Akıllı Şebekelerde Siber Güvenlik (*)

Günümüz şebekelerine çağımızın bilgisayar ve ağ teknolojisi entegre ederek elde edilen şebeke sistemine "Akıllı Şebeke" (Smart Grid) denilmektedir [1]. Akıllı şebekeler, enerjinin üretiminden, tüketimine kadar her aşamada gerçek zamanlı iki yönlü bilgi transferi sağlayarak, sürdürülebilir, güvenli ve enerji verimliliği yüksek bir enerji ağı sunmaktadır [1]. İşte bu yazımızda bu iki yönlü bilgi transferleri sırasında oluşabilecek Siber Güvenlik tehditlerine bakacağım.

Bütünleşik Siber Güvenlik anlayışı gereği sadece SCADA, PLC vb. gibi bileşenlerin güvenliğe bakarak bu gibi karmaşık ve kritik altyapıların güvenliğinin alınabileceğinin düşünülmesi doğru değildir. Bu altyapılara bakıldığında sadece üstte saydığım öğelerin değil aşağıda ismi geçen tüm bileşenlere ait güvenliği konuşmamız ve bunlara ait önlemleri sıralamamız doğru olacaktır:

1) Akıllı Üretim
2) Akıllı İstasyonlar
3) Akıllı Dağıtım
4) Akıllı Sayaçlar
5) Bütünleştirilmiş Haberleşme
6) İleri Kontrol Metotları

Bu başlıkların da kendi içinde yazılım ve donanım bileşenlerinin olduğunu unutmamak gerekiyor.

Yazılım: Veri altyapısı, internet tabanlı sistemler, sezgisel çalışan yazılımları
Donanım: Akıllı sayaçlar ve akıllı ev aletleri vb.

Akıllı şebeke güvenliğinde esas alınacak Siber Güvenlik standardından ilki ISA 99 yani endüstriyel otomasyon ve kontrol sistemleri güvenlik standardıdır. Bu standardın amacı ağ üzerinde etkin ve güvenli üretim uygulamalarının tasarlanması için politikaları ve yapıları tanımlamak ve kontrol etmektedir [2]. ISA99 standartları geliştirme komitesi, endüstriyel otomasyon ve kontrol sistemleri güvenliği konusunda ISA standartlarını geliştirmek için dünya genelindeki endüstriyel siber güvenlik uzmanlarını bir araya getirir.

ISA/IEC 62443 ise ISA99 komitesi tarafından geliştirilmiş standartlar serisidir [3]. Bu standart ile şirketlerin kritik altyapı ve kontrol sistemlerindeki olası açıkları incelenmesi ve etkin koruma önlemleri geliştirilmesi için temel oluşturulması hedeflenmektedir. Endüstriyel otomasyon ve kontrol sistemlerine yönelik IT güvenliği, bu standardın odak noktasıdır.

Sadece bunlar değil ISA 99 komitesi, Purdue Enterprise Reference Architecture (PERA) modeli ve ICS ağ bölümlemesi için bu modeli kullanmıştır [4]. Bu model güvenliğin ayrılacak katmalara göre çok katmanlı mimari ile alınması, her katmanın gereksinimlerini dikkate alarak BT ve endüstri ağlarını alt ağlara ayırma ilkesine dayanır. Purdue modeli 6 katmandan oluşur ve her bu seviye için 4 ana başlıkta giriş kontrolü, log Yönetimi, ağ güvenliği ve uzaktan erişim odak alanlarının kontrol edilmesini söyler.

Seviye 5: Kurumsal ağ
Seviye 4: Yerel ağ
Seviye 3: Saha işlemleri
Seviye 2: Saha kontrolü
Seviye 1: Mantık kontrol
Seviye 0: Sensör, sürücü vb.

Akıllı şebekeler güvenliğinde sadece üstteki methodların kullanılması yeterli gelmeyecektir, çünkü bu ağlara klasik bir kritik altyapı öğelerinden daha fazla sayıda aktör ve taraf konuya dahildir. Bu aktörlere görsel 2 den göz atabilirsiniz.

Bilgi güvenliği 3 ana öğesi olan gizlilik, bütünlük ve erişebilirlik açısından akıllı şebekeler aşağıdaki şekilde tanımlanabilir:

Gizlilik, güç sistemi güvenilirliği için en az kritik olandır.

- Müşteri bilgilerinin gizliliği;
- Elektrik piyasası bilgisi;
- Bordro, iç stratejik planlama, genel kurumsal bilgiler vb.

Erişilebilirlik, güç sistemi güvenilirliği için en önemli güvenlik hedefidir. Kullanılabilirlikle ilişkili zaman gecikmesi değişebilir.

- Koruyucu röle için 4 ms;
- Trafo merkezi ve besleyici SCADA verileri için saniye;
- Sayaç okuma ve uzun vadeli piyasa fiyat bilgisi için saatler;
- Güç kalitesi bilgisi gibi uzun vadeli veri toplamak için günler / haftalar / aylar.

