Siber Saldırıların Kritik Altyapılar Üzerindeki Etkileri

Ender Şahinaslan[1], Önder Şahinaslan[2], Selçuk Selimli[3]

[1] Bank Asya, BT Risk Yönetimi, Uyum ve Bilgi Güvenliği, İstanbul

[2] Maltepe Üniversitesi, Bilişim Bölümü, İstanbul

[3] Karabük Üniversitesi, Teknoloji Fakültesi, Karabük

Özet: Bu çalışmada, ülkeler, kurumlar ve bireyler için hayati önem taşıyan kritik bilgi ve sistem alt yapılarını tehdit eden siber tehdit ve saldırıları, bu siber saldırıların kritik altyapılar üzerindeki olumsuz etkileri ve bunlara karşı alınması gereken önlemler ele alınmıştır.

Anahtar Sözcükler: Bilgi ve bilgi teknolojileri güvenliği, standartlar(ISO/IEC 27005, ISO/IEC 31000, RISK IT, COBIT vb), siber saldırı, siber tehdit, siber güvenlik, kritik altyapılarda siber önlem.

Effects of Cyber Attacks on Critical Infrastructures

Abstract: In this study, cyber threats and attacks which threat the vitally important critical information and system infrastructures for countries, organizations and individuals, additionally, the adverse effects of these cyber threats on the critical infrastructures and the active countermeasures should have to be taken were discussed.

Keywords: Information and information technology security, standards(ISO/IEC 27005, ISO/IEC 31000, RISK IT, COBIT etc), cyber-attacks, cyber threats, cyber security, cyber critical infrastructures precaution.

1. Giriş

Birey, toplumun bir bölümü ya da tamamını ilgilendiren, yaşamsal fonksiyonlarını yerine getirmede temel ihtiyaç duydukları hizmetlere erişmelerini sağlayan sistem ve alt yapılar kritik olarak nitelendirilir. Bunlar daha çok sunulacak bir hizmetin kesintisiz biçimde sunulmasında rol alırlar. Hizmetlerin kesintisiz olduğu kadar güvenli biçimde sunulabilmesi önemlidir.

Günümüzde artık bireysel saldırılardan öte bir takım grupların birlikte hareket ettiği hatta devletlerin bile savaş olarak kullanmaya başladığı siber saldırılar kritik alt yapılar üzerinde gerçekleştirildiğinde toplumda telafisi mümkün olmayan hasarlara sebep olabilir. Hizmete konu olan ve hayati önem taşıyan bu kritik sistem ve altyapıların korunması gerekir. Örneğin bir havaalanı kontrol sistemini düşünelim, uçak ve kule haberleşmelerinde yaşanacak bir kesintinin ya da iletişimde araya girecek bir yanlış bilgi ya da yönlendirmenin oluşturacağı kargaşa ortamı, doğuracağı olumsuz etkileri giderebilmek zor olsa gerek. Burada iletişimi sağlayan haberleşme ve bilgi sistemleri altyapısı, aydınlatma ve bilişim sistemlerinin çalışmasında rol oynayan enerji sistemleri, bunların koordinasyonda rol oynayan uygulamalar gibi pek çok unsurun dikkate alınması gerekir.

Bu kritik altyapı ve sistemler üzerine gerçekleştirilecek bir siber saldırının vereceği hasarların önceden öngörülebilmesi, bir risk değerlendirmesinin yapılması, kritik altyapılar üzerinde var olabilen zayıflık ve bunları kullanabilecek tehditlerin belirlenmesi, bunları önlemeye yönelik tedbirlerin önceden alınması önemlidir.

2. Siber Güvenlik

Siber terimi sibernetik kökeninden gelmektedir. İlk olarak 1958 yılında, canlılar ve/veya makineler arasındaki iletişim disiplinini inceleyen Sibernetik biliminin babası sayılan Louis Couffignal tarafından kullanılmıştır[1].

Bilgi ve iletişim teknolojileri kullanılarak dünyada hedef seçilen bir birey, kurum, bina, sistem ve kritik altyapıları hedef alan ve bunların istenilen şekilde hizmet vermesini engellemeye, işleyişini bozmaya veya bilgilere izinsiz erişim, bilgininin bütünlüğünü bozmaya dönük saldırılar ise siber saldırı olarak adlandırılmaktadır [2].

Siber güvenlik, siber saldırılara karşı alınan tedbirler bütünüdür[3].

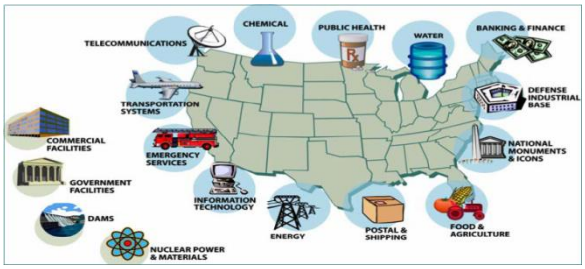
Daha çok devletler ya da çeşitli gruplar tarafından başlatılan siber savaşlar artık bireylerin yaşam koşullarını da olumsuz etkilemeye başlamıştır. Bu durum "ITU Telecom World 2012" konferansında konuşan Kaspersky Lab CEO'su ve tarafından; siber savaş sadece devletleri ve işletmeleri değil, sokaktaki vatandaşı da tehdit ettiği vurgulanmaktadır[4].

3. Kritik Altyapı

"Kritik altyapı" terimi ilk defa Ekim 1997 tarihli "Amerika Birleşik Devletleri Başkanlık

Komisyonu'nun Kritik Altyapıların Korunması Hakkında Raporu"nda kullanılmıştır [5]
Toplum ve devlet düzeninin sağlıklı biçimde işletilebilmesi için gerekli, birleriyle bağı olan sistemler, bu sistemlerin istenilen biçimde çalışmasını sağlayan alt yapılar bütününe denir. Enerji, sağlık, su, gıda, sağlık, haberleşme, güvenlik gibi birey veya kurumların temel ihtiyaçlarını karşılamada kullanılan sistem ve fiziksel alt yapılardan oluşur.

Amerika Birleşik Devletleri tarafından kabul edilen kritik altyapı örnekleri Şekil-1'de gösterilmektedir.



Şekil 2. Kritik Altyapı Örnekleri

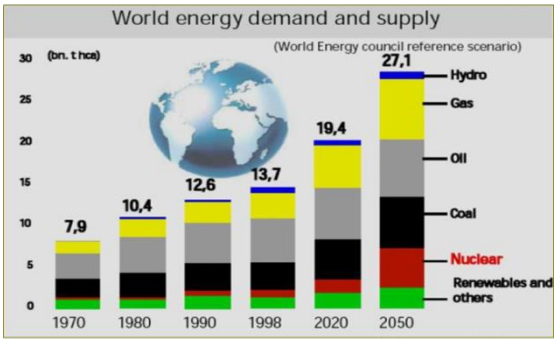
Bunl
ara bakıldığında daha çok toplumun çoğunlunu ilgilendiren haberleşme, ulaşım, enerji, nükleer enerji, su, gıda-tarım, kimya, sağlık, acil servisler, bankacılık-finans, kamu faaliyetleri, savunma endüstrisi gibi hizmet ya da alt yapılar öne çıkmaktadır.
Avrupa Birliği tarafında ise yine AB Komisyonu tarafından yayınlanan listede ise; sağlık, enerji, su, gıda, ulaşım, finans, sivil yönetim, uzay araştırmaları, kamu düzeni ve güvenliği öne çıkmaktadır.

4. Tehdit ve Saldırın Etkileri

Bilgi varlığının korunması gereken niteliklerini bozmaya yönelik mevcut ya da olabilecek her türlü algıya tehdit denir[6]. Tehdit korunması gereken bir varlık üzerinde yer alan bir zayıflığı kullanarak olaya dönüşebilir. Siber bir tehdit olan saldırgan saldırısında amacına ulaşabilmek için sürekli zafiyet arar ya da gözler. Bu zafiyetler bazen tek bir sistemden kaynaklı olduğu gibi bazen normalde tek başına iken zafiyet oluşturmayan ya da etkisi önemsenemeyecek kadar küçük olan bir husus birden fazla sistemin bir arada konuştuğunda beklenmedik bir etkiye sahip hasarlara yol açabilir.
Kritik altyapılar arasında çok fazla sayıda ve karmaşık bağımlılıklar, ilişkiler bulunmaktadır[7]. Örneğin elektrik üreten baraj ya da tesislerin her hangi biçimde zarar görmesi ve uzun süre elektrik enerjisi üretilemediğini düşünelim. Bu durumda elektrikle çalışan enerji iletişim şebekeleri, bilgi ve haberleşme alt yapı ve sistemleri, ulaşım hizmetleri, sağlık hizmetleri, su dağıtım şebekeleri, finans ve güvenlik sistemleri gibi pek çok sistemin durması ya da hizmet verememesi demektir. Yine bireysel olarak etkilerine bakacak olursa bir gün içinde elektriksiz kalmamızın doğuracağı etki malumdur.
Bu sayılan hizmetlerin bir toplumda sunulamaması demek toplumun iç huzur ve güvenliği ile de büyük oranda ilintilidir.

5. Sonuç ve Öneriler

Kritik altyapılar, hizmetlerin güvenli ve ihtiyaç duyulduğunda kesintisiz biçimde sunulmasında önemli görevler üstlenir. Sunulan bir hizmetin güvenli ve kesintisiz bir şekilde sunulabilmesi önemlidir.
Bireyden öte bir toplumu ilgilendiren enerji, su, gıda, sağlık, finans, haberleşme, güvenlik gibi temel hizmetlerin güvenli, kesintisiz ve bozulmadan sunulabilmesi gerekmektedir. Bu hizmet kanallarının sağlıklı ve güvenli sunulmasını engellemeye ya da bilginin gizlilik ve bütünlüğüne yapılabilecek bir saldırı kabul edilemez etkiler doğurmaya, toplum huzur ve güvenliğini bozabilir.
Birçok sistemin çalışmasında ya da hizmetin sunulabilmesinde önemli yapı taşı olan enerji sistemleri öncelikli ele alınması gereken sistemlerden biri olarak karşımıza çıkmakta. Burada enerji sistemlerinin güvenli şeklide dağıtılması, bu istemlerin kontrol ve yönetimini büyük oranlarda sağlayan SCADA denilen otomasyon sistemlerinin güvenliği kadar enerjiyi sağlayan kaynakların ihtiyaçlarda dikkate alınarak çoğullanması farklı alternatif kaynakların yedekli çalıştırılması önemlidir. Şekil-2'de dünyada artış gösteren enerji ihtiyacının yıllara göre hangi kaynaklardan ne kadar oranda elde edileceğinin bir tahmine yer verilmiştir.



Şekil 3. Yıllara Göre Dünya Enerji Talebi ve Sağlanan Kaynaklar Öngörüsü

Ülkemizde de benzer çeşitlendirmeye gidilebilir. Bu aynı zamanda enerji kaynağına yapılabilecek bir saldırının doğurabileceği olumsuz etkiyi de ortadan kaldırabilir.
Toplum ve devlet düzeni sağlıklı işleyebilmesi bireylerin bu hizmetleri güvenli ve sağlıklı biçimde almasına bağlıdır. Bir birleriyle etkileşimli çalışan sistemlere yapılacak bir olası saldırı bir anda tüm toplumu etkileyebilecek boyutlara ulaşabilir, telafisi

güç sonuçlar doğurabilir. Bu ve benzeri nedenlerle artık devletlerin bile bir savaş aracı olarak kullanabildikleri siber tehditlerin dikkate alınması, kritik varlıkların tespiti, olası saldırıların vereceği zararların kestirilerek ek önlemlerin zaman geçirilmeden alınması önemlidir.

Siber saldırılar karşısında birey, toplum ve kamu otoritelerine büyük görevler düşmektedir. Öncelikle kritik varlıklar belirlenmeli, varlıklar üzerindeki zafiyetler ve tehditler saptanmalı ve bunlara karşı kontroller ivedilikle alınmalı, toplum bilinci artırılmalıdır.

Hayatı yaşanmaz kılacak siber saldırılardan korunmak için kritik altyapılar üzerindeki risklerden başlanarak bir plan program dâhilinde gerekli çalışmaların devlet düzeyinde etkin biçimde yürütülmesi önemlidir.

6. Kaynaklar

[1] http://tr.wikipedia.org/wiki/Siber, Aralık 2012'de erişilebilir durumda.

[2] Sahinaslan, E., Sahinaslan, Ö., VI.İstanbul Bilişim Kongresi, Akıllı Yapılarda Siber Güvenlik Farkındalığı, TBD- T.C. Bahçeşehir Üniversitesi, 7-8 Kasım 2012, İstanbul http://www.istanbulbilisimkongresi.org.tr/?page_id=545

[3] Ulusal Siber Güvenlik Stratejisi, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Sayfa:11, Haziran 2012, Ankara

[4] ITU Telecom World 2012, Siber Savaşa Karşı Eylem Çağrısı!, Haber. http://www.zaman.com.tr/ekonomi/siber-savasa-karsi-eylem-cagrisi/2009041.html (30 Ekim 2012'de erişilebilir durumda)

[5] Karabacak, B., İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları, http://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html, (07 Aralık 2012'de erişilebilir durumda)

[6] Sahinaslan, Ö., Sahinaslan, E., Kantürk A, EMO-Ağ ve Bilgi Güvenliği Sempozyumu, Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık, Şubat 2010, Ankara www.emo.org.tr/ekler/e0fddb885736051_ek.pdf

[7] Lewis T. G., "Critical Infrastructure Protection In Homeland Security - Defending A Networked Nation", A John Wiley & Sons, Inc., Publication, 2006