Siber Güvenliğe İlişkin Temel Bilgiler

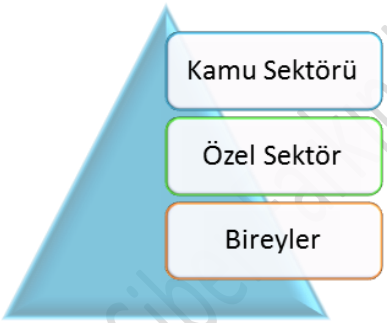
Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Telekomünikasyon İletişim Başkanlığı
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: usom@usom.gov.tr

Temmuz 2014
UR.RHB.001

İÇİNDEKİLER

1.GİRİŞ

Günümüz dünyasında teknoloji, insanların günlük yaşantılarından tutun da iş dünyasına, kamuya ait genel ve milli güvenliği ilgilendiren tüm alanları içine alacak şekilde hayatımızın içine kadar girmiştir. Bir millete ait siber uzayın sacayaklarını oluşturan birey, özel ve kamu sektörü kullandıkları teknolojiler yolu ile kişisel ve kritik verilerini bir şekilde siber uzaya aktarmaktadırlar. Teknolojinin gelişmesi ve hayatımıza daha fazla girmesi neticesinde milli güvenliği ilgilendiren kritik veriler ve milyonlarca lira dünya siber uzayında saldırılara açık bir biçimde dolaşabilmektedir [1].



Şekil 1: Siber Uzayın Bileşenleri

Yukarıda bahsedilen kritik süreçlerin yanı sıra, bireylerin dahi kişisel bilgilerini siber uzayda barındırmaları nedeni ile kullanmış olduğumuz teknolojilerin istikrarlı, güvenli, güvenilir ve esnek bir yapıda olmaları gerekmektedir. Çünkü günümüzde siber suçlular veya teröristler artan bir oranda bilgisayarları, bilgisayar ağlarını, mobil cihazları ve akıllı cihazları amaçlarına ulaşmak için kullanmaktadır. Siber suçlular tarafından gerçekleştirilen bireysel verilerin elde edilmesi ve kötü amaçlı kullanılması, kritik süreçlerin engellenmesi veya yok edilmesi, ekonomiye büyük maliyetler getirecek saldırıların gerçekleştirilmesi ve milli sırların ele geçirilmesi ya da teşhir edilmesi gibi birçok siber saldırı günden güne artarak devam etmektedir. Bahsedilen birçok siber saldırının önüne geçilmesi yukarıda Şekil 1'de belirtilen siber uzay bileşenlerinin korunmasını sağlayacaktır.

Yapmış olduğumuz bu çalışma temel biçimde siber güvenlik kavramları ve tehditleri hakkında giriş içeriklerini kapsayacak şekilde bilgilendirme amacı taşımaktadır. Okuyucunun temel siber güvenlik kavramlarını ve önemini örnekleri ile birlikte öğrenmesi hedeflenmektedir.

Hızlı bir biçimde teknoloji kullanımının artması neticesinde günümüz bireyleri, iş dünyası ve devlet kurumları kritik öneme haiz istihbarı, ekonomik ve kişisel bilgilerini bu teknoloji araçları vasıtası ile depolamakta ya da transfer etmektedir. Transfer edilen bu verilerin dolaşım sırasında bozulması ya da transferinin gerçekleşememesi gibi durumlarda çok büyük ekonomik veya itibari kaybın olacağı da bilinen bir gerçektir. Siber güvenlik hakkında detaylı bilgi vermeden önce siber güvenliğin ne olduğu ve temel kavramları hakkında bilgi verilmesi konunun daha iyi kavranması açısından da bir zorunluluktur. Bu alt bölümde siber güvenlik, siber ortam, siber saldırı, bilgi güvenliği ve bilgisayar güvenliği gibi kavramları Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı çerçevesinde tanımları aşağıda sunulmuştur [2].

a) Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri,

b) Siber ortam: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamı,

c) Kamu bilişim sistemleri: Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/veya kamu kurum ve kuruluşları tarafından işletilen bilişim sistemlerini,

