KRİTİK ALTYAPILARA YÖNELİK SİBER TEHDİTLER VE TÜRKİYE İÇİN SİBER GÜVENLİK ÖNERİLERİ

Bilge Karabacak
bilgek@gmail.com

Özet

Kritik altyapılar devlet ve toplum düzeninin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Kritik altyapıların korunması konusu gelişmiş ülkelerin önemli gündem maddelerinden birisidir. Çalışma yapan ülkeler, kritik altyapıların korunması ile ilgili yasal ve teknik çalışmalarda ciddi yol almışlardır. Ülkemizde, kritik altyapılar konusunda resmileşmiş herhangi bir politika veya mevzuat çalışması bulunmamaktadır. Kritik altyapıların güvenliği konusunda ülkemizin önünde uzun bir yol olduğu söylenebilir. Makalede kritik altyapı tanımı yapılmış ve kritik altyapıların siber altyapıya olan bağlılığı konusunda değerlendirmelere yer verilmiştir. Kritik altyapılara yönelik gerçekleştirilen siber güvenlik olaylarına değinilmiştir. Ülkemizin hâlihazırdaki durumu aktarıldıktan sonra kritik altyapı güvenliği için gerçekleştirilmesi gereken çalışmalara yer verilmiştir. Makale, siber tehditler ilgili gelecek öngörüsü ile sona erdirilmiştir.

Anahtar Kelimeler: *Kritik altyapı, SCADA sistemleri, siber tehdit*

1. Giriş

Günümüzde bilgi teknolojileri enerji, sağlık, ulaşım, finans gibi birçok sektörde temel iş süreçlerinin sayısallaştırılması ve otomasyonunda kullanılmaktadır. Kurumların ve bireylerin bilgi ve iletişim teknolojilerine bağımlılığı gün geçtikçe artmaktadır. Bilgi teknolojileri, devlet ve toplum düzeninin sağlanması adına kritik bir rol üstlenmiş durumdadır. Bilgi ve iletişim teknolojilerin sağladığı birçok faydanın yanı sıra bu teknolojiler ile birlikte yeni bir tehdit türü olarak siber tehditler hayatımıza girmiştir. Siber tehditlerden korunmak için birey seviyesinden ülke seviyesine kadar alınması gereken karşı önlemler bulunmaktadır. Ülke seviyesinde gerçekleştirilmesi gereken önemli çalışmalardan birisi de kritik altyapıların korunması (Critical Infrastructure Protection-CIP) başlığı altına değerlendirilmektedir. Bu kapsamda bir devlet politikası olarak belirlenen adımlar ülkede faaliyet gösteren kritik altyapı işletmecileri tarafından gerçekleştirilmektedir.

Kritik altyapı terimi ilk defa 15 Temmuz 1996 tarihli Amerika Birleşik Devletleri Başkanlık Emri'nde kullanılmıştır [1]. Bu başkanlık emrinin ardından Ekim 1997'de "Amerika Birleşik Devletleri Başkanlık Komisyonu'nun Kritik Altyapıların Korunması Hakkında Raporu" hazırlanmıştır [2]. Yeni bir kavramı tanıtmak ve bu kavram hakkında bilgilendirme yapmak amacıyla hazırlanan Başkanlık Komisyonu Raporu'ndan yedi ay sonra "Başkanlık Karar Direktifi" dönemin başkanı Bill Clinton tarafından 22 Mayıs 1998 tarihinde imzalanmıştır [3, 4]. Bu direktif, Amerika Birleşik Devletleri'nin kritik altyapılarını işleten tüm kurumlarına (kamu ve özel sektör) gönderilmiştir. Söz konusu direktifte kritik altyapılar ekonominin ve devletin sağlıklı bir işlemesi için ciddi öneme sahip olan fiziksel ve siber sistemler olarak tanımlanmıştır. Ayrıca kritik altyapıların kamu ve özel sektör tarafından işletilen iletişim, enerji, finans, ulaşım, su sistemleri, acil durum servislerini kapsadığı ancak bu sistemlerle de sınırlı olmadığı ifade edilmiştir. Direktifte ulusal hedefler, kritik altyapıların listesi, kurumların gerçekleştirmesi gereken adımlar, eşgüdüm ile ilgili hususlar, yeni yapılanmalar ve ulusal koordinatör ile ilgili bilgilere yer verilmiştir. Başkanlık karar direktifinde, geçmiş senelerde kritik altyapıların fiziksel ve mantıksal olarak ayrı ve bu nedenle bağımlılığı olmayan sistemler olduğu belirtilmiş, bilgi

teknolojilerindeki gelişmelerin hem altyapıların kendisini etkilediğini hem de altyapılar arasındaki ilişkileri ve bağımlılığı ciddi bir şekilde artırdığı ifade edilmiştir. Başkanlık Karar Direktifi'nin ardından Amerika Birleşik Devletleri'nde gerek kamu sektöründen gerekse özel sektörden kritik altyapı işletmecileri altyapıların güvenliğinin sağlanması ile ilgili koordineli çalışmalara başlamışlardır.

Ülkemiz, kritik altyapılarını henüz belirlemiş durumda değildir. Bu nedenle, kritik altyapıların birbirleri ile olan ilişkileri, bu altyapıların bilgi teknolojilerine bağımlılıkları, kritik altyapıların barındırdığı fiziksel ve sayısal açıklıklar ve kritik altyapılara yönelik siber tehditlerin kabiliyetleri konusunda da veri bulunmamaktadır. Gelişmiş birçok ülke kritik altyapıların korunması ile ilgili programlar yürütmektedir. Bu programlarda, siber tehditler ve bu tehditlere karşı alınması gereken karşı önlemler çok önemli bir yer tutmaktadır. Ülkemizde de kritik altyapıların korunması ile ilgili çalışmalar gerçekleştirilmelidir.

