Siber Tehditler ve Enerji Altyapısının Güvenliği

Aydın KARADEMİR

Özet

Enerji sistemlerin ve birçok alanlarda olduğu gibi sistemsel bağlantı ayarları bulunmaktadır. Ve birçok alanlarda ister fiziksel ister psikolojiksel ve siber güvenliği tehdit eden bir çok dizi izlenmektedir. Tabi ki enerji de siber güvenliği önemli hatta çok zarurî bir noktadır. Artık internetin yani kendi aralarında (bağlantı ayarların) olmadığı bir alan yok. Enerji sistemleri güvenliği de bunun tam merkezinde yer alıyor, ve daima fiziksel tehditleri yanında siber tehditler de almaktadır. Enerji güvenliğinde bir kalkan vazifesi gören gelişmiş son nesil bilgisayarlarla uluslararası enerji sistemini korumaktadır. Bu çalışmanın amacı Siber Tehditler ve Enerji Altyapısını güvenliğini sağlamak amacıyla ortaya koymak. SCADA kritik altyapılarının Siber tehditler ne kadar açık olduğu ve savunma mekanizması ile nasıl siber güvenliğini ortaya koymaktadır. Araştırmada açıklayıcı ve betimleyici tasvirler kullanılmıştır. Bu önemli husus Enerji sistemlerin de enerji güvenliği ve bu tehditleri savuşturmak hayati önem taşımaktadır. Siber tehditlere açık bir şekilde maruz kalınsa devasal maliyetin yanında insan sağlığını tehdit edecek boyuta gelecek. Türkiye'de enerji sektörü; yönetimi ve güvenliği ulusal siber güvenlik testlerinde geçmiş ve ulusal siber güvenlik sertifikasyonu verilmektedir.

Anahtar kelimeler: Siber tehditler, Enerji Sistemlerin de Siber Güvenliği, Ulusal Güvenliği

Abstract

There are system connection settings in energy systems and many other areas. And many series that threaten physical, psychological and cyber security are watched in many areas. Of course, cyber security in energy is an important and even a very necessary point. There is no area where there is no internet, namely (connection settings) among themselves. Energy system security is also at the very center of this, and it always receives cyber threats as well as physical threats. It protects the international energy system with advanced latest generation computers that act as a shield in energy security. The purpose of this study is to reveal Cyber Threats and Energy Infrastructure in order to ensure its security. SCADA reveals how vulnerable critical infrastructures are to cyber threats and how cyber security is with its defense mechanism. Explanatory and descriptive descriptions are used in the research. This important issue is that energy security in energy systems and warding off these threats are of vital importance. If exposed to cyber threats openly, it will reach a level that will threaten human health in addition to huge costs. The energy sector in Turkey; management and security have passed national cyber security tests and national cyber security certification is given

Keywords: Cyber threats, Cyber Security in Energy Systems, National Security

GİRİŞ

Enerji kontrol sistemlerinde verinin güvenli bir şekilde akışının sağlanması, bilgi teknolojilerin önemi çok büyük. Elektrik sayaçların da, doğal gaz depolama kısımların vb. Diğer enerji altarnetiflerde depolama ve dağıtım da BT çok önemli bir misyonu bulunmaktadır. Yaşamın her olay evresinde yaşamın yanında, yaşamı tehdit eden fiziksel ve psikolojik tehditler de bulunmaktadır. Enerji sistemlerin daima tehdit ile yüzleşmektedir; bu kesinti hayatı durma noktasına kadar getirmektedir, enerji sistemlerin BT gelişmesiyle sistem entegre edilmesi siber tehditlerle karşı karşıya getirmektedir. Enerji sistemlerine yönelik siber olaylar, ulusal güvenliği ve ekonomik istikrarı tehdit edebilecek potansiyele sahip ciddi risklerdir. Bu nedenle ülkeler, enerji altyapılarını korumak amacıyla çeşitli siber güvenlik stratejileri ve politikalar geliştirmektedir. İşte bu bağlamda dikkat edilmesi gereken bazı temel noktalar ve stratejiler:

SCADA sistemleri, enerji altyapılarında kritik rol oynamaktadır. Bu sistemler, santraller ve şebeke kontrol merkezleri arasındaki iletişimi sağlar. SCADA sistemlerinin güvenliği için şunlar önemlidir, kullanıcıların güçlü kimlik doğrulama yöntemleriyle sisteme erişmesi sağlanmalıdır. Enerji sistemleri Kriptoloji adı altında yeni bir ana bilim dalının oluşması zaruri bir durum olabilir.