Bütünlük, Güç sistemi operasyonlarının bütünlüğü, aşağıdakileri garanti eder:

- Veriler izinsiz olarak değiştirilmedi;
- Veri kaynağı doğrulandı;
- Verilerle ilişkili zaman damgası bili-

nir ve doğrulanır;
• Veri kalitesi bilinir ve doğrulanır.

Bu 3 ana öğe etrafında Akıllı Şebekelerde ki Siber Güvenlik gereksinimlerini aşağıdaki ana başlıklar incelenmeli ve her biri için ayrı ayrı önlemler alınmalıdır [5].

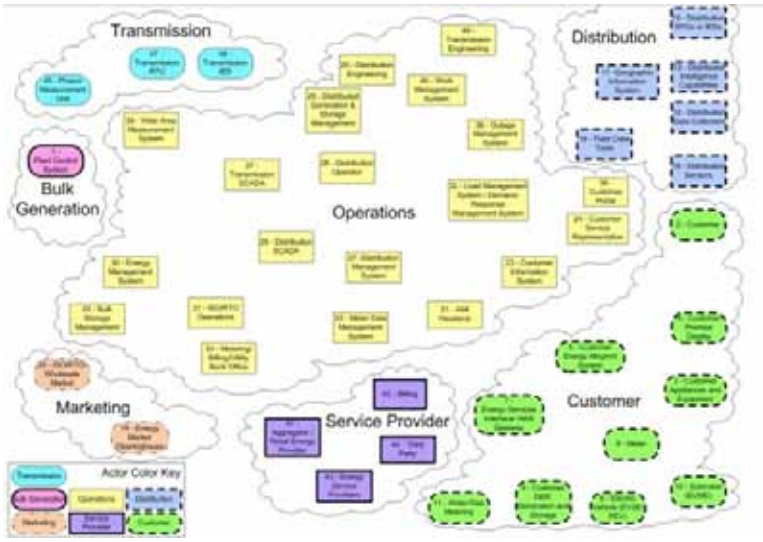
-Erişim Kontrol (Erişim Kontrol Politika, Uzaktan Erişim Politikası ve Prosedürleri, Hesap Yönetimi, Erişim Uygulaması, Bilgi Akışı Uygulaması, Görevlerin Ayrılığı, En Düşük Ayrıcalık, Başarısız Giriş Denemeleri, Akıllı Şebeke Bilgi Sistemi Kullanım Bildirimi, Önceki Oturum Açma Bildirimi, Eşzamanlı Oturum Kontrolü, Oturum Kilitlenmesi, Uzak Oturum Sonlandırma, Kimlik Tespiti veya Kimlik Doğrulaması Olmadan İzin Verilen Faaliyetler, Uzaktan Erişim, Kablosuz Erişim Kısıtlamaları, Taşınabilir ve Mobil Cihazlar için Erişim Kontrolü, Dış Bilgi Kontrol Sistemlerinin Kullanımı, Kontrol Sistemi Erişim Kısıtlamaları, Genel Olarak Erişilebilir İçerik, Şifre)

-Farkındalık ve Eğitim (Farkındalık ve Eğitim Politikası ve Prosedürleri, Güvenlik farkındalığı, Güvenlik Eğitimleri, Güvenlik Farkındalığı ve Eğitim Kayıtları, Güvenlik Grupları ve Birlikleri ile İletişim, Güvenlik Sorumluluk Eğitimi, Süreç Eğitimi Planlaması)

-Denetim ve Hesap Verebilirlik (Denetim ve Hesap Verebilirlik Politikası ve Prosedürleri, Denetlenebilir Etkinlikleri, Denetim Kayıtlarının İçeriği, Denetim Depolama Kapasitesi, Denetim İşleme Hatalarına Yanıt, Denetim İzleme, Analiz ve Raporlama, Denetim Analiz Araçları ve Rapor Üretimi, Zaman Damgası, Denetim Bilgilerinin Korunması, Denetim Kayıtları Muhafaza, Denetimlerin Yapılması ve Sıklığı, Denetçi Yeterliliği, Denetim Araçları, Güvenlik Politikası Uyumluluğu, Denetim Üretimi, İnkar edilemezlik)

-Güvenlik Değerlendirmesi ve Yetkilendirme (Güvenlik Değerlendirme ve Yetkilendirme Politikası ve Prosedürleri, Güvenlik Değerlendirmeleri, Sürekli gelişme, Akıllı Şebeke Bilgi Sistemi Bağlantıları, Güvenlik Yetkilendirmesi, Sürekli izleme)

-Yapılandırma Yönetimi (Yapılandırma Yönetimi Politikası ve Prosedürleri, Temel Yapılandırma, Yapılandırma Değişikliği için Erişim Kısıtlamaları, Fabrika Varsayılan Ayarları Yönetimi, Yapılandırma Yönetim Planı, ...)



Görsel 1: Akıllı Şebeke Aktörleri

-Operasyonların Sürekliliği (Operasyon Politikasının Sürekliliği ve Prosedürleri, Operasyon Planının Sürekliliği, Operasyon Rollerinin Sürekliliği ve Sorumlulukları, Alternatif Telekomünikasyon Hizmetleri, ...)

