thinktech
STM Teknolojik Düşünce Merkezi

Şebeke Saldırılarına Karşı Erken Uyarı Sistemi

2013 yılının Nisan ayında Kaliforniya Silikon Vadisi'ndeki bir trafo merkezine düzenlenen silahlı saldırı uzun araştırmalardan sonra yeni bir araç geliştirilmesine yol açtı. Bu yeni araç, sadece şebeke operatörlerinin uğradığı fiziksel saldırıları değil, aynı zamanda şebekenin kritik bağlantılarındaki saldırıya açık noktaları araştıran hacker'lara dair en ufak bir işareti bile tespit edebilecek.

Kuzey Amerika'daki elektrik şebekesinin bağlantı noktalarını oluşturan binlerce trafo merkezi, enerji santrallerinden iletim hatlarıyla taşınan enerjinin voltajını düşürerek, evlere ve şirketlere enerji ileten yerel dağıtım ağlarına iletir. Bu dağıtım düzenli bir şekilde gerçekleşse bile, birkaç kritik trafo merkezinin devre dışı kalması, tüm bölgeye yayılabilecek, nihayetinde de kentleri felç edebilecek bir kesintiyi tetikleyebilir.

Wall Street Journal, 2014 yılında, Federal Enerji Düzenleme Komisyonunun gizli raporundaki şaşırtıcı bulguları haberleştirmişti: ABD genelindeki 30 trafo merkezi, şebeke operasyonlarında fazlasıyla büyük bir rol oynuyordu. Bunların dokuzunun devre dışı kalması, dalga dalga yayılarak ülkedeki tüm elektrik şebekesini çökertebilecek bir kesintiye yol açabilirdi.

Müfettişler, Pacific Gas&Electric şirketinin Kaliforniya, Coyote'deki, yani Silikon Vadisi'ne ev sahipliği yapan San Jose yakınlarındaki Metcalf trafo merkezine 2013 yılında düzenlenen silahlı saldırının amacının, bu şekilde dalga dalga yayılan bir kesintiye yol açmak olduğundan şüpheleniyordu. Henüz çözülemeyen olayda, saldırganlar merkeze giden fiber optik kabloları kesmiş, ardından da 17 trafoya ateş açarak, toplam 15 milyon dolarlık maddi hasara yol açmıştı. Şirket gerekli onarımları tamamlayana dek, elektriği farklı trafo merkezleri üzerinden dağıtmak zorunda kalmıştı. Düzenlenen silahlı saldırı, saldırganların trafo merkezine, havaya uçurabilecek kadar yaklaştığının göstergesiydi.

Ancak, şebeke operatörleri açısından çok daha kaygı verici olan durum, dünyanın herhangi bir yerinden düzenlenebilecek bir siber saldırı olasılığı. Aslında sadece operatörler değil, ABD halkı da şebekeye yönelik bir siber saldırıdan çekiniyor. Gerçekleştirilen bir ankete göre, Amerikan halkının yüzde 90'ı devletin elektrik şebekelerini siber saldırılardan koruma konusunda yeterince çalışmadığını düşünüyor[1].

Temelleri 100 yıl öncesine dayanan günümüz elektrik sistemleri, binlerce santral ve trafo merkezinden, yüz binlerce kilometre iletim hattından, milyonlarca müşteriye hizmet eden ve milyarlarca cihaza

1 http://thehill.com/opinion/energy-environment/379980-us-power-grid-needs-defense-against-looming-cyber-attacks

enerji ileten dağıtım sistemlerinden oluşuyor. Yakın geçmişe kadar seri hatlar üzerinden birbirleri ile iletişime geçen ve manuel yöntemlerle yönetilen bu sistemler, günümüz bilgi teknolojilerinin ve IP altyapılarının bu alana adapte edilmesi ile tüm bilişim teknolojileri risklerini de kendi üzerinde barındırır hale getirdi.

Bu karmaşık "sistemler sistemi" bugüne dek başarıyla hizmet verdi. Ancak altyapıların IP ağları üzerinden haberleşir hale gelmesiyle günümüzde ortaya çıkan güçlükler, sistemin zayıf ve hassas noktalarını ortaya çıkardı. Gizlilik prensibinin, güvenliğin de dayanağı olarak kabul edildiği bu alandaki gelişmeler ile ortaya çıkan yeni atak alanları, IP ağları üzerinden erişim imkânları gibi durumlar güvenliği sıfır seviyelerine kadar çekti. Yaşlanan altyapı, arz ve talepte yaşanan değişkenlikler, iklim değişikliği ve yeni ortaya çıkan atak alanları üzerinde siber saldırılar sistemin kolaylıkla çökme tehlikesini doğurdu[2].