Özellikle stratejik enerji sistemlerin de çalışan personelin erişimin günden güne güncellemesi gerek. Enejinin ileti, depolanma ve dağıtım merkezi olan konuta merkezine şahsî elektronik metallerin koyması sakıncalı bir durum çünkü siber terörizmin algoritmaları günden gelişiyor, farklı casus yazılımları gelişmekte. Buna karşı en önemli anti tez ise donanımlı eğitimli bireyler yetiştirmek. Siber güvenlik alanında çalışan ulusal şirketleri finanse edip yanı zamanda hali hazırda personelleri kendi bünyesinde istihdam etmek. Dijital işletim algoritmaların günden güne gelişmesi ile tehdidi an itibari ile beltaraf etmesi ise yapay zekanın birçok kısımda önemli görevleri var; Siber saldırıların an itibari ile savunmaya geçmesi, Saldırıdan önce bırakacağı hasarı önceden analiz etmesi ve daha sonra ise saldırı dan sonra ise komplike istatiksel hesabı hızlı bir şekilde tesbit edip doğru bir şekilde ilgili uzman ve yöneticilere uyarıda bulunması. Uluslararası ve ulusal siber güvenlik standartlarına uyum, güvenlik seviyesinin korunmasına yardımcı olur. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ve Uluslararası Standardizasyon Organizasyonu (ISO) standartlarına uygun politikalar geliştirilmelidir. Yerel ve uluslararası yasalara ve düzenlemelere uyum sağlanmalıdır. Enerji sektöründe iş birliği ve bilgi paylaşımı, genel siber güvenlik seviyesini artırır. Enerji şirketleri ve devlet kurumları arasında etkin iş birliği mekanizmaları kurulmalıdır. Diğer ülkelerle bilgi paylaşımı ve ortak güvenlik girişimleri oluşturulmalıdır. Olası bir saldırı durumunda sistemlerin hızla toparlanabilmesi için yedekleme ve kurtarma planları kritik önemdedir.Düzenli olarak yedekleme yapılmalı ve bu yedekler güvenli yerlerde saklanmalıdır.Saldırı sonrası hızla toparlanma ve sistemi geri yükleme planları detaylı bir şekilde hazırlanmalıdır. Bu stratejilerin etkin bir şekilde uygulanması, enerji sistemlerinin siber güvenliğini artırarak kritik altyapıların korunmasına yardımcı olabilir. Her zaman güncel

tehditler ve güvenlik önlemleri hakkında bilgi sahibi olmak, bu stratejilerin başarısını devamlı kılacaktır.

