Enerji Altyapılarının Siber Güvenliği

Barış Sanlı, barissanli2@gmail.com

Not: Söz konusu yazıdaki görüşler, yazarın kendi görüşleri olup, adının birlikte anıldığı kurumlarla ilişkilendirilemezler. Ayrıca yazar bir siber güvenlik uzmanı değildir.

Dünyada eşi olan hiçbir yazılım ve donanım sistemi yoktur ki, herhangi bir şekilde bir güvenlik riski barındırmasın. Birler ve sıfırlar üzerine kurulu olan sistemlerin sanal işleyiş düzleminde, bir sistemin planlanan akışını değiştirmek sadece bir başka bir ve sıfırlar serisine bağlıdır. Bu seriler bir başka bilgisayar veya yazılımla üretilip söz konusu sisteme taşınabildiği sürece de bu sistemler risk altındadır.

Bu sanallığın ise fiziksel bir yansımasının olması ise ayrı bir problemdir. Yanı sayısal bir sürecin fiziksel bir etkisi olmaz ise düşük tehdit kategorisi iken, fiziksel bir etkisinin olması özellikle enerji sektöründe önemli bir problemdir. Bu makalede, somut örnekler üzerinden enerji altyapılarını bekleyen tehditler ve olası önlemler tartışılacaktır.

Giriş – SCADA ve Açılıp Kapanan Pompalar

8 Kasım 2011'de Springfield Illinois'te şehrin SCADA (Supervisory Control and Data Acquisition System) sistemine giren bilgisayar korsanlarının, pompa sistemini sürekli açıp kapayarak yaktıkları raporlandı. Hackerlerin sisteme Eylül ayında girmiş olduklarının tahmin edildiği belirtildi. Saldırganların Rusya'daki bir IP adresi üzerinden sisteme eriştikleri görülmüş olmakla birlikte, daha da vahim olanı, sisteme girişin SCADA sisteminin üreticisinin ağı üzerinden yapılmış olmasıdır.

Pek çok insan farkında olmasa da, aslında modern hayatımızın önemli hizmetlerinin arkasında SCADA veya daha geniş tanımıyla Endüstriyel Kontrol Sistemleri(EKS) bulunmaktadır. Mesela, ulaşım altyapı sistemlerinden, su, elektrik, haberleşme altyapılarına kadar bir çok hizmetin sağlanmasında bu yapılar büyük öneme haizdir. Bu sistemler özel sistemler olduğu için, genellikle bu sistemleri kuran firmalar kurdukları sistemlere uzaktan erişim sistemleri kurmakta ve zaman zaman bu sistemlerden performans ve iyileştirme amaçlı bilgi toplamakta, yazılım güncellemektedirler.

Illinois'te gerçekleşen olay gerçekten korkutucu bir olaydır. Olayın başlangıcı SCADA sistemini kuran firmadan elde edilen veri üzerinden gerçekleşmiş gibi gözüküyor. Misal olarak, bir yazılımcının bu firmanın ana merkezini bulup buradan dünyada işletmede olan diğer sistemlerle haberleşmesini gözlemlemesi, sonra topladığı bilgiler üzerinden sistemlere saldırması çok da imkansız bir yöntem değildir. Bunun nispeten kolay bir çaresi var, EKS sistemlerini internete kapatarak, güncellemeler esnasında kısa bir süre sistemi açık tutarak iki taraftan birden operasyonun gözlemlenmesidir.

Petrol Sistemlerine Siber Saldırı

2012 yılı Nisan ayında İran, Kharg adası ve diğer petrol tesistelerini internetten çekmek zorunda kaldı. Aynı zamanda İran Petrol Bakanlığının ve Ulusal Petrol Şirketinin de websitelerine bir süre erişilemedi. Kharg adası, İran'ın ana ham petrol ithalat noktalarından olduğu için stratejik bir öneme sahiptir. Söz konusu saldırının planlanış biçimi aslında bildiğimiz bilgisayar korsanlarının boyunu biraz aşıyordu.

2011 yılında İran'da Duku'ya yapılan bir başka siber saldırıda, 2012 saldırısı için bilgi toplandığı yetkililer tarafından iddia edilmektedir. Aslında bu da bize, saldıranların heyecan değil, bir metodoloji ve strateji ile saldırıyı planladıklarını anlatıyor.

