BİLİŞİM SALDIRGANLIĞI, NEDENLERİ VE SINIFLANDIRILMASI

Nazım İMAL[1] *Mehmet ESER*[2]
[1,2]Bilgisayar Mühendisliği A.B.D, Bilecik Üniversitesi, Bilecik

[1]e-posta: nazim.imal@bilecik.edu.tr [2]e-posta: mehmet.eser@bilecik.edu.tr

Özet

Bilgi farklı biçimlerde tanımlanabilecek sanal bir kavram olmasına rağmen, çoğu durumda somut sonuçlara yol açabilen bir anahtar görevini üstlenir. Bu sebeple, tarihin derinliklerinden bu yana, bilgi ve bilgiye ulaşabilme insanoğlu için yoğun bir uğraş gerektirmiştir. Birçok konu ve durumda yoğun emek, zaman yada para harcanarak elde edilen bilgilerden maddi, manevi, güvenlik gibi açılardan önemi olanların, diğer insanlardan, diğer toplumlardan yada ülkelerden saklı tutulmaları gerekmektedir. Yani bilginin çok önem kazandığı durumda sır kavramı ortaya çıkmaktadır. Sır kavramının günümüzdeki karşılığı bilgi güvenliği olarak adlandırılmakta ve yoğun olarak teknoloji, bilişim ve ticaret ile birlikte yaşayan günümüz insanı için sık sık karşılaşılan bir kavram olmaktadır. Bilginin elde edilmesindeki güçlük arttıkça veya rastlantısal olarak elde edilen önemi çok büyük bir bilgiye ulaşıldıkça, o bilgiyi korumak için gerekli duyarlılık da fazlasıyla artmaktadır.

Anahtar Kelimeler: Bilgi, bilişim, bilişim saldırganlığı, bilişim saldırganlığının nedenleri

Abstract

Information can be defined in different ways although a imaginary concept, in most cases assumes a key role that lead to concrete results. Therefore, since the depth of history, knowledge and accessibility to information for human beings has required intensive work. In issues and many cases, intensive labor, time or the money obtained spent from the information material, spiritual, such as security, significance in terms of those other people, other societies or countries must be kept hidden. That concept of secret appears in information is very important. Secrets of the concept of today's money, information security is called and intense as technology, information and trade with people living for today is a concept frequently encountered. The higher the difficulty of obtaining information or randomly obtained a great importance of access to information, that information necessary to protect the highly sensitive increase.

Keywords:*Information, information, information of aggression, information of the causes of aggression*

1. Bilişim Saldırganlığı

Bilişim saldırganlığı kavramını açıklayabilmemiz için öncelikle "Bilgi ve ağ güvenliği açısından saldırganlık nedir ? İnsanlar ne amaçla saldırgan olur ? "sorularını cevaplandırabilmemiz gerekir. Bilgi ve bilişim sektörünün hızlı ilerlemesinin sonucu olarak saldırı eylemleri artık sadece bilgisayarlar ve bilgisayar ağları ile sınırlı eylem değildir. Mikroişlemcilerin kullanıldığı programlanabilir sistemlere sahip birçok cihaz bilişim saldırılarının hedefi durumundadır. Geçmişte sadece bilgisayarları ilgilendiren saldırılar, günümüzde bir IPHONE'u, bir navigasyon cihazını, bir PALM'i v.b.'ni de yakından ilgilendirir hale gelmiştir.

Şekil 1. Saldırıya uğramış bir site

Saldırı eylemlerinin birçoğu macera arayan bilgisayar kullanıcıları tarafından, bilinmeyeni keşfetme arzusuyla aşırı merak nedeniyle gerçekleştirilmektedir. Bilişim alanında çok şey bildiği halde bu bilgilerini değerlendiremeyen ve bilgilerinden ötürü bir fayda ve itibar sağlayamayan kesimde saldırgan potansiyeli içerisinde yer almaktadır. Örneğin şekil 1'de saldırıya uğramış bir sitenin girişine yerleştirilen sayfa her ne kadar ürkütücü görünse de, saldırganın kendisini açıkça belli etmesi, çoğu kez sitenin güvenlik açığını belirleme amacına yönelik bir yardım olmaktadır. Saldırganın site içerisinde kendisini belli etmeksizin yapabileceği sinsi müdahalelerin sonucu ise çok daha ürkütücü olabilmektedir.