Enerji Sistemlerinde Siber Güvenliğin Rolü

Günümüz teknoloji ve dijitalleşme çağında epeyce kritik bir konu haline gelmiştir. Enerji sistemleri, toplumun neredeyse tüm sektörleri için hayati öneme sahiptir. Bu sistemlerin kesintisiz ve güvenilir bir şekilde çalışması, ekonomi, sağlık, ulaşım ve kamu güvenliği gibi birçok alanın düzenli işleyişini doğrudan etkiler. Dolayısıyla, enerji sistemlerinin siber güvenliği üzerine yapılan çalışmalar, bu alandaki riskleri en aza indirgemek ve daha güvenli bir altyapı oluşturmak amacıyla sürekli olarak gelişmektedir. Modern enerji sistemleri, akıllı şebekeler, otomatik kontrol sistemleri ve diğer dijital teknolojiler sayesinde daha verimli ve esnek hale gelmiştir. Ancak bu dijitalleşme, aynı zamanda siber saldırılara karşı daha fazla savunmasızlık anlamına gelir. Özellikle kritik altyapılara yönelik siber saldırılar, enerji arzını kesintiye uğratabilir, mali kayıplara yol açabilir ve hatta ulusal güvenliğe ciddi tehditler oluşturabilir. Birincil siber güvenlik stratejileri, enerji sistemlerinin güvenliği için önleyici tedbirler ve hızlı müdahale mekanizmaları geliştirilmesini içerir. Bu stratejiler, siber tehditlerin tespitini ve analizini kolaylaştıran gelişmiş izleme sistemlerini, güvenlik açıklarını gidermeye yönelik yamaları ve yazılım güncellemelerini ve kullanıcı farkındalığını artırıcı eğitim programlarını kapsamaktadır. Bir diğer önemli konu başlığı, enerji sistemlerinde kullanılan endüstriyel kontrol sistemlerinin (ICS) güvenliğidir. ICS'ler, enerji üretimi ve dağıtımını kontrol eden sistemlerdir ve bu nedenle saldırılara karşı özel bir koruma gerektirir. Günümüzde ICS'ler, geleneksel güvenlik duvarları ve antivirüs yazılımlarının ötesine geçerek, ağ segmentasyonu, çok faktörlü kimlik doğrulama ve gelişmiş tehdit tespit sistemleri gibi daha kapsamlı güvenlik çözümleri ile korunmaktadır. Ayrıca, enerji sektöründeki tüm paydaşların, sürekli olarak değişen ve gelişen siber tehditlere karşı ortak bir mücadele içinde olması gerekmektedir. Bu bağlamda, bilgi paylaşımı ve işbirliği, siber güvenlik alanında daha etkili sonuçlar elde edilmesine yardımcı olur. Örneğin, sektörler arası işbirlikleri, siber tehditlerin daha geniş bir perspektiften ele alınmasını ve hızlı bir şekilde yanıt verilmesini sağlar. Sonuç olarak, güvenlik çalışmaları içerisinde bir yer edinmeye çalışan "enerji güvenliği ve siber güvenlik" güvenlik çalışmaları içerisinde yer edinmiştir. enerji sistemlerinde siber güvenlik, sadece teknik tedbirlerden ibaret değildir. Bu kritik altyapıların korunması, teknik çözümlerle birlikte organizasyonel politika ve prosedürleri, düzenleyici çerçeveleri ve geniş çaplı işbirliklerini de içeren bütüncül bir yaklaşımı gerektirir. Siber güvenlik tehditlerinin sürekli evrildiği günümüzde, enerji sistemlerinin güvenliği için sürdürülebilir ve dinamik bir stratejiye ihtiyaç duyulmaktadır. Bu strateji, etkili risk yönetimi, ileri teknolojiler ve yerleşik güvenlik kültürü ile desteklenmelidir. Son zamanlarda enerji sistemlerinde iletim, dağıtım ve depolama sahasında yaşanan siber tehditler kaçınılmaz bir gerçektir. Yayınlanan raporlara göre 2014 yılında 317 milyon, 2015 yılında ise 431 milyon yeni zararlı yazılım internette dolaşıma verilmiştir (Çiftçi, 2013). Enerji güvenliği ekonomik, toplumsal, siyasi ve jeopolitik risklerin yönetilebilmesi için ana unsur olma özelliğine sahiptir (Lewis, 2002; Özev, 2017). Enerji güvenliği kavramınıifade etmek için enerji ve güvenliğe ağırlık veren iki farklı yaklaşımdan birincisi olan enerjiye olan yaklaşımda enerji kaynaklarının bulunabilirliği, erişilebilirliği ve kabul edilebilirliği kavramlarını içine alırken,

ikinci yaklaşım olan güvenliğe yönelik yaklaşımda ise tesislerin her türlü saldırıya karşı fiziki olarak korunması ağırlık yaklaşımdır (Gençtürk, 2012). Enerji sistemlerinde bir çok farklı alanlarda ifade edilmektedir; siber savunma, siber istihbarat, siber uzay, ki son zamanlarda "siber vatan" kavramı oldukça popüler olmaya çalışılmıştır, siber terörizmin, dijital faşizm vb. Bir çok unsur siber güvenlik ve enerji sistemleri güvenliğine eklenmiştir. Enerji sistemlerinde siber saldırılar, uzay da yer alan enerji üretim tesislerin de üretim esnasında oluşan döngüsel olguda yaşanan frekanslar ve gerilimde sabitliğini ortadan kaldırarak. Yaşanan sorunlar meydana gelir; maddiyat ve can kayıplar meydana gelir. Siber tehditlerin en çok hedef aldığı nokta jeopolitik öneme haiz olan ulusal güvenliğin huzur ve düzeni sağlayan ve milli güç unsur olarak tanımlanan kritik altyapıları; petrol boru hatları, doğal gazın transit geçiş noktaları, nükleer santrallerin ve hiper internet ağı vb. Stratejik noktaları hedef alan siber lejyonerler tarafında daima karşı atağa geçirilir.

