4. Ağ ve Bilgi Güvenliği Sempozyumu

Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği

Mehmet Kara[1] Soner Çelikkol[2]

[1]TÜBİTAK BİLGEM UEKAE, Kocaeli
[2]Kullar Meslek Yüksek Okulu, Kocaeli Üniversitesi, Kocaeli
[1]e-posta: mkara@uekae.tubitak.gov.tr, [2]e-posta: scelikkol@kocaeli.edu.tr

Özetçe

Elektrik üretim ve dağıtım sistemleri ülkedeki önemli kritik altyapılardan biridir. Bu altyapıların daha kolay ve etkin yönetim için büyük ölçüde SCADA sistemleri kullanılmaktadır. Günümüzde SCADA sistemlerinin internet protokollerini yaygın olarak kullanmaya başlaması siber güvenlik tehditlerine varabilecek tehditleri de beraberinde getirmektedir. Çünkü bir ülkenin veya bir bölgenin kısa bir süreliğine bile elektriğinin kesilmesi çok ciddi sonuçlar doğurabilir. Bu makalede SCADA sistemlerinin genel yapısı iletişim protokolleri ele alınmış, enerji iletim ve dağıtım altyapılarında kullanılan SCADA sistemlerinin güvenli çalışması için alınması gereken önlemler vurgulanarak, Türkiye'deki durum irdelenmiştir.

1. Giriş

Kritik altyapılar, bir ülkede ekonomi ve sosyal hayatın sağlıklı bir şekilde işlemesi için ciddi öneme sahip olan fiziksel ve sayısal sistemler olarak tanımlanmıştır. Enerji üretim ve dağıtım sistemleri de önemli kritik altyapıların başında gelmektedir. Geçmiş senelerde, kritik altyapılar fiziksel ve mantıksal olarak değerlendirildiğinde güvenlik denildiğinde daha çok fiziksel güvenliğe önem verilmiştir. Fakat bilgi teknolojilerindeki gelişmeler hem altyapıları hem de altyapılar arasındaki ilişkileri ve bağımlılığı etkilediği için bu sistemlerin fiziksel güvenlik yanında mantıksal güvenliği de ön plana çıkmıştır. Çünkü günümüzde kritik altyapı BT (Bilgi Teknolojileri) sistemleri genellikle bilgisayar sistemleri ile kontrol edilmekte ve izlenmektedir. Bilgisayar sistemleri de TCP/IP protokol ailesini kullandığı için internete bağlı olsa da olmasa da güvenlik riskleriyle karşı karşıyadır.

Kritik altyapı kavramının ortaya çıkmasının en önemli nedeni bilgi teknolojilerinin yaygın bir şekilde kullanılmasıdır [1]. Kritik altyapılar ve bilgi teknolojileri birçok yönden, ciddi şekilde kesişmektedir. Bu kesişimler bilgi teknolojilerinin önemini çok açık bir şekilde göstermektedir. Bu önem, "kritik bilgi altyapıları" teriminin ortaya çıkmasına yol açmıştır. OECD (Organisation for Economic Co-operation and Development) kritik bilgi altyapılarını, fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, vatandaşların ekonomik refahına veya hükümetin/ekonominin verimli çalışmasına ciddi yönde tesir eden bilgi ağları ve sistemleri olarak tanımlamaktadır [2].

2. Elektrik Üretim ve Dağıtım Sistemlerinin Otomasyonu

Günümüzde enerji üretim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesini de sağlayan SCADA (Supervisory Control And Data Acquisition) sistemleri tarafından yapılmaktadır. Bu sistemlerin büyük bir bölümü bilgi ve iletişim teknolojilerinden oluşmaktadır.

Prosesler için gözetleyici denetim ve veri toplama anlamına gelen SCADA uygulaması ilk olarak 1960'lı yıllarda Kuzey Amerika'da hayata geçirilmiştir. İlk yıllarda, SCADA sistemlerinin kurulum ve bakım maliyetleri oldukça yüksek olmasına karşın, teknolojideki gelişmeler hem bu sistemlerin maliyetlerini düşürmüş hem de sistemin işletilmesi için gerekli olan iş gücü gereksinimini azaltmıştır. Bunun sonucu olarak da daha çok tercih edilir hale gelmiştir [3].

