Enerji Piyasası Düzenleme Kurumundan:

ENERJİ SEKTÖRÜNDE KULLANILAN ENDÜSTRİYEL KONTROL SİSTEMLERİNDE BİLİŞİM GÜVENLİĞİ YÖNETMELİĞİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç

MADDE 1 - (1) Bu Yönetmeliğin amacı; kritik enerji altyapılarında kullanılan endüstriyel kontrol sistemlerinin (EKS) bilişim süreçlerinin izlenmesi, sistem sürekliliğinin sağlanması ile siber güvenliğinin sağlanmasına ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 - (1) Bu Yönetmelik; enerji piyasasında faaliyet gösteren ve Enerji Piyasası Düzenleme Kurumu tarafından kritik altyapı olarak belirlenen yükümlü kuruluşların EKS'lerinde kullanılan bilişim sistemlerinin güvenliği ve güvenilirliğinin sağlanması için risklerin değerlendirilerek azaltılması veya ortadan kaldırılmasına ilişkin uygulanacak usul ve esasları kapsar.

Dayanak

MADDE 3 - (1) Bu Yönetmelik; 20/2/2001 tarihli ve 4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanunun 5 inci maddesinin altıncı fıkrasının (e) bendi ile Ulusal Siber Güvenlik Stratejisi ve Eylem Planına dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 - (1) Bu Yönetmelikte geçen;

a) Başkan: Enerji Piyasası Düzenleme Kurumu Başkanını,

b) Bildirim: Yükümlü kuruluşlarca Kuruma verilen beyanı,

c) Endüstriyel Kontrol Sistemi (EKS): Enerjinin üretilmesi, enerji sağlayan ham petrol, taş kömürü ve benzeri hammaddelerin işlenip tüketime hazır hale getirilmesi, enerjinin iletim veya dağıtım katmanları aracılığı ile aktarılması gibi süreçlerin bir veya birden fazla merkezden izlenmesini, bazen de yönetilmesini sağlayan, kendisi ve/veya bileşenleri bilinen işletim sistemleri üzerinde koşan ya da bilinen zafiyetleri bulunan özel işletim sistemine sahip yönetim ve kontrol sistemlerini (Veri Tabanlı Kontrol ve Gözetleme Sistemi "SCADA", Dağıtılmış Kontrol Sistemi "DKS", Gelişmiş Süreç Kontrol Sistemi "APC", Programlanabilir Mantık Kontrolcüsü "PLC", Uzak Terminal Ünitesi (RTU) vb.),

d) İlgili mevzuat: Enerji piyasasına ilişkin kanun, yönetmelik, tebliğ, genelge, lisans ve Kurul kararlarını,

e) Kanun: 20/2/2001 tarihli ve 4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanunu,

f) Kurumsal Bilişim Sistemi (KBS): Kuruluş çalışanları tarafından kullanılan bilgisayarlar, bunlara hizmet veren dosya, uygulama, veri tabanı ve e-posta sunucusu ve ağ altyapısının tamamını,

g) Kritik Enerji Altyapısı: İşlevlerini kısmen veya tamamen, yerine getiremediğinde, toplumsal düzenin sürdürülebilirliğinin ve/veya kamu hizmetlerinin sunumunun olumsuz etkileneceği enerji ağı, varlığı, sistemi ve yapıları bütününü,

h) Kurul: Enerji Piyasası Düzenleme Kurulunu,
i) Kurum: Enerji Piyasası Düzenleme Kurumunu,
j) Yükümlü kuruluş: Bu Yönetmelik çerçevesinde tanımlanan sorumlu tüzel kişileri,
ifade eder.

(2) Bu Yönetmelikte geçen ve birinci fıkrada yer almayan tanım ve kısaltmalar için ilgili mevzuatta geçen tanım ve kısaltmalar geçerlidir.

İlkeler

MADDE 5 - (1) Bu Yönetmeliğin uygulanmasında aşağıda belirtilen temel ilkeler gözetilir:

a) Hizmet kalitesinin yükseltilmesi ve enerji arzının sürekliliğinin sağlanması,
b) Ulusal düzenleme ile ulusal ve/veya uluslararası standartların dikkate alınması,
c) Kaynakların düzenli, şeffaf ve etkin kullanımının sağlanması,
d) Lisans sahibi tüzel kişilerin bu Yönetmelik kapsamında EKS bilişim güvenlik önlemlerini almalarının ve uygulamalarının temini,
e) Enerji zincirindeki kritik sistemlerin tehdit ve zafiyetlere karşı güvenliğinin arttırılması.

İKİNCİ BÖLÜM
Yükümlü Kuruluşlar ve Yükümlülükleri

Yükümlü kuruluşlar

MADDE 6 - (1)Yükümlü kuruluşlar elektrik iletim lisansı sahibi, OSB dağıtım lisansı sahipleri hariç olmak üzere elektrik dağıtım lisansı sahibi, OSB üretim lisansı sahibi hariç olmak üzere geçici kabulü yapılmış ve işletmedeki kurulu gücü 100 MWe ve üzeri lisansa sahip her bir elektrik üretim tesisi sahibi, boru hattı ile iletim yapan doğal gaz iletim lisansı sahibi, sevkiyat kontrol merkezi kurmakla yükümlü doğal gaz dağıtım lisansı sahibi, doğal gaz depolama lisansı sahibi (LNG, yer altı depolama), ham petrol iletim lisansı sahibi ile rafinerici lisansı sahibi tüzel kişilerden oluşur.

