yedaş
Yeşilırmak Elektrik Dağıtım A.Ş.

Akıllı Şebekede Siber Güvenlik Standardizasyonu

PROJEYE NEDEN İHTİYAÇ DUYULDU

İhtiyaçlar

Mevzuatlar

Teknoloji

SİBER GÜVENLİK TEHDİTLERİ NELERDİR

- Endüstriyel kontrol sistemlerinin ele geçirilmesi
- Zararlı yazılımlar vasıtası ile bilginin dışarı sızması veya çalınması
- Bilgi işlem sistemine veya akıllı şebeke kontrol sistemine yetkisiz erişim olması
- Akıllı sayaç ile merkez arasındaki iletişime yetkisiz erişilmesi ve manipüle edilmesi
- Personel kaynaklı bilinçli veya bilinçsiz şekilde kritik altyapının zarar görmesi

AVRUPA VE ABD'DE YAYINLANMIŞ YÖNETMELİKLER

- **2004** : Avrupa Birliği tarafından ağ ve bilgi güvenliği konuları ile ilgili üye devletlerin siber güvenlik stratejilerine destek olması amacıyla **ajans kuruldu** (ENISA – The European Union Agency for Network and Information Security).

- **2009** : Avrupa Komisyonu tarafından yayınlanan yönetmelikte (2009/72-73/EC) belirlemiş olduğu 20-20-20 hedefine yani 2020 yılında enerjinin %20'sinin yenilenebilir kaynaklardan üretilmesi, CO2 emisyonunun %20 oranında azaltılması ve enerji verimliliğinin %20 artırılmasına bağlı olarak, AB ülkeleri akıllı şebekeleri kurmak için gerekli altyapı çalışmalarına başlamıştır. Yayınlanan yönetmelikte yapılan çalışmaların Avrupa Komisyonu tarafından yayınlanan 95/46/EC Direktif'e (Kişisel Verilerin Koruma Direktifi) uygun olması gerektiği belirtilerek **veri güvenliğinin öneminin altı çizilmiştir**.

- **2012** : Avrupa Komisyonu tarafından 2011 yılında akıllı şebekelerin standartlaştırılması ile ilgili yayınladığı yönetmeliğe (M/490) istinaden CEN-CENELEC-ETSI **Smart Grid Coordination Group kurulmuştur**. Bu grup tarafından Avrupa Birliği akıllı şebekeler için referans alınacak mimari yapı yayınlanmıştır.

- **2013** : Uluslararası Elektroteknik Komisyonu tarafından 2013 yılında endüstriyel kontrol sistemlerinde ağ ve sistem güvenliği üzerine bir **standart yayınlanmıştır** *(IEC 62443 (Industrial communications network, Network and System Security).*

- **2014** : Avrupa Komisyonu tarafından "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems" yayınlayarak akıllı şebekelerin uygulanması esnasında **kişisel verilerin güvenliğinin sağlanması gerektiği belirtilmiştir**.

- **2016** : Avrupa Parlamentosu tarafından "**Cyber Security for the Energy Sector**" çalışması yayınlanmıştır.

- **ABD'de** de bu konuda **2003** yılından beri hemen hemen **her yıl yeni yönetmelikler** yayınlanmaktadır.

PROJE KAPSAMINDA YAPILAN ÇALIŞMALAR

- Mevcut durum tespiti
- Siber Güvenlik hedef olgunluk modelinin belirlenmesi
- Hedef olgunluk modeline ulaşılması için yol haritasının oluşturulması

Mevcut durum tespiti

- Belirli standartlar üzerine kurulmuş mudur?
- Personellere özel siber güvenlik eğitimleri verilmiş midir?
- Mimari yapısı siber güvenlik bakış açısı ile değerlendirilmiş midir?
- Teknik zafiyetler tespit edilmiş midir?
- Destek veren firmalar ile siber güvenlik gereklilikleri belirlenmiş midir?
- Kurumsal bilgi teknolojileri altyapısı incelenmiş midir?
- Düzenli olarak siber güvenlik performansı değerlendirilmekte midir?
- Siber tehditlere karşı hazırlıklı mıdır?
- Olası bir siber saldırıda neler yapılması gerektiği bilinmekte midir?

