Enerji Sektöründe Bilgi Güvenliğinin Yönetilmesi: Mevzuat Ve Standartlar

Fikret Ottekin[1] – Orhan Çalık[2]
[1] ICterra A.Ş. Genel Müdür Danışmanı fikret.ottekin@icterra.com
[2] TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü, Uzman Araştırmacı orhan.calik@tubitak.gov.tr

***Özetçe*— Kritik altyapıları barındıran en önemli sektörlerden biri enerji sektörüdür. Enerji altyapılarının kurumsal bilişim sistemlerine ilave olarak endüstriyel kontrol sistemleri dolayısı ile de bilgi sistemlerine bağımlılığı tartışmasız durumdadır. Bu bilgi sistemlerine kurum içinden veya dışından çeşitli saldırıların yapıldığı, saldırılar sonucunda çeşitli ölçekte zararların oluştuğu bilinmektedir.**

Aralık 2014 tarihinde EPDK bilgi güvenliğine dönük gereksinimleri göz önünde bulundurarak konu ile ilgili üç yönetmeliği güncellemiş ve lisans sahiplerine bilişim sistemleri güvenliğini sağlama doğrultusunda yükümlülükler getirmiştir. Ancak enerji sektöründe yer alan kuruluşların önemli bölümünde konu ile ilgili farkındalık eksikliği bulunmaktadır. Makalenin amacı bu eksiği bir nebze olsun gidermek, bilgi güvenliği kapsamında enerji sektöründe faaliyet gösteren kuruluşların uygulaması gereken önlemleri ortaya koymaktır.

***Anahtar Kelimeler*— Kritik altyapılar, bilgi güvenliği, enerji sektörü,risk yönetimi,**

***Abstract*— Energy sector is by far one of the most important sectors that utilize critical infrastructures. Energy infrastructures' dependance on information systems is indisputable due to the presence of Industrial Control Systems as well as corporate information systems. It is common knowledge that these information systems are targeted by various attacks from inside and outside the organizations that cause consequences of various degrees.**

In December 2014, Energy Market Regulatory Authority has revised three directives and brought the obligation of assuring the security of their information systems to license holders. However, awareness regarding information security is insufficient in most of the institutions operating in the energy sector. The objective of this article is improving the information security awareness and defining the controls that should be applied by the institutions operating in the energy sector.

***Index Terms*— Critical infrastructure, information security, energy sector, risk management.**

I. GİRİŞ

Bu makalenin konusu, EPDK'nın kritik enerji altyapılarında önemi giderek artan bilgi güvenliği ihtiyacına dayanarak kuruluşlara uyum zorunluluğu getirdiği bilgi güvenliği standartlarıdır. Enerji sektöründe bilgi güvenliği konusunda yeterli miktarda uzman bulunmadığı göz önünde bulundurularak bilgi güvenliği standartlarına ve standartlarda gözden kaçabilecek hususlara dikkat çekilmekte, standartların birleştiği ve ayrıldığı noktalar tablo ve şekillerle vurgulanarak bir bakışta anlaşılacak şekilde gözler önüne serilmektedir. Böylece bilgi güvenliğine dönük önlemler kurumlarda uygulanırken konu ile ilgili standartların ve standartların önemli bölümlerinin gözden kaçırılmadan eksiksiz şekilde uygulanması ve ulusal kritik altyapı güvenliğinin en kritik bileşenlerinden kritik enerji altyapıları güvenliğine katkı yapılması hedeflenmektedir.

II. DÜNYA'DA KRİTİK ENERJİ ALTYAPILARI VE GÜVENLİK

20 Haziran 2013'te yayınlanarak yürürlüğe giren "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" belgesinde kritik altyapı,

"İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda,

- Can kaybına,
- Büyük ölçekli ekonomik zarara,
- Ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına
- yol açabilecek bilişim sistemlerini barındıran altyapıları ifade eder" şeklinde tanımlanmıştır [1].

Bu tanım göz önünde bulundurulduğunda, kritik altyapıları barındıran ilk sektörlerden biri olarak akla enerji sektörü gelmektedir.

AB ve ABD'de kritik altyapı güvenliği konusunda yapılan çalışmalar da enerji sektörünün önemine işaret etmektedir.

23 Aralık 2008'de AB Resmi Gazetesi'nde yayınlanan "Avrupa Kritik Altyapılarının Belirlenmesi ve Güvenliklerinin İyileştirilme Gereksiniminin Değerlendirilmesine İlişkin 2008/114/AB Konsey Yönergesi" dokümanının 5. maddesinde yönergenin enerji ve ulaştırma sektörlerine odaklandığı, ilave olarak bilgi ve iletişim sektörlerinin de gözden geçirilebileceği belirtilmektedir [2].