ç) Gerçek ve tüzel kişilere ait bilişim sistemleri: Türkiye Cumhuriyeti kanunlarına tabi olarak gerçek ve tüzel kişilere ait olan ve/veya gerçek ve tüzel kişilerce işletilen bilişim sistemlerini,

***d) Ulusal siber ortam**: Kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan ortamı,*

e) Kritik altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- *Can kaybına,*
- *Büyük ölçekli ekonomik zarara,*
- *Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına,*

yol açabilecek bilişim sistemlerini barındıran altyapıları,

f) Siber güvenlik olayı: Bilişim sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini,

g) Siber güvenlik: Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini,

h) Ulusal siber güvenlik: Ulusal siber ortamda bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem ve verinin ve bunların sunumunda yer alan sistemlerin siber güvenliğini tanımlar.

Günümüz siber dünyasında bilgisayarlar ve bilgisayar ağlarının kötü niyetli kullanımı ve virüsler, trojan atları ya da klavye okuyucular gibi siber tehditler nedeni ile milyon liralık ekonomik sorunlar meydana gelmektedir. Bu tip sorunların genellikle bireylere ait TC Kimlik Numaralarının elde edilmesi, banka hesaplarının çalınması ya da kredi kartı numaralarının elde edilmesi gibi kimlik hırsızlığı neticesinde meydana geldiği bilinmektedir. Kimlik hırsızlığı, bireylere ait ekonomik sorunlar oluşturmasının yanı sıra finansal şirketler açısından da hem para hem de itibar kaybına neden olmaktadır. Bu nedenle hem bireylere hem de finansal kuruluşlara kişi/müşteri bilgilerinin korunmasında siber önlemleri almak ve kamuoyunu bilinçlendirme konusunda büyük görevler

düşmektedir. Bahse konu görevlerden en önemlisi, bilgi güvenliği perspektifi açısından verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin (GBE) korunmasıdır.

Bilgiyi saklayan kurumların, kurumsal verilerin ve müşterileri verilerinin gerçekliğini, eksiksizliğini, ulaşılabilirliğini ve yetkili kişiler arasında paylaşılabilirliğini garanti etmesi gerekmektedir. Bununla birlikte yukarıda belirtilmiş amaçlar doğrultusunda oluşturulmuş ve kullanılan programların da GBE kavramları doğrultusunda işlevlerini yerine getirmesi gerekmektedir. Bu kavramlar Ulusal Siber Güvenlik Stratejisi 2013-2014 Eylem Planı'nda aşağıdaki Şekil 2'de verildiği şekilde tanımlanmıştır.

Şekil 2: Bilgi Güvenliği Anahtar Kavramları

a) Gizlilik: Bilişim sistem ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini; bilişim sistemlerine ait veya sistemdeki gizli verinin yetkisiz kişi veya sistemlerce ifşa edilmemesi.

b) Bütünlük: Bilişim sistemlerinin ve bilginin sadece yetkili kişilerce veya sistemlerce değiştirilebilmesi.

c) Erişilebilirlik: Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine ve bilgiye erişebilmesi.

2.TEMEL SİBERGÜVENLİK KAVRAMLARI

Günümüz siber dünyasında, bütünlük veya erişilebilirliğin yanında gizliliğin de sağlanması, kullanılan teknolojik cihazlar ve bilgisayarların internete bağlı olmasından dolayı oldukça zordur. Bireylerin kullanmış olduğu bu teknolojik cihazlar çalıştırdıkları programlar nedeni ile gizliliğin ihlaline yol açabilmektedirler. Siber güvenlik süreçlerini, saldırılarını, savunma mekanizmalarını açıklamadan önce aşağıda yer alan genel kavramlardan ve terimlerden bahsedilmesinin gerekli olduğu değerlendirilmektedir.

Erişim Kontrolü: Bilgiye erişimin denetlenmesi, bilgi sistemlerine yetkisiz erişimin engellenmesi, yetkisiz kullanıcı erişimine izin verilmemesi, hizmetlerin korunması, yetkisiz işlemlerin tespit edilmesi ve uzaktan çalışma ortamlarında bilgi güvenliğinin sağlanmasıdır [3].

Kimlik Denetimi: Herhangi bir kişiye ait rol ya da kimliğin doğrulama mekanizmasıdır.

Yetkilendirme: Kimliğin belirli kaynaklara erişiminin olup olmadığının karar verilmesi sürecidir.

Varlık: Saldırılara karşı korunması gereken değerli bilgi kaynaklarını tanımlar (TC Kimlik numarası veritabanı, kredi kartı veritabanı ya da personel veritabanı gibi).

Güvenlik Açığı: Sistem üzerindeki yazılım ve donanımdan kaynaklanan ya da sistemin işletim kuralları ve/veya yönergelerindeki açık noktalar ve zayıf kalmış yönlerdir.

Risk: Siber saldırı neticesinde meydana gelebilecek olası zararlı sonuçlar.

Tehdit: Zararlı sonuçlar doğurabilecek olası saldırı ya da açıklık durumlarıdır.

3.SİBER SALDIRILARIN KAYNAKLARI

Siber saldırı kaynaklarını genel olarak Şekil 3'te görülen dört grupta toplamak mümkündür.

Hacker & Siber Suçlular: Kişisel bilgisayarlar ya da mobil cihazlara veya organizasyon – şirket – kamu bilgisayar ağlarına izinsiz giriş yapan kişilerdir. Türk Dil Kurumu sözlüğünde "Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kişi" olarak tanımlamaktadır.[4].

İç (Dahili) Saldırganlar: Organizasyon içerisinde, belirli amaçlar çerçevesinde dahili sistemlere saldırı düzenleyen kurumsal kişilerdir.

Siber Aktivistler: Dünya görüşleri çerçevesinde kötü veya uygunsuz gördükleri toplumsal ya da politik sorunları dile getirmek amacı ile kamu ya da özel sektör siber uzaylarına saldırı düzenleyen şahıs ya da gruplardır [5].

İstihbarat Kurumları: Uluslararası siber dünyada ülkeler birbirlerini siber tehdit olarak da görmeye başlamışlardır. Bu tehdit algısı nedeni ile ülkeler siber savunma ve siber saldırı takımları oluşturmakta ve diğer ülkelere ait kritik verilere erişmeye çalışmanın yanında hedef ülkenin kritik altyapılarına siber saldırılar yapmaya da devam etmektedir.

Şekil 3: Siber Saldırı Kaynakları

4. SİBER SALDIRI TÜRLERİ

Siber uzayda, siber güvenlik uzmanlarının kendi bilgisayar ve bilgisayarlarını korumalarını gerektirecek çok fazla saldırı ve saldırı çeşidi bulunmaktadır. Örneğin trojan atları, virüsler, solucanlar, mantık bombaları, DDOS, sosyal mühendislik atakları, oltalama saldırıları vb … Saldırganlar bu saldırı yöntemlerini kullanarak sızmış oldukları bilgisayar ya da bilgisayar ağlarına değiştirici, yıkıcı, hizmet aksatıcı ya da verileri sızdırma şeklinde çeşitli zararlar verebilmektedir. Bu zararların organizasyon ya da kamu kurumuna maddi zararları olabileceği gibi itibarının azaltılması şeklinde zararları da olmaktadır. Çalışmanın bu bölümünde gündemdeki en popüler siber saldırı türlerinden bahsedilecektir.

Zararlı Yazılımlar (Malware): En genel ifade ile bilgisayar sistemlerini kötü amaçlı kullanmak için sistem bilgilerine erişim sağlamaya yarayan ya da bilgisayar sistemlerine ciddi zararlar veren kötücül bilgisayar programlarıdır. Zararlı yazılımlar genel bir kavram olup virüsler, solucanlar, truva atları, rootkitler ve casus yazılımlar bu konseptin içerisinde kendine yer bulabilirler [6]. Zararlı yazılımlara ilişkin görsel Şekil 4'te verilmiştir.