-Tanımlama ve Kimlik Doğrulama (Kimlik ve Kimlik Doğrulama Politikası ve Prosedürleri, Kullanıcı Kimliği ve Kimlik Doğrulama, ...)

-Bilgi ve Belge Yönetimi (Bilgi ve Belge Yönetimi Politikası ve Prosedürleri, Bilgi Değişimi, ...)

-Olay Müdahalesi (Olay Müdahale Politikası ve Prosedürleri, Olay Müdahale Rolleri ve Sorumlulukları, Eğitim, İzleme, Raporlama, ...)

- Akıllı Şebeke Bilgi Sistemi Geliştirme ve Bakım (Akıllı Şebeke Bilgi Sistemi Bakım Politikası ve Prosedürleri, Uzaktan Bakım, ...)

- Ortam Koruması (Ortam Koruma Politikası ve Prosedürleri, Ortam Hassaslık Seviyesi, Ortam Temizlik ve Bertarafı, Ortam Taşınması, ...)

- Fiziksel ve Çevre Güvenliği (Fiziksel ve Çevre Güvenliği Politikası ve Prosedürleri, Fiziksel Erişim Yetkileri, Fiziksel Erişimi İzleme, Ziyaretçi Katıları, Ziyaretçi Kontrol, Fiziksel Erişim Günlüğü Tutma, ...)

- Planlama (Stratejik Planlama Politikası ve Prosedürleri, Akıllı Şebeke Bilgi Sistemi Güvenlik Planı, Güvenlikle İlgili Aktivite Planlama, ...)

-Güvenlik Programı Yönetimi (Güvenlik Politikası ve Prosedürleri, Güvenlik Program Planı, Üst Yönetim Otoritesi, Güvenlik Mimarisi, Risk Yönetim Stratejisi, ...)

-Personel Güvenliği (Personel Güvenlik Politikası ve Prosedürleri, Personel Kategorisi, Transferi, Görevleri, Sorumluluk Sonlandırma, ...)

- Risk Yönetimi ve Değerlendirmesi (Risk Değerlendirme Politikası ve Prosedürleri, Risk Yönetim Planı, Güvenlik Etki Seviyesi, Güvenlik Açığı

Değerlendirmesi ve Farkındalık, Risk Değerlendirmesi, ...)

- Akıllı Şebeke Bilgi Sistemi ve Servis Satın Alma (Akıllı Şebeke Bilgi Sistemi ve Hizmetleri Satın Alma Politikası ve Prosedürleri, Yaşam Döngüsü Desteği, Yazılım Lisansı Kullanım Sınırlamaları, Güvenlik Mühendisliği İlkeleri, Geliştirici Güvenlik Testi, ...)

- Akıllı Şebeke Bilgi Sistemi ve İletişim Koruması (Akıllı Şebeke Sistemi ve İletişim Koruma Politikası ve Prosedürleri, Güvenlik Fonksiyonu İzolasyonu, Hizmet Reddi Koruması (DoS), İletişim Bütünlüğü, İşletim Sisteminden Bağımsız Uygulamalar, Genel Anahtar Altyapı Sertifikaları, Güvenlik Rolleri, heterojenite, VoIP, Balküpleri, İletişim Gizliliği,)

-Akıllı Şebeke Bilgi Sistemi ve Bilgi Bütünlüğü (Akıllı Şebeke Sistemi ve Bilgi Bütünlüğü Politikası ve Prosedürleri, Kusur Düzeltme, Kötü Amaçlı Kod ve Spam Koruması, Akıllı Şebeke Bilgi Sistemi İzleme Araçları ve Teknikleri, Güvenlik Uyarıları ve Tavsiyeler, Bilgi Girişi Doğrulama, Hata işleme, Yazılım ve Bilgi Bütünlüğü, ...)

Sonuç olarak akıllı şebekelerde siber güvenliği konuşmak için tek başına her hangi bir kritik altyapı güvenlik önlemlerini almak tek başına yeterli olmayacaktır. Burada önerdiğim önce bir mevcut durum tespiti yaptıktan sonra üstteki başlıklara ulaşmak için yapılacak bir yol haritası ile akıllı şebeke güvenlik anlayışı olarak bütünsel güvenlik yaklaşımını benimseyerek gerekli güvenlik önlemleri almak olacaktır.

(*) EMO İzmir Şubesi 33. Olağan Genel Kurulu'nda sunulan Enerji Komisyonu Raporu'ndan alınmıştır.

KAYNAKÇA

[1] Mehmet Oktay ELDEM, Akıllı Şebekeler, http://www.emo.org.tr/ekler/e8fff8ce0a6ccb5_ek.pdf?dergi=1101

[2] https://otomasyonadair.com/2014/11/07/bilinmesi-gereken-4-it-standardi/

[3] https://www.isa.org/intech/201810standards/

[4]https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems

[5] Guidelines for Smart Grid Cybersecurity, Smart Grid Cybersecurity Committee, https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

Görsel 1: Guidelines for Smart Grid Cybersecurity, Smart Grid Cybersecurity Committee, https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf