NÜKLEER SİBER GÜVENLİK

TREND ANALİZİ MAYIS 2018

thinktech
STM Teknolojik Düşünce Merkezi

Seyide DOĞRU

1. GİRİŞ

Türkiye'nin 2023 hedefleri arasında öne çıkan maddelerden biri nükleer santrallere sahip olmaktır. Böylelikle enerji çeşitliliğini artırarak ve dışa bağımlılığı azaltarak artan enerji talebini karşılamak amaçlanmaktadır. Türkiye'nin enerji kaynağı olarak doğalgazda dışa bağımlılığı yüzde 90'ı aşmaktadır. O yüzden Türkiye bugün nükleer güç santrali kurma projelerine hız vermiş bulunuyor.

Nükleer santraller konusunda, siber güvenlik hususu en kritik güvenlik tehditlerinden biri olarak karşımıza çıkmaktadır. Nükleer güvenlik, nükleer malzeme veya tesislere yönelik kötü niyetli eylemlerin tespiti ve önlenmesi için alınması gereken önlemleri içermektedir. Siber saldırı teşebbüsleri, yalnızca bilgisayar virüsleriyle bilgisayar sistemlerine ve verilere yönelik saldırılardan ibaret değildir. NATO'nun Talinn El Kitabı'nda siber saldırı, şahısların yaralanmasına veya ölümüne ya da nesnelerin zarar görmesine veya yok olmasına neden olan siber operasyon olarak tanımlanmaktadır. Bunlar, bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine zarar vermeyi hedefleyen saldırılardır. Özellikle nükleer santrallerde çok sayıda tehlikeye yol açabilen ve karmaşıklığı gün geçtikçe artan bu tür saldırıların engellenmesi ve kontrolsüz biçimde yayılmasının önlenmesi oldukça zordur[1].

