SİBER GÜVENLİK BÜLTENİ

Bilişim ve endüstriyel otomasyon teknolojilerinin kritik enerji altyapılarında yaygın kullanımının bir sonucu olarak bu yapılarda siber güvenliğin sağlanmasına yönelik çalışmalar giderek hız kazanmıştır.

Periyodik olarak yayınlanması planlanan sektör bülteni ile bu alandaki farkındalığa katkı sağlanması amaçlanmaktadır.

Enerji Sektöründe Siber Güvenlik (ESSG) Çalışma Grubu tarafından hazırlanan Siber Güvenlik Bülteninde dünyadan ve ülkemizden güncel siber güvenlik haberlerinin derlenip sunulması planlanmaktadır.

HABERLER

1. Enerji Sektöründe Kritik Araştırma

Bank Info Security sitesinde yer alan habere göre, Massachusetts merkezli CyberX şirketi tarafından 375 kurum üzerinde yapılan bir çalışmada, kurumların sistemlerindeki zayıf noktalar ve zafiyetler araştırıldı.

Çalışma süresince, söz konusu kurumların ağ trafiği incelenerek ağa bağlı cihazlar tespit edildi. Daha sonra derin paket muayenesi ve ağ trafiği analizini ile kurumların %58'inin Modbus kullandığı görüldü. Uzmanlar tarafından Modbus TCP'de çok sayıda güvenlik açığı ve zafiyet bulundu. Bu açıklıkların saldırganlar tarafından istismar edilebileceğini söylendi.

Kurumların %76'sının Windows'un eski versiyonlarını kullandığı da tespit edildi. Microsoft'un güncellenmeyen sistemler için ücretsiz güvenlik desteği sağlamıyor olması kullanıcıları güncelleme konusunda dikkatli olmaya zorlamaktadır. Bununla yanı sıra araştırma, kurumların bilgi teknolojileri bütçesine ilişkin yatırım planları konusunu da öncelikli olarak ele almadığını göstermiştir. Windows'un eski versiyonlarının kullanılmasının EKS için risk teşkil ettiği uzmanlar tarafından ifade edilmiştir. Yapılan araştırmada birkaç noktaya dikkat çekilmektedir.

Söz konusu kurumların neredeyse %60'ı şifrelenmemiş kullanıcı girişi bilgileri kullanıyor ve bu bilgiler ağ içinde serbestçe gezebiliyor. Saldırganların bu şifrelere ulaşmasının çok kolay olduğu değerlendirilmektedir.

Ayrıca kurumların neredeyse yarısı Windows işletim sisteminde antivirüs kullanmıyor. EKS sağlayıcılarının antivirüs kullanımı durumunda garantiyi geçersiz sayması sebebiyle bu programlara rağbet olmuyor. Son olarak kurumların %10'u kötü amaçlı yazılımların vermiş olduğu zarardan habersiz. Bunların içinde WannaCry, NotPetya ve Conficker solucanı gibi neredeyse geniş çaplı etkileri olan saldırılar da var.

Haberin kaynağı için siteyi ziyaret ediniz.

2. ENCS, enerji sektörü için RTBT Siber Güvenlik Eğitimi başlattı

ENCS, Avrupa çapında güvenli kritik enerji şebeke ve altyapı entegrasyonu için çeşitli paydaş grupları ve güvenlik uzmanları ile ortak çalışma yapan bir kuruluştur. ENCS, RTBT ekiplerini kurarak enerji sektöründe siber güvenlik uygulamaları üzerine eğitimlere başladı.

RTBT siber güvenlik eğitimi ile katılımcılar, hacker ve savunma grubu olarak, enerji sektörüne özel tasarlanmış canlı bir saldırı senaryosuna tabi tutulacak. Canlandırma senaryolarının, bu tür tehditlerin nasıl tespit edileceği ve çözüleceği konusunda ihtiyaç duyulan bilginin pekiştirilmesine yardımcı olacağı tahmin ediliyor.