Şekil 4. Genel Zararlı Yazılımlar

Zararlı yazılımlar insanlara, süreçlere ve/veya teknolojilere karşı kullanılabilir. Burada ki temel ve en önemli nokta ise zararlı yazılımların amacının sistemlere yetkisiz erişim hakkını elde etmek veya kritik – önemli verilerin elde edilmesini sağlanması olduğudur.

Virüsler; bilgisayar virüsleri en genel manada kendini sistemdeki dosyalardan ya da programlar biri olarak değiştiren bilgisayar kodlarıdır. Virüslerin anlaşılmasındaki kritik nokta ise bir kullanıcı tarafından çalıştırılmaları gerektiğidir. Genellikle bir kullanıcıdan gelen e-postanın açılması, ya da USB'nin otomatik çalıştırılması şeklinde meydana gelebilmektedir.

Solucanlar; virüs gibi kendini bir bilgisayardan başka bilgisayara kopyalamak için tasarlanmış zararlı yazılımlardır. Virüslerden farkı yayılma işlemini ağ üzerinden otomatik olarak yapmasıdır. Otomatik yayılmanın olması nedeni ile zamanla bilgisayar ağının yavaş çalışması, internet sayfalarının geç gelmesine neden olurlar.

Solucanların genel yayılma yöntemleri arasında;

- E-posta eki olarak gönderilen dosyalar ile yayılma,
- Web veya FTP kaynağı bağlantısı ile yayılma,
- ICQ veya IRC mesajında gönderilen bağlantılar ile yayılma
- P2P (eşdüzeyler arası) dosya paylaşım ağları üzerinden yayılma

sayılabilmektedir. Bununla birlikte bazı solucanlar, ağ paketleri olarak yayılmaktadır. Bunlar bilgisayar belleğine doğrudan girmekte ve ardından solucan kodu etkinleştirilmektedir. [7].

Truva Atı; bilgisayar kullanıcılarının içeriği hakkında derinlemesine bilgisi olmadan yükledikleri zararlı yazılımlardır. Örneğin bir kullanıcının "Flash Player" yüklediğini düşünürken aslında "Adobe" ya da güvenilir bir kaynak yerine rastgele bir kaynaktan "Flash Player" yüklemesi olarak düşünülebilir. Genel olarak Truva atı olan programlar,

dosyanın sisteme indirilmesi sonrasında yüklenmesi neticesinde bilgisayar sistemlerine bulaşırlar. Truva atlarının karakteristiği kullanıcı bilgisayarının uzaktan kontrol edilebilmesi ya da izlenmesinin sağlanmasıdır. Truva atı yüklenmiş olduğu bilgisayarların zombi bilgisayarlar olarak da kullanılmasına izin vermektedir [8-9].

Rootkit; bilgisayara bulaşan, çalışan işlemler arasında kendini gizleyen, kötü niyetli kişilere, uzaktan bilgisayarınızın tam hakimiyetini sağlayan tespit edilmesi oldukça zor olan bilgisayar programıdır. Virüsler gibi amacı sisteminizi yavaşlatmak ve yayılmak değildir. Bilgisayarınızın kontrolünü ele geçirmek ve bulunduğu sistemde varlığını gizlemektir. Önceleri çok kullanıcılı sistemlerde sıradan kullanıcıların yönetim programlarına ve sistem bilgilerine erişimini gizlemek için geliştirilmiş ve kullanılmış olmasına rağmen, kötü niyetli kullanımına da rastlamak mümkündür [10].

Güvenilir bir kaynaktan geldiğine inanılan bir programın üst düzey yetki ile (root gibi) çalıştırılması zararlı bir rootkitin sisteme kurulmasına sebep olur. Benzer şekilde, çok kullanıcılı bir sistemde kernel vs açıkları kullanılarak sistemde root yetkisi kazanıp rootkit kurulması en yaygın görülen bulaşma şeklidir.

Rootkitin gerçekte hangi dosyaları değiştirdiği, kernele hangi modülü yüklediği, dosya sisteminin neresinde kayıtlı olduğu, hangi ağ servisi üzerinde dinleme yaparak uygun komutla harekete geçeceğini tespit etmek güçtür. Yine de, belli zamanlarda en temel komutların ve muhtemel rootkit bulaşma noktalarının öz değerlerinin saklanarak bunların daha sonra kontrol edilmesi gibi metodlar kullanılabilir.

Yemleme (Phishing); yasadışı yollarla kullanıcıların herhangi bir sistem için kullandıkları kullanıcı adı, şifre, kimlik bilgileri, kredi kartı ayrıntıları gibi bilgilerin ele geçirilmesidir [11]. Sözcük, İngilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş phishing ifadesinin Türkçe karşılığıdır. "Yemleyici" diye tanımlanan şifre avcıları, genelde e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi ister. Bu tip mailleri cevaplayan kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır.

Örnek olarak; format açısından resmi bir banka konseptinde bir e-posta alınır, ve bu e-postada şifre, kredi kartı numarası vb. bilgilerin verilmesi önerilir.

Yemleme karşısında tüm bankalar vb. kurumlar hiçbir zaman kullanıcılarından e-posta aracılığı ile özel bilgilerini istemeyeceklerini, böyle bir durumda e-postayı vb. talepleri kendilerine iletmelerini önerirler.

Casus Programlar (Spyware); Casus programlar bilgisayarınızda casusluk yapmak için yaratılmış programlardır. Casus yazılım, kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanır. Bu casus yazılımlar, diğer kötücül yazılımlara göre özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadırlar [12].

Casus yazılımlar, virüs ve solucanların aksine sisteme bulaştıktan sonra yayılmaya ihtiyaç duymaz. Amaç, bulaştırılan sistemde gizliliği sağlayarak bilgi toplamaktır. Bu bilgi kimi zaman bir kredi kartı numarası gibi önemli bir bilgi bile olabilir. Bunun dışında, Ticari firmalar İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedirler.

Sosyal Mühendislik; temel olarak bilgisayar ya da bilgisayar ağlarındaki açıklıklardan faydalanarak bilgisayar sistemlerine zarar veren yaklaşımların aksine "sosyal mühendislik" yöntemi insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir [13].

5. KAYNAKLAR

[1] Canvas, *Learning and assessment activities.*

https://learn.canvas.net/courses/95/wiki/m1-learning-and-assessment-activities

[2] Resmi Gazete, 2013. *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*,

http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

[3] Nazlı, M. 2009. *Bilgi Güvenliği Açısından Erişim Kontrolü,* Ulusal Bilgi Güvenliği Kapısı.

http://www.bilgiguvenligi.gov.tr/kimlik-yonetimi/bilgi-guvenligi-acisindan-erisim-kontrolu-2.html

[4] Yılmaz, S. & Sağıroğlu, S. 2013. *Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri*, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTU.

[5] Technopedia, *Cyberactivism.*

http://www.techopedia.com/definition/27973/cyberactivism

[6] ATK Bilişim, *Adware, Spyware, Malware, Virus Nedir?,* Bilgisayar ve Güvenlik.

http://www.atkbilisim.com/bilgilendirme-bolumu/31-bilgisayar-ve-guvenlik/18-adware-spyware-malware-virus-nedir.html

[7] Kaspersky. *Bilgisayar Virüsü veya Solucanı Nedir?*

http://www.kaspersky.com/tr/internet-security-center/threats/viruses-worms

[8] Bilişim Terimleri. *Truva Atı*

http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/76.html

[9] Şahinoğlu, M., Öztemür, M & Sosyal, B. 2013. *Donanımsal Truva Atı Tespiti Etkinlik Analizi*, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTU.

[10] Wikipedia. *Rootkit*.

http://en.wikipedia.org/wiki/Rootkit

[11] Wikipedia. *Phishing.*

http://tr.wikipedia.org/wiki/Phishing

[12] Canbek, G. & Sağıroğlu, Ş. 2006. *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri,* Grafiker Yayıncılık.

[13] Bican, C. 2008. *Sosyal Mühendislik Saldırıları*, Ulusal Bilgi Güvenliği Kapısı.

http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html