ABD Anayurt Güvenliği Bakanlığının, resmi web sitesinde ilan ettiği "Kritik Altyapı Sektörleri" arasında enerji sektörü de yer almaktadır [3].

Enerji altyapılarının, kurumsal bilişim sistemlerine ilave olarak endüstriyel kontrol sistemleri dolayısı ile de bilgi sistemlerine bağımlılığı tartışmasız durumdadır. Bu bilgi sistemlerine kurum içinden veya dışından çeşitli saldırıların yapıldığı, saldırılar sonucunda çeşitli ölçekte zararların oluştuğu bilinmektedir. ABD'de faaliyet göstermekte olan EKS-BOME (Endüstriyel Kontrol Sistemleri - Bilgisayar Olaylarına Müdahale Ekibi) 2013 yılı içinde kendilerine

işletmeci kurumlar tarafından 257 olay bildirildiğini, saldırıya uğrayan kurumların %57'sinin enerji sektöründe bulunduğunu bildirmiştir [4].

Tüm bu bilgiler, hem kurumların ve tüketicilerinin ekonomik zarardan korunması, hem de vatandaşın can güvenliğinin ve kamu düzeninin muhafaza edilmesi için kritik enerji altyapılarında bilişim sistemlerinin güvenliğinin sağlanmasına yönelik yatırım yapılması gerekliliğini gözler önüne sermiştir

III. EPDK'NIN GETİRDİĞİ YÜKÜMLÜLÜKLER

4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanun, Enerji Piyasası Düzenleme Kurulu'na,

- "Tüketicilere güvenilir, kaliteli, kesintisiz ve düşük maliyetli elektrik enerjisi hizmeti verilmesini teminen gerekli düzenlemeleri yapmak" (Madde 5, c bendi).
- "Üretim, iletim ve dağıtım şirketleri ile otoprodüktör ve otoprodüktör grubu tesisleri için güvenlik standartları ve şartlarını tespit etmek ve bunların uygulanmasını sağlamak" (Madde 5, e bendi).

görevlerini vermiştir [5].

EPDK, Aralık 2014 tarihinde bilgi güvenliğine dönük gereksinimleri göz önünde bulundurarak aşağıda belirtilen üç yönetmeliği güncellemiş ve lisans sahiplerine bilişim sistemleri güvenliğini sağlama doğrultusunda yükümlülükler vermiştir. Bu kapsamda,

1. Elektrik Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik
2. Doğal Gaz Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik ve
3. Petrol Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik,

26 Aralık 2014 tarihinde Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. [6, 7, 8] Yönetmeliklerle bilgi güvenliği kapsamında yükümlülüğe tabi olan kurumlar şunlardır:

1. Elektrik piyasasında,
    a. OSB (Organize Sanayi Bölgesi) üretim lisansı sahipleri hariç olmak üzere, kurulu gücü 100MW ve üzerinde olan ve geçici kabulü yapılmış bütün üretim tesisleri,
    b. İletim lisansı sahibi,
    c. Piyasa işletim lisansı sahibi,
    d. OSB dağıtım lisansı sahipleri hariç olmak üzere dağıtım lisansı sahipleri (elektrik dağıtım şirketleri) [6]
2. Doğal gaz piyasasında,
    a. İletim lisansı sahibi şirketler,
    b. Sevkiyat kontrol merkezi kurmakla yükümlü dağıtım lisansı sahibi şirketler [7]
3. Petrol piyasasında,
    a. Rafinerici lisansı sahipleri [8].

Tüm bu kurumlara, aşağıdaki yükümlülük getirilmiştir:

"Kurumsal bilişim sistemi ile endüstriyel kontrol sistemlerini TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına uygun bir şekilde işletmek, TS ISO/IEC 27001 standardına uygun faaliyet gösterdiğini Türk Akreditasyon Kurumuna akredite olmuş bir belgelendirme kurumuna ispat ederek sistemlerini belgelendirmek ve söz konusu belgelerin geçerliliğini sağlamak,"

Yükümlülükler 1/3/2016 tarihinde yürürlüğe girecektir.

IV. KURUMLARIN UYUM SAĞLAMASI GEREKEN BİLGİ GÜVENLİĞİ STANDARTLARI

Bilgi Güvenliği konusunda yönetmelikte belirtilen TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Gereksinimleri standardının son sürümü 2013'te yayınlanmış olup, uzun süreden beri yürürlükte olan 2005 sürümü ile arasında dikkate değer farklar vardır [9].

ISO 27001 standardı, bilgi güvenliğini sağlamaya çalışan kurumun hangi sektörde yer aldığı ile ilgilenmez. Yıl boyunca yapılması gereken risk analizi, eğitim, iç tetkik ve iyileştirme gibi başlıca faaliyetleri ve yönetimin sorumluluklarını, yani ana hatları ile yönetim sürecini tanımlar [10]. Somut güvenlik önlemleri ise ISO 27002 standardında yer almaktadır [11]. 27002 standardının 27001:2005'te "vazgeçilmez" olduğu belirtilmektedir. 27001:2013'te bu ifade bulunmasa da, 6.1.3 Bilgi Güvenliği Risk Tedavisi başlığı altında 27002:2013'ün dikkatle gözden geçirilmesi, uygulanmayan güvenlik önlemlerinin neden uygulanmadığının kaydedilmesi gerektiği belirtilmektedir.

Bu makalenin özelinde incelenecek olan ISO/IEC 27019 ve ISO/IEC 27011 standartları da, sırasıyla bilgi güvenliğinin enerji ve iletişim sektörlerinde sağlanmasına yönelik olarak yayınlanmış standartlardır [12, 13]. Bu makalenin yayınlanma tarihi itibarı ile standartların son sürümleri 27019:2013 ve 27011:2008 olup, bu standartlar 27002:2005 standardına yapılan ilavelerle oluşturulmuştur.

27002:2005 standardında bulunan önlemlere iki tip ilave yapılmıştır.

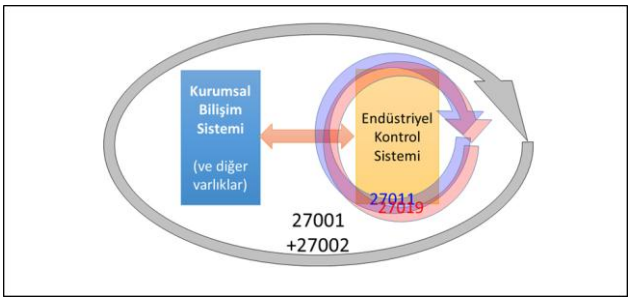
a. 27002'de hiç bulunmayan, "Sektöre Özel Önlemler" tanımlanmıştır.
b. 27002'de zaten mevcut olan bazı önlemlerde "Sektöre Özel Uygulama Kılavuzu" başlığı altında birkaç paragraf eklenerek ek tavsiyeler yapılmıştır.

Enerji sektöründe bulunan ve bilgi güvenliğini tesis etmeye çalışan kurumların, 27011 ve 27019 standartlarına uyum yükümlülüğü bulunmamakla birlikte bu ilavelerden fikir alabilecekleri ve kurumsal bilgi güvenliğine katkı sağlayabilecekleri söylenebilir.

Bu aşamada enerji sektöründe bilgi güvenliğinin sağlanması ile iletişim sektörüne özel bilgi güvenliği standardının ne ilgisi olduğu sorusu akla gelebilir. Özellikle enerji iletim ve dağıtımı ile uğraşan kuruluşlar, geniş alanlara yayılmış durumda bulunan sistemlerin kontrolünü sağlarken çeşitli iletişim

sistemlerine bağımlı duruma gelmektedir. Bu nedenle, 27019 standardının birinci bölümünde, "Süreç kontrol sistemlerini destekleyen iletişim sistemlerinde ve bileşenlerinde 27011 standardında yer alan önlemlerin uygulanması" tavsiye edilmektedir.

Yönetmeliklerde yer alan "Kurumsal Bilişim Sistemi ve Endüstriyel Kontrol Sistemleri" kapsamı bilgi güvenliği standartları ile birlikte değerlendirildiğinde, 27001'in kurumun genel bilgi güvenliği yönetim sürecini tanımladığı, Kurumsal Bilişim Sistemlerinde ve insan kaynağı da dahil olmak üzere diğer varlıklarda alınacak önlemlerle ilgili olarak 27002, Endüstriyel Kontrol Sistemlerinde alınacak önlemlerle ilgili olarak ise 27002, 27011 ve 27019 standartlarının göz önünde bulundurulması gerektiği söylenebilir. Bu durum aşağıdaki şekille de ifade edilebilir.



Şekil-1. Kurumsal Bilgi Sistemleri ve ilgili standartlar

V. ENERJİ VE İLETİŞİM SEKTÖRÜNE ÖZEL STANDARTLARIN GETİRDİKLERİ

Aşağıdaki tabloda, 27011 ve 27019 standartlarında yer alan ilave bilginin 27002 ile eşleştirilerek gözler önüne serilmesi amaçlanmıştır. Tabloda yer alan kontroller, yani güvenlik önlemleri, üç kategoride toplanabilir:

1. Tablonun 27011 ve 27019 sütunlarında '→' ve '←' sembollerinin bulunduğu satırlar 27002'de tanımlanan önlemin 27011 ve/veya 27019'da da aynen mevcut olduğu, herhangi bir ek yapılmadığı anlamına gelmektedir.
2. Bazı önlemlerde, 27002'deki tanıma ilave olarak 27011 ve/veya 27019'da "Sektöre özel uygulama kılavuzları" bulunmaktadır.
3. 27002'de yer almayan, iletişim sektörüne veya enerji sektörüne özel güvenlik önlemleri de mevcuttur. 27011 veya 27019 standardında bu önlemlerin nasıl uygulanacağı açıklanmaktadır. Kırmızı yazı karakteri kullanılarak belirtilen önlemler 27019 (Enerji), Lacivert yazı karakteri kullanılarak belirtilen önlemler ise 27011 (İletişim) sektörüne özel olarak tanımlanmış ve standartlara eklenmiş olan kontrollerdir. Bu önlemler Standartların EK-A bölümlerinde yer almaktadır.