Bugüne dek meydana gelen doğal afetler, böyle bir durumda yaşanabilecekleri gözler önüne sererek, insanların korkmakta ne kadar haklı olduğunu gösteriyor. Örneğin, 2003 yılında ABD'nin kuzeydoğusunda yaşanan kesinti, 50 milyon insanın dört gün boyunca elektriksiz kalmasına yol açmış, ekonomiye 10 milyar dolar zarar vermişti. Porto Riko'da da Maria kasırgasının ardından 400 bin insan altı ay boyunca elektriksiz kalmıştı.

Bir siber saldırı ise çok daha büyük boyutlarda zarara ve yıkıma yol açma riski taşıyor. 2017 yılının Ocak ayında bu konuda bir araştırma yapan ABD Enerji Bakanlığı ve İç Güvenlik Bakanlığı, tüm ABD elektrik sisteminin ele alındığı çalışmada, şebekelere yönelik geniş çaplı bir siber saldırının ülkenin ekonomisine ve ulusal güvenliğine ağır darbe indireceği sonucuna vardı -su, ulaşım, finans, doğal gaz, petrol, iletişim, bilişim sistemleri tamamen elektrik enerjisine bağımlıydı.

The Hill sitesinin haberine göre, daha önce, 2012 yılında Ulusal Araştırma Konseyi tarafından hazırlanan bir rapor da, bir siber saldırının kentleri aylarca karanlıkta bırakabileceğini, sağlık sisteminin çökebileceğini, çok sayıda can kaybı olabileceğini ortaya koymuştu[3].

İşin ekonomik boyutu da tüyler ürpertici. 2015 yılında Londra merkezli Lloyds tarafından yapılan bir araştırmaya göre, ABD'nin kuzeydoğusundaki 50 trafo merkezine yapılacak bir siber saldırı 93 milyon insanı enerjisiz bırakabilir ve 234 milyar dolar ekonomik zarara yol açabilir.

Dünya, siber saldırıların yaratabileceği felaketle 2011 yılında İran'da tanışmıştı. Natanz uranyum zenginleştirme tesisi bilgisayarlarına sızan korsanlar, Stuxnetx adlı virüsle sadece bilgileri çalmamış, tesisteki sistemlerde de arızalara yol açmıştı. Santrifüjdeki vanaları otomatik olarak açan virüs, basıncın artmasına ve hem cihazların hem de zenginleştirme sürecinin zarar görmesine yol açmıştı. Bu siber silah belki İran'ın nükleer silah yapmasını engellemek gibi "iyi niyetli" olarak değerlendirilebilecek bir amaçla kullanılmıştı ancak kötü niyetli insanların elinde neler yapılabileceğini de ortaya çıkarmıştı[4].

Bilgisayar ağlarının ilk kez bir ülkenin altyapısını çökertmek amacıyla kullanılması da -2015 yılının Aralık ayında Ukrayna'nın elektrik şebekesine düzenlenen saldırı- bu kaygıları körüklüyor. Ukrayna'daki saldırıda, hacker'lar enerji dağıtım şirketlerinin 30 trafo merkezini devre dışı bırakmış, 230.000 son kullanıcının altı saat elektriksiz kalmasına yol açmıştı.

2 https://www.energy.gov/policy/initiatives/quadrennial-energy-review-qer/quadrennial-energy-review-second-installment

3 http://thehill.com/opinion/energy-environment/379980-us-power-grid-needs-defense-against-looming-cyber-attacks

4 https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Bu saldırılar iki aşamada gerçekleştiriliyor. Birinci aşamada sistem hakkındaki bilgiler çalınıyor ve sistemin çalışma esasları öğrenilerek hedefe yönelik yapılacak ana saldırının destekleyici unsurları belirleniyor. İkinci aşamada ise elde edilen bu istihbaratın kullanılması ile sistemin tamamen devre dışı bırakılması ve elektriklerin kesilmesi sağlanıyor.