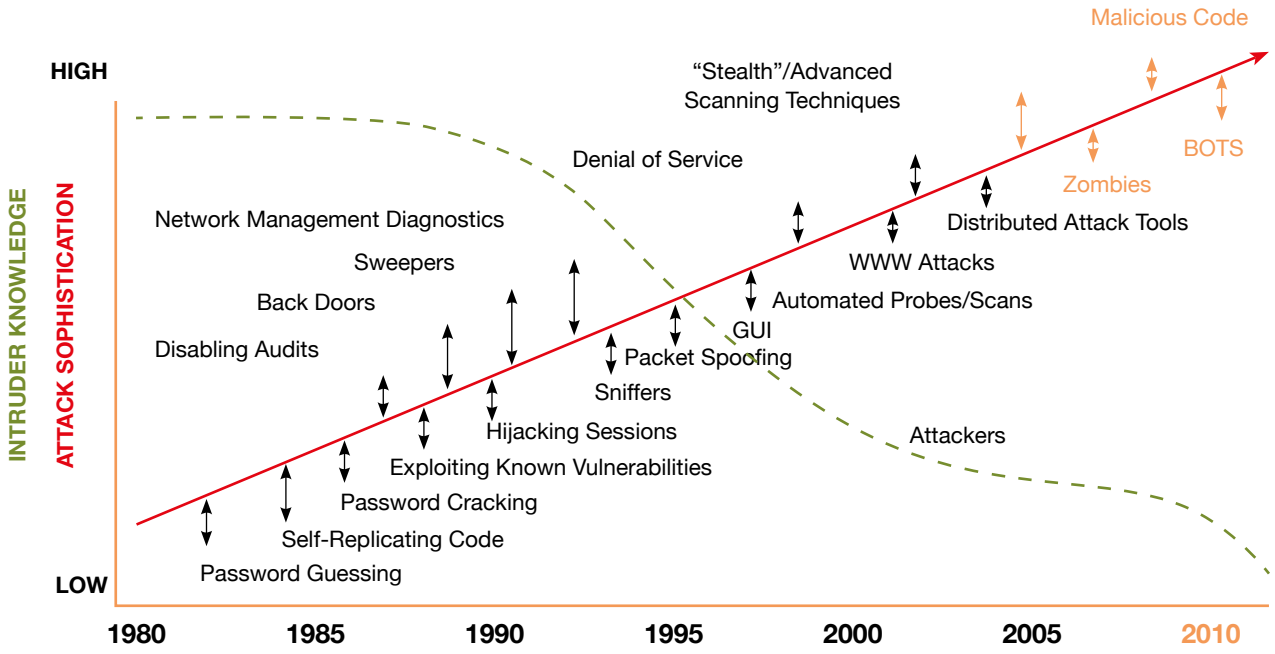
2. NÜKLEER SİBER GÜVENLİK

Şekil 1'de siber saldırıların sayısındaki artış ve bu tip saldırıları gerçekleştirebilmek için gereken bilgi seviyesindeki düşüş gösterilmektedir.

Siber saldırılar, kurum içi saldırılar ve dış saldırılar olarak sınıflandırılabilir. Türkiye'de 2010'dan bugüne kadar gerçekleşen siber saldırıların iç saldırı olduğu bilinmektedir. Ayrıca, iç saldırıların dış saldırılara oranla, söz konusu kuruma yüzde 46 daha fazla maliyet yarattığı ortaya konmuştur. Bu kuruluşlardan yüzde 43'ünün saldırıların içeriden mi yoksa dışarıdan mı kaynaklandığını belirleme yeteneğine sahip olmadığı görülmüştür. Saldırının kurum içi saldırı olması, başarı ihtimalinin artması anlamına geldiği için, tesis içi unsurların oluşturacağı riskler kritik önem taşımaktadır. O nedenle kurumda gelişmiş bir emniyet/güvenlik kültürünün oluşturulması gerekmektedir[1].

Nükleer tesislerin çalışması için gerekli fiziksel altyapıların yanı sıra sağlıklı işleyen bilişim sistemlerine ihtiyaç vardır. Bu tesislerin fiziki güvenliği ile siber güvenliğinin birbirini tamamlayacak şekilde tasarlanması önem arz etmektedir. Ancak günümüzde bir yandan tehditlerin karmaşıklığı ve sayısı geçmişe kıyasla ciddi oranda artarken, bir yandan da her bakımdan bilişim altyapısına bağımlı bir hale gelinmektedir. Bu durum güvenlik açıklarının gittikçe çoğalmasını getirirken bunlara karşı alınacak önlemler sınırlı kalmaktadır.

Siber tehditlerin hedefinde, en başta kritik enerji altyapıları ve enerji şebekeleri bulunmaktadır. 2014 yılında ABD'de yapılan siber saldırıların yaklaşık yüzde 35'inin kritik enerji altyapısını hedef aldığı, bunların yüzde 2'sinin de nükleer tesislere yönelik olduğu düşünüldüğünde, siber güvenliğin ne kadar kritik olduğu gözler önüne serilmektedir. Ancak ekipman üreticilerinin, analog sistem üretiminden dijital sistem üretimine geçmesi ve nükleer enerji santrallerinin bilgisayarla çalışan dijital sistemlere dönüşerek bilişim altyapısına bağımlı hale gelmesi, bu sistemlerin internet üzerindeki iletişimini olağanüstü artırmaktadır. Bu durum siber güvenlik riskini büyütmekte ve santrallerin saldırılara ve çalışanların kasıtlı veya ka-



Şekil 1: Tehditlerin Artan Karmaşıklığı[2]

sıtsız eylemlerine karşı savunmasızlığını artırmaktadır. Bütün bunlar nükleer güvenliğin sağlanmasını daha da zorlaştırmıştır. Bu bağlamda, kritik altyapının korunması için yazılım temelli çeşitli sistemler geliştirilmeye ve kullanılmaya başlanmıştır[1].