Makalenin ikinci bölümünde siber altyapının kritik altyapılar içerisinde yeri ve önemi anlatılmıştır. İkinci bölümde kritik altyapıları kontrol etmek ve izlemek amacıyla kullanılan SCADA (Supervisory Control and Data Acquisition) teknolojisinden bahsedilmiş ve siber tehditlerin SCADA sistemlerini kullanarak kritik altyapılara verdiği zararlar örnek olaylarla anlatılmıştır. Makalenin üçüncü bölümünde ülkemizde kritik altyapılar konusunda geçmiş senelerde gerçekleştirilen çalışmalar özetlenmiş ve ülkemizin hâlihazırdaki durumu ortaya konmuştur. Makalenin dördüncü bölümünde ülkemizde gerçekleştirilmesi gereken teknik ve yasal çalışmalar ayrıntılı olarak aktarılmıştır. Makalenin beşinci bölümü sonuç bölümüdür. Sonuç bölümünde siber tehditler ile ilgili gelecek öngörüsü yapılmış ve sonuç ifadelere yer verilmiştir.

2. Siber Altyapı, Siber Tehditler ve SCADA Sistemleri

Bilgi teknolojileri istisnasız olarak bütün kritik altyapılarda kullanmaktadır. İletişim altyapısı, Internet altyapısı gibi kritik altyapılar tamamen bilgi teknolojilerinden oluşmaktadırlar. Bankacılık, acil durum servisleri gibi kritik altyapılar bilgi teknolojilerini yoğun şekilde kullanmaktadırlar. Enerji üretim tesisleri, barajlar gibi kritik altyapılar SCADA olarak adlandırılan ve bu yapıları kontrol eden ve izleyen bilgi teknolojilerini içermektedirler. Sonuç olarak, bilgi teknolojilerinin kritik altyapılar için bir siber altyapı oluşturduğu söylenebilir. Bu siber altyapının en önemli aktörü ise Internet olarak karşımıza çıkmaktadır; Amerika Birleşik Devletleri'nde kritik altyapılar, verimlilik ve kullanılabilirliği artırdığı ve maliyetleri düşürdüğü için gün geçtikçe Internet ile daha çok bağlantılı hale gelmektedir [5].

Barajlar, termik santraller, enerji dağıtım üniteleri gibi kritik altyapıların yönetimi ve izlenmesinde uzun yıllardan bu yana SCADA olarak adlandırılan endüstriyel kontrol sistemleri kullanılmaktadır [6]. Yetmişli ve seksenli yıllarda SCADA sistemlerinin başka ağlar ile bağlantısı yoktu, dokümante edilmemişti, herkes tarafından bilinen bilgi ve iletişim teknolojilerini içermemekte; bunun yerine altyapıya özel olarak geliştirilmiş teknolojileri içermekteydi. SCADA sistemleri günümüzde yaygın olarak kullanılan ve bilinen standart yazılım, donanım, işletim sistemi ve ağ protokollerini barındırmaya başlamıştır. Ayrıca, kritik altyapıları yöneten ve izleyen birçok SCADA sistemi kurumsal ağlara ve Internet'e bağlantılı hale gelmeye başlamıştır [5]. Sonuç olarak, SCADA sistemleri sayısal savaşa ve sayısal terörist ataklarına çok daha fazla bir şekilde açık duruma gelmiş ve güvenlikleri geçmişe göre ciddi şekilde sorgulanmaya başlamıştır [7, 8, 9]. Internet fiziksel olarak milyonlarca alt ağdan oluşan ancak mantıksal olarak birleşik bir alandır. Internet erişimi olan bir kurum veya kişi aslında Internet erişimi olan milyonlarca diğer nokta ile iletişim halindedir. Bu hem çok büyük bir avantajdır; hem de siber tehdit açısından bakıldığı zaman korkunç bir gerçektir. Çünkü artık

günümüzde kritik altyapıların bağlantılı hale getirildiği Internet aynı zamanda siber teröristlerin ve bilgisayarlar korsanlarının da kullandığı bir ortamdır.

Kuzeydoğu Elektrik Kesintisi, kritik altyapıların bilgi teknolojilerine bağımlılığını ortaya koymak için oldukça çarpıcı bir örnektir. Kuzeydoğu Elektrik Kesintisi, Amerika Birleşik Devletleri'nin sekiz eyaletinde ve Kanada'nın bazı şehirlerinde 50 milyon kişiyi etkileyen, bazı şehirlerde iki gün süren, 11 kişinin ölümüne ve altı milyar dolar zarara yol açan Amerika Birleşik Devletleri tarihinin en ciddi elektrik kesintisidir. "Kuzeydoğu Kesintisi 2003" olarak tarihe geçen olay bir dizi hatanın ve teknik arızanın aynı anda yaşanması sonucu oluşmuştur. Arızalardan birisinin de, enerji yönetim sisteminde kullanılan bir yazılımdaki böcek (bug) olduğu tespit edilmiştir [10].

Siber uzaydaki tehditler asimetrik tehditlerdir. Tehditlerin asimetrikliğine katkı yapan en önemli iki unsur anonimlik ve elde edilebilirliktir. Bir kritik altyapıyı hedef alan ve ciddi bir zarara yol açan siber saldırı yan dairede bulunan bir kişisel bilgisayardan veya alışveriş merkezindeki kablosuz ağı kullanan bir diz üstü bilgisayardan yapılmış olabilir. Saldırıyı gerçekleştiren siber teröristleri bulmak neredeyse imkânsız olabilir. Örneğin, yan dairedeki komşumuz gerçekte suçsuz olabilir. Bilgisayar, delil bırakmak istemeyen siber teröristler tarafından ele geçirilmiş olabilir. Siber araçların mali açıdan elde edilebilirliği diğer gerçek savaş ekipmanları ile karşılaştırılmayacak kadar düşüktür. Bir sıcak savaşta kritik altyapılara zarar verebilecek bir bombardıman uçağının maliyeti 100 milyon dolarken ve bu uçağı parası olan herkes elde edemezken, kritik altyapılara zarar vermek için kullanılabilecek yazılım ve donanımlara sadece 1000 dolar karşılığında ve zahmetsiz bir şekilde sahip olunabilir.