Örneğin, 2015 yılındaki saldırıların öncesinde, 2012-2014 yılları arasında da BlackEnergy 2 ve Havex adlı virüsleri kullanan Ruslar, Ukrayna elektrik şebekesine yönelik öncü saldırılar gerçekleştirmiş, asıl büyük taarruzun hazırlıklarını yapmıştı[5].

ABD istihbaratına göre, Ukrayna'yı siber saldırılar için bir test alanı olarak kullanan Rusya'nın asıl hedefi, ABD'ye yönelik bir siber saldırı. FBI ve İç Güvenlik Bakanlığı yetkililerine göre, Rus hükümeti adına çalıştığı tespit edilen Dragonfly 2.0 adındaki hacker grup, 2015 yılından bu yana ABD enerji santrallerine ve elektrik şebekesini kontrol eden bilgisayar ağlarına yönelik siber saldırılar düzenleme hazırlığında. ABD yönetimi, 2016 başkanlık seçimlerine müdahale etmekle de suçladığı Rusya'ya yönelik yeni yaptırımları yürürlüğe almış durumda[6].

Scientific American sitesinin iddiasına göre, 2017 yılında İrlanda elektrik şebekesi, ABD enerji şirketleri ve bir nükleer santral de muhtemelen Ruslar tarafından gerçekleştirilen siber saldırılardan nasibini aldı[7].

Geçtiğimiz aylarda İngiltere Savunma Bakanı Davin Williamson, Rusya tarafından İngiltere'nin elektrik şebekesine yönelik casusluk faaliyetleri yürütüldüğünü, şebekeye yönelik bir siber saldırının on binlerce kişinin ölümüne yol açabileceğini açıkladı[8].

Kuzey Kore'nin Güney Kore'ye, Çin'in de Tayvan'a sıklıkla benzer saldırılar gerçekleştirdiği de yine iddialar arasında[9].

Bu tehditlerin giderek büyümesinin ve felaket senaryolarının gündeme gelmesinin iki temel nedeni var. Bunların ilki kötü niyetli saldırganların sadece bilgisayar sistemleri ve ağları konusunda değil, sanayi tesislerinin, santrallerin ve şebekelerin yapısı konusunda da daha fazla bilgi sahibi olması. Bu bilgi, yeni ve öngörülemeyen saldırıların kapısını aralıyor. Bir diğer sıkıntı ise, santrallerin ve şebekelerin gelişen teknolojilere paralel olarak giderek bilgisayar sistemlerine daha fazla bağımlı hale gelmesi. Ekonomik nedenlerden dolayı tüm iş, insanlar yerine sistemlere bırakıldı. Yani, bir saldırı gerçekleştiği anda, birçok santral ve şebekede sistemi manuel olarak sürdürme olanağı kalmadı[10].

Şebeke Saldırılarına Karşı Yeni Çözümler

Bu gelişmeleri göz önüne alan ABD Kongresi, 2015 yılında şebekeye yönelik siber saldırılar karşısında alınacak önlemler konusunda Enerji Bakanlığının yetkilerini artırma kararı aldı. Şebekedeki açıkların ve zayıf noktaların devlet desteğiyle güçlendirilmesine yönelik de yasa tasarıları gündeme geldi. Alınacak önlemler çerçevesinde enerji şirketleri de 2020 yılına dek siber güvenlik önlemlerini artırmak amacıyla 7 milyar dolar tutarında yatırım yapacak. Alınacak önlemlerin yeterli görülmediği

5 https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/
6 https://edition.cnn.com/2018/03/15/politics/dhs-fbi-russia-power-grid/index.html
7 https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/
8 https://www.telegraph.co.uk/news/2018/03/17/britain-four-meals-away-anarchy-cyber-attack-takes-power-grid/
9 https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/
10 https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/

durumlarda eyalet yönetimleri ve federal hükümet, şirketleri gerekli önlemleri almaya zorlayabilecek[11].

Siber Saldırılara Karşı Teknoloji

IEEE Spectrum'da yayınlanan David C Wagman imzalı bir habere göre bu tür saldırılarla mücadele amacıyla çalışmalar yürüten ABD Enerji Bakanlığına bağlı Lawrence Berkeley Ulusal Laboratuvarı uzmanları, bu yılın başında enerji dağıtım merkezlerindeki siber saldırıları ve fiziksel saldırıları tespit edebilen bir proje üzerindeki çalışmalarını tamamladı[12].

UC Berkeley öncülüğünde yürütülen ve Enerji Bakanlığı ARPA-E programı tarafından finanse edilen bir proje çerçevesinde Power Standards Laboratuvarı'nda geliştirilen mikro fazör ölçüm birimleri, enerji dağıtım şebekelerinin durumsal farkındalığını artırma amacı taşıyor.

Üç yıllık çalışma sonucunda geliştirilen araç, mikro fazör ölçüm birimleri kullanarak, enerji dağıtım şebekesinin durumu hakkında bilgi topluyor. Bu verilerin SCADA (veri tabanlı kontrol ve gözetleme sistemi) verileriyle bir araya getirilmesi ile sistemin performansına dair gerçek zamanlı bilgi sağlıyor ve operatörleri en ufak bir değişiklikte bile uyarıyor.

Şebeke operatörleri, sistemin sağlığının temel göstergesi olarak değerlendirilen frekans ölçümlerine bakar -Kuzey Amerika'da 60 hertz, Avrupa'da 50 hertz. Senkrofazör adı verilen araçlar, elektrikte bulunan sinüs dalgalarının büyüklüğünü ve faz açısını ölçerek operatörlerin frekansı takip etmesine yardımcı olur. Senkrofazörler, dalga büyüklüğü verilerini, dünyadaki elektrik şebekelerinde yaygın olarak kullanılan SCADA sistemlerinden daha hızlı hesaplar. Trafo merkezleri benzeri tesislere kurulacak senkrofazörler, frekansı takip edebilir ve sistemdeki, ilgilenilmesi gereken anormallikler konusunda operatörleri uyarabilir.

Berkeley Laboratuvarı Bilgisayarlı Araştırma Bölümünde görevli bilgisayar uzmanı Sean Peisert, laboratuvarda geliştirilen tehdit tespit uygulamasının, güvenlik mühendisliğiyle bilgisayar güvenliğini bir araya getirdiğini söylüyor. Sean Peisert; Arizona Devlet Üniversitesi, senkrofazörün öncüsü Power Standards Laboratuvarı, Elektrik Enerjisi Araştırma Enstitüsü, yazılım tedarikçisi OSISoft ve dağıtım şirketleri Riverside Public Utilities ile Southern Company uzmanlarıyla birlikte araştırmalara öncülük eden ekipte yer alıyor.

OSİSoft'un Müşteri İnovasyonu ve Akademik Çalışmalar Direktörü John Matranga, laboratuvarda gerçekleştirilen bu evliliğin büyük önem taşıdığını söylüyor[12]: "Sean, verinin şebekenin siber güvenlik durumunu belirleme açısından kritik bir unsur olduğu fikrini ortaya attı." Şebeke operatörleri, kontrol sisteminden elde edilen somut verileri şebekenin nasıl çalışması gerektiğine dair temel fiziksel ilkelerle karşılaştırarak, şüpheli bir durumun söz konusu olup olmadığını ortaya çıkarabiliyor.

Örneğin, 2015 yılında Ukrayna'da gerçekleştirilen saldırıyı araştıran uzmanlar, saldırganlardan birinin ya da birkaçının, ekipman kontrol fonksiyonlarına sızarak, gizlice saldırıya açık noktaları araştırdığını ortaya çıkardı. Bu sızma eylemi, trafo merkezi saldırılarından aylar önce gerçekleşmişti. Berkeley Laboratuvarı üst düzey Bilimsel Mühendislik görevlisi Ciaran Roberts, bu tür "keşif saldırıları"nın, eşik ayarları gibi küçük değişiklikler yaparak gerçekleştirildiğini söylüyor. Bu tür bir yoklama tehdidine karşı koyabilmek için, makine öğrenmesini kullanarak sistemin uzun vadeli nominal operasyon modunu gerçek zamanlı SCADA verileriyle karşılaştıran yeni tespit araçları kullanılıyor[12].