Mimari yapı olarak SCADA'yı birinci nesil monolitik, ikinci nesil dağıtık (distributed) ve üçüncü nesil ağ tabanlı (networked) olarak üç nesle ayırmak mümkündür. Birinci nesil sistemlerde ağ yapısı mevcut değildir uzak terminal birimleriyle haberleşmeler özel protokollerle yapılmaktadır. Ayrıca bu tür sistemlerde yedeklemede bulunmamaktadır.

İkinci nesil SCADA sistemlerinde; bilgiyi gerçek zamanlı paylaşan ve LAN(Local Area Network) ile birbirlerine bağlanan çoklu istasyonlar kullanılmıştır.

Üçüncü nesil olarak günümüzde kullanılan ağ tabanlı SCADA sistemleri, RTU (Remote Terminal Unit) imalatçılarına ait özel protokoller yerine açık sistem mimarisini daha çok kullanmaktadır. Bu nesil SCADA sistemlerinin kullandığı açık sistem protokolleri, LAN'dan daha ziyade WAN üzerinden fonksiyonel olarak kullanılmaktadır. Açık mimaride yazıcılar, disk sistemleri, veri kaydediciler gibi üçüncü parti çevre aygıtlar sisteme daha kolay bağlanabilmektedir. WAN protokolleri (IP ve benzeri) sunucuyla iletişim

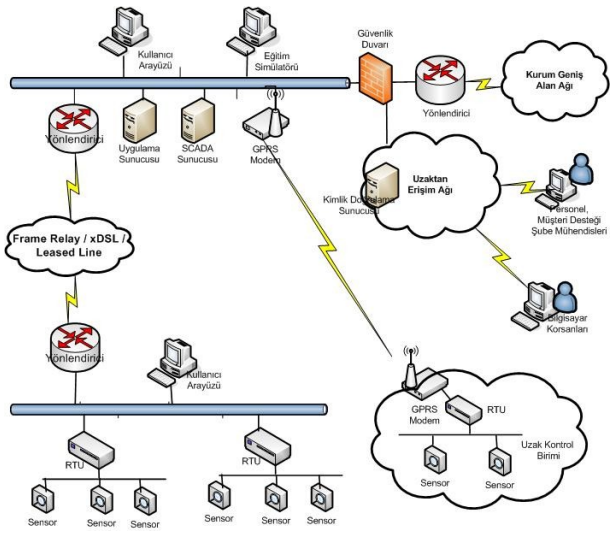
ekipmanları arasındaki iletişimi sağlamaktadır. Diğer yandan bu SCADA sistemlerinin siber savaşlara ve siber terörist girişimlere açık olması gibi bir güvenlik sorununu gündeme getirdiği de aşikârdır [4].

2.1. SCADA Sunucuları

Geniş bir alana yayılmış uzak terminal birimlerinin koordineli çalışması, uzak terminal birimlerinden gelen bilgilerin yorumlanarak kullanıcılara sunulması, kullanıcıların isteklerinin uzak terminal birimlerine iletilerek kumanda fonksiyonlarının sağlanması, diğer yazılım katmanları ile entegrasyonunu SCADA sisteminde merkezi yönetim birimi yerine getirmektedir. Merkezi yönetim birimi, uzak terminal birimlerinden bilgileri alır, istenilen bilgileri düzenli olarak kayıt eder, verileri değerlendirerek operatörlerin algılayacağı sesli ve görüntülü şekle dönüştürür. Merkezi yönetim birimi; sunucu, bilgisayar destekli paket uygulamaları, insan makine iletişimi için arayüzler, ağ anahtarları, yönlendiriciler, yazıcılar, modemler, işletme fonksiyonlarını yerine getirecek yazılımlar ve destek donanımlarından oluşur. Küçük SCADA sistemlerinde merkezi terminal birimi tek bir PC'den oluşabilir. Buna karşın daha büyük SCADA sistemleri çoklu sunucular, dağıtılmış yazılımlar ve yedekleme birimlerinden oluşur. Herhangi bir sunucu arızasında izleme ve kontrol faaliyetlerinin sürekliliğini sağlayarak sistemin bütünlüğünü artırmak için; aktif yedekleme yapısında aktif-aktif şeklinde yapılandırılan çoklu sunucular kullanılmaktadır.

