsiz bir ağ protokolü analizcisidir. Canlı bir ağdan veya daha önceden diske kaydedilmiş bir ağ verisi üzerinde çalışarak ağ incelemesi yapar. Kullanıcı, interaktif bir şekilde incelenen veri hakkında ayrıntılı bir bilgi alabilir. Bu bilgi tek bir paket için de söz konusudur. Güçlü özellikleri arasında zengin bir süzme diline sahip olması ve TCP oturumunu birleştirerek analiz imkanı sağlaması vardır. Wireshark programı ethereal olarak adlandırılan programın yenilenmiş versiyonudur. Wireshark 750 den fazla protokolü analiz etme özelliğine sahiptir. Belirli kriterlere göre filtreleme yapabilmesi de kullanımını kolaylaştırmaktadır. Diğer paket yakalama yazılımlarının dosyalarını da açabilmektedir.

D. SNORT

IP ağları için gerçek zamanlı trafik analizi yapabilen ve paket kaydedebilen açık kaynak kodlu bir sızma belirleme sistemidir. Protokol analizi, içerik araştırması/eşlemesi dahil daha birçok inceleme yaparak saldırıları veya yoklamaları (tampon taşırma, gizli port taraması, CGI saldırıları, SMB yoklamaları, OS belirleme, vs.) tespit edebilir. Snort izin verilen/verilmeyen trafik tanımlanması için esnek bir kural yazma diline ve modüler bir tespit etme motoruna sahiptir. Ayrıca, çeşitli alarm mekanizmaları sayesinde herhangi bir saldırı tespitinden sonra kullanıcıyı uyarır.

E. TCPDUMP

Ağ izleme ve veri inceleme yapmaya olanak veren en eski ve en çok sevilen ağ analiz (dinleme) programıdır. Ağ hareketlerini inceleme amacıyla kullanılır. Verilen deyimleri eşleyerek bir ağ ara yüzündeki paket bilgilerini gösterebilir. Nmap, Tcpdump'ın altyapısını oluşturan libpcap paket yakalama kütüphanesini kullanır. Günümüzde Tcpdump çok kullanılmamakla beraber ağ inceleme için genellikle wireshark kullanılmaktadır.

F. DSNIFF

Ağ denetlemesi ve içeri sızma testleri yapmaya yarayan bir araçlar takımıdır. Dsniff; filesnarf, mailsnarf, msgsnarf, urlsnarf ve webspy gibi programlar içerir. Bu programlar pasif bir şekilde ağı dinleyerek ilgi çeken verinin (Şifreler, epostalar, vs.) yakalanmasını sağlarlar. Arpspoof, dnsspoof, ve macof normalde bir saldırganın erişemeyeceği ağ trafiğine (2. katman) ulaşmasını sağlar. Sshmitm ve webmitm araçları da yönlendirilmiş HTTPS ve SSH bağlantıları için araya girme saldırılarında kullanılır.

G. GFI LANguard

Windows platformları için ücretli bir ağ güvenliği tarama aracıdır. LANguard ağı tarayarak her makine için çeşitli bilgiler sunar. Bu bilgiler makinelerin hangi servis paketlerini kullandığı, eksik güvenlik yamaları, herkese açık paylaşımları, açık portları, çalışan servisler/uygulamalar ve zayıf şifreler

olabilir. Tarama sonuçları HTML formatında raporlanır ve sorgulanabilir. Web sayfasında deneme sürümü mevcuttur.

H. ETTERCAP

Ethernet ağlarında kullanılan terminal tabanlı bir koklama (sniff)/araya girme/kaydetme aracıdır. Aktif ve pasif olarak, şifreli olanlar dâhil birçok protokolü izleyebilir ve araya girebilir. Kurulmuş bir bağlantıya veri enjeksiyonu yapma ve hızlı bir şekilde süzme yapma özellikleri vardır. Uyumlu ek yazılımları vardır. Anahtarlamalı ağda olduğunu anlayabilir ve işletim sistemi izlerini kullanarak ağ geometrisini çıkarabilir.