Yapılan saldırıda, edinilen bilgilere göre ciddi bir sorun yaşanmamakla birlikte petrol bakanlığının kendi medya ağı, bazı verilerin etkilendiğini fakat major bir sorun yaşanmadığını belirtti. Aynı şekilde Petrol Bakanlığındaki Sivil Savunma Başkanı Hamdullah Mohammednejad ise İranlı yetkililerin bir kriz grubu kurarak, saldırıyı etkisiz hale getirmeye çalıştıklarını belirtti.

Söz konusu saldırıya karşı ne yapılması gerektiğinin basit bir cevabı yok, çünkü sistemler kompleksleştikçe bir sorunu saptamak veya bir açığı yakalamak daha fazla zaman almaktadır. Kritik enerji altyapılarını internetten uzak tutmak riski azaltan en önemli unsurdur.

Fakat İran söz konusu saldırıdan çok şey öğrenmiş olabilir. Bu görüş de olaydan 6 ay sonra yayınlanan bir makalede The New York Times'a ait ve makalenin başlığı “Suudi Şirketine Saldırıda, Amerikaya göre İran Karşı Saldırıya Geçti”. Bu makalede, bilgisayar korsanlarının, dünyanın en değerli şirketlerinden olan ve dünya petrol üretiminin %10'unu yapan Saudi Aramco şirketine, hem de o şirkete en büyük zararı verebilecekleri günde, saldırdıkları anlatılıyor. 15 Ağustos'ta, 55000 Saudi Aramco şirketinin çalışanı Kadir Gecesini kutlamak üzere evlerinde kaldılar. Ertesi sabah saat 11:08'te ise şirketin bilgisayarlarına ayrıcalıklı erişim hakkı olan birileri tarafından sistem ağına virüs bırakıldı. Raporlara göre, virus Aramco bilgisayarlarındaki verilerin 3/4'ünü sildi ve bu dosyaların yerine yanan Amerikan Bayrağı bıraktı. Kendilerine “Adaletin Keskin Kılıcı” adını veren aktivistlerin, Shamoon adı verilen virüs ile önce mevcut bilgisayarlardaki verileri silerek değiştirdikleri ve bu bilgisayarların adreslerini de merkezdeki bir bilgisayara bildirdikleri anlaşıldı.

Bu saldırının Nisan'daki saldırının karşı atağı olduğu ise sonra ortaya çıktı. Daha da ilginç olan ise virusün internetten değil, içerdeki bir çalışan tarafından USB bellek ile, hem de muhtemelen yönetici erişimi olan biri tarafından bulaştırılmasıdır.

Bu tip durumlarda tüm USB sistemlerinin canlı izlenebiliyor olması bile sistemi saldırıdan korumamakla birlikte, saldırganları daha hızlı yakalama imkanı sunacaktır. Bu da siber saldırıların sayısal dizinler haricinde personel politikası ve bilinçlendirilmesi ile de ilgili olduğunu gösteriyor. Bu saldırıda alınan bir diğer ders de, EKS sistemlerinin kurumsal bilişim ağından ayrı olmasının sağladığı faydadır. Saudi Aramco örneğinde virüs petrol kontrol sistemine büyük çapta etki yapmamış ve sadece kurumsal ağda sınırlı kalmıştır.

Bulut bilişim sistemlerinde ise söz konusu saldırıların etkisi ayrı bir tartışma konusudur.

Nükleer Tesislere Saldırılar

Yine The New York Times'da yayınlanan bir başka makaleye göre, ABD Başkanı Barack Obama, göreve geldiği ilk aylarda, İran'ın nükleer tesislerine saldırıların arttırılması talimatını verdiği iddia edilmektedir. Pek çok kişinin bildiğinin aksine, İran nükleer tesislerine bir değil birden çok saldırı yapılmıştır. Natanz tesisi en az iki defa saldırıya uğramıştır. Aynı şekilde uranyum zenginleştirmesi için kullanılan 5000 santrifuj ünitesinin

1000 tanesi devre dışı kalmıştır.

Bu saldırılarda başrol oynayan virüs ise bilgisayar tarihinde Flame ile birlikte en bilinen virüslerden biri olarak yerini alan Stuxnet virüsüdür. Stuxnet aslında virüs nesilleri arasında özel bir yere sahiptir. Tahmini olarak Haziran 2009'dan önce aktif olan virüs, Haziran 2010'da VirusBlokAda tarafından tespit edildi. Tespit edildiği tarihe kadar Iran, Endonezya ve Hindistan da binlerce bilgisayara bulaştığı tahmin ediliyordu.