2.2. Uzak Terminal Birimleri (RTU)

Uzak terminal birimleri fiziksel saha ekipmanları ile bağlantıyı sağlarlar. RTU'lar sistemdeki yerel ölçüm ve kumanda noktaları ile haberleşerek ya da I/O (giriş/çıkış) terminalleri yardımıyla yerel ekipmanlardan gelen sinyalleri değerlendirdikten sonra haberleşme hattı üzerinden merkezi terminal birimine bilgi verirler. RTU'lar aynı şekilde merkezi terminal biriminden gönderilen komutları değerlendirdikten sonra sahadaki ekipmanlara kumanda sinyalleri gönderirler. Sistemdeki röle, enerji analizörü, sayaç gibi cihazlarla RTU'lar haberleşerek, akım, gerilim, güç, tüketim gibi elektriksel bilgileri doğrudan alırlar. Aynı şekilde kesici, şalter, yük ayırıcı, solenoid gibi kumanda edilebilir ekipmanları kumanda ederler. Haberleşme imkanı olmayan saha ekipmanlarından bilgileri I/O modülleri vasıtasıyla alırlar. Sahadan gelen sonuçlar, cihazların çalışma durumları ve operatör tarafından girilen komutlar RTU tarafından saha ekipmanlarına iletilir. RTU'ların programlanabilir cihazlar olması sebebiyle merkez istasyonu üzerindeki işlem yükünün bir kısmını üzerine alarak sistem veriminin ve performansının artmasını sağlamaktadır. RTU'lar tüm alternatifleri değerlendirmek suretiyle merkezi terminal birimine bilgi vermeksizin alarm uyarıları üretebilir ve bu durumlarda ne yapılacağına anında kendileri karar vererek yerinde müdahaleler yapabilirler. Merkezi terminal birimine sadece olayın sonucunu aktarırlar. Tipik bir SCADA sistemi ağ topolojisi Şekil 1'de görülmektedir.



Şekil 1: SCADA sistemi genel ağ topolojisi

3. İletişim Ağı

İletişim, SCADA sistemlerinin omurgasını teşkil eder. Merkezi terminal biriminin uzak bölgelerde bulunan çeşitli RTU, bilgisayar veya sistemlerle bilgi alışverişi yapması için bir iletişim hattının olması gerekir. İletişim hatlarını kablolu ve kablosuz iletişim olmak üzere iki gruba ayırmak mümkündür. Büyük SCADA uygulamalarında kablolu ve kablosuz iletişim hatlarından oluşan karma bir yapı söz konusu olabilmektedir. Direk kablo bağlantısı geniş coğrafyaya yayılmış büyük sistemler için uygulamada birtakım sorunları da beraberinde getirmektedir. Direk kablo bağlantısının mümkün olduğu kritik uygulamalarda fiber optik kablo teknolojisi, daha yüksek veri transferi ve arttırılmış güvenlik sağlaması yönünden tercih edilir. Direk kablo bağlantısının mümkün olmadığı durumlarda diğer kurumlardan hat kiralamak (Leased-line, ADSL, DSL gibi), radyo frekans (RF), uydu iletişim, GSM, GPRS, 3G hatlarını kullanmak iyi bir çözüm yoludur.

SCADA sistemlerinin güvenilirliğini ve performansını etkilemede iletişim ağının çok büyük rolü vardır. İletişim ağı seçilirken iletişim hızı, güvenilirlik, maliyet gibi parametrelerin göz önünde bulundurularak titiz bir çalışmadan sonra karar verilmesi gerekir. Bazı kritik SCADA projelerinde iletişimin sürekliliğini sağlamak için yedek iletişim hatları kullanılmaktadır. Ana haberleşme hattında bir sıkıntı olması durumunda yedek olarak bekleyen hat otomatik devreye girmektedir. Ana haberleşme hattının ve yedek hattın farklı tipte

olması tercih edilir (ADSL-RF, RF-GPRS, Fiber Optik-RF gibi). [4]