İkisi Amerika Birleşik Devletleri'nde biri de yoğun olarak İran'da gerçekleşmiş olan ve kritik altyapıları hedef alan üç adet siber saldırı, asimetrik tehditlerin verebileceği zararları anlamak açısından faydalı olacaktır. Ağustos 2001'de Amerika Birleşik Devletleri'nin Kaliforniya eyaletinin büyük kısmına elektrik dağıtımında kullanılan bilgisayar sistemine siber saldırganların yetkisiz bir şekilde girdiği medyada yer almıştır. Sızmanın iki hafta boyunca gerçekleştiği tespit edilmiştir. Elektrik dağıtımında kullanılan SCADA sistemine Internet'ten erişilebilmektedir. Sızmaya sebep olan sistem açıklığının bilgisayar korsanları sisteme herhangi bir zarar vermeden kapatıldığı bildirilmiştir. Olay enerji endüstrisinde yaşanan ilk siber saldırılardan birisi olduğu için ciddi bir şok dalgası yaratmıştır.

İkinci olay Ağustos 2003'te gerçekleşmiştir. Ohio eyaletindeki Davis-Besse nükleer santralindeki özel bir bilgisayar ağına "Slammer" isimli zararlı yazılım bulaşır ve bu zararlı yazılım güvenlik izleme sistemini beş saat boyunca devre dışı bırakır. Basında yer alan haberlere göre santral personeli kurum ağı önünde yer alan güvenlik duvarı tarafından korunduklarını düşünürken bu olayın gerçekleşmesi şaşkınlığa yol açmıştır. Bu örnekte de santralin özel bilgisayar ağı Internet ile bağlantılı durumdadır. Güvenlik duvarları Internet'ten gelen tehditlere karşı %100 koruma sağlamaz. Güvenlik duvarları servis bazında kısıtlama sağlarlar. İzin verilen servisler üzerinden yapılan sızmaları ve illegal siber aktiviteleri güvenlik duvarları tespit edilip engellenmeyebilir.

Üçüncü örnek, ilk iki siber olaydan çok farklı bir kategoridedir. Üçüncü örnek Stuxnet isimli SCADA sistemlerine yönelik programlanmış olan ve en karmaşık siber silah olarak nitelendirilen zararlı yazılımdır. Stuxnet, SCADA sistemler için yazılmış bilinen ilk zararlı yazılımdır. Özellikle İran'ın nükleer tesislerini etkilemiştir. Bilgi güvenliği uzmanları böylesine karmaşık bir yazılımın ancak ulusal düzeyde bir çabayla yazılmış olabileceğini ve bağımsız bilgisayar korsanlarının başaramayacağı bir çalışma olduğu belirtmişlerdir. Stuxnet yazılımı, İran'ın nükleer enerji altyapısını hedef alan bir yazılım olarak uzunca bir süre bilgi ve enerji güvenliği profesyonellerinin gündemini meşgul etmiştir. Zararlı yazılım

Temmuz 2010'da keşfedilip tanımlanmıştır. Ağustos 2010 tarihi itibarıyla dünyada etkilenen bilgisayarların %60'ının İran'da olduğu tespit edilmiştir [11]. Stuxnet, İran'ın Natanz şehri uranyum işleme merkezindeki santrifuj sistemlerini ve Bashehr şehrindeki nükleer reaktör türbinlerini hedef almıştır. Bu ekipmanların kontrol sistemlerini ele geçirmiş ve operatörler tarafından kullanılamaz duruma getirmiştir. Stuxnet'in daha önce hiç bir zararlı yazılımda görülmeyen özellikleri tespit edilmiştir. Öncelikle, sadece nükleer santrallerde kullanılan belli marka ve model SCADA sistemlerini hedef alan bir yazılımdır. Eğer bulaştığı bilgi sisteminde hedef aldığı SCADA sistemi yoksa kendisini etkisiz hale getirmekte ve sisteme bir zarar vermemektedir. Zararlı yazılımların hazırlanmasında yaygın olarak kullanılmayan bir programlama diliyle hazırlanmıştır. Microsoft Windows işletim sisteminin o zamana kadar bilinmeyen dört adet açıklığını aynı anda kullanmıştır. Ayrıca, işletim sistemi seviyesinde güvenin oluşması ve kolaylıkla yayılması için Güney Kore'deki iki adet firmaya ait sayısal sertifikaların gizli anahtarlarını kullanmıştır. Stuxnet yazılımı tespit edilince yapılan inceleme sonucunda bu anahtarların çalındığı ortaya çıkmıştır. Bu özelliklerinde de görüldüğü üzere Stuxnet kendisinden önceki zararlı yazılımların hiç birisine birçok yönden benzememektedir. Gerek bu özellikleri gerekse hedef aldığı sistemler göz önüne alındığı zaman bireylerden ziyade ülkeler seviyesinde bir çalışma sonucunda oluşturulmuş olması küçük bir ihtimal değildir.

Stuxnet'in amacı, kendini gizleyerek SCADA sistemlerinin kontrolü ele almak ve SCADA sistemlerini çalışmaz duruma getirmekti. Diğer taraftan, SCADA sistemlerinin çalışmasını engellemeyen, kendisini belli etmeden çalışan, aynı zamanda uzun süreli istihbarat toplayan ve kendisinden önceki yazılımlardan dersler çıkarılarak hazırlanmış bir yazılımın vereceği zararlar çok daha ciddi olacaktır.

3. Türkiye'deki Durum

Ülkemizde, kritik altyapılara yönelik olarak herhangi bir yasal düzenleme bulunmamaktadır. Hâlihazırda bir mevzuat çalışması da yapılmamaktadır.

Geçtiğimiz senelerde, kritik altyapıların korunmasını içeren bilgi güvenliğine yönelik iki adet çalışma yapılmış ancak bu çalışmalar sonuca ulaşmamıştır. Bu çalışmalardan ilki Ulusal Sanal Ortam Güvenlik Politikası hazırlanması çalışmalarıdır. Estonya bilgi sistemlerine Rus bilgisayar korsanları tarafından Nisan ve Mayıs 2007'de koordine ataklar gerçekleştirilmiştir. Bu ataklar, Dünya'da yaşanan ilk siber savaş olarak nitelendirilmiştir. Bu ataklardan sonra NATO Sayısal Savunma Konsept belgesi hazırlanmıştır. Bu belgenin bir gereği olarak NATO üyesi ülkeler Sanal Ortam Savunma Politikalarını hazırlamaya başlamışlardır. NATO'nun Sanal Ortam Savunma Politikası hazırlanması talebi Dışişleri Bakanlığı tarafından Başbakanlık'a iletilmiş, Başbakanlık Mayıs 2008'te söz konusu politikanın TÜBİTAK koordinasyonunda hazırlanmasını resmen talep etmiştir. Politika dokümanı TÜBİTAK ile birlikte 19 adet kamu kurumunun katılımı ile hazırlanmıştır. Politika belgesi hazırlanması çalışmalarına katılacak kurum listesi, Başbakanlık tarafından koordinatör kurum olarak TÜBİTAK'a bildirilmiştir. Bu kurumlar, Cumhurbaşkanlığı, Başbakanlık, Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı, Milli Savunma Bakanlığı, Maliye Bakanlığı, Ulaştırma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı Müsteşarlığı, Dış Ticaret Müsteşarlığı, Hazine Müsteşarlığı, Merkez Bankası, Milli Güvenlik Kurulu Genel Sekreterliği, Milli İstihbarat Teşkilatı Müsteşarlığı, Bankacılık Düzenleme ve Denetleme Kurumu, Emniyet Genel Müdürlüğü ve Bilgi Teknolojileri ve İletişim Kurumu'dur. Politika dokümanı, Temmuz 2008 – Kasım 2008 ayları arasında hazırlanmış; bu sürede tüm kurumların katıldığı üç adet toplantı gerçekleştirilmiştir. Üçüncü toplantının ardından, politika belgesinde son düzenlemeler yapılmış, katılımcı kamu kurumlarının çoğunluğunun onayı ile belge Başbakanlık'a Ocak

2009'da resmi olarak teslim edilmiştir. Hâlihazırda, Başbakanlık'ın belgeyi onaylaması beklenmektedir. Ülkemizde kritik altyapıların güvenliği ile ilgili atılmış ilk adım bu politika belgesidir. Politika belgesinde "Ulusal kritik bilgi ve iletişim altyapıları tespit edilecek ve bu altyapılar sanal ortamdan gelecek tehdit ve saldırılara karşı korunacaktır. Ayrıca, ülke içerisindeki kritik bilgi ve iletişim sistem altyapıları, bunların birbirleriyle ilişkileri, kritiklik seviyeleri ve sorumluları da tespit edilecektir." ifadeleri yer almaktadır. Ayrıca "Kritik bilgi ve iletişim sistem altyapısına sahip kurumlar için personelin ve kurumun sahip olduğu teknik birikim, imkân ve kabiliyetlerin artırılması sağlanacaktır." ifadesi de politika belgesinde yer almaktadır. Belgede "Ulusal Kritik Bilgi ve İletişim Sistem Altyapısı"; işlediği bilginin gizliliği, bütünlüğü veya sürekliliği zarara uğradığı takdirde,

a. Askeri, milli, kültürel, toplumsal ve iletişimsel güç unsurlarının,
b. Ülke ekonomisinin,
c. Halk sağlığının,
d. Kişisel mahremiyetin,
e. Kamu emniyetinin ve kamu düzeninin,

zarar görmesine yol açabilecek sistemler ve bu sistemleri oluşturan altyapılar olarak tanımlanmıştır.

Ülkemizde kritik altyapıların güvenliğini içeren ikinci çalışma bir mevzuat çalışmasıdır. Bu çalışma 2009 sonbaharında gerçekleştirilmiştir. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü bünyesinde oluşturulan ve çalışmalarına fiilen 3 Mart 2009 tarihinde başlayan e-Mevzuat Çalışma grubu, 7 Ağustos 2009 tarihi itibarıyla "e-Devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı"nı hazırlamıştır. E-devlet ve Bilgi Toplumu Kanun Tasarısı Taslağı'nda kritik altyapı ve kritik bilgi altyapısı terimleri geçmemiş; bunun yerine "Kritik Bilgi Sistemi" ifadesi kullanılmıştır. Taslak içerisinde "Kritik Bilgi Sistemi"nin tanımı "İşlevlerinin tamamen veya kısmen yerine getirilememesi halinde kamu güvenliği ve düzenini önemli derecede etkileyen bilgi sistemleri" olarak tanımlanmıştır. Kanun taslağında geçen "Bilgi Toplumu Ajansı" içerisindeki "Bilgi Toplumu Dairesi"nin görevlerinden bir tanesi de "kritik bilgi sistemlerini belirlemek ve bu sistemler için uygulanacak asgari güvenlik standartlarını tespit etmek" şeklinde belirtilmiştir. Söz konusu kanun tasarısı ile ilgili olarak da 2009 sonbaharından bu tarihe kadar herhangi bir gelişme olmamıştır. Sonlandırılmamış olan bu iki taslak çalışma dışında ülkemizde kritik altyapılar konusunda resmi bir çalışma bulunmamaktadır.