27011:2008 (İletişim)	**27002:2005**	**27019:2013 (Enerji)**
	5.1 Bilgi Güvenlik Politikası	
→	5.1.1, 5.1.2	←
	6.1 Kurum İçi Organizasyonu	
→	6.1.1, 6.1.2, 6.1.3, 6.1.4	←
Sektöre özel uygulama kılavuzu vardır.	6.1.5 Gizlilik anlaşmaları	←
Sektöre özel uygulama kılavuzu vardır.	6.1.6 Otoritelerle iletişim	**Sektöre özel uygulama kılavuzu vardır.**
→	6.1.7 Uzmanlık grupları ile iletişim	**Sektöre özel uygulama kılavuzu vardır.**
→	6.1.8	←
→	**6.2 Üçüncü Taraf Erişiminin Güvenliği**	
→	6.2.1 Üçüncü taraf erişiminde risklerin tanımlanması	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	6.2.2. Müşterilerle çalışırken güvenlik	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	6.2.3 Üçüncü taraf sözleşmelerinde güvenlik gerekleri	**Sektöre özel uygulama kılavuzu vardır.**
	7.1 **Varlıklarla ilgili sorumluluklar**	
Sektöre özel uygulama kılavuzu vardır.	7.1.1 Varlık Envanteri	**Sektöre özel uygulama kılavuzu vardır.**
→	7.1.2 Varlıkların sahipleri	**Sektöre özel uygulama kılavuzu vardır.**

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
→	7.1.3	←
	7.2 Bilgi Sınıflandırması	
Sektöre özel uygulama kılavuzu vardır.	7.2.1 Sınıflandırma rehberleri	**Sektöre özel uygulama kılavuzu vardır.**
→	7.2.2	←
	8.1 İşe almadan önce	
Sektöre özel uygulama kılavuzu vardır.	8.1.1 Roller ve sorumluluklar	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	8.1.2 Personel gözetleme	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	8.1.3 İşe alınmanın şartları	**Sektöre özel uygulama kılavuzu vardır.**
	8.2 Çalışma Sırasında	
→	8.2.1, 8.2.2, 8.2.3	←
	8.3 Görev değişikliği veya işten ayrılma	
→	8.3.1, 8.3.2, 8.3.3	←
	9.1 Güvenlik Alanı	
Sektöre özel uygulama kılavuzu vardır.	9.1.1 Fiziksel güvenlik sınırı	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	9.1.2 Fiziksel giriş kontrolleri	**Sektöre özel uygulama kılavuzu vardır.**
→	9.1.3, 9.1.4, 9.1.5, 9.1.6	←
9.1.7 İletişim merkezlerinin güvenliği (Securing communication centres)	**X**	**X**

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
9.1.8 İletişim teçhizat odalarının güvenliği (Securing telecommunications equipment room)	**X**	**X**
9.1.9 Fiziksel olarak izole edilmiş operasyon alanlarının güvenliği (Securing physically isolated operation areas)	**X**	**X**
X	**X**	**9.1.7 Kontrol merkezlerinin güvenliği** (Securing control centers)
X	**X**	**9.1.8 Teçhizat odalarının güvenliği** (Securing equipment rooms)
X	**X**	**9.1.9 Çevresel mekânların güvenliği** (Securing peripheral sites)
	9.2 Ekipman Güvenliği	
Sektöre özel uygulama kılavuzu vardır.	9.2.1 Ekipman yerleşimi ve koruması	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	9.2.2 Destek hizmetleri	**Sektöre özel uygulama kılavuzu vardır.**
→	9.2.3 Kablolama güvenliği	**Sektöre özel uygulama kılavuzu vardır.**
→	9.2.4, 9.2.5, 9.2.6, 9.2.7	←