4. SCADA Protokol Tipleri

Protokol; iletişim hattı üzerinden veri alışverişinin formatını, zamanlamasını, önceliğini ve denetimini tanımlayan bir dizi kurallar kümesidir. Eğer protokol iyi tasarlanmamışsa iletişim hattı ne kadar esnek ve hızlı olursa olsun haberleşmede trafik tıkanıklığı ve emniyet zafiyeti ihtimali vardır. Özellikle kritik altyapılar gibi gerçek zamanda işlem yapılan uygulamalarda uzak terminal birimlerinden gelen alarm, uyarı mesajları, hızlı değişime uğrayan fiziksel veriler iletişim yolunun tıkanmasına sebep olabilir. SCADA sisteminde kullanılan iletişim hattına bağlı olarak kullanılan RTU ve dağıtılmış saha ekipmanları arasında değişik haberleşme protokolleri kullanılabilmektedir. Modbus RTU, RP-570, Profi-Bus, Can-Bus gibi haberleşme protokollerini günümüzde birçok SCADA programları desteklemektedir. Günümüzde IEC60870-5-101, IEC 60870-5-104, IEC870-6, IEC 61850 ve DNP3 gibi açık iletişim protokolleri SCADA ekipman üreticileri ve çözüm ortakları arasında giderek daha popüler olmaktadır [5].

5. Elektrik Altyapısının Güvenliği İçin Teknik ve Yönetimsel Uygulamalar

İlk geliştirilen SCADA sistemleri hem üreticiye özel protokoller kullandığı hem de diğer ağlarla bağlanmadığı için daha çok fonksiyonellik ön plana çıkmış, çok fazla güvenlik özelliği eklenmemiştir. Fakat süreç içerisinde SCADA sistemleri için standart protokollerin yaygınlaşması sistemlerin internet ya da kapalı bilgisayar ağaları üzerinden kontrol edilmesi güvenlik risklerini de artırmaya başlamıştır. Bu riskler SCADA sisteminin internete bağlılık düzeyine göre artmaktadır. Bazı kurumlar SCADA sistemlerinin internete bağlı olmadığını öne sürerek güvenli olduklarını düşünmektedir. Siber atakların arttığı günümüzde Stuxnet zararlı yazılımı bunun doğru olmadığını açıkça göstermiştir. İran nükleer araştırmalarının yapıldığı sistemler internete bağlı olmamasına karşın Stuxnet zararlı yazılımı sisteme bulaşmıştır [11]. Daha önceki yıllarda da birçok kritik altyapının bilgi sistemlerine saldırı yapılmış ve çok ciddi zararlar verilmiştir. Son yıllarda özellikle siber savunma kapsamında kritik altyapılara bilgisayar sistemleri aracılığıyla saldırılar geçekleştirilmektedir.

Kritik altyapılarda kullanılan BT sistemlerinin güvenliğinin ön plana çıkmasıyla birlikte hem teknik hem de yönetimsel güvenlik önlemleri alınmaya başlanmıştır. Bu sistemler ülke için kritik öneme sahip olduğundan kurumun alacağı önlemler yanında Kritik altyapıları işleten kurumların çalışmalarını düzenleyen ve denetleyen kurumlar tarafından gerekli düzenlemeler yapılmaktadır. Örneğin ülkemizde faaliyet gösteren bankalar için BDDK (Bankacılık Düzeleme ve Denetleme Kurumu) düzenleme ve denetleme yapmaktadır. Bu çerçevede BDDK bankaların bilgi sistemlerinde almaları gereken önlemleri yayınlamıştır[13]. Sonrasında da her yıl periyodik olarak yapılan güvenlik testlerin sonuçlarını inceleyerek. Bankaların güvenliğini kontrol etmektedir. Aynı şekilde GSM operatörlerini, internet servis sağlayıcıları, elektronik sertifika hizmet sağlayıcıları düzenleyen ve denetleyen Bilgi Teknolojileri ve İletişim Kurumu bilgi sistemleri güvenliği konusunda düzenlemeler yapmaktadır. Benzer düzenlemeleri elektrik üretim ve dağıtım sistemleri, metrolar, hava limanları, hastaneler gibi kritik altyapıları düzenleyen ve denetleyen kurumların yapması gerekmektedir. Yurt dışında birçok ülkede kritik altyapıları düzenleyen ve denetleyen kurumlar altyapı BT sistemlerin güvenli hale getirilmesi için direktifler ve kılavuzlar yayınlamaktadır.