Stuxnet bir virus olarak oldukça zekice tasarlanmış bir virüs olarak değerlendiriliyor. Çünkü 3 faz halinde saldırıya geçiyor:
- Faz 1: Sıradan bir worm gibi kendini çoğaltıyor, gizliyor ve güncelliyor, bu arada da etrafına bakıyor. Eğer bu faz esnasında bir Siemens PLC sistemi görür ise faz 2'ye geçiyor.
- Faz 2: Siemens+PLC sistemine saldırıda ise, önce Siemens sistemine bulaştıktan sonra, PLC programını değiştiriyor.
- Faz 3: Sabotaj: Belirli bir tesis kurulumuna bakıyor, eğer uygun kurulumu bulamazsa hiçbir şey yapmıyor. Dolayısıyla sebepsiz yere kendini açık etmiyor.

Sisteme ilk defa USB ile giren Stuxnet, ağ üzerinde USB'ler, printer sunucuları ve ortak klasörler üzerinden yayılıyor. Burada en ilginç olanı ise 4 tane zero-day (yani daha bilinmeyen) açıklığı kullanmış olmasıdır. Aslında virüs yapısı itibari tasarımcıları o kadar çok ihtimali hesaba katmış gözükmektedir ki, bu virüs yapısının bir bilgisayar korsanı felsefesinin ötesinde kombine çoklu ve stratejik bir zeka ürünü olduğu görülmektedir. Ayrıca virüs hedef bir sistem için yazılmış olup, muhtemelen daha önce olduğu gibi bir bilgi toplanma evresinin ardından tasarlanmış olduğu görülmektedir.

EKS Üzerine Bir Değerlendirme

Tüm bunlara bakıldığında, bir değerlendirme, bilgi toplama, strateji belirleme, kodlama, sistemlere bulaşma ve toplanan bilgilere göre kodun uzaktan güncellenmesi, hedefin belirlenmesi ve nihai işlemin gerçekleştirilmesi işlemleri yapılmaktadır. Burada belki dikkat çekilmesi gereken bir diğer nokta ise, bu süreçlerin virüse maruz kalanlar tarafından kolaylıkla kopyalanabilmesi ve yeni karşı tehditlerin oluşturulabilmesidir.

Tüm bu anlattıklarımız EKS sistemleri temelinde gerçekleşen saldırılar oldukları için aslında sıradan kullanıcılara uzak gelebilir. Fakat zaman geçtikçe, bu tip saldırı ve stratejiler kopyalanacak, belki bir istihbarat servisinin işi olan bu saldırılar kısa zamanda bir kaç bilgisayar korsanının da tasarlayabileceği yapılara dönüşecektir.

EKS saldırılarının önemli bir kısmı muhtemelen türünün tek örneği olacağından virüs programlarının ne kadar işe yarayabileceği bir soru işaretidir. Dolayısıyla, sistemi yönetenler bir virüsü beklemekten çok belirli bazı belirtileri bekleyerek sistem anormalliklerinden bu saldırıları tespit etmek zorunda kalacaklardır. Şüphesiz bu tip saldırılara karşı hazırlanmak için en önemli yöntemlerden biri de tatbikatlardır.

ABD Elektrik Şebekesine Saldırı

2013 yılının Kasım ayının ikinci haftasında, California'da neredeyse 10000 elektrik mühendisi, siber güvenlik uzmanı, şirket yöneticileri ve FBI ajanları, 48 saat boyunca ABD elektrik şebekesini kapatmaya çalışan görünmez bir düşmana karşı tatbikat yaptı. Tatbikat boyunca, düşman şebeke kontrol sistemlerine virüs bulaştırarak, trafo sistemlerini hedef

aldı. Tatbikat sonucunda, 100lerce iletim hattı ve trafo zarar gördü veya tahrib edildi. 150 kişi öldü, tabii ki sanal olarak.

Aslında tüm bu egzersizin hem fiziksel, hem insan kaynaklı hem de siber saldırıları bir araya getirmesi oldukça etkileyici olmakla birlikte, bu kadar geniş yoğunluklu bir aktiviteyi yapabilen bir yapı, büyük bir sistemi nasıl çökerteceğini de çözmüş demektir. Bir diğer taraftan da siber saldırılara karşı ne yapacağını bulmaya çalışanlar ile çok daha organize ve detaylı planlarla tatbikat yapanların olması, saldırıların önümüzdeki dönemde nereleri hedef alacağını göstermektedir.

Düşman Kim

Trend Micro tarafından EKS sistemlerine kimlerin saldırdığına dair hazırlanan rapor ilginç sonuçlar ile doludur. Raporda, bal tuzağı olarak kurulan ve su pompa istasyonu gibi tanıtılan iki SCADA makinesine yapılan saldırılar üzerinden sisteme hangi ülkelerden saldırı yapıldığı raporlamaktadır. Sistem internette görülebilir olduktan sonraki 18 saat içinde ilk saldırılar gelmeye başlamış, 28 günde 14 farklı ülkeden 39 saldırı yapılmıştır. Bunlardan 12 tanesi doğrudan hedefe yönelik olarak değerlendirilmiştir. Saldırıların IP'sinin bir ülkeden olması, saldırının illa o ülkeden yapıldığı anlamına gelmemektedir.

Yine de saldırıların önemli bir kısmı, Çin'den (%35), ABD'den (%19) , Lao'dan (%12), İngiltere'den(%8) ve Rusya'dan(%6) yapılmıştır. Diğer taraftan saldırıların cinsi de ülkelere göre değişmektedir. Mesela, bir kısmı zararlı yazılım enjekte etmeye çalışırken, bazıları sistemin işletme değerlerini değiştirmeye çalışmıştır.

Kim saldırıyor sorusunun cevabı ise daha ilginçtir. Aslında siber dünyada düşük yoğunluklu bir savaş olduğu görülmektedir. Bu savaş alanının da geniş bir coğrafyada otomatik kodlar ve yeraltı yapıları ile bir arada yürürtüldüğü düşünülmektedir.

Siber Saldırı ve Nihai Enerji Tüketicisi

Akıllı şebekenin neden bir elektrik sistem sorununa cevap olduğu pek anlaşılmadan, akıllı sayaçlar kurulunca sistemin akıllı olacağı zannedilmektedir. Hatta yazılım verisi üzerine biraz program ile sistemin gerçekten akıllı olacağını zannedenler de vardır. Akıllı şebekeler, aslında bir elektrik mühendisliği sorununa cevaptır, yani merkezi üretim ve nihai tüketim dengesi üzerine tasarlanmış bir sistemde, tüketici üretici olursa sistem nasıl dengelenecektir? Fakat sayaç üreticilerinin bir kısmı “akıllı şebeke”yi bir pazarlama sloganı olarak kullanmaktadır.

Elektrik sistemini bilmeyenler için sistemin anlık olarak, stok yönetimi olmadan milisaniyeler içinde dengelendiğini söylemek faydalı olacaktır. Yani ne üretiliyorsa o anda tüketilmektedir, daha doğrusu, tüketilen elektrik o anda üretilmektedir. Bu da şebekenin frekansının anlık olarak 50 Hertz (salınım) da tutulmasıyla yapılmaktadır. Daha önce iletim sisteminin altını okuyamayan sistem yöneticileri, akıllı sayaçlar ile dağıtım sistemini de okuma imkanını bularak sistemi daha akılcı ve tüketicinin kendi elektriğini üreterek sisteme satmasını sağlayacak şekilde yönetebileceklerdir. Eğer tüketici sisteme elektrik satmayacak ise, şebekenin böyle bir değişime gitmesi şu an için sadece bir maliyet kalemidir.

Akıllı sayaçların ise, sayaçların ortalama 10 sene sistemde kalacağı düşünülür ise, en

kuvvetli sistemlerle donatılsalar da muhtemelen 2-3 sene içerisinde teknolojik gelişimden dolayı hızlıca hacklenebileceği düşünülmektedir. Kaldı ki, ABD ve İngiliz tüketicilerinin bu konuda ciddi çekinceleri vardır. Uzaktan kapatma yapamayan akıllı sayaçlar için ise risk şirketin tarafındadır.

Bir örnek olarak, FBI Siber Güvenlik raporunda yayınlanan bir olay açıklayıcı olacaktır. 2009 yılında Porto Rico'daki bir elektrik dağıtıcısı, FBI'dan akıllı şebeke sisteminin kırılarak gerçekleştirilen elektrik hırsızlığı olayının araştırmasını istemiştir. FBI soruşturması 2010 yılına kadar sürmüştür. Soruşturma sonucunda, sayaç şirketinin ve dağıtım şirketinin eski çalışanlarının para karşılığı akıllı sayaçları kırdığı saptanmıştır. Bu kişilerin konut sayaçları için 300-1000 aldığı, ticarethane sayaçları için ise 3000$ istedği raporda belirtilmiştir.

Bu sayaçları manipule etmek için gereken donanım 400$ civarında internetten elde edilebilirken, yazılım da ücretsiz indirilebiliyor. Diğer taraftan, uygulanan metodların hiçbirinde sayacın açılması, ellenmesi, veya bağlantılarının değiştirilmesi gerekmemektedir. Sayaç üzerinde yapılan uzaktan oynama ile sayacın %50 daha az yazması sağlanırken, ortalama da %50 ile %75'lik bir fatura düşüşü sağladığı görülmektedir. Dağıtım şirketi sayaçların %10'unda bu yöntemle değişiklik yapıldığını farketmiştir.

Görüldüğü üzere içerden bilgi ile sisteme hiç dokunmadan, uzaktan bile sayaç bilgileri manipule edilmektedir. Ama uzaktan kapatma imkanı olan sayaçlarda tüketici için bir risk bulunmaktadır. Bu yüzden kamu güvenliği ve hizmetleri için hassas hiçbir kurumun uzaktan kapatmalı akıllı sayaç (ki uzaktan okumalı sayaç teknik olarak akıllı sayaç olarak nitelendirilemez) kullanmaması tavsiye edilmektedir.

Sonuç Yerine

Belgesel kanallarında yayınlanan “Uçak Kazası” programında çok önemli bir mesaj vardır ki, ülkemiz için de çok önemlidir. Uçak kazasında uçağı yapan firma yetkilileri kazayı detaylıca soruşturduktan sonra, suçlu bulmaktan daha fazla, kazanın sebebi olan eksikliği gidermek veya personelin o eksikliği tekrarlamasını zorlaştırmak üzerine bir işlem değişikliğine giderler. Çünkü bu tip olaylar akla gelmedik binbir şekilde olabilir.

Benzer örnekleme ile enerji altyapı ve sistemlerinde siber saldırıları engellemenin yolu yoktur. Internetten çekseniz, birileri saldırmak istiyor ise içerden bir personelin USB belleğine virüsü yerleştirebilir. Sistem virüsü daha önceden görmediğinden de yayılmasını engelleyemeyecektir. Zaten EKS sistemlerinin internete açık olması olabilecek en büyük zafiyettir. Diğer taraftan özellikle yeni sorunlara verilen yeni cevaplar(Akıllı Şebekeler) gibi, sistemde daha önce akla gelmeyen yeni sorunlara yol açacaktır.

Tüm bunların ortasında, çaresizlik bir çözüm değildir. En önemlisi, bir kurum hiçbir şey yapamıyorsa, piyasada kullanılan ISO 27001 veya 27019 gibi standartları içselleştirmeye çalışabilir. Kurumlar içinden ciddi bir direnç olma ihtimaline rağmen özellikle hassas müşteri bilgilerine haiz kurumlar bunu bir başlangıç olarak görmelidir. Ülkemizde, bu standartlar bankacılık sektörü gibi kritik sektörler için yeterli değildir, bunların üzerine sızma testlerinin yaptırılması sistem açıklarının kapatılması için önemlidir.

Enerji sektöründe gittikçe daha fazla molekül ve elektron, bir ve sıfırlara göre hareket etmektedir. Artan sistem kompleksitesi ile daha tehlikeli olan virüs sistemlerinin arasında,

sistem anormalliklerini doğru izlemek ve raporlamak çok önemlidir. Bu makalede yazdığımız olaylardan öğrenilen bir gerçek vardır ki, hiç bir saldırı üzerinden belirli bir zaman geçmeden farkedilememektedir. Enerji sistemleri için de durum farklı olmayacaktır. Farkedildiğinde ise ekonomik etkilerin en az olması temel hedef olmalıdır.

Referanslar

H(ackers)2O: Attack on City Water Station Destroys Pump, Kim Zetter, 11 Kasım 2011, http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/
Suspected Cyber Attack Hits Iran Oil Industry, Reuters, 23 Nisan 2012, http://www.reuters.com/article/2012/04/23/us-iran-oil-cyber-idUSBRE83M0YX20120423
In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, 23 Ekim 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=2
Obama Order Sped Up Wave of Cyberattacks Against Iran, David E. Sanger, 1 Haziran 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
Stuxnet Explained, Sandro Etalle, TU Eindhoven & Univ of Twente
Attack Ravages Power Grid . (Just a Test), Matthew L. Wald, 14 Kasım 2013, http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html
SCADA honeypots attract swarm of international hackers, John Leyden, 20 Mart 2013, http://www.theregister.co.uk/2013/03/20/scada_honeypot_research/
FBI: Smart Meter Hacks Likely to Spread, 12 Nisan 2012, KrebsonSecurity, http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/