Yayınlayan Kurum	Yayın Adı
NIST	Guide to Industry Control System Security NIST 800-82 Rev.2
International Electrotechnical Commission	IEC62443-3-3 (Industrial communications network, Network and System Security)
International Electrotechnical Commission	IEC 62443-2-1 (Industrial communications network, Network and System Security)

Teknik Zafiyet değerlendirme fazı için, NIST (National Institute of Standards and Technology) tarafından yayınlanmış **Endüstriyel Kontrol Sistem Güvenliği Kılavuzu** temel yöntem olarak benimsenmiş olup diğer kaynaklar da incelenerek YEDAŞ endüstriyel kontrol sistemleri topolojisine özel bir yöntem geliştirilmiştir.

Siber Güvenlik hedef olgunluk modelinin belirlenmesi

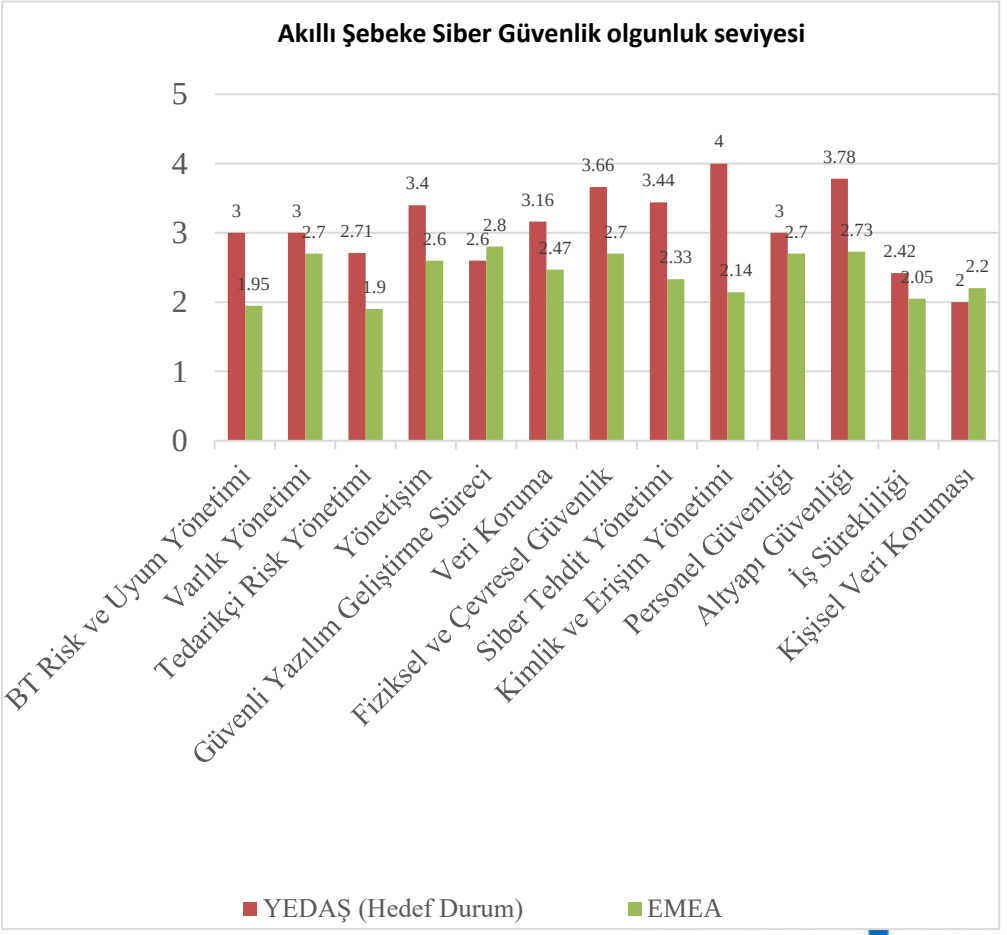
YEDAŞ on dört (14) farklı kontrol alanında siber güvenlik mevcut durum olgunluk değerlendirmesi yapmış ve hedeflerini belirlemiştir. Avrupa'da da benimsenen NIST tarafından yayınlanmış **Akıllı Şebeke Siber Güvenlik Kılavuzu** temel kaynak olarak benimsenmiştir. Siber güvenlik olgunluk modeli, BT ve Akıllı Şebeke olmak üzere 2 ayrı kısım için geliştirilmiştir.