Bu iki çalışmanın yanı sıra kritik altyapı işletmecilerinin katılımı ile yapılan ve Ocak 2011'de düzenlenen Ulusal Siber Güvenlik Tatbikatı'ndan bahsetmek uygun olacaktır. TÜBİTAK BİLGEM UEKAE (Ulusal Elektronik ve Araştırma Enstitüsü) ve Bilgi Teknolojileri ve İletişim Kurumu koordinasyonunda gerçekleştirilen hazırlık çalışmaları 2010 yılı Şubat ayında başlamıştır. Tatbikatın planlanma süreci yaklaşık bir yıl sürmüştür. Bu süreçte tatbikata katılacak taraflar davet edilmiş, ilgili taraflarla görüş alışverişinde bulunulmuş ve tatbikatın düzenleneceği yerin belirlenmesiyle lojistik ihtiyaçların karşılanması için çalışmalar yapılmıştır. Bu çalışmalara paralel olarak gerçekleştirilecek saldırıların ve yazılı enjeksiyonların planlaması yapılmıştır. Ulusal Siber Güvenlik Tatbikatı 2011, finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşunun katılımıyla 25-28 Ocak 2011 tarihlerinde gerçekleştirilmiştir. Tatbikatta katılımcı kurum/kuruluşlardan bilişim, hukuk ve halkla ilişkiler uzmanı statüsündeki 200'e

yakın personel görev almıştır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkilerin gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle, kurumların hem teknik kabiliyetleri hem de kurum içi ve kurumlar arası koordinasyon yetenekleri değerlendirilmiştir.

25-28 Ocak 2011 tarihleri arasında gerçekleştirilen Ulusal Siber Güvenlik Tatbikatı 2011'in (USGT – 2011) ilk iki günlük bölümünde katılımcılar çalışmalara kendi kurumlarından katılmıştır. USGT - 2011'in son iki günlük bölümü ise toplu halde TOBB Ekonomi ve Teknoloji Üniversitesi (ETÜ) Konferans Salonu'nda gerçekleştirilmiştir. USGT – 2011'de katılımcı kurumların teknik kabiliyetlerini tespit etmek ve kurumlara olası saldırılara karşı müdahalede deneyim kazandırmak amacıyla hem gerçek saldırılar hem de yazılı ortamda senaryolar gerçekleştirilmiştir.

USGT – 2011 kapsamında, hem yazılı ortamda gerçekleştirilen senaryolar, hem de gerçek saldırılar sonucunda bazı temel eksiklikler tespit edilmiştir. Bu eksiklikler arasında, sistem yöneticilerinin teknik yetersizliği, sistem yöneticilerinin bilgi güvenliği boyutunda yetersizliği, kurumsal bilgi güvenliği yönetim sistemi eksikliği, kurum içi koordinasyonun yetersizliği ve sistem tasarımı aşamasında güvenliğin göz ardı edilmesi dikkat çekmektedir. Bu eksikliklerin, kritik altyapı işletmecisi kurumlarda bulunması doğrudan kritik altyapıların güvenliğini etkileyebilecek birer unsur olarak karşımıza çıkmaktadır.

Kritik altyapıların güvenliği konusunda ilerleme kaydetmiş ülkelerin çalışmaları incelendiği zaman, çalışmaların temelini tüm kritik altyapıları birden kapsayan hükümet çalışmaları olduğu görülmektedir. Tüm kritik altyapıları içerisine alan bir çerçeve çalışma ile temel atılmadığı durumda - makalenin ilk bölümünde ifade edilmiş olan ilişkilerden ve bağımlılıklardan dolayı- birçok hususun gözden kaçacağı ve eksik bir çalışma olacağı değerlendirilmektedir. Amerika Birleşik Devletleri'nin tüm kritik altyapıları içine alan çalışmaları makalenin birinci bölümünde aktarılmıştı. Bu temel çalışmaların ışığında ve çerçevesinde kritik altyapı işletmecisi kurumlar sektörlere özel çalışmalar yapmışlar ve ciddi yok kat etmişlerdir.

4. Yapılması Gereken Çalışmalar

Kritik altyapıların güvenliğine yönelik farklı seviyelerde yapılması gereken birçok çalışma bulunmaktadır. Bu çalışmaların bir kısmı mevzuat çalışmaları gibi tüm ülkeyi ilgilendiren çalışmalarken bir kısmı da bireylerin yapması gereken teknik çalışmalardır. Bu başlık altındaki karşı önlemler, gelişmiş ülkelerin ve uluslararası organizasyonların hazırlamış oldukları kılavuz dokümanlardan faydalanılarak hazırlanmıştır. [3, 12, 13, 14].

OECD ve NATO üyesi ülkelerin birçoğunun hükümetler seviyesinde tanımlanmış kritik altyapıların korunması programı bulunmaktadır. Bu ülkelerde kritik altyapıların korunması ülke mevzuatı içerisine girmiştir. 2007 senesinde hazırlanmış olan bir OECD dokümanında Avustralya, Kanada, Japonya, Güney Kore, Hollanda, İngiltere ve Amerika Birleşik Devletleri'nin kritik altyapıların korunması ile ilgili yaptıkları çalışmalar karşılaştırılmıştır [15]. Kritik altyapılar ile ilgili çalışma yapan ülkelerin tamamı ilk aşamada bütün altyapıları ilgilendiren temel karşı önlemleri belirlemektedir.