İngiltere'de kritik altyapıların güvenliği konularında çalışma yapan CPNI (Center for Protection of National Infrastructure) proses kontrol ve SCADA sistemlerin güvenliği konusunda bir rehber yayınlamıştır. Yayınlanan rehberde aşağıdaki güvenlik önlemelerinin alınması tavsiye edilmiştir[6].

- İş risklerinin anlaşılması
- Güvenli mimarinin gerçeklenmesi
- Olayları ele alma yeteneğinin oluşturulması
- Farkındalığın artırılması ve yeteneklerin geliştirilmesi
- Üçüncü parti risklerin yönetimi
- Projelerin güvenlikle birlikte ele alınması
- Sürekli bir yönetişim modelinin kurulması

Ayrıca CPNI tarafından yayınlanan rehberde ABD, Kanada, Avustralya ve Avrupa Birliği ile bu konularda bilgi paylaşıldığı ifade edilmiştir.

2006 yılında NERC (North America Electric Reliability Concuil) ABD'de elektrik alt yapılarının güvenli hale getirilmesi için elektrik sistemi üretim ve dağıtımdaki taraflara siber güvenlik standartları gerçekleme planını yayınlamıştır. 2010 yılı sonuna kadar bütün elektrik üretim, dağıtımı yapan kurumların, olası siber ataklara karşı, BT altyapı güvenliklerini denetlenebilir bir seviye getirmeleri istenmiştir. Yıllar içerisinde alınması gereken önlemleri belirtilmiştir [7].

NERC tarafından elektrik üreten ya da ileten kuruluşların almaları gereken güvenlik önlemleri aşağıda belirtilmiştir:

5.1. Kritik Siber Varlıkların Tanımlanması

Söz konusu kurum yönlendirme yapan, yönlendirme tablosu barındıran, uzaktan erişilebilen kritik altyapıların envanterini oluşturacaklar ve bunları düzenli olarak güncelleyeceklerdir.

5.2. Güvenlik Yönetim Kontrolleri

Siber Güvenlik Politikası: İlgili kurum, yönetimin katılımını ve kritik varlıkların güvenliğini içeren siber güvenlik politikasını yazmalı ve gerçeklemelidir. Bu politika ilgili herkes tarafından bilinmeli ve her yıl üst yönetim tarafından gözden geçirilip güncellenmelidir.

Bilginin Koruması: Ağ topolojisi, kritik BT varlıkları içeren binanın kat planları, siber güvenlik varlıklarının resimleri, felaketten kurtarma planları, olay müdahale planları, güvenlik yapılandırmaları gibi sisteme ait bilgiler ve saklandığı ortamlar korunmalıdır. Kritik altyapılardaki bilgiler sınıflandırılmalıdır. İlgili kurum kritik varlık bilgi koruma planının uyguluğunu her yıl değerlendirmeli ve bulunan eksiklikler için yapılacakları belirlemelidir.

Erişim Kontrolü: İlgili kurum, kritik siber varlık bilgilerini korumak için bu varlıklara erişimi denetim altına almalıdır. Yetkili erişim için isim, unvan ve diğer bilgileri tanımlanmalı. Her yıl erişim yetkileri gözden geçirilmeli. Yetkili kurum korunacak bilgiye erişim yapanların listesini her yıl gözden geçirip yeniden düzenlemelidir.

Değişim Kontrolü ve Konfigürasyon Yönetimi: İlgili kurum, kritik siber yazılım ve donanım varlıklarının değiştirilmesi, sisteme eklenmesi, sistemden çıkarılması, konfigürasyonunun değiştirilmesini sağlayacak değişim kontrol ve konfigürasyon yönetim sürecini oluşturmalı ve dokümante etmelidir. Aynı zamanda kritik siber varlıklara ait üretici ve satıcı değişikliklerini de izlemelidir.

5.3. Personel ve Eğitim

Farkındalık: İlgili kurum, personellerine siber ve fiziksel ortamlara yetkisiz erişim riskleri konusunda bilgilendirecek program oluşturmalı, dokümante etmeli ve güncellemelidir. Program her bir dört ayda eposta, hatırlatma notu, bilgisayar destekli eğitim, poster, intranet, broşür, sunu, toplantı gibi yollarla personeli bilgilendirmelidir.