I. JOHN THE RIPPER

John the Ripper çok güçlü bir şifre kırma aracıdır. Hızlı bir şekilde çalışma ve birden çok platform için şifre özü kırma özelliklerine sahiptir. UNIX'in neredeyse her versiyonu dâhil DOS, Windows, BeOS ve OpenVMS'te çalışabilir.

İ. TRIPWIRE

Bütünlük kontrolü yapan araçların büyük babası olarak tanımlanan tripwire belirlenen dosya ve dizinlerin zaman içinde bütünlüklerinin bozulup bozulmadığını araştırır. Düzenli bir şekilde sistem dosyalarını kontrol ederek herhangi bir değişiklik halinde sistem yöneticisini uyarır. Linux için ücretsiz bir versiyonu olmakla birlikte diğer platformlar için ücretli bir yazılımdır.

J. SUPERSCAN

Windows tabanlı çalışan ve kapalı kaynak olan superscan yazılımı kullanışlı port tarama yazılımlarından olup IP aralığına dayalı port taraması yapar. Sadece TCP değil UDP taramalarını da yapabilmektedir.

K. CAIN & ABEL

Ağ yöneticileri, güvenlik uzmanları ve geliştiriciler için geliştirilmiş hedef ağda paket analizi yapma, ağdan şifre gibi bilgileri çekme, encrypt edilmiş şifreleri Brute Force ve Cryptanalysis metotları ile çözme gibi işlevlerinin yanında kötü niyetli kullanılmak istendiğinde tam bir silaha dönüşebilmektedir. ARP Poison alanında da en iyi sayılabilecek yazılımlardan biridir. Güvenli protokollerde bile ARP poison yaparak paket analizi yapabilir, şifrelenmiş veriyi okuyabilir. Ayrıca Cain & Abel Microsoft işletim sistemleri için bir password kırma aracı olarak da kullanılabilmektedir. Cain & Abel programının Linux sistemler için kullanılan formatı DSniff programıdır.

L. METASPLOIT

Metasploit, 2004 yılında piyasaya çıkan, korunmasızlık sömürücülerin geliştirilmesi, test edilmesi ve kullanılması için geliştirilen açık kaynak kodlu yazılımdır. Tamamıyla ücretsiz olarak ortaya çıkan bu platformu 2009 yılında Rapid7 satın almıştır ve böylece bu yazılımın ticari varyasyonları çıkmıştır. Günümüzde limitli kullanım sunan Framework yapısı hala ücretsizken, gelişmiş versiyonları yıllık üç bin dolar değerindedir.

M. BURP SUITE

Web atakları için kullanılabilecek çok güçlü bir tümleşik platformdur. Web saldırılarını kolaylaştırmak ve hızlandırmak için çok çeşitli arabirimler ve araçlar içerir. Ücretsiz bir deneme sürümü de mevcuttur.

N. W3AF

W3af, web uygulama açıklarını bulmak, istismarları tespit etmek için son derece güçlü, popüler ve esnek bir yazılımdır. Kullanımı ve genişletilmesi kolaydır. Web değerlendirme ve korunmasızlık sömürücü eklentileri vardır. En güçlü web penetrasyon araçlarından biridir.

O. SCAPY

Scapy etkili interaktif bir paket manipülasyon, paket üretici, ağ keşif ve paket dinleme aracıdır. Scapy düşük seviye bir araç olup, Python dili ile etkileşim kurabilir. Scapy paket yada paket kümeleri oluşturmak, bunları işlemek, hat üzerinden göndermek, hat üzerindeki diğer paketlerin dinlenmesi, soruların ve cevapların eşleştirilmesi için sınıflar sağlar.

P. SQLMAP

Sqlmap açık kaynak kod bir penetrasyon test aracıdır. Saldırı tespiti, korunmasızlık sömürücü ve Sql enjeksiyon açıklarını bulma gibi işlemlerde otomatik olarak işlem yapan çok güçlü bir araçtır.

IV. KİŞİSEL VE KURUMSAL AÇIDAN GÜVENLİK STRATEJİLERİ

Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür [21]. Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması için tüm bilgi güvenlik faaliyetlerini kapsayan ve yönlendiren talimatlar olup kurumsal bilgi kaynaklarına erişim yetkisi olan tüm çalışanların uyması gereken kuralları içeren belgelerdir. Bilgi güvenliği politikaları her kuruluş için farklılık göstersede genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı

genel ifadeleri içermektedir. Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikadan sorumlu olan çalışanların ve gruplarının belirlendiği, uygulanması ve yapılması gereken kuralların, ihlal edildiğinde uygulanacak cezai yaptırımların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı 7 bölümden oluşur [19]. Kurumsal güvenlik politikası içerisinde bulunması gereken bölümler Tablo 2'de özetlenmiştir. Belirli konularda çalışanın daha fazla bilgilendirilmesi, dikkat etmesi gereken hususlar, ilgili konunun detaylı bir şekilde ifade edilmesi istendiğinde alt politikalar geliştirilmelidir. Örneğin kullanıcı hesaplarının oluşturulması ve yönetilmesi, şifre unutma, şifre değiştirme, yeni şifre tanımlama gibi durumlarda uyulacak kurallar alt politikalar aracılığı ile açıklanmalıdır [19].

Tablo 2: Güvenlik Politikası [19]

Bölüm Adı	**İçerik**
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlamasını kapsar
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğunu açıklar
Kapsam	Politikaya uyması gereken çalışan grupları (ilgili bir grup veya kurumun tamamı) ve bilgi varlıklarını belirler.
Politika	Uygulanması ve uyulması gereken kuralları veya politikaları içerir.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımları açıklar.
Tanımlar	Teknik terimler ile açık olmayan ifadeler listelenerek açıklanır.
Düzeltme Tarihçesi	Politika içerisinde yapılan değişiklikler, tarihler ve sebepleri yer alır.

E-posta gönderme ve alma konusunda, üst yönetimin kararlarını, kullanıcının uyması gereken kuralları ve diğer haklarını alt politika içerisinde ifade etmek bir başka örnek olarak verilebilir. Alt politikayla üst yönetimin, gerekli gördüğünde çalışanlarının epostalarını okuyabileceği, e-postalar yoluyla gizlilik dereceli bilgilerin gönderilip alınamayacağı gibi hususlar, e-posta alt politikası içerisinde ifade edilebilir. Alt politikalar içerisinde, izin verilen yazılımlar, veri tabanlarının nasıl korunacağı, bilgisayarlarda uygulanacak erişim denetim ölçütleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular da açıklanabilir.

Kurumsal bilgi güvenliği politikaları kuruluşların ihtiyaçları doğrultusunda temel güvenlik unsurlarının (gizlilik, bütünlük, erişilebilirlik, vb.) bazıları üzerinde yoğunlaşabilir. Örneğin askeri kurumlarda, bilgi güvenliği politikalarında gizlilik ve bütünlük unsurları ön plana çıkmaktadır. Askeri bir savaş uçağının kalkış zaman bilgilerinin onaylanıp yürürlüğe girmesi için düşmanlar tarafından görülmemesi (gizlilik) ve değiştirilmemesi (bütünlük) gereklidir. Bir diğer örnek ise kâr amacı gütmeyen kurumlarda uygulanan bilgi güvenliği politikalarında genellikle erişilebilirlik ve bütünlük unsurları ön planda gelmektedir. Üniversite sınav sonuçlarının açıklandığı yükseköğretim kurumunda uygulanan güvenlik politikasında öğrenciler sınav açıklandıktan sonra istediği zaman diliminde (erişilebilirlik) doğru bir şekilde (bütünlük) sınav sonuçlarına bakabilmelidir [19].

İyi bir güvenlik politikası, kullanıcıların işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve sistem yöneticilerinin eldeki imkânlarla uyabilecekleri ve uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Alınan güvenlik önlemleri ve politikaları uygulayan yetkililer veya birimler yaptırımları uygulayabilecek idari ve teknik yetkilerle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri tanımlanarak kullanıcılar, sistem yöneticileri ve diğer kişilerin sisteme ilişkin sorumlulukları, yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıkça tanımlanmalıdır. Politikalar içerisinde uygulanacak olan yasal ve ahlaki mahremiyet koşulları ile elektronik mesajların ve dosyaların içeriğine ulaşım, kullanıcı hareketlerinim kayıt edilmesi gibi denetim ve izlemeye yönelik işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır.