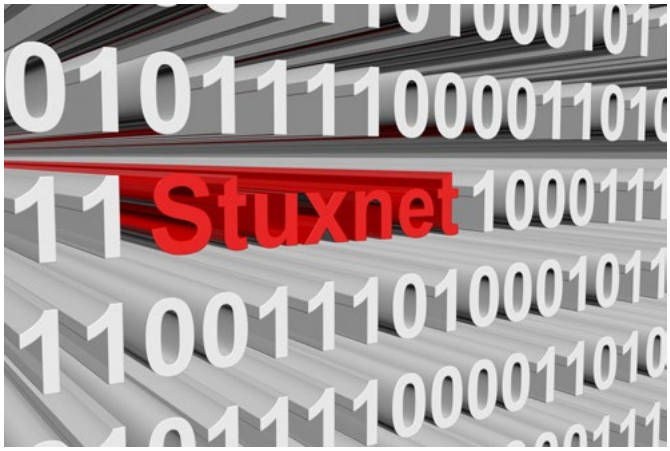
Nükleer altyapı güvenliği ve nükleer güvenlik standardizasyonu konularında faaliyet gösteren kurumların başında Uluslararası Atom Enerjisi Kurumu (IAEA) gelmektedir. IAEA; artan siber saldırı tehdidine karşı, fiziki koruma ve bilgisayar güvenliği önlemlerinin alınmasının nükleer güvenliği sağlamak açısından zorunlu olduğunu vurgulamaktadır. IAEA tarafından nükleer tesislerin siber güvenliği konusunda yayınlanan bir belgede derinlemesine savunma (defence in depth) kavramından yola çıkılmaktadır. Derinlemesine savunma, bilgisayar sistemini tehlikeye düşürecek saldırıları başarısız kılacak ya da engelleyecek, birbirinden bağımsız ve art arda çalışan koruma seviyelerinin birleşimini ifade etmektedir. Eğer bir koruma seviyesi başarısız olursa bir sonraki koruma seviyesi devreye girecektir. Farklı koruma seviyelerinin bağımsız olarak etkinliği derinlemesine savunmanın zorunlu bir gereksinimidir[2].

IAEA ayrıca, nükleer güvenlik kültürüne öncelik verilmesini özellikle vurgulamaktadır. IAEA, güçlü bir güvenlik planının geliştirilmesinin ön şartı olarak kapsamlı bir güvenlik kültürünün oluşturulması gerektiğini belirtmektedir. Böyle bir kültürün şekillenmesinde karar alıcıların, düzenleyicilerin, yöneticilerin, çalışanların ve belli oranda kamuoyunun rolü büyüktür. Nükleer güvenlik kültürünün geliştirilmesi ve yaygınlaştırılması ancak uluslararası bir yönlendirmeyle ve ilgili tüm tarafların farkındalığını sağlamakla mümkündür. Bu nedenle IAEA, bu konuda uluslararası standartlar geliştirmeyi amaçlamakta ve kapsamlı bir nükleer güvenlik yönetimi oluşturulması çağrısı yapmaktadır[1].

Nükleer tesislere yönelik siber saldırılar çok yaygın olmamakla birlikte büyük riskler taşıdığı için; risk yönetiminin tasarım, geliştirme, işletim ve bakım olmak üzere nükleer tesislerin tüm yaşam döngüsü boyunca kapsamlı olarak yürütülmesi gerekmektedir.

Nükleer tesislere yönelik siber saldırılara örnek olarak, 2010 yılında İran'ın Natanz'daki uranyum zenginleştirme tesisine İsrail ve ABD tarafından düzenlendiği iddia edilen saldırı gösterilebilir. Endüstriyel bilgisayar sistemlerine yönelik Stuxnet isimli kötü amaçlı yazılımın kullanıldığı bu saldırı neticesinde tesis zarar görmüştür. İstatistiklere göre zenginleştirme için kullanılan aktif santrifüjlerin sayısı saldırının etkisiyle yüzde 10 azalmış ve IR-1 santrifüjünün hızı 1.064 hertzden 1.410 hertze çıkmıştır. Bu hız santrifüjlerin pervanesinin mekanik olarak dayanabileceği maksimum hıza eşittir[3]. Bu örnekle, ülkelerin nükleer tesisleri korumasının kritikliği daha da belirginleşmektedir. Doğrudan internete bağlı olmayan SCADA sistemlerinin saldırılara karşı tamamen korunduğu inancını boşa çıkaran Stuxnet saldırısı, fiziki altyapının internete bağlı olmamasının tek başına yeterli olmadığını göstermiştir. Nükleer santrallerde çalışanların akıllı telefonları ve tabletleriyle internete devamlı bağlı olmaları, kendi başına siber güvenliğe yönelik önemli bir tehdit oluşturmaktadır[4] [5] Bu gibi olgular teknoloji değişiminin siber ve hibrit tehditlerin her geçen gün geometrik biçimde artmasını getirdiği koşullarda, nükleer güvenliğin sürdürülebilirliğinin nasıl sağlanabileceği konusunu gündeme getirmektedir[6].

Ülkemizde inşa edilecek nükleer santrallerde de benzer risklerin söz konusu olacağı açıktır. O nedenle siber güvenlik ve nükleer güvenlik kültürü kavramlarının, kurum kültürü olarak geliştirilip yaygınlaştırılması için nükleer santrallerin yapımı için seçilen uluslararası ortaklarla



işbirliği içinde hareket edilmesi, kritik önem arz etmektedir. Ancak Akkuyu ve Sinop nükleer güç santrallerinin yapımı için farklı uluslararası ortaklarla anlaşılmış olmasının nükleer güvenlik ve siber güvenlik uygulamaları arasında farklılıklara yol açmaması için Türkiye'nin özel bir dikkat göstermesi gerekecektir. Türkiye, nükleer ve siber güvenlik yaklaşımları farklı olan bu tarafların yaklaşımlarının uyumlulaştırılması sürecinde, kendisine bir yol haritası çizmeli ve yeni girmekte olduğu bu sektörün IAEA standart ve düzenlemeleriyle uyumlu hareket etmesi konusunda elinden geleni yapmalıdır. Bu kapsamda, Türkiye'nin dünyadaki en iyi uygulama örneklerini takip ederek kendi model ve düzenlemelerini oluşturması da sahip olduğu konumu avantaja çevirebilecektir[1].

Siber güvenlik kültürünün öncelikli bir konu haline gelmesi; görece yeni bir gündem başlığı olup, geçmişte birçok nükleer enerji tesisi herhangi bir siber saldırı endişesi taşımadan tasarlanmıştır. Bugün fiziki ve siber güvenliğin yanı sıra, ulaştırma ve depolama güvenliğini de içeren bir nükleer güvenlik kültürünün oluşturulması nükleer enerji tesislerinin korunmasının zeminini hazırlayacaktır[6].

Nükleer enerji santrallerinin tehditlere karşı dayanıklılığını ve işlevselliğini, tasarım özellikleri belirler. İyi tasarlanmış bir sistemin kurulması nükleer güvenliğin sağlanmasının ilk ve önemli bir adımıdır. Dolayısıyla, tasarım aşamasında yapılacak en ufak bir hata, santrali daha baştan siber ve fiziki saldırılara karşı kırılgan hale getirecektir. Nükleer tesislerde kullanılacak donanımın ne olacağı da tasarım aşamasında belirlenir. 2013 yılında bir Rus haber kaynağı, bir teknisyenin Çin'den ithal edilen bir ürünün şarj cihazında "spy chip" bulduğunu iddia etmiştir. Bu devrelerin, 200 metrelik yarıçapa sahip bir alanda korumasız kablosuz ağ kullanan herhangi bir bilgisayara bağlanarak virüs bulaştırdığı iddia edilmektedir[7]. Dolayısıyla, nükleer santrallerin yedek parçalarının güvenilir tedarikçilerden sağlanması ve bu parçaların ilgili tesisteki donanımla uyumunun yerleşik bir doğrulama süreciyle kontrol edilmesi gerekmektedir.

Hackerların ve İleri Düzey Kalıcı Tehdit (Advanced Persistent Threats) saldırganlarının çoğu zaman geri dönüşüme verilen ya da açık artırmayla satılan eski dona-

nımları satın alarak, saldırı için ihtiyaç duydukları bilgileri edindikleri düşünüldüğünde, bu tesislerdeki atık yönetiminin özel güvenlik önlemlerini dikkate alması gerektiği görülür. Güvenlikten çok işlevsellik ve dayanıklılık gözetilerek tasarlanan ısıtma, soğutma ve havalandırma (HVAC) sistemleri gibi sistemler, nükleer enerji santrallerinin en az güvenli unsurlarını oluşturmaktadır. Bu sistemlere, sistemin dışından IP tabanlı uygulamalarla ulaşılabilmekte, yazılımları yükseltilebilmekte ve gerekli yamalar yapılabilmektedir. Bu nedenle, nükleer enerji santrallerinin işletmecileri, HVAC sistemlerinin güvenliğine yönelik önlemleri ihmal etmemeli, her seviyede güvenliğin sağlandığından emin olmalıdır[6].

Nükleer enerji santrallerinde kurum içi tehditler öncelikli zafiyetler olarak değerlendirilmekte, insan kaynağının güvenilirliğinin en sorunlu ve sağlanması en zor parametre olduğu bilinmektedir. Nükleer enerji tesislerinde bir kazanın fark edilmesi veya önlenmesinde, güvenlik zincirinin ilk aşamasını kullanıcılar oluşturur. Bir güvenlik kültürü oluşturulduktan sonra, personelin bu konuda motive edilmesi ve eğitilmesi kritik önem arz etmektedir.

Nükleer tesislerin işletmecileri, farklı güvenlik seviyeleri uygulamaktadır. Nükleer tesislerin güvenlik bölgelerine ayrılması, tesislerin inşası başlamadan önce yerine getirilmesi gereken bir görevdir. Siber güvenlik mimarisinde Seviye 1'den başlayarak ilerleyen seviyeleri öngören farklı yaklaşımlar söz konusudur:

- Seviye 4: Hayati Bölge – Kontrol ve Emniyet Sistemi
- Seviye 3: Korumalı Alan – Bilgi Edinme Ağı
- Seviye 2: Mülkiyet Sahibi Kontrollü Saha – Tesis Yerel Ağı
- Seviye 1: Kurumsal Erişim Alanı – Geniş Ağ Alanı
- Seviye 0: Kamusal Erişime Açık Alan

Güvenlik seviyelerinden, Seviye 4 iletişim özellikleri açısından mutlak koruma altındaki kritik ekipmanlardan oluşan bölgeleri; Seviye 0 düşük seviyeli siber tehditlerin söz konusu olduğu sistemleri içeren güvenlik seviyelerini tanımlamaktadır.

3. SONUÇ VE DEĞERLENDİRMELER

Türkiye'nin, nükleer güç santralleri ve bunların fiziki ve siber güvenliğinin sağlanması konularında sınırlı deneyimi olduğu ortadadır. İstikrarlı bir güvenliğin sağlanmasında temel unsur, güvenlik konseptinin devlet tarafından belirlendiği; kurumsal uygulamalarla ilgili ayrıntılı yazılı düzenlemelerin, ilgili kurumlar tarafından hazırlandığı özenle geliştirilmiş açık bir güvenlik politikasının mevcudiyetidir. Nükleer alanında faaliyet gösteren diğer ülkelerde olduğu gibi, Türkiye için planlanan nükleer güç santrallerinin de siber güvenlikleri açısından ele alınması gereken sorun, bu konuda gerekli kanun ve düzenlemelerin eksikliğidir. Türkiye'de Telekomünikasyon İletişim Başkanlığı bünyesinde faaliyet gösteren bir Siber Olaylara Müdahale Ekibi olmakla birlikte, nükleer santrallerin siber güvenliğinin kritik bir konu olduğu düşünüldüğünde, bunun nükleer sektör için yetersiz olduğu değerlendirilmektedir[6].

Nükleer siber güvenlikte, öncelikli hedef güvenlik durumunu ve olası tehditleri sürekli olarak izlemektir. Bu faaliyet nükleer santrale odaklanmakla birlikte, derin bir istihbaratı ve bir tür veri madenciliğini gerektirmektedir. Türkiye'de Milli İstihbarat Teşkilatı (MİT) ve Emniyet Genel Müdürlüğü (EGM) bünyesindeki istihbarat birimleri tarafından istihbarat amaçlı veriler toplanmaktadır. Bu istihbarat bilgilerinin Akkuyu nükleer güç santralinin gü-

venliğinden sorumlu birimlerle, ne düzeyde ve ne hızda paylaşılacağı sorusu akıllara gelmektedir. Bu nedenle, nükleer santrallerin işletiminden sorumlu yönetim bilgi akışını düzenli ve gerektiği hızda paylaşabilecek bir birimin varlığına ihtiyaç duyabilecektir. Ayrıca, inşa edilecek nükleer güç santralleri ürettikleri elektriği aktarmak için elektrik şebekesiyle de bağlantılı olacaktır. Elektrik şebekesindeki herhangi bir zafiyet veya bu şebekeyi hedef alan herhangi bir siber saldırı, nükleer tesisi de kolaylıkla etkileyebilecektir. Dolayısıyla, Akkuyu ve Sinop nükleer güç santrallerinin bu tür risklere karşı da güçlendirilmesi gerekecektir[6].

Bütün koruma ve güvenlik önlemlerine rağmen, değişen teknoloji ve koşullar yeni saldırı biçimlerini de beraberinde getirmektedir. Dünyada inşa edilmiş ve kullanılmakta olan nükleer güç santrallerinin hiçbirinin siber saldırılara karşı tamamıyla korunduğu söylenemez. Bir yandan İran'a yapılan Stuxnet saldırısının, diğer yandan Rusya'nın Estonya, Gürcistan ve Ukrayna'ya gerçekleştirdiği siber saldırıların ve son olarak Suriye Elektronik Ordusu'nun saldırıları ve IŞİD'in siber ağlara sızma girişimlerinin sonrasında kritik altyapıların korunması hususuna uluslararası platformda daha çok önem verilmeye başlanmıştır. IAEA, bu konuyla ilgili olarak bilgisayar güvenliği için bir yol haritası oluşturmaya ve üyelerini yönlendirmeye çalışmaktadır.

Geleneksel savaşın yerini zamanla aynı yıkıcı etkiyi oluşturacak olan siber savaşların alacağı göz önünde bulundurulduğunda, günümüz tehditlerinin en kritik olanının siber saldırılar olduğu açıktır. Siber saldırılar konusunda gerekli önlemlerin alınmaması ve gerekli savunma sistemlerine sahip olunmaması, günümüzün bu en büyük tehdidinin etkilerini artıracaktır. Nükleer endüstriye ve askeri endüstriyel tesislere düzenlenecek siber saldırıların ülkeler açısından yıkıcı etkilerinin önüne geçilmesi için devletler kendi savunma ve saldırı amaçlı siber güvenlik kapasitelerini geliştirmek zorundadır[6]. Nükleer endüstri güvenlik zafiyetlerinden doğacak hasarı kaldıramayacak kadar kritik bir endüstridir; bu nedenle yatırım maliyetlerinin yarısını güvenlik önlemlerinin oluşturduğu nükleer santrallerde, santral işletmecileri nükleer güvenlik kültürünün kurumsal olarak içselleştirilmesini sağlamak zorundadır.

KAYNAKÇA

[1] EDAM, «Uluslararası Çerçevede Siber Güvenlik ve Enerji».
[2] I. A. E. Agency, «Computer Security at Nuclear Facilities,» 2011.
[3] P. B. C. W. D. Albright, «Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?,» Institute for Science and International Security, 2010.
[4] K. Zetter, «Wired,» 27 Temmuz 2015. Available: https://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/. [Erişildi: 24 Nisan 2018].
[5] K. Zetter, «Wired,» 03 Kasım 2014. Available: https://www.wired.com/2014/11/airhopper-hack/. [Erişildi: 24 Nisan 2018].
[6] EDAM, «Nükleer Tesislerin Siber Güvenliğine Giriş».
[7] BBC, 2013. Available: http://www.bbc.com/news/blogs-news-from-elsewhere-24707337.

thinktech
STM Teknolojik Düşünce Merkezi
http://thinktech.stm.com.tr