Ülkemizde kritik altyapıların korunması ile ilgili olarak gerçekleştirilmesi gereken en öncelikli dört adım sırası ile aşağıdaki gibidir:

- Üst seviye yürütmeden (Örn: Başbakanlık) destek ve katılım

- Destekleyen mevzuatın hazırlanması ve yürürlüğe girmesi
- Kritik altyapıların korunması ile ilgili politika belgesi hazırlanması
- Çalışmalar için yeterli seviyede bütçe ayrılması

Bu dört adet maddedeki adımlar gerçekleşmeksizin kritik altyapıların korunması adına gerçekleştirilecek daha alt seviyedeki adımların başarısızlıkla sonuçlanması kaçınılmazdır [16].

Kritik altyapıların korunması ile ilgili olarak gelişmiş ülkelerde olduğu gibi ülkemizde de resmi çalışmaların başlatılması gerekmektedir. Bu kapsamda, kritik altyapıların korunmasına yönelik politika belgesinin, politika belgesini detaylandıran stratejinin ve eylem planının hazırlanması gerekmektedir. Bütün bu belgeler için destekleyici mevzuat hazırlanmalı, güncellenmesi ve değiştirilmesi gereken hâlihazırdaki mevzuat tespit edilmeli ve değişiklikler yapılmalıdır. Gerek mevzuat gerekse politika belgesi kritik altyapıların korunması için rol ve sorumlulukların belirlenmesinde kritik bir yol oynayacaktır.

Sayısal savunma ile ilgili çalışmaları organize edecek bir ulusal yürütme organı oluşturulmalıdır. Bilgi paylaşımı için hükümet ile kritik altyapı işleticileri (özel veya kamu) arasında ortaklık kurulmalıdır. Yürütme organının asıl sorumluluğu koordinasyon olmalıdır. Kritik altyapıları işleten kamu sektörüne ve özel sektöre yapılması gereken çalışmaları bildirmelidir. Yürütme organının yapacağı ilk çalışmalardan birisi de kritik altyapıların ve aralarındaki bağımlılıkların belirlenmesi için ülke çapında yapılacak risk analizi çalışmasını organize etmek olmalıdır. Yürütme organı, devletin belirlediği politikaları kritik altyapı işletmecilerine uygulatan bir kurum olmalıdır. Yürütme organı hâlihazırdaki düzenleyici ve denetleyici kurum temsilcilerinden oluşmalıdır. Kritik altyapıların göz ardı edilmeyecek önemli bir kısmının özel sektörün işlettiği düşünülürse özel sektör ile işbirliği ve koordinasyon diğer önemli bir çalışma kalemi olarak değerlendirilebilir.

Kullanıcı bilincini artırmak en öncelikli alınması gereken karşı önlemlerden birisidir. Kullanıcı, bilgi sistemleri ile az veya çok teması olan herkestir. Bilinçlendirme sürekli yapılması gereken bir süreçtir. Uzun süreli eğitimler ile karmaşık kavramları tanıtmak ve “ne” sorusuna yanıt aramak gerekir. Kısa süreli kurslarla, “nasıl” sorusunun cevaplanması ve bu bağlamda işlerin nasıl düzgün bir şekilde yapılacağının öğretilmesi gerekir. Ayrıca, belli bir zaman dilimine sıkıştırılmamış olan sürekli bilinçlendirme faaliyetleri ile “niçin” sorunun personel tarafından yanıtlanabilir duruma getirilmesi gerekir. Sayısal savunma ve kritik altyapıların korunması ile ilgili ulusal bilincin oluşturulması adına çalışmalar da gerçekleştirilmelidir. Kritik altyapıları işleten kurumların gerçekleştirmesi gereken çalışmalardan, vatandaşın yapması gerekenlere kadar birçok konuyu kapsayan bilinçlendirme programı için ulusal medya, Internet siteleri gibi kaynaklar kullanılmalıdır.

Siber olaylara karşı tepki yeteneği geliştirmek amacıyla ulusal çapta bilgisayar olaylarına müdahale ekibi oluşturulmalıdır. Kritik altyapıları işleten kurumlar da etkin bilgisayar olaylarına müdahale ekiplerini oluşturulmalıdırlar. Ayrıca farklı bilgisayar olaylarına müdahale ekipleri arasında koordinasyon yeteneği olmalıdır. Bilgisayar olaylarına müdahale ekiplerinin ülke çapında etkinliği olmalıdır. Hükümetlerle birlikte çalışan, olaylara müdahale eden, hacker gruplarını takip eden ve izleyen ekiplerin faaliyete geçmesi siber güvenlik için önemli bir adım olacaktır.

Internet altyapısının güçlü ve alternatifli bir duruma getirilmesi dağıtık servis dışı bırakma saldırılarından en az seviyede zarar görmek için gereklidir. Telekomünikasyon altyapısı ve Internet

önemli kritik altyapılardır. Gelişmiş ülkelerin durumu da göz önüne alındığı zaman kritik altyapılarının çok daha fazla şekilde kritik iletişim altyapısına ve Internet'e bağlı olacağı öngörüsü yapılabilir. Bu bağlamda, Internet servis sağlayıcılarının etkin yönetimi ve koordinasyonu diğer önemli bir karşı önlemdir. Ayrıca, güçlü ve alternatifli Internet altyapısının oluşturulması gerekmektedir.