Eğitim: İlgili kurum personellerine siber ve fiziksel ortama yetkisiz erişim riskleri konusunda eğitim programı oluşturmalı, dokümate etmeli ve gerçekleştirmelidir.

Bu eğitim kritik varlıklara erişim yapacak satıcı, teknik servis personellerine verilmelidir. Bu eğitimler politikalar, erişim kontrolleri ve prosedürleri içermelidir. Uygun rol ve sorumluluklar için minimum aşağıdaki eğitimler verilmelidir:

- Kritik siber varlıkların uygun kullanımı
- Kritik siber varlıklara fiziksel ve elektronik erişim kontrolü
- Kritik siber varlık bilgilerinin ele alınması
- Siber güvenlik olayı durumunda neler yapılacağının belirlenmesi

5.4. Elektronik Sınır Güvenliği

İlgili kurum tüm kritik varlıkların sınır güvenliği içinde kalmasını sağlamalı, sınır güvenliği ve ona olana erişim noktalarını tanımlamalı ve dokümante etmelidir.

İlgili kurum sınır güvenliği cihazlarına yapılacak elektronik erişimleri kontrol altına almalıdır. Sınır güvenliğinde kullanılan varlıklarda sadece ilgili portları ve servisleri çalıştırmalıdır.

Sınır güvenliği cihazlarına yapılan erişimleri izlemeli ve bu erişimlere ait kayıtları yedi gün 24 saat tutulmalı ve düzenlemelerin gerektirdiği süre kadar saklamalıdır.

İlgili kurum yılda en az bir defa sınır güvenliği cihazlarına açıklık analizi yapmalıdır.

İlgili kurum yasalara ve düzenlemelere uygun sistemi gerçekleyebilmek için gerekli tüm dokümantasyonu gözden geçirmeli ve güncellemelidir.

5.5. Sistem Güvenlik Yönetimi

Elektronik sınır güvenliğine yeni eklenen ve var olan siber varlıklarda yapılan değişiklikler siber güvenliği zayıflatmamalıdır. Bu kapsamda güvenlik yamaları, servis paketleri, satıcı sürümleri, işletim sistemi güncellemeleri, uygulamalar, veritabanları, üçüncü parti bellenimler dikkatli uygulanmalıdır.

Bu kapsamda ilgili kurum siber güvenlik test prosedürleri tanımlamalı, gerçeklemeli ve güncellemelidir. Yapılan testler gerçek ortamı simüle etmeli testlere ait sonuçları kayıt altına almalıdır.

İlgili kurum sadece normal işlemlerde ve acil durumlarda gerekecek portları açık tutmalıdır. Elektronik sınır güvenliğinde bulunan cihazlardaki diğer tüm portlar kapatılmalıdır. İlgili kurum teknik nedenlerden dolayı kapatılmayan portlar veya servisler için risk azaltıcı önlemler almalı ve bunları dokümante etmelidir.

Elektronik sınır güvenliği sisteminde bulunan kritik siber varlıklara ait yamaların izlenmesi, değerlendirilmesi, testi ve yamaların yapılması için program oluşturmalıdır.

İlgili kurum antivirüs veya zararlı yazılım önleme araçlarını kullanmalıdır. Zararlı yazılım imza güncellemeleri için prosedür oluşturmalıdır.

İlgili kurum elektronik sınır güvenliği içindeki siber varlıkların siber güvenlikle ilgili olaylarının izlenmesi için gerekli izleme sistemini oluşturmalıdır. Bu sistemler güvenlik olayı olduğunda otomatik veya manuel alarm oluşturmalıdır. Oluşturulan bir kayıt yasalar ya da düzenleyici kurumun öngördüğü süre kadar saklamalıdır.

İlgili kurum elektronik sınır güvenliği varlıkları için yılda en az bir defa siber açıklık analizi yapmalıdır. Bu analizde açık değerlendirme süreci dokümante edilmeli,

sadece gerekli olan servis ve portların çalıştığı kontrol edilmeli, varsayılan kullanıcı hesapları kontrol edilmelidir. Açıklık analizi sonucunda, ortaya çıkan açıkları, açıklıkları ortadan kaldırmak veya azaltmak için alınacak önlemleri dokümante etmelidir.

5.6. Olay Raporlama ve Olay Müdahale Planlama

Siber Güvenlik Olay Müdahale Planı: İlgili kuruluş siber güvenlik olay müdahale planı oluşturmalı ve sürdürmeli. Bu plan minimum aşağıdakileri içermelidir.

- Siber güvenlik olaylarını raporlanabilir ve sınıflandırılmış şekilde karakterize edecek prosedürler
- Müdahale takımındaki rol ve sorumluluklar, müdahale eylemleri, olay ele alma prosedürleri ve haberleşme planları
- Siber güvenlik olayını elektrik sektöründeki CERT ile paylaşabilecek süreç
- Herhangi bir değişiklik olması durumunda bu değişikliği plana belirli süre içinde yansıtma
- Siber güvenlik olayı ele alma prosesini yılda bir defa gözden geçirme
- Siber güvenlik olayı ele alma planını yılda en az bir defa test etme

6. Türkiye Elektrik İletim Altyapısı Kontrol Sistemi

Elektrik üretim ve dağıtım sistemlerinde SCADA/EMS sistemlerine geçilmesi çalışmaları 1980'lerin ortalarında başlamıştır. Hala yenileme ve güncelleme çalışmaları devam etmektedir. Bu çerçevede sistem kolay yönetilebilir ve izlenebilir hale gelmiştir. Elektrik üretim ve dağıtım sistemlerinin BT altyapısı ile ilgili güncel bilgilerin büyük bir bölümü TEİAŞ 2010 yılı faaliyet raporundan alınmıştır [8].

Tüm elektrik altyapısı sisteminin kontrolü Ankara Gölbaşı'nda bulunan Ulusal kontrol merkezinden yapılmaktadır. Bu merkez Genel Müdürlük binasında bulunan Acil Durum Kontrol Merkezi ile yedeklenmektedir. Hali hazırda Adapazarı, Gölbaşı, İzmir, Keban, İkitelli, Keban Samsun olmak üzere 6 adet bölgesel kontrol merkezi bulunmaktadır. Bölge kontrol merkezleri de elektrik üretim testilerinden aldıkları bilgileri ulusal kontrol merkezine iletmektedir.

2010 yılı itibari ile 235 trafo merkezi ve santral, Merkezi Kontrol Sistemine bağlanmıştır. SCADA Sistemi kapsamında uzaktan kumanda fonksiyonu pilot uygulama olarak 12 istasyonda gerçekleştirilmiş bulunmaktadır [8, 10].

EÜAŞ'a bağlı 51 Hidrolik santral, 20 Termik santral bulunmaktadır. Bunların dışında elektrik üreten birçok kurum ve kuruluştan da elektrik alınmaktadır [9].

Avrupa Elektrik Sistemine (ENTSO-E) bağlantı çalışmaları devam etmektedir. Bu çerçevede Komu ülkeler Yunanistan Bulgaristan ve ENTSO-E Güney Koordinasyon Merkezi (Swiss-Grid-İsviçre) bağlantıları gerçekleştirilmiş veri tabanlarında gerekli tanımlamalar yapılmıştır. Mısır, Irak, Ürdün, Libya, Lübnan, Filistin, Suriye ve Türkiye elektrik sistemlerinin eterkonneksiyonu konusunda çalışmalar da devam etmektedir.

Smart Grid konusunda İspanya'nın Mercados firmasından alınan danışmanlık projesi kapsamında çalışmalar devam etmektedir. Dünyada da bu konuda çok sayıda araştırma yapılmaktadır.

720 yerde bulunan 300 civarındaki sayacın uzaktan okunması için çalışmalar sürmektedir. Sayaçlardan okunan bilgiler GPRS ile taşınması için bir GSM operatörü ile anlaşılmıştır.

Amacı "elektriğin yeterli, kaliteli, sürekli, düşük maliyetli ve çevreyle uyumlu bir şekilde tüketicilerin kullanımına sunulması için, rekabet ortamında özel hukuk hükümlerine göre faaliyet gösterebilecek, mali açıdan güçlü, istikrarlı ve şeffaf bir elektrik enerjisi piyasasının oluşturulması ve bu piyasada bağımsız bir düzenleme ve denetimin sağlanması" olan EPDK'nın (Enerji Piyasası Düzenleme Kurumu) elektriğin sürekli sağlanması için düzenleme ve denetleme yetkisi bulunmaktadır. Elektrik üretim ve iletim sistemlerinin kontrol ve izlemesinde de kullanılan SCADA sistemlerinin güvenliğinin sağlanması için düzenlemeler yapıp, sistemlerin düzenli olarak denetlenmesi sağlanmalıdır.