Günümüzde SCADA sistemler, nükleer santrallerin sistemlerin hayati önem altyapılar daima siber teröristlerin daima hedef aldığı nokta, teröristlerin ana hedeflerin de bir diğeri ise var olan devlet düzenine karşı hareket etmek. Bunun en büyük örneği militanların sadece kritik enerji altyapı sistemlerine hedef alması değil de bunun yanında kimlik avcılığı, finans, bankacılık ve borsa alanında hedef almaktadır. Kamu yönetiminde halk sağlığı, düzeni ve güvenliğin tehdit eden yelpazesi geniş bir kaç alanda üçüncü kol faaliyeti yapmaktadır. Kimlik avcılığı ile ilgili faaliyet ve alanlarına göre kategorize edilmektedir. Stratejik öneme sahip bir olan geniş alanlarda yayınlan enerji hatları ve nükleer ve atom teknolojileri konusunda çalışan; uzman, mühendis ve teknikerler hakkında bilgi toplamak ve onlar üzerinde yapacak yıldırma, güçsüz bırakma ve önüne geçemeyecek hataları yapmaları için kimlik avcılığı yapmaktadır. Bu sadece sektörde çalışan personellerle sınırlı kalmıyor çevre ve aile fertlerine kadar oluşan bir "kimlik avcılığı haritası" meydana gelmektedir. Enerji sistemlerinde bilgi güvenliği konusunda göz önünde bulundurulması gereken SCADA sistemlerinin bilgi güvenliğidir. Kritik altyapıların yönetiminde, hizmet sağlamak için coğrafi anlamda geniş alana yayılmış sistemdir. Datalara aktarılan verilerin güvenliği de en az gelebilecek tehditlere karşı alınacak önlemler kadar önemli bir durum her an izlenilmeli ve kontrol edilmeli hatta bir ek olarak da denetimi bir zati teknokratlar yapmalı ve güveli bir şekilde SCADA sistemlerini (geniş alanlara yayılan bilişim sistemleri) kullanılmalıdır.

SCADA (Supervisory Control and Data Acquisition) sistemleri, endüstriyel süreçlerin izlenmesi ve kontrolünde kullanılan yazılım ve donanım sistemleridir. Bu sistemler, hem büyük ölçekli endüstriyel operasyonlarda hem de küçük ölçekli tesislerde etkili bir şekilde kullanılabilir. İşte popüler bazı SCADA sistemler nelerdir:

1. Siemens SIMATIC SCADA

- Siemens'in SCADA sistemi, geniş ölçekli endüstriyel uygulamalarda yaygın olarak kullanılır.
- Özellikle otomasyon ve kontrol sistemlerinde öne çıkar.

2. Wonderware InTouch

- Schneider Electric tarafından geliştirilen InTouch, kullanıcı dostu grafik arayüzleri ve güçlü veri analitiği yetenekleriyle tanınır.
- Özellikle üretim ve enerji yönetimi için uygundur.

3.GE Digital iFIX

- General Electric'in SCADA sistemi, esnek ve ölçeklenebilir bir yapıya sahiptir.
- Sağlık hizmetleri, enerji, imalat ve diğer birçok sektörde kullanılır.

4. Rockwell Automation FactoryTalk

- Rockwell Automation'ın SCADA çözümleri, özellikle üretim ve proses sektörlerinde popülerdir.
- Güçlü veri toplama, analiz ve görselleştirme yetenekleri sunar.

5. Ignition by Inductive Automation

- İleri düzeyde esneklik sunan bu açık kaynak SCADA platformu, endüstriyel otomasyon projelerinde kullanılır.
- Web tabanlı ve modüler yapısıyla dikkat çeker.

6. Emerson Ovation

- Özellikle enerji ve su yönetimi gibi kritik altyapı endüstrilerinde kullanılır.
- Yüksek güvenilirlik ve performans sunar.

7. Honeywell Experion PKS

- Petro-kimya, rafineriler ve enerji üretim tesislerinde sıklıkla kullanılır.
- Güçlü entegrasyon yetenekleri ve ileri düzey kontrol sistemleriyle bilinir.