Ülkemiz sayısal savaş konusunda uluslararası işbirliğine önem vermelidir. Gelişmiş ülkeler ve OECD, NATO gibi organizasyonlar sayısal güvenlik ve sayısal savunma konusunda ciddi yol almışlardır. Türkiye bu tecrübelerden faydalanmalıdır. Tüm dünyayı içine alan ve sınırları olmayan devasa bir ağ durumundaki Internet sayısal saldırıların da kaynağıdır. Ülkemiz bilgi sistemlerine yapılacak bir sayısal saldırının kaynağı başka bir ülkedeki bilgisayarlar olabilir. Uluslararası işbirliği saldırılara karşı kısa sürelerde önlem almak için gerekli bir şarttır. OECD gibi çok uluslu organizasyonların çalışmalarını takip etmek ise ortak politika oluşturmak, standardizasyona kavuşmak ve birlikte çalışma kültürü edinmek için önemli fırsatlar sunmaktadır.

Üst seviyede bir politika ve program dâhilinde yapılmadığı zaman ve ülke çapında bir sahiplenme olmadığı müddetçe teknik seviyedeki karşı önlemlerin süreklilik arz etmesi beklenemez. Diğer taraftan, teknik karşı önlemler, kritik altyapılara yönelik siber saldırıları engelleyen veya zararları en aza indirgeyen olmazsa olmaz karşı önlemlerdir. Ancak, mutlaka belli bir denetim çerçevesi ve sistematik içerisinde gerçekleştirilmelidir. Makalenin dördüncü bölümünde son olarak teknik karşı önlemlere yer verilmiştir.

SCADA sistemlerindeki teknik açıklıkları sürekli olarak takip etmek ve gerekli yamaları yapmak gerekir. Güvenlik marketini yakından takip edip en son çıkmış güvenlik önlemlerinden haberdar olmak ve bu önlemlerden faydalanmak kritik altyapı güvenliği adına kritik bir çalışmadır.

Bilgi güvenliğini sistemler kurulduktan sonra gerçekleştirilmesi gereken adımlar olarak değil; en baştan itibaren dikkate alınması gereken bir tasarım bileşeni olarak değerlendirmek gerekir. Birçok güvenlik açığının nedeni, güvenliğin en baştan düşünülmemiş olması ve güvenlik çözümlerinin yama mantığı ile sonradan yapılmasıdır. Güvenlik, sistemlere sonradan eklenebilecek bir bileşen olarak görülmemelidir.

Piyasada standart olarak kullanılan ticari yazılımlardan veya yabancı firmalara yaptırılan yazılımlardan ziyade mümkün olduğu kadar SCADA sistemlerine özel olarak tasarlanmış yazılımların milli imkânlarla geliştirilmesi de bir diğer güvenlik önlemidir. Böylece açıklıkların birçok kişi tarafından bilinip keşfedilmesinin önüne geçilmiş olacaktır. Amaca uygun milli yazılımların kolaylıkla geliştirilebilmesi için kritik altyapıların güvenliği ile ilgili araştırma ve geliştirme faaliyetlerinin başlatılması ve bu faaliyetlerin desteklenmesi gerekir. Siber güvenlik konusunda araştırma ve geliştirme faaliyetlerinin yapılması ve bu faaliyetlerin finanse edilmesi faaliyetlerinin bir devlet politikası olması gerekir. Bir araştırma geliştirme faaliyeti sonucu olarak; ortak kullanılabilecek ve tutarlı bilgiler içeren siber güvenlik kılavuzları hazırlanmalı, standartlara katkı yapılmalı ve iyi pratikler belirlenmelidir.

Güvenlik sertifikası almış yazılım ve donanımların kullanımı da SCADA sistemleri için dikkat edilmesi gereken diğer bir husustur. Bilgi işleyen yazılım ve donanımlar için Ortak Kriterler (Common Criteria) standardı dünyada genel kabul görmüş bir güvenlik değerlendirme ve sertifikalandırma standardıdır.

Bilgi güvenliği ihlallerinin çoğunluğu yetkisiz kullanımdan kaynaklanmaktadır. Sadece yetkili personele işini yapacak kadar sınırlı alanda yetki verilmesi ve bunun profesyonel bir yazılım ile takip edilmesi de güvenliği artıracak diğer bir husustur.

Kritik altyapıyı kontrol eden SCADA sisteminin Internet'e bağlı olmasının gerçekten bir gereksinim olup olmadığı gözden geçirilmelidir. "Internet'e bağlı olmasının getirdiği faydalar, getirdiği risklerden fazla mıdır?", "kritik altyapının Internet'e bağlı olmadığı durumda oluşan maliyet karşılanabilecek bir maliyet midir?" gibi soruların yanıtı aranmalıdır. Bu konuda bir durum analizi ve risk analizi yapılmalıdır.

Kritik altyapının açıklıklarını belirlemek ve gerekli önlem almak için periyodik güvenlik testleri ve tatbikatlar düzenlenmesi diğer kritik bir karşı önlemdir. SCADA sistemlerinin bağımsız kuruluşlar tarafından periyodik olarak test ve denetimden geçirilmesi güvenliği ciddi şekilde artıracaktır.

Son olarak taşınabilir USB depolama cihazları ile ilgili sıkı politikaların uygulanması gerekmektedir. Stuxnet'in sıkı bir şekilde korunan belki de Internet'e bağlı olmayan İran nükleer santralinin SCADA sistemlerine USB depolama cihazı yardımı bulaşmış olma ihtimali yüksektir. Personel, evindeki Internet'e bağlı bilgisayarında kullandığı USB depolama cihazını nükleer santral kontrol bilgisayarlarında da kullanmış olabilir. SCADA sistemlerinde kurumsal kriptografik yazılımlardan güvenlik duvarlarına, saldırı önleme sistemlerinden biyometrik güvenliğe kadar birçok karşı önlem kullanıyor olsa da en zayıf halka prensibi bilgisayar güvenliğinde de karşımıza çıkmaktadır. En zayıf halka insandır ve sistemlerin güvenlik seviyesi insanların bilinç seviyesi kadar olmaktadır. Sistem kullanıcılarının ve teknik sistem yöneticilerinin bilerek veya bilmeden yaptıkları basit hatalarla birçok karmaşık güvenlik önleminin pratikte bir faydası kalmamaktadır. Bilgisayar ağının önüne ne kadar güvenlik duvarı, saldırı önleme sistemi konulsa da, SCADA sistemini kullanan bir operatör evinde kullandığı bir USB depolama cihazını SCADA bilgisayarına takarsa o sistemi tehditlere açık hale getiriyor demektir. Gerçekten de USB depolama cihazları zararlı yazılımların bulaşmasında çok büyük pay sahibidir. Çünkü bu cihazlar, hemen hemen herkes tarafından kullanılmaktadır. Bu cihazlar yardımı ile farklı güvenlik seviyesindeki iki bilgi sistemi arasında veri taşıma oldukça pratikleşmiştir.

5. Sonuç

Önümüzdeki zaman diliminde Stuxnet benzeri kritik altyapıları hedef alan siber silahlar üretilecektir. Stuxnet bir başlangıçtı ve devamı gelecektir. SCADA sistemlerine yönelik siber saldırılarda ve servis dışı bırakma girişimlerinde artış olması da olasıdır. Bu siber ataklara, gizlice, açıkça veya dolaylı olarak hükümetler sponsor olacaklardır. Eğer bir devletin veya hükümetin siber yeteneği yeterli değilse, yetenekli bilgisayar korsanları para karşılığı çalıştırılacaktır. Bu "outsource" faaliyeti günümüzde yapılmaya başlanmıştır, daha da yaygınlaşacaktır. Ayrıca, geçtiğimiz aylarda Türkiye gündemine giren "anonymous" gibi hacker gruplarının sayısı ve faaliyetleri önümüzdeki zaman diliminde artacaktır. Din, dil, millet farkı olmaksızın belli bir amaç ve ülkü doğrultusuna ve para almaksızın toplu bir siber taarruz içerisinde bulunmak prestijli bir durum ve bir gençlik başkaldırısı olarak da görülmektedir.

Bütün bu gelecek öngörülerini makalenin ikinci bölümünde yer verilen yaşanmış örneklerle yan yana koyduğumuz zaman gelecek adına kaygılanmamak elde değildir. Eğer yeterli önlemler alınmazsa gelecekte siber saldırıların ciddi sonuçlar doğurması kaçınılmazdır. Makalenin üçüncü bölümünde de ifade edildiği gibi ülkemizde kritik altyapılar belirlenmesi ve güvenliği konusunda hâlihazırda bir

çalışma yoktur. Siber tehditler, kritik altyapıları ciddi şekilde etkileyecek bir boyuta gelmiştir. Bu nedenle, makalenin dördüncü bölümündeki karşı önlemlerin hayata geçirilmesi önem arz etmektedir.

Kaynakça

[1] Executive Order EO 13010, Critical Infrastructure Protection, http://www.fas.org/irp/offdocs/eo13010.htm, 1996 (10 Ağustos 2011'de erişildi)

[2] The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, 1997

[3] USA Presidential Decision Directive/NCS-63, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, 1998 (10 Ağustos 2011'de erişildi)

[4] Jones A., "Critical Infrastructure Protection", Computer Fraud & Security, s. 11-15, 2007

[5] Fischer W., Lepperhoff N., "Can Critical Infrastructure rely on the Internet", Computers & Security, Cilt. 24, s. 485-491, 2005

[6] Jayawickrama, W., "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001", Book Chapter: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Cilt 4277/2006, s. 565-574, 2006

[7] Shea D. A., "Report for Congress, Critical Infrastructure: Control Systems and the Terrorist Threat", 2003

[8] Lemos R., "SCADA System Makers Pushed Toward Security". SecurityFocus. http://www.securityfocus.com/news/11402, 2006 (10 Ağustos 2011'de erişildi)

[9] Maynor D., Graham R., "SCADA Security and Terrorism: We're Not Crying Wolf", Blackhat Conference, http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf, 2006 (10 Ağustos 2011'de erişildi)

[10] Andersson G., Donalek P., Farmer R., Hatziargyriou N., Kamwa I., Kundur P., Martins N., Paserba J., Pourbeik P., Sanchez-Gasca J., Schulz R., Stankovic A., Taylor C., Vittal, V., "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance", IEEE Transactions on Power Systems, Cilt. 20, No. 4, s. 1922-1928, 2005

[11] Chen T. M., "Stuxnet, the Real Start of Cyber Warfare?", IEEE Network, The Magazine of Global Internetworking, Cilt 24, No. 6, s. 2-3, 2010

[12] OECD, Working Party on Information Security and Privacy, "Recommendations of the Council on the Protection of Critical Information Infrastructures", 2008

[13] Commission of the European Communities, "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience- COM(2009) 149 final", 2009

[14] G8 Principles for Protecting Critical Information Infrastructures, G8 Justice & Interior Ministers, 2003

[15] OECD, Ministerial Background Report, “Development of Policies for Protection of Critical Information Infrastructures”, 2007

[16] Karabacak B., Özkan S., “Critical Infrastructure Protection Status and Action Items of Turkey”, International Conference on eGovernment Sharing Experiences, eGovShare2009, 8-11 Aralık 2009, Antalya

[17] McDaniel P., McLaughlin S. “Security and Privacy Challenges in the Smart Grid”, IEEE Security & Privacy, Cilt 7, No. 3, s. 75-77, 2009

[18] Watson J., “Co-provision in sustainable energy systems: the case of micro-generation”, Energy Policy, Cilt 23, No. 17, s. 1981-1990, 2004