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
9.3 Diğer tarafın sağladığı güvenlik (Security under the control of other party)	**X**	**X**
9.3.1 Diğer taşıyıcının tesisindeki cihazların güvenliği (Equipment sited in other carrier's premises)	**X**	**X**
9.3.2 Müşterinin tesisindeki cihazların güvenliği (Equipment sited in user premises)	**X**	**X**
9.3.3 Birbirine bağlı iletişim servislerinin güvenliği (Interconnected telecommunications services)	**X**	**X**
X	**X**	**9.3 Üçüncü tarafların tesislerinde güvenlik** (Security in premises of 3rd parties)
X	**X**	**9.3.1 Diğer enerji kuruluşlarının tesislerinde bulunan cihazlar** (Equipment sited on the premises of other energy utility organizations)
X	**X**	**9.3.2 Müşterinin tesislerinde bulunan cihazlar** (Equipment sited on customer's premises)
X	**X**	**9.3.3 Birbirine bağlı kontrol ve iletişim sistemleri** (Interconnected control and communication systems)
	10.1 İşletme Prosedürleri ve Sorumluluklar	
Sektöre özel uygulama kılavuzu vardır.	10.1.1 Belgelenmiş işletme prosedürleri	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	10.1.2 Değişim kontrolü	←
→	10.1.3 Görevler ayrılığı	←
Sektöre özel uygulama kılavuzu vardır.	10.1.4 Geliştirme sistemi, test sistemi ve aktif sistemlerin ayrılması	**Sektöre özel uygulama kılavuzu vardır.**
	10.2 Üçüncü taraflardan alınan hizmetin yönetilmesi	
→	10.2.1, 10.2.2, 10.2.3	←
	10.3 Sistem Planlama ve Kabul Etme	
→	10.3.1, 10.3.2	←

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
	10.4 Kötü Niyetli Yazılımlara Karşı Korunma	
→	10.4.1 Kötü niyetli yazılımlara karşı kontroller	**Sektöre özel uygulama kılavuzu vardır.**
Sektöre özel uygulama kılavuzu vardır.	10.4.2 Mobil yazılımlarla ilgili denetimler	**Sektöre özel uygulama kılavuzu vardır.**
	10.5 Yedekleme	
→	10.5.1	←
	10.6 Ağ Güvenliğinin Yönetilmesi	
→	10.6.1	←
Sektöre özel uygulama kılavuzu vardır.	10.6.2 Ağ hizmetlerinin güvenliği	←
10.6.3 Verilen iletişim hizmetlerinin güvenliğinin yönetimi (Security management of telecommunications services delivery)	**X**	**X**
10.6.4 İstenmeyen e-Posta'ya müdahale (Response to spam)	**X**	**X**
10.6.5 DDoS saldırılarına müdahale (Response to DoS/DDoS attacks)	**X**	**X**
X	**X**	**10.6.3 Süreç kontrol verilerinin iletişim güvenliği** (Securing process control data communication)

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
	10.7 Bilgi ortamı yönetimi ve güvenlik	
→	10.7.1, 10.7.2, 10.7.3, 10.7.4	←
	10.8 Bilgi ve Yazılım Değiş Tokuşu	
→	10.8.1, 10.8.2, 10.8.3, 10.8.4, 10.8.5	←
	10.9 Elektronik Ticaret Hizmetleri	
→	10.9.1, 10.9.2, 10.9.3	←
	10.10 Sistem Erişiminin Gözlenmesi ve Kullanımı	
Sektöre özel uygulama kılavuzu vardır.	10.10.1 Olay kayıtlarının tutulması	**Sektöre özel uygulama kılavuzu vardır.**
→	10.10.2, 10.10.3, 10.10.4, 10.10.5	←
→	10.10.6 Saat senkronizasyonu	**Sektöre özel uygulama kılavuzu vardır.**
X	**X**	**10.11 Eski sistemler** (Legacy systems)
X	**X**	**10.11.1 Eski sistemlere müdahale** (Treatment of legacy systems)
X	**X**	**10.12 Güvenlik işlevleri** (Safety functions)

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
X	**X**	**10.12.1 Güvenlik işlevlerinin bütünlüğü ve erişilebilirliği** (Integrity and availability of safety functions)
	11.1 Erişim Denetimi Gereksinimleri	
Sektöre özel uygulama kılavuzu vardır.	11.1.1 Erişim denetimi politikası	**Sektöre özel uygulama kılavuzu vardır.**
	11.2 Kullanıcı Erişiminin Yönetilmesi	
→	11.2.1, 11.2.2, 11.2.3, 11.2.4	←
	11.3 Kullanıcı Sorumlulukları	
→	11.3.1 Parola kullanımı	**Sektöre özel uygulama kılavuzu vardır.**
→	11.3.2, 11.3.3	←
	11.4 Ağ Erişimi Denetimi	
→	11.4.1, 11.4.2, 11.4.3, 11.4.4	←
→	11.4.5 Ağlardaki ayrım	**Sektöre özel uygulama kılavuzu vardır.**
→	11.4.6, 11.4.7	←
11.4.8 Kullanıcıların taşıyıcı sistemlerin kimliğini doğrulaması (Telecommunications carrier identification and authentication by users)	**X**	**X**