Elektrik Piyasası Şebeke Yönetmenliği'nde TEİŞ ile kullanıcı arasında arasındaki hattın yedekliliğinden bahsedilmiş [12]. Fakat güvenlik olayları ayrıntılı ele alınmamıştır. İletişim ağı güvenlik kriterleri tanımlanmalı, uygulanmalı ve ilgili kurumlar tarafından denetlenmelidir.

7. Sonuç ve Öneriler

Elektrik üretim ve dağıtım sistemleri en önemli kritik alt yapılar arasında yer almaktadır. Dünyadaki gelişmelere paralel olarak ülkemizde de enerji sistemlerinin altyapı yönetimi ve izlenmesi büyük oranda BT teknolojileri ile bütünleşen SCADA sistemleri ile yapılmaktadır. SCADA sistemlerinin BT sistemleri ile bütünleşmesi birçok kolaylık ve esneklik sağlaması yanında ciddi güvenlik risklerini de beraberinde getirmektedir. Birçok ülke bu risklerin kapatılması veya seviyelerinin düşürülmesi için yönetimsel, teknik önlemler almakta ve yasal düzenlemeler yapmaktadır.

Enerji sistemlerinin kesintisiz, güvenli ve istenilen kalitede hizmet vermesi tüm ülkemizi yakından ilgilendirmektedir. Bu çerçevede dünyadaki birçok ülkede olduğu gibi ülkemizde de enerji üretim ve dağıtım sistemlerinin SCADA güvenliğinin sağlanması için gerekli düzenleme ve denetim mekanizmaları oluşturulup uygulanmalıdır.

8. Kaynaklar

[1] USA Presidential Decision Directive/NCS-63, "http://www.fas.org/irp/offdocs/pdd/pdd-63.htm", 1998 (25 Ocak 2011 erişilebilir durumda)

[2] OECD, Working Party on Information Security and Privacy, "Recommendations of the Council on the Protection of Critical Information Infrastructures", Ocak 2008

[3] http://www.dpstele.com/dpsnews/techinfo/scada/scada_knowledge_base.php, (25 Ocak 2011 erişilebilir durumda)

[4] Ten C., Liu C., Manimaran G., "*Vulnerability Assessment of Cybersecurity for SCADA Systems",* IEEE Transactions On Power Systems, Vol. 23, No. 4, 2008

[5] Kalapatapu R., *SCADA Protocols And Communication Trends,* ISA2004 Paper, http://www.isa.org/journals/intech/TP04ISA048.pdf (25 Ocak 2011 erişilebilir durumda)

[6] http://www.cpni.gov.uk/protectingyourassets/scada.aspx (25 Ocak 2011 erişilebilir durumda)

[7] http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf (25 Ocak 2011 erişilebilir durumda)

[8] http://www.teias.gov.tr/Faaliyet2010/TEIASfaaliyetraporu%20TURKCE.pdf (10 Ağustos 2011 erişilebilir durumda)

[9] http://www.teias.gov.tr/projeksiyon/KAPASITEPROJEKSIYONU2009.pdf (25 Ocak 2011 erişilebilir durumda)

[10] http://www.teias.gov.tr/TEIAS_Strtj_2011.pdf (10 Ağustos 2011 erişilebilir durumda)

[11] http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/zararli-yazilimlarin-yeni-hedefi-hangi-kritik-altyapi-sistemleri-olacak.html (10 Ağustos 2011 erişilebilir durumda)

[12] Elektrik Piyasası Şebeke Yönetmeliği, http://www.epdk.gov.tr/web/elektrik-piyasasi-dairesi/24 (10 Ağustos 2011 erişilebilir durumda)

[13] Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2007/09/20070914.htm&main=http://www.resmigazete.gov.tr/eskiler/2007/09/20070914.htm (6 Eylül 2011 erişilebilir durumda)