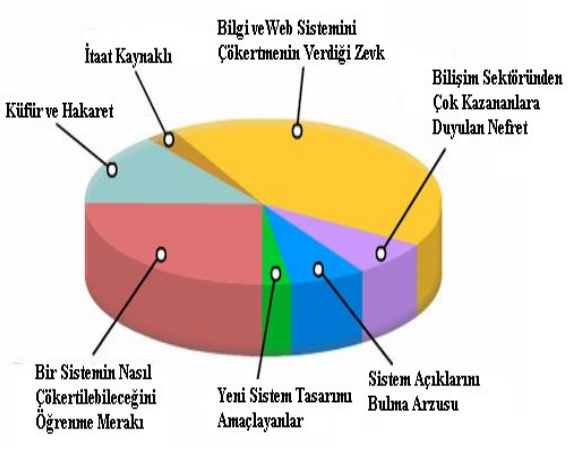
2. Bilişim Saldırganlığının Nedenleri

Bilişim saldırılarının günümüzdeki zararlarının etkileri dikkate alınmakla birlikte bilişim sistemlerinin geliştirilmesinde bilişim

Tablo 1. Siber Saldırıların (Sanal ortamda gerçekleştirilen güvenlik ihlallerinin) Hedef ve Yöntemleri

	MOTİVASYON	HEDEF	YÖNTEM
Siber Terör	Politik değişiklikler	Masum kullanıcılar	Bilgisayar tabanlı şiddet ve yıkım
Siber Protesto	Politik değişiklikler	Karar vericiler	Saldırı
Cracking[1]	Ego, Kişisel düşmanlık	Şahıslar, Firmalar, Devletler	Saldırı, Açıklık kullanımı (Alenen yapılabilmektedir)
Siber Suç	Ekonomik fayda	Şahıslar, Firmalar	Sahtekarlık, Kimlik çalma, Şantaj, Saldırı, Açıklık kullanımı
Siber Casusluk	Ekonomik fayda	Şahıslar, Firmalar, Devletler	Saldırı, Açıklık kullanımı (Nadiren alenen yapılmaktadır)
Devletler seviyesinde bilgi savaşları (Siber Savaş)	Politik veya askeri fayda	Kritik altyapılar, askeri bileşenler	Saldırı, Açıklık kullanımı, Fiziksel saldırılar

saldırganlarının ister istemez katkıları bulunmuş ve bulunmaktadır. Örneğin bu tip saldırganlarca, yazılımlarının son derece güvenilir olduğunu iddia eden bilgi güvenliği ağ sistemlerine, kolaylıkla girilebildiği, hatta girişte herhangi bir şifre ve parola gerekmeyebildiği zamanla ortaya çıkartılmıştır. Bu saldırganların çoğunun, kötü niyetli olmamaları ve saldırı sonrası güvenlik açığının nereden kaynaklandığını belirtir notlar bırakabilmeleri, yazılımlardaki güvenlik açıklarının daha hızlı kapatılmasını sağlamış ve sağlamaya devam etmektedir.



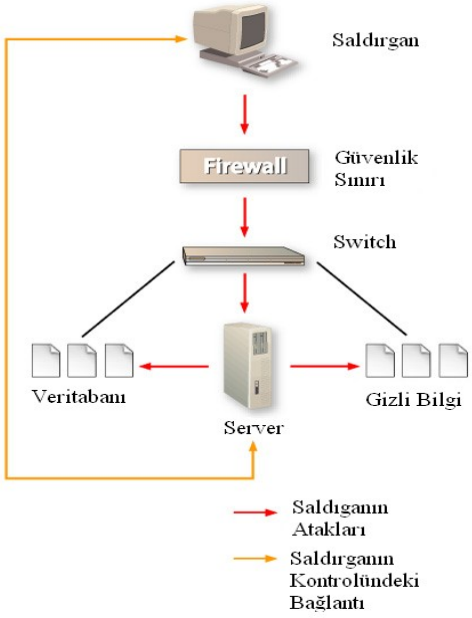
Şekil 2. Bilişim saldırganlığı nedenleri

Bilgisayar kullanıcısını bilişim saldırganlığına iten nedenler arasında, bireyleri suç işlemeye sürükleyen sebeplerden farklı sebepler aramamak gerekir. Açgözlülük, bencillik, haksız rekabet, ahlaki yoksunluk, macera arayışı ve yasaklanana duyulan arzu gibi bireyleri suç işlemeye götüren nedenler, bilişim suçları anlamında da bireyleri suç işlemeye itebilmektedir. (Şekil 3)

Ama bütün bilişim saldırganlarının iyi niyetli olduğunu iddia etmek insanlığın doğasına ters olan bir durumdur. Şekil 3. de görüldüğü gibi bir saldırganın firewall duvarını aşarak sistem kaynaklarına ulaşması, sistemin bütün işlerliğini ve güvenirliğini saldırganın insafına bırakmaktadır ki, bu durum hiçbir surette kabul edilemez ve ancak bilişim suçu kapsamında değerlendirilebilir.