8. Yokogawa CENTUM VP

- Özellikle Asya pazarında yaygın olarak kullanılan bu sistem, yüksek performans ve güvenilirlik sunar.
- Kimya, petrol ve gaz endüstrilerinde tercih edilir.

9. ABB System 800xA

- Geniş entegrasyon olanakları sunan ABB'nin SCADA sistemi, enerji, kimya ve petrol & gaz gibi sektörlerde kullanılır.
- İleri düzey kontrol ve izleme yetenekleri sağlar.

Birçok alanlarda bu tür karmaşık sistemler oluşmaktadır. Coğrafi bilgi sistemleri bunda dahil Türkiye de Monopol işletmelerin en başında gelen elektrik dağıtım şirketleri coğrafik konumlarına göre tanımlamaktadır.

Siber militanlar, birçok kritik altyapıyı hedef alabilir ve bu altyapılar üzerindeki saldırılar, ciddi ekonomik, çevresel ve sosyal etkileri olabilir. İşte siber militanların tehdit edebileceği önemli kritik altyapılar:

1. Enerji Sistemleri:

- Elektrik Şebekeleri:Elektrik dağıtım ve iletim sistemlerinin hedef alınması, geniş kapsamlı elektrik kesintilerine ve ekonomik kayıplara yol açabilir.
- Petrol ve Doğal Gaz Altyapıları: Boru hatları, rafineriler ve depolama tesisleri, enerji arzını kesintiye uğratabilir.

2. Su Temini ve Atık Su Sistemleri:

- Su arıtma tesisleri, pompalar ve dağıtım ağları üzerindeki saldırılar, su kıtlığı ve kirliliğe yol açabilir.

3.Ulaşım Sistemleri

- Demiryolu ve Metro Sistemleri: Ulaşım sistemlerine yönelik saldırılar, ulaşım ağlarında kesintilere ve güvenlik risklerine neden olabilir.
- Havacılık: Hava trafik kontrol sistemlerine saldırı, hava trafiğinde aksamalara yol açabilir.
- Denizcilik:Limanlar, gemiler ve deniz taşımacılığı sistemleri hedef olabilir.

4. Sağlık Sektörü:

- Hastane sistemleri, tıbbi cihazlar ve sağlık veri tabanları üzerindeki saldırılar, hasta bakımı ve sağlık hizmetlerinde kesintilere neden olabilir.

5. Finansal Sistemler:

- Bankalar, borsalar ve ödeme sistemleri üzerindeki saldırılar, finansal işlemlerde kesintilere ve büyük ekonomik kayıplara yol açabilir.

6. Tesis Otomasyonu ve Endüstriyel Kontrol Sistemleri (ICS):

- Üretim tesisleri, kimyasal tesisler ve çeşitli endüstriyel süreçleri kontrol eden sistemlere yönelik saldırılar, üretim süreçlerinde kesintilere ve tehlikeli durumlara neden olabilir.

7. Telekomünikasyon ve Bilgi Teknolojileri

- Telefon hatları, internet hizmeti sağlayıcıları ve uydu iletişim sistemlerine yapılacak saldırılar, geniş çaplı iletişim kesintilerine yol açabilir.

8. Kamu Politikası ve Yönetimi

- Belediye ve devlet hizmetleri (örneğin, acil durum yanıt sistemleri, trafik ve su yönetimi) üzerindeki saldırılar kamu hizmetlerinde ciddi aksamalara neden olabilir.

Bu kritik altyapılar, toplumların günlük işleyişini sağlamak için hayati öneme sahiptir. Siber militanlar bu sistemlere saldırarak büyük ölçüde zarar verebilir ve kamu güvenliğini tehlikeye atabilir. Bu yüzden, bu altyapıların güvenliğini sağlamak için sürekli olarak geliştirilmiş siber güvenlik önlemleri ve savunma stratejileri gereklidir.bunu içersinde en belirgin olan ve ülkemizde yaşanan elektirik kesintileri büyük bir alanı kapsayacak yani bir bölgenin veya ülkenin genelinde yaşanan elektirk kesinti bir siber saldırının örneğidir. Ve saldrıyı gerçekleşen siber suçluları ilgili makamlarca gözaltına alındı. [1] Enerji sistemlerinde, toplumların işleyişinde kritik bir role sahiptir: bu birbağımsızlı meselesi gibi onun için başta türkiye olmak diğer ülkeler bu konuyu milli güvenlik meselesi olarak algılıyor.Ve siber tehditler bu sistemlerde ciddi zararlara yol açabiliyor. Enerji sistemlerinin siber tehditlerden korunması ve savunma mekanizmalarının oluşturulması karmaşık, çok katmanlı ve sürekli güncellenen bir süreçtir.

İşte bu konuda izlenecek bazı temel adımlar:

I. Durum Analizi ve Risk Değerlendirmesi

- Sistemler ve Bileşenler İncelenmeli: Tüm bileşenler, ağlar ve cihazlar düzenli olarak gözden geçirilmeli ve değerlendirilmelidir.
- Tehditlerin Tanımlanması: Potansiyel tehditler ve zayıf noktalar belirlenmelidir. Siber saldırı senaryoları oluşturulmalı ve sistemlerin bu tehditlere karşı nasıl tepki vereceği test edilmelidir.

II. . Güvenliğe Yönelik Politikaların Oluşturulması

- Güvenlik Politikaları ve Standartlar Oluşturma:Siber güvenlik protokolleri ve prosedürleri oluşturulmalı ve güncellenmelidir.
- Yasal ve Yapısal Düzenlemeler:Yasal düzenlemelere uygunluğun sağlanması ve şirket içindeki güvenlik yönetiminin belirlenmesi gereklidir.

III. Ağ Segmentasyonu ve İzolasyon

- Ağ Segmentasyonu:Kritik bileşenler farklı ağlarda segmente edilmeli, bu sayede bir segmentin tehlikeye girmesi diğerlerini etkilememelidir.
- İzole Ağlar: Enerji üretim ve dağıtım ağları, kurumsal IT ağlarından tamamen izole edilmelidir.

IV. Güvenlik Teknolojileri ve Protokoller

- Ağ Güvenliği: Güvenlik duvarları, Intrusion Detection Systems (IDS) ve Intrusion Prevention Systems (IPS) gibi teknolojiler kullanılmalıdır.
- Şifreleme: Veri iletişimi sırasında şifreleme kullanılmalı, özellikle SCADA sistemlerinde güvenlik protokolleri uygulanmalıdır.

V. Sürekli Denetim ve İzleme

- Gerçek Zamanlı İzleme: Kritik sistemlerin ve ağların gerçek zamanlı izlenmesi sağlanmalıdır.
- Siber Güvenlik Analitiği: Anomalilere karşı sürekli analiz ve izleme sistemleri kurulmalıdır.

---

[1] 2015/04/02 https://www.hurriyet.com.tr/ekonomi/elektrik-santrallarina-buyuk-gozalti-28622645 er:07.09.2024

VI. Eğitim ve Farkındalık

- Personel Eğitimi: Çalışanlar ve yönetim sürekli olarak siber güvenlik eğitimleri almalı ve farkındalık durumu yüksek tutulmalıdır.
- Olay Müdahale Durumları: Simülasyonlar ve saldırı tatbikatları düzenlenmeli, böylece personelin olaylara nasıl tepki vereceği pratik edilmelidir.

VII. Yedekleme ve Kurtarma Prosedürleri

- Yedekleme: Kritik sistemlerin ve veri tabanlarının düzenli yedeklemesi yapılmalıdır.
- Kurtarma Planları: Etkili bir veri kurtarma ve iş sürekliliği planı oluşturulmalı ve tatbikatlarla desteklenmelidir.

VIII. İşbirliği ve Bilgi Paylaşımı

- İşbirliği: Diğer enerji firmaları, hükümet organları ve siber güvenlik kurumlarıyla işbirliği yapılmalı ve bilgi paylaşımı sağlanmalıdır.
- Güvenlik Habitleri: Uluslararası güvenlik standartlarına ve sektör spesifik kurallara uyulmalıdır.

Enerji sistemlerinde siber güvenlik, teknolojik gelişmeler ve saldırı yöntemleri doğrultusunda sürekli yenilenmesi ve güçlendirilmesi gereken bir alan olup, bu yönde oluşturulan savunma mekanizmaları sistem güvenilirliğinin sağlanmasında kritik rol oynar.

Türkiye'de Enerji Sistemlerinde Siber Güvenlik

Dünyanın gelişmiş ve gelişmekte olan bütün topluluklarda siber terörizm mi yaşamaktadır. Hizmet sektörüne yönelik daima siber terörstlerin; bankacılık,finans ve jamu hizmetini gerçekleştiren her alanda kamuoyuna sindirme,korkurtma gibi kötü davranışlar sergilemektedir. Enerji sistemleri siber zorbaların hedef odağında çünkü insan hayatının en kritik öneme sahip ve bağımsızlığının bir nişanesi olarak görülmekte onun için siber güvenlik alanında çalışma yürüten kamu kurumlarda ve özel sektörde yaşanan siber tehditleri beltaraf etmektedir. Siber güvenlik alanında çok ciddi mesai yapılmatadır. Seminerler,konferanslar ve eğitimler verilmektedir. Bu çalıştaylarda enerji sistemleri güvenliği başlıca ana konulardan bir tanesi haline gelmektedir. Enerji ile ilgili ulusal ve uluslarası think tanks (düşünce kuruluşlar) ciddi görevler üstlenmektedir.

Sonuç

Enerji sistemlerin de siber tehdit ve güvenliği ele alınan önemli hususlarında "sistem ağı"tehdit edilmektedir. özelikle geniş alanlara ve startejik enerji sistemlerin tehdit etmesi kamu güvenliğini ve sağlığını tehdit etmektedir. Enerji kontrol sistemlerinde verilerin güvenli akışının sağlanması ve bilgi teknolojilerinin rolü gerçekten kritik bir öneme sahiptir. Günümüzde enerji altyapıları ve dağıtım sistemleri, sadece fiziksel güvenlikle değil, siber güvenlikle de korunmalıdır. İşte bu konuyu derinlemesine anlamak ve enerji sistemlerini koruma yöntemleri üzerine bir genel bakış: şifreleme algoritması ile siber tehditleri en asgari

düzeye indirilebilinir SCADA sistemleri ve nükleer reaktörler gibi stratejik öneme sahip enerji sistemlerin güvenliğini koordinasyon kurul tarzında ilgili bakanlık ve güvenlik bürokrasisinde oluşan bir uzman bir ekip ile daima korunmalı, revize etmeli ve en önemlisi personeli teknik ve fiziki anlamda takip edilmesi. Kamu düzeni; sağlığı ve güvenliği için öneme haiz dir. Enerji sistemlerine görevli olan personellerin mesleki kariyerine yönelik eğitimler, seminerler ve konferanslar verilmeli. Özellikle kritik durumlarda ne tür izlenim ve çalışmaları sanal gerçeklik (VR gözlük) ve simülasyon ortamında acil durum müdahale protokolleri nasıl hızlı bir şekilde beltaraf edilmesine dair eğitimlere ağırlık vermeli.

Kaynakça

Enerji Sektöründe Siber Güvenlik. (2021., 07. .25). 09. 30, 2024. tarihinde Kron Teknoloji: https://krontech.com/tr/enerji-sektorunde-siber-guvenlik adresinden alındı

Dr. Selim ÇAPAR, M. K. (, Eylül-Ekim 2017.). "GÜVENLİK VE KRİZ YÖNETİMİ". *İdarecinin Sesi dergisi,*, Sayı: 179.

Enerji Kontrol Sistemlerinde Siber Güvenlik: Tehditler ve Çözümler. (tarih yok). 09. 30., 2024 tarihinde CATO TEKNOLOJİ: https://krontech.com/tr/enerji-sektorunde-siber-guvenlik adresinden alındı

ERGİL Doğu. (tarih yok). "Terörizm Mantığı ve Hedefi".

GEDİK, D. (Haziran(2018)). *"SİBER GÜVENLİK VE TERÖRİZMİN EVRİLİŞİ:TÜRKİYE ÜZERİNE ETKİLERİ.* Düzce : DÜZCE ÜNİVERSİTESİ,SOSYAL BİLİMLER ENSTİTÜSÜ.

Karabacaki, B. (29 Eylül 2011). Kritik Altyapılara Yönelik Siber Tehditler Ve Türkiye için Siber Güvenlik Önerileri. *Siber Güvenik Çalıştayı, Bilg Güvenliği Derneği*, 2-9.