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
X	**X**	**11.4.8 Harici süreç kontrol sistemlerinin mantıksal bağlantısı** (Logical coupling of external process control systems)
	11.5 İşletim Sistemi Erişim Denetimi	
→	11.5.1	←
→	11.5.2 Kullanıcı tanımlaması ve doğrulaması	**Sektöre özel uygulama kılavuzu vardır.**
→	11.5.3, 11.5.4	←
→	11.5.5 Oturum zaman aşımı	**Sektöre özel uygulama kılavuzu vardır.**
	11.6 Uygulama Erişimi Denetimi	
→	11.6.1, 11.6.2	←
	11.7 Mobil Bilgi İşlem ve Uzaktan Çalışma	
→	11.7.1, 11.7.2	←
	12.1 Bilgi Sistemlerinin Güvenlik Gereksinimleri	
→	12.1.1 Güvenlik gereksinimlerinin analizi ve özelleştirilmesi	**Sektöre özel uygulama kılavuzu vardır.**
	12.2 Uygulamaların Doğru Çalışması	
→	12.2.1, 12.2.2, 12.2.3, 12.2.4	←
	12.3 Kriptografik Kontroller	

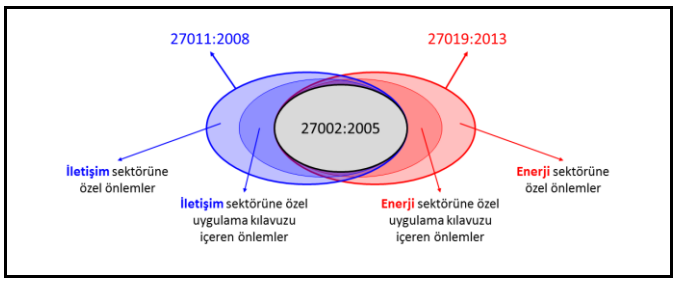
27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
→	12.3.1, 12.3.2	←
	12.4 Sistem Dosyalarının Güvenliği	
Sektöre özel uygulama kılavuzu vardır.	12.4.1 Çalışmakta olan sistem yazılımın denetimi	**Sektöre özel uygulama kılavuzu vardır.**
→	12.4.2, 12.4.3	←
	12.5 Geliştirme ve Destek Süreçlerinde Güvenlik	
→	12.5.1, 12.5.2, 12.5.3, 12.5.4, 12.5.5	←
	12.6 Teknik Açıklık Yönetimi	
→	12.6.1	←
Sektöre özel uygulama kılavuzu vardır.	13.1.1 Bilgi güvenliği olaylarının rapor edilmesi	←
→	13.1.2 Bilgi güvenliği zafiyetlerinin rapor edilmesi	←
	13.2 Bilgi Güvenliği Olaylarının Yönetimi ve İyileştirmeler	
Sektöre özel uygulama kılavuzu vardır.	13.2.1 Sorumluluklar ve prosedürler	←
Sektöre özel uygulama kılavuzu vardır.	13.2.2 Bilgi güvenliği olaylarından deneyim edinme	←
	14.1 İş Sürekliliği Yönetiminin Bilgi Güvenliği Boyutu	

27011:2008 (İletişim)	27002:2005	27019:2013 (Enerji)
Sektöre özel uygulama kılavuzu vardır.	14.1.1 İş sürekliliği yönetim sürecinin bilgi güvenliğini içermesi	**Sektöre özel uygulama kılavuzu vardır.**
→	14.1.2	←
Sektöre özel uygulama kılavuzu vardır.	14.1.3 Bilgi güvenliğini içeren iş sürekliliği planlarının geliştirilmesi ve uygulanması	←
→	14.1.4, 14.1.5	←
X	**X**	**14.2 Başlıca acil hizmetler** (Essential emergency services)
X	**X**	**14.2.1 Acil durum iletişimi** (Emergency communication)
	15.1 Yasal Gereklere Uyumluluk	
→	15.1.1 İlgili yasaların belirlenmesi	**Sektöre özel uygulama kılavuzu vardır.**
→	15.1.2, 15.1.3, 15.1.4, 15.1.5, 15.1.6	←
15.1.7 İletişimin Gizliliği (Non-disclosure of communciations)	**X**	**X**
15.1.8 Temel haberleşme (Essential communications)	**X**	**X**
15.1.9 Acil eylemlerin yasallığı (Legality of emergency actions)	**X**	**X**

27011:2008 (İletişim)	**27002:2005**	**27019:2013 (Enerji)**
	15.2 Güvenlik Politikası ile Uyum ve Teknik Uyum	
→	15.2.1, 15.2.2	←
	15.3 Bilgi Sistemi Denetimi İle İlgili Hususlar	
→	15.3.1, 15.3.2	←
13 sektöre özel önlem ***26 sektöre özel uygulama kılavuzu***	***133 Kontrol***	***11 sektöre özel önlem*** ***31 sektöre özel uygulama kılavuzu***

Tablo-1. 27002, 27011 ve 27019 standartlarındaki önlemlerin karşılaştırılması

Tablonun içeriğini aşağıdaki şekille özetlemek de mümkündür:



Şekil-2. 27002, 27011 ve 27019 standartlarındaki önlemlerin karşılaştırılması

27002 standardında bulunmayıp enerji sektörüne özel uygulama kılavuzu 27019'da yer alan önlemler gözden geçirildiğinde, şu konularda hassasiyet gösterildiği gözlenmektedir:

a. Sistem kontrol merkezlerinde yaşanabilecek aksaklıkların neden olabileceği geniş kapsamlı etkiler göz önünde bulundurularak, kontrol merkezlerinin, merkezlerde kritik cihazların bulunduğu odaların ve kontrol merkezlerine ev sahipliği yapan tesislerin fiziksel ve çevresel güvenliğinin sağlanması.

b. Enerji sektörünün (üretim, iletim, dağıtım vb.) çok katmanlı, kurumlararası etkileşimli yapısı göz önünde bulundurularak, paydaş kurumların ve müşterilerin tesislerinde yer alan sistem bileşenlerinin güvenliğinin sağlanması, kontrol ve iletişim sistemleri arasındaki bağlantıların yönetilmesi, izlenmesi ve gerektiğinde paydaşların sistemlerinden ayrılmak üzere tedbirler alınması.

c. Özellikle geniş alanlara yayılan dağıtım ve iletim sistemlerinde söz konusu olabilecek riskler göz önünde bulundurularak, süreç kontrol verisinin gizlilik, bütünlük ve sürekliliğinin güvence altına alınması.

d. Kurumsal bilişim sistemlerinden çok daha uzun süre hizmet veren ve güvenlik işlevlerinden yoksun olabilen Endüstriyel Kontrol Sistemlerin'den kaynaklanan risklerden korunma.

e. Kurum içinden ve paydaş kurumlardan afet ve acil durumlarda iletişim halinde kalınması gereken personel ile ve vazgeçilmez kontrol sistemleri ile muhaberenin sürdürülmesini ve olağanüstü durumun atlatılmasını güvence altına alacak planlamanın yapılması, önlemlerin alınması.

27019 standardında yukardaki konuların herbiri ile ilgili olarak son derece somut öneriler bulunmaktadır.

27011 standardının da benzer başlıklara yoğunlaştığı görülmektedir. İlave olarak SPAM (yığın E-posta) ve DoS (servis dışı bırakma) saldırılarına dikkat çekilmekte ve bu bağlamda alınabilecek önlemlerden bahsedilmektedir.

Standartlarda dile getirilen risklerin tamamı, Türkiye için de söz konusu olan risklerdir. Şöyle ki, kritik enerji altyapıları her tür fiziksel ve çevresel riskle karşı karşıyadır. Türkiye, geniş bir coğrafyaya yayılmış olması dolayısı ile enerji altyapıları geniş alan ağları ile haberleşmektedir. Enerji altyapılarında miyadı dolmuş kontrol sistemleri ile karşılaşmak sürpriz olmamaktadır. Afet ve acil durumlar Türkiye'de gündelik yaşamın ayrılmaz, nerede ise kanıksanmış parçası haline gelmiştir. Her tür bilgi sistemine SPAM ve Dos saldırıları yapılmaya devam etmektedir. Dolayısı ile standartlarda dile getirilen önerilerin yurdumuz için de gerekli ve geçerli olduğu, Kritik Enerji Altyapısı işleten kuruluşlar tarafından gözden geçirilmelerinin son derece faydalı olacağı kesindir.

VI. SONUÇ

EPDK, elektrik, petrol ve doğal gaz piyasalarında lisanslı faaliyet gösteren kurumların bazılarına TS ISO/IEC 27001 standardına uyum mecburiyeti getirmiştir. 27001 standardına uyum kapsamında, kurumda mevcut risklerin işlenmesi için 27002 standardında yer alan önlemlerin bir bölümünün uygulanması da gerekir. Bu aşamada, enerji ve iletişim sistemlerine özel 27011 ve 27019 standartlarının da faydalı olacağı unutulmamalıdır. Yürürlüğe girme tarihi olarak belirtilen 1 Mart 2016 ile birlikte bilgi güvenliği yönetim sistemini bir kurumda kurmak ve çalıştırmak için bir yılı aşkın süre gerektiği de kurumlar tarafından göz önünde bulundurulmalıdır.

REFERANSLAR

[1] 4890 sayılı Bakanlar Kurulu Kararı-Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, T.C. Resmi Gazete, 20 Haziran 2013

[2] "COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", Official Journal of the European Union, 23.12.2008.

[3] Kritik Altyapı Sektörleri, ABD Anayurt Güvenliği Bakanlığı resmi web sitesi, http://www.dhs.gov/critical-infrastructure-sectors 10 Ocak 2015'de erişildi.

[4] EKS-BOME 2013 Yılsonu Raporu, (ICS-CERT Year in Review, Industrial Control Systems Cyber Emergency Response Team, 2013), https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf , 10 Ocak 2015'de erişildi.

[5] 4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanun, EPDK resmi web sitesi, http://www.epdk.gov.tr/index.php/epdk-hakkinda , 10 Ocak 2015'de erişildi.

[6] Elektrik Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik, EPDK resmi web sitesi, www.epdk.gov.tr/documents/elektrik/mevzuat/yonetmelik/elektrik/lisans/Epdk_Ynt_Deg_EPLY_26122014_29217.doc , 10 Ocak 2015'de erişildi.

[7] Doğal Gaz Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik, EPDK resmi web sitesi, www.epdk.gov.tr/documents/dogalgaz/mevzuat/yonetmelik/dogalgaz/lisans/Ddp_Ynt_Deg_Lisans_26122014.docx , 10 Ocak 2015'de erişildi.

[8] Petrol Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik, EPDK resmi web sitesi, www.epdk.gov.tr/documents/petrol/mevzuat/yonetmelik/petrol/lisans/Ppd_Ynt_Deg_Lisans_26122014.docx , 10 Ocak 2015'de erişildi.

[9] Orhan Çalık, "ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardındaki Değişiklikler ve Yenilikler", Ulusal Bilgi Güvenliği Kapısı. http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html , 10 Ocak 2015'de erişildi.

[10] Fikret Ottekin, "Çok Katmanlı ISO 27001 Süreci", Ulusal Bilgi Güvenliği Kapısı. http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/cok-katmanli-iso-27001-sureci.html , 11 Ocak 2015'de erişildi.

[11] Fikret Ottekin, "Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli 27002 Kontrolleri", Ulusal Bilgi Güvenliği Kapısı. http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html , 11 Ocak 2015'de erişildi.

[12] ISO/IEC TR 27019:2013 (en) Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27019:ed-1:v1:en , 10 Ocak 2015'de erişildi.

[13] ISO/IEC 27011:2008 (en) Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 https://www.iso.org/obp/ui/#iso:std:iso-iec:27011:ed-1:v1:en , 10 Ocak 2015'de erişildi.

Fikret Ottekin, 1990 yılında Orta Doğu Teknik Üniversitesi Elektrik–Elektronik Mühendisliği Bölümünden mezun olmuştur. 1992 yılında aynı bölümde yüksek lisans çalışmasını tamamlamıştır.
1992-2007 tarihleri arasında ASELSAN Haberleşme Cihazları Grubunda çeşitli sivil ve askeri projelerde yazılım mühendisi ve tasarım lideri olarak çalışmış, yurt içinde ve yurt dışında görevlerde bulunmuştur.
2007-2015 yılları arasında TÜBİTAK Siber Güvenlik Enstitüsü'nde başuzman araştırmacı olarak görev yapmıştır. Bilişim teknolojileri ürünlerinin ortak kriterler uyarınca belgelendirilmesi, siber güvenlik ve ISO 27001 tabanlı bilgi güvenliği yönetim sistemleri konularında danışman olarak çalışmıştır. 2012-2013 yıllarında "Kritik Altyapılarda Bilgi Güvenliği Yönetimi" projesinin yöneticiliğini yapmıştır. Siber Güvenlik Kurulu Sekreterya'sına Ulusal Siber Güvenlik Yönetimi konusunda danışmanlık yapmış, Ulusal Siber Güvenlik Stratejisi ve Eylem Planlarının hazırlanmasına katkı sunmuştur.
Fikret Ottekin Eylül 2015 tarihinden itibaren ICterra A.Ş.'de Genel Müdür Danışmanı olarak görev yapmaktadır.

Orhan Çalık, 2011 yılında Berlin Teknik Üniversitesi Bilişim (İnformatik) Bölümünden lisans ve yüksek lisans derecesini alarak mezun olmuştur.
Şu anda Tübitak Bilgem Siber Güvenlik Enstitüsü'nde Siber Güvenlik Hizmetleri Birimi'nde Uzman Araştırmacı olarak çalışmaktadır.
ISO 27001 tabanlı bilgi güvenliği yönetim sistemleri konularında çeşitli kamu kurum ve kuruluşlarında danışman olarak çalışmıştır.
Kritik altyapılarda bilgi güvenliği, ülkelerin siber güvenlik stratejileri, kurumsal bilgi güvenliği yönetimi, risk analizi ve yönetimi konularında çalışmaya devam etmektedir.