Bilişim alanında suç işleyebilmek için yüksek bilgi düzeyi gerektiği düşünüldüğünde, saldırganların bir çoğunun, karmaşık yapıdaki bilgi güvenlik sistemlerine zarar verme yoluyla, kendilerini ispatlama veya bir meydan okuma hissiyle hareket ettikleri sonucunu çıkmaktadır. Bir bilişim sistemi üzerinde yasal olmayan tarzda etkin olmak, maddi bir menfaat sağlamasa da, bir güç gösterisi olarak saldırganı fazlasıyla mutlu edebilmektedir. Haksız şekilde işinden atılan bir bilgisayar mühendisi yada bilgi işlemcinin, eski şirketinin bilgi ağına verdiği

zarar intikam duygusu ile gerçekleştirilen saldırılara örnek olabilir.



Şekil 3. Bilişim saldırganlığı akış şeması

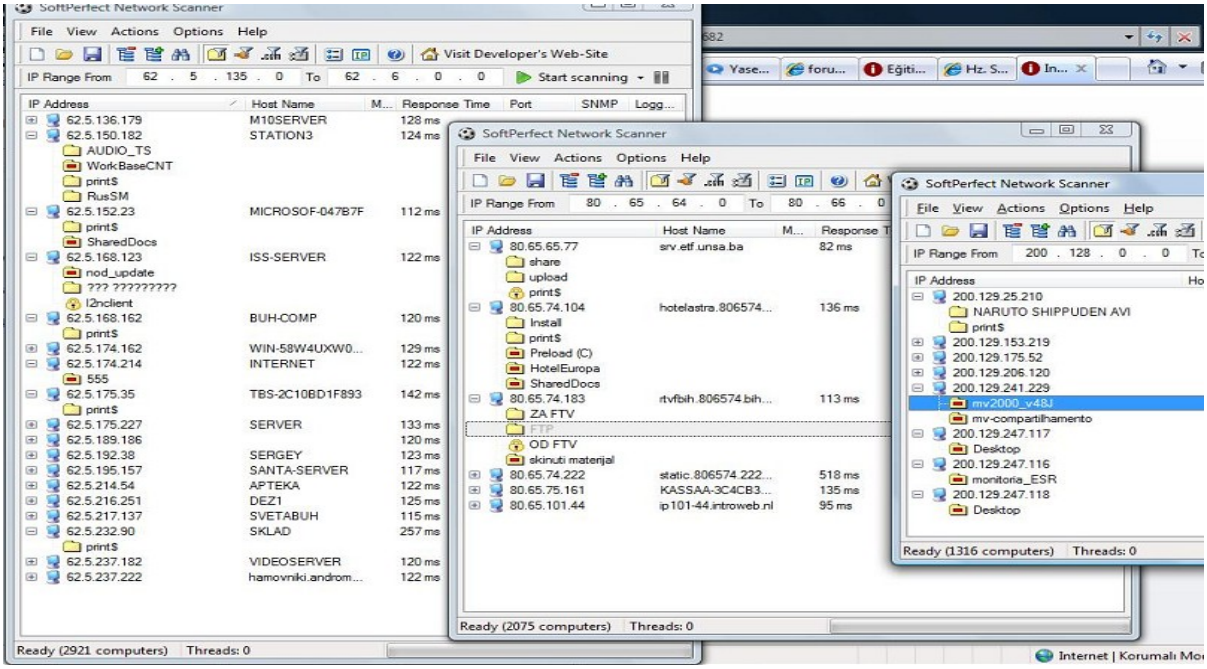
Yeterince tedbir alınmaması da saldırıların artmasına neden olmaktadır. Çok fazla teknik bilgiye sahip olunmasa bile, yardımcı programlar vasıtasıyla saldırı gerçekleştirilebilmektedir. Eğer, bilgisayarda yeterince önlem alınmadıysa yetkisiz erişimin zor olmayacağını göstermek için bir port tarayıcı programıyla tarama yapıp güvenliği alınmadan paylaşıma açılan klasörler şekil-4'te görülmektedir.Hatta öyle ki bunların içinde, veri tabanı olarak kullanılan ve üstelik dosyalar üzerinde değiştirme ve silme yapabileceğiniz şekilde paylaşıma açılanı da bulunmaktadır. Bu durumda özellikle lamerların ilgisini çekip artan düzeyde girişimde bulunmasına yol açmaktadır.