Eğitim kapsamında Gridnet adı verilen bir simülasyon ortamı tasarlanmıştır. Eğitim ortamına orta gerilim devre kesiciler, yönlendiriciler, protokol ağ geçitleri ve koruma röleleri gibi fiziksel yardımcı cihazları yerleştirilmiştir.

Eğitimin ilk iki günü için güvenlik uzmanları tarafından farklı siber saldırı tekniklerine ve çeşitli savunma önlemlerine ilişkin detaylı bilgilendirme yapılması planlanmıştır. Üçüncü gün ise, enerji sektöründen katılımcıların, kırmızı takım ve mavi takım olarak ikiye ayrılması planlanmıştır.

Son gün yapılması planlanan uygulamalı eğitimde kırmızı takım, operasyonel teknoloji risklerine karşı yüksek donanıma sahip Gridnet'i kapatmaya çalışacaktır. Kırmızı takım katılımcıları bilgisayar korsanı gibi düşünmeye zorlanacaktır. Mavi takım ise güvenlik izleme, ihlal tespiti ve olay çözümlemesi üzerinde çalışarak simüle edilmiş bu enerji şebekesini savunmaya çalışacaktır.

Haberin kaynağı için siteyi ziyaret ediniz.

3. Kaspersky Lab EKSler için 2017 yılını değerlendirdi

2017, Endüstriyel sistemlerde bilişim güvenliğinin yoğun olarak gündeme geldiği bir yıl oldu. Güvenlik araştırmacıları tarafından, yüzlerce yeni güvenlik açığı keşfedildi ve raporlandı; EKS ve teknolojik süreçlerde yeni tehdit vektörleri konusunda uyarılar yapıldı; hedefli saldırılar tespit edildi(örneğin, Shamoon 2.0 / StoneDrill). Stuxnetten sonra ilk defa fiziksel sistemleri hedef alan "cyber weapon" adı verilen bir toolset keşfedildi.

Bununla birlikte, 2017 yılında endüstriyel sistemler için en önemli tehdit, şifreleme fidye saldırıları oldu. Kaspersky Lab ICS CERT raporuna göre, yılın ilk yarısında 33 farklı şifreleme yazılımı keşfedildi. Dünyadaki 63 ülkede sayısız saldırı engellendi. WannaCry ve ExPetr'ın yıkıcı ransomware saldırıları, endüstriyel işletmelerinin temel üretim sistemlerini koruma yönelik bakış açısını değiştirmiş görünüyor.

Haberin kaynağı için siteyi ziyaret ediniz.

4. Bad Rabbit Fidye Yazılımı 'EternalRomance' Exploitini Kullanıyor

Cisco's Talos Security Intelligence tarafından yayınlanan yeni bir raporda Bad Rabbit fidye yazılımının EternalRomance exploitini kullandığı ortaya çıktı. Microsoft ve F-Secure de Bad Rabbit fidye yazılımındaki exploitin varlığını doğruladı.

EternalRomance, birbirine bağlı Windows bilgisayarları arasında veri aktarımı için bir protokol olan Microsoft'un Windows Server Message Block (SMB)'undaki bir kusurdan (CVE-2017-0145) yararlanır ve böylece Windows istemcileri ve sunucuları üzerinde uzaktan kod yürütülmesine olanak tanır.

Kendinizi Bad Rabbit'ten korumak için WMI hizmetini devre dışı bırakmanız önerilir. Böylece, kötü amaçlı yazılımın ağınıza yayılmasını önlenir. Ayrıca, sistemlerinizi düzenli olarak güncelleyin ve sisteminizde iyi ve etkili bir antivirüs güvenlik paketi bulundurun.

Haberin kaynağı için siteyi ziyaret ediniz.

ETKİNLİK TAKVİMİ

- 27 Şubat 2018, Brüksel – European Cyber Security Forum (CYBERSEC)
- 27-29 Mart 2018, Abu Dabi - Cyber Security for Energy And Utilities