Saldırıların ve diğer sorunların tespitinde kullanıcıların, yöneticilerin ve teknik personelin sorumluluk ve görevleri ile tespit edilen sorun ve saldırıların hangi kanallarla kimlere ne kadar zamanda rapor edileceği güvenlik politikalarında açıkça belirtilmelidir. Sistemlerin gün içi çalışma takvimleri, veri kaybı durumunda verinin geri getirilmesi koşulları gibi kullanıcının sisteme erişmesini sınırlayan durumlara politikalar içerisinde yer verilmelidir. Bu durumlarda kullanıcıya, izlemesi gereken yolu anlatacak ve yardımcı olacak kılavuzlara da yer verilmelidir [19, 20,23].

V. SONUÇ

Günümüzde ticari şirketler ve devlet kurumları işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin korunması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir. Bilgiye yönelik olası saldırılar, tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır. Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin

sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar. Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kullanılabilirlik (Availability)

Bu kavramları biraz daha açacak olursak gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz. Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

KAYNAKLAR

[1] DeNardis L., The History of Information Security: A coprehensive handbook, Elsevier, 2007.

[2] Brendan P. Kehoe, Zen and Art of the Internet, http://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html#SEC91 , 1992,CERT Advisory CA-90:01, Sun sendmail vulnerability, January 29 (1990).

[3] *Internet:*http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd803fcbbe.pdf, Erişim Tarihi: 24.04.2013.

[4] G. Canbek, Ş. Sağıroğlu, "Bilgisayar sistemlerine yapılan saldırılar ve türleri: Bir inceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23 (1-2) 1 - 12 (2007).

[5] *Internet:* https://www.hlncc.com/docs/CSIsurvey2008.pdf, Erişim Tarihi:25.04.2013.

[6] Isaca, Cisa Review Manual 2009, Isaca Press, Rolling Meadows, 2009.

[7] M. Gülmüş, "Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği ", Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2010.

[8] G. Canbek, Ş. Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9(3):69-72.

[9] TÜBİTAK, Bilgem, "UEKAE BGYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulumu".

[10] *Internet:* http://tr.wikipedia.org/wiki/Bilgisayar_güvenliği, Erişim Tarihi: 25.04.2013.

[11] Gündüz M. Z., "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, 2013.

[12] Çağlayan, U., "Bilgi Güvenliği: Dünyadaki Eğilimler", Ulaknet Sistem Yönetimi Konferansı, 5-6, 2003, Ankara.

[13] *Internet:* http://en.wikipedia.org/wiki/Information_security, Erişim Tarihi: 24.05.2013.

[14] Code Of Practice for Information Security Management, ISO: 27002:2005, ISO Publications, Switzerland, 2005.

[15] Solms, B., "Information Security—The Fourt Wave", Computers & Security, 25(3):166-167, 2006.

[16] Tioia, The Institute Of Internal Auditors, Information Technology Controls, Iaa Gtag, Florida, 2006.

[17] Civelek Y. D., "Kişisel Verilen Korunması ve Bir Kurumsal Yapılanma Önerisi", DPT Uzmanlık Tezi, 2011.

[18] Y. Vural, "Kurumsal Bilgi Güvenliği ve Sızma Testleri", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 40, 2007.

[19] Y. Vural, Ş. Sağıroğlu, "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme", Gazi Üniv. Müh. Mim. Fak. Der. Cilt 23, No 2, 507-522, 2008.

[20] Ş. Sağıroğlu, E. Ersoy, M. Alkan, "Bilgi Güvenliğinin Kurumsal Bazda Uygulanması", Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 2007.

[21] S. Kalman, "Web Security Field Guide", Cisco Press, Indianapolis, sf.36, 37, 2003.

[22] *Internet:* Network Security Tools, http://sectools.org/, Erişim Tarihi:25.04.2013.

[23] R. Daş, Ş. Kara, M. Z. Gündüz, "Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.