3. Bilişim Saldırganlığının Sınıflandırılması

Bilişim saldırganlarını üç temel gurupta ele almak mümkündür;

Birincisi amatör saldırganlar olup, bunların genel amacı zarar vermek olmamakla birlikte, özellikle kendilerini ispat etme, macera arama veya meydan okuma gibi nedenlerle saldırırlar. Bu kişilerin yaptığı saldırılar suç kapsamına girse bile, kötü niyet ve eylem içermedikleri için çoğu kez takibe alınmaz, uyarılmakla yetinilir.

İkinci grup, maddi bir menfaat elde etme amacında olmasa bile, etnik, dini yada sosyal bir amaç uğruna saldırı gerçekleştirenlerdir. Bir spor klübüne ait sitenin rakip takım taraftarları tarafından saldırıya uğrayarak ele geçirilmesi bu gruba örnek olarak gösterilebilir.



Şekil 4. Farklı ülkelere ait ip aralıklarında, güvenliği alınmadan paylaşılan bilgisayar taraması

Üçüncü grup yani profesyonel saldırganlar olarak nitelendirilen grup ise farklı olarak ele alınmak zorundadır. Bu gruba mensup olanlar bu işi meslek olarak ele alıp, bu işten kazanç sağlama yada karşı

tarafa zarar verdirme amacında olanlardır. Borsa şirketleri üzerine manipülasyon, banka hesaplarının boşaltılması, kişilere yasal olmayan sanal alışveriş yaptırılması, kişilerin borçlandırılması, v.b. yöntemler bu grubun saldırılarında ticari olarak ulaşma çabasında olduğu hedeflerden bir kaçıdır.

SONUÇ

Bu çalışmada bilginin önemi vurgulanmış, bilişim saldırganlığından bahsedilmiş, bilişim saldırganlığı nedenleri ortaya konmuş ve bilişim saldırganlığının sınıflandırılması yapılmıştır. Sanal ortamda gerçekleştirilen güvenlik ihlallerinin hedef ve yöntemleri verilmiş, ayrıca ip tarayıcı programı ile bir saldırı örneği sunulmuştur. Bilginin önemi, teknolojinin hızla ilerlemesi ve yeterli güvenlik tedbirlerinin alınmayışı bilişim saldırganlığını ve hatta türlerini arttıracağı muhakkaktır.

Bilişim saldırılarını saldırganlıktan vazgeçirebilmek mümkün olmadığına göre, saldırganlara karşı savunma tedbirlerini arttırma zorunluluğu ortaya çıkmaktadır. Saldırganlığın boyutları arttıkça, çoğu savunma önlemi de ne yazık ki zamanla işe yaramaz hale gelebilmektedir. Savunma tedbirlerinin sürekli olarak güncellenmesi zorunluluğu, farkında olalım yada olmayalım, dinamik yapısı sebebiyle, giderek bilişim dünyasında daha fazla öne çıkan bir sektör haline dönüşmektedir.

KAYNAKLAR:

[1] Gümüş, Çetin (2008)
Bilişim Suçlarıyla Mücadelede Polisin Eğitimi
Doktora Tezi

[2] TATAR, Ünal (2009-TÜBİTAK-UEKAE)
Siber Savaş Ve Sanal Ortam Güvenlik Politikası

[3] http://firstmonday.org/
Vegh, Sandor(2005)
The media's portrayal of hacking, hackers, and hacktivism before and after September 11
Erişim Tarihi: 01 Eylül 2009

[4] YILMAZ, Murat (2007) - "Bilişim Suçları"

[5] http://catb.org/
Raymond, Eric S.
The New Hacker's Dictionary
Erişim Tarihi: 20 Eylül 2009.

[6] Shinder, D. L. (2002). Scene of Cybercrime.
Computer Forensics Handbook.
Syngress Publishing, USA, 2002.

[7] http://www.kom.gov.tr/ (İçişleri Bakanlığı - Kaçakçılık Ve Organize Suçlarla Mücadele Daire Başkanlığı 2007 ve 2008 Yılı Raporları)
Erişim Tarihi: 07 Kasım 2009.

[8] Wikipedia (2008). Bilişim.
http://tr.wikipedia.org/wiki/Bili%C5%9Fim_bilimi.
Erişim Tarihi: 01 Kasım 2009.

[9] KOM Daire Başkanlığı (2008). Bilişim Suçları ve Yükselen Trentler
http://www.kom.gov.tr/
Erişim Tarihi: 16 Eylül 2009.

[10] http://www.siberarsiv.com/forum/bilisim-hukuku/bilisim-guvenligi-e-book-557.html
Erişim Tarihi: 05 Aralık 2009

[11] Pekgözlü, İ. (2008). Küresel Tehdit: Bilişim Suçları.