Akıllı Şebeke için en yüksek üç kontrol alanı :

- **Personel Güvenliği**
- **Kimlik ve Erişim Yönetimi**
- **Tedarik Zinciri ve Dış Kaynaklar Yönetimi**

BT için en yüksek üç kontrol alanı :

- **Fiziksel ve Çevresel Güvenlik**
- **Kimlik ve Erişim Yönetimi**
- **Altyapı Güvenliği**



Yayınlayan Kurum	Yayın Adı
NIST	Guidelines for Smart Grid Cyber Security - NISTIR 7628 Rev.4
NIST	Security and Privacy Controls for Federal Information Systems and Organizations - NIST800-53
British Standard Institute	ISO/IEC 27001 : 2013
Information Systems Audit and Control Association	COBIT 5

Hedef olgunluk modeline ulaşılması için yol haritasının oluşturulması

Belirlenen kontrol listelerindeki her bir kontrol alanı ve alt başlıklar ayrı ayrı ele alınarak değerlendirilir ve hedeflenen olgunluk seviyelerine ulaşılabilmesi için şirketin alması gereken aksiyonlar yol haritasında projelendirilir.

BT Siber Güvenlik olgunluk seviyesinin artırılması için toplamda 10 proje;

BT - Proje Adı	2018				2019			
Güvenlik Operasyon Merkezi			6 ay					
Güvenlik Bilgisi ve Olay Yönetimi					6 ay			
Veri Koruma		9 ay						
Bilgi Güvenliği Olay ve Kriz Yönetimi				3 ay				
İş Sürekliliği Yönetimi							6 ay	
Kurumsal Açıklık ve Tehdit Yönetimi		3 ay						
Yönetim için Bilgi Güvenliği Farkındalığı	3 ay							
Altyapı Güvenliği	Sürece yayılacaktır							
Kimlik ve Erişim Yönetimi					6 ay			
Tedarikçi Risk Yönetimi					3 ay			

Akıllı Şebeke Siber Güvenlik olgunluk seviyesinin artırılması için toplamda 4 proje;

Akıllı Şebeke - Proje Adı	2018				2019			
Siber Güvenlik Yönetimi	3 ay							
Veri Koruma	Sürece yayılacaktır							
Siber Kriz ve Olay Yönetimi				3 ay				
Süreklilik							6 ay	

Bu projelerin hayata geçirilmesi, Risk, Fayda ve Maliyet açılarından değerlendirilerek önceliklendirilir.

PROJE ÇIKTILARI

- Akıllı Şebeke için Siber Güvenlik standartları

1	Risk Yönetimi Standardı
2	Siber Güvenlik Farkındalık Standardı
3	Siber Güvenlik Program Yönetimi Standardı
4	Kişisel Veri Mahremiyeti Standardı
5	Erişim Yönetimi Standardı
6	Varlık Yönetimi Standardı
7	Bilgi Bütünlüğü Standardı
8	Personel Güvenliği Standardı
9	Kriptogtrafi ve Anahtar Yönetimi Standardı

10	Ağ Güvenliği Standardı
11	Veritabanı Güvenliği Standardı
12	Yapılandırma Standardı
13	Yazılım Geliştirme, Değişim ve Bakım Standardı
14	Tedarikçi Risk Yönetimi Standardı
15	Denetim İzleri Standardı
16	Siber Güvenlik Olay Yönetimi Standardı
17	İş Sürekliliği Standardı
18	Fiziksel ve Çevresel Güvenlik Standardı

- Akıllı Şebeke Siber Güvenlik standartları için kontrol listeleri

Örnek :
Erişim Yönetimi Standardı için kontrol listesi

1	*Genel Kurallar*
2	*Teknik Kurallar*
3	*Hesap Yönetimi Kuralları*
4	*Ayrıcalıklı Hesaplarla İlgili Kurallar*
5	*Görevler Ayrılığı İlkesi ile İlgili Kurallar*

6	*Uzaktan Erişim Kuralları*
7	*Üçüncü Taraflar İçin Uzaktan Erişim Kuralları*
8	*Taşınabilir Cihazlar İçin Erişim Kuralları*
9	*Dış Sistemlerden Erişim Kuralları*
10	*Şifre (Parola) Belirleme ve Kullanım Kuralları*

- Personel organizasyonunda yeni görevler

"**BT Risk Sorumlusu**" ve "**Altyapı Güvenlik Sorumlusu**"

SORULARINIZ

TEŞEKKÜRLER ...