11 https://www.forbes.com/sites/constancedouris/2018/02/06/cyber-assault-on-electric-grid-could-make-u-s-feel-like-post-hurricane-puerto-rico/2/#45f311ad405e

12 https://spectrum.ieee.org/energywise/energy/the-smarter-grid/cyber-defense-tool-targets-grid-vulnerability

Uzmanlar, bu amaçla, 1954 yılında geliştirilen CUSUM adlı algoritmayı, günümüzdeki makine öğrenmesi ihtiyaçlarına uyarladı. Bu sayede beklenmedik davranışlar anında ortaya çıkıyor; operasyon sistemi mühendisleri bilişim teknolojisi ortaklarını devreye sokarak, neler olup bittiğini öğrenebiliyor[13].

OSISoft'un Güvenlik Şefi Bryan Owen, şebekeleri güçlendirme çalışmalarının 11 Eylül saldırısı sonrası başladığını söylüyor. Çalışmalar kapsamında, ilk aşamada, Federal Enerji Düzenleme Komisyonu ve şebekenin genel durumundan sorumlu olan Kuzey Amerika Elektrik Güvenliği Kurumunun kuralları çerçevesinde kontrol merkezlerine ve enerji santrallerine odaklanıldı. Owen, Metcalf saldırısının ardından güvenlik önlemlerinin kapsamının genişletildiğini söylüyor.

Bu alandaki bir diğer çalışma da ABD Savunma Bakanlığı İleri Araştırma Projeleri Dairesi (DARPA) finansmanıyla, savunma şirketi Raytheon tarafından gerçekleştiriliyor. Raytheon'un geliştirdiği sistem, siber saldırıları henüz gerçekleşmeden tespit ederek yetkilileri uyarabiliyor. Proaktif Tehdit Avcısı adlı sistem, sürekli bir şekilde bilgisayar ağlarını ve veritabanlarını tarayarak analiz ediyor ve geliştirilen algoritma çerçevesinde olası tehditleri tespit ediyor[14].

Güneş Panelleri de Yakın Takipte

Endüstri 4.0 ile beraber verimlilik, yapay zekâ, otomasyon gibi kavramlar enerji sektörüne uyarlandı ve çevresel faktörlerin etkisiyle yenilenebilir enerji kaynaklarının sisteme dahil edilmesi durumu söz konusu oldu. Bu yapılar akıllı şebekeler denilen, IP altyapılarını yoğunlukla kullanan, büyük oranda yenilenebilir enerji sistemlerinden oluşan sistemlerdir. Bu yapılar ile kullanıcı kendi üretimini kendi yapabilir, hatta fazlasını sisteme dahil ederek bundan gelir elde edebilir. Bütün olarak değerlendirildiğinde verimli ama bir o kadar da saldırı ortamı geniş olan yapılardır. Bu kapsamda Berkeley Laboratuvarı ekibi, çalışmalarını trafo merkezlerinin ötesinde taşıyarak, çatılardaki güneş panelleri benzeri üretim kaynaklarını da kapsayacak şekilde genişletiyor. Binlerce güneş panelinin ve bu panellerin elektronik ekipmanlarının, hacker'ları invertörlere erişerek, bölgedeki şebekeyi çökertmeye teşvik edebileceğinden çekiniliyor. Böyle bir sızma, bir ekipman tedarikçisinin sürdüğü yazılım güncellemesi aracılığıyla bile gerçekleştirilebilir.

Sektörün ve devletin güneş invertörlerinin şebekeyle iletişimi konusunda standartlar geliştirme çalışmaları, bir saldırı olasılığını daha da artırıyor. Projeyi duyuran Berkeley Laboratuvarı araştırmacısı Daniel Arnold, bu standartlaştırma çalışmalarının, şebekeyi saldırılara açık hale getirebileceğini söylüyor.

Berkeley Laboratuvarı, güneş paneli invertörlerine yönelik saldırıları önlemek amacıyla, kötü amaçlı yazılımları etkisiz hale getiren algoritmalar geliştirme çalışmaları yürütüyor -gürültü önleyici kulaklıklara benzer bir sistem. Mart ayında başlayan, üç yıl sürecek olan 2,5 milyon dolar bütçeli proje, Ulusal Kırsal Elektrik Kooperatifleri Birliği ve Sacramento Belediyesi Elektrik İdaresi işbirliğiyle gerçekleştiriliyor.

13 https://www.techrepublic.com/article/power-grid-cybersecurity-tool-uses-machine-learning-and-sensors-to-detect-threats/

14 https://www.raytheon.com/cyber/rtnwcm/groups/iis/documents/content/proactive-hunting-datasheet.pdf