EKS tanıma ve EKS envanter formları

MADDE 7 - (1) EKS tanıma formu, yükümlü kuruluşların EKS'lere ilişkin işlettikleri süreçlerin, bilgi güvenliği konusunda yaptıkları çalışmaların ve kaynak bilgilerinin yer aldığı formdur.

(2) Kurum tarafından EKS envanterine ilişkin talep edilecek varlık grupları, türleri ve bu varlıklara ilişkin özel bilgilerin yer aldığı form yükümlü kuruluşlara iletilir.

(3) EKS'ler ile ilişkili olmayan KBS bileşenleri kapsam dışındadır.

(4) EKS tanıma formunun yer aldığı bildirim, 27/5/2014 tarihli ve 29012 sayılı Resmî Gazete'de yayımlanan Enerji Piyasası Bildirim Yönetmeliği kapsamında bildirim yükümlülük tablolarında belirlenen yöntemlerle ve tanımlanan süreler içerisinde yükümlü kuruluşlarca Kuruma bildirilir, EKS envanter formu ise talep edildiğinde Kurum tarafından erişilebilecek bir altyapıda oluşturulur ve kuruluşun kendi sistemlerinde saklanır.

Risk yönetimi

MADDE 8 - (1) Risk yönetiminin amacı, yükümlü kuruluşların sahip olduğu EKS'lere yönelik risklerin tespit edilmesi, değerlendirilmesi, risklerin ortadan kaldırılması veya gerçekleşmesi durumunda etkilerinin azaltılması için aksiyonların tespit edilmesi, bu aksiyonların hayata geçirilmesi ve gereklerinin yerine getirilip getirilmediğinin takibini sağlamaktır.

(2) Yükümlü kuruluşların EKS'lere yönelik risklerinin tespiti için yaptırdıkları güvenlik analizi ve testlerinin usul ve esaslarını belirlemeye Kurul yetkilidir.

(3) Kurum tarafından belirlenerek risk envanterine eklenen riskler, yükümlü kuruluşlarca kendi EKS'leri dikkate alınarak değerlendirilir. Değerlendirilen riskler ile ilgili mevcut durumda uygulanan kontroller de dikkate alınarak, çok yüksek, yüksek ve normal risk seviyesinde bulunan riskler risk işlemeye tabi tutulur ve yükümlü kuruluş tarafından risk azaltma yöntemi belirlenen riskler için riskleri azaltmaya yönelik aksiyonlar planlanır.

(4) Kurum tarafından belirlenen risklerin yanında yükümlü kuruluşlar kendi faaliyetleri doğrultusunda belirledikleri riskleri de değerlendirir. Bu risklerin yer aldığı geri dönüşler değerlendirilerek risk envanterinin zenginleştirilmesi sağlanır.

Risklerin işlenmesi ve yükümlü kuruluşların sorumluluğu

MADDE 9 - (1) Kurum tarafından belirlenen ve yükümlü kuruluşların kendilerinin belirlediği risklerde hangilerinin azaltılması gerektiği, hangilerinin ise kabul edildiği yükümlü kuruluş tarafından kararlaştırılır.

(2) Azaltılması kararlaştırılan riskler için kuruluşun sorumluluğunda olacak risk azaltıcı aksiyonların açıkça planlandığı bir tedavi planı oluşturulur. Risk tedavi planında her bir risk için aşağıdaki bilgilere yer verilir:

a) Risk ile ilgili kısa açıklama,

b) Riski azaltmak için uygulanacak kontrol(ler),

c) Uygulanması planlanan kontrollerle ilgili aktiviteler,

d) Kontrolün uygulanması ile ilgili zaman sınırı.

(3) Yükümlü kuruluş;

a) Kurum tarafından belirlenen riskler ile kendi belirlediği risklerin yılda bir kez değerlendirilmesini sağlar,

b) Risk tedavi planını risk değerlendirme akabinde hazırlar ve altı ayda bir risk tedavi planının güncellenmesini içeren çalışmanın yapılmasını sağlar,

c) Riskleri azaltmak için, Kurul tarafından belirlenen enerji sektöründe EKS güvenlik kontrolleri arasından ilgili kontrolleri seçebilir veya ulusal/uluslararası standartlardan, dünyadaki en iyi uygulamalardan ve kendisinin belirleyeceği özel önlemleri uygular,

d) Risklerin gerçekleşme olasılığına göre önceliklendirilmesini ve yüksek dereceli risklerin öncelikle tedavi edilmesini sağlar,

e) İnsan kaynağı ve maddi kaynak sağlayarak risk tedavi planını uygular,

f) EKS envanterinde veya ağ topolojisinde önemli değişikliklerin gerçekleşmesi ile sunucularda meydana gelen kesinti/yetkisiz erişim vb. olayların ardından ilişkili risk değerlendirmesini dolayısıyla risk tedavi planı ve önlemlerin gözden geçirilmesini, gerekiyorsa ilave önlemlerin alınmasını sağlar.

(4) Herhangi bir nedenle azaltılamayan riskler hakkında Kurum adına gerçekleştirilecek denetim sonrasında karar verilir.

Enerji sektöründe EKS güvenlik kontrolleri

MADDE 10 - (1) EKS Güvenlik kontrolleri, EKS'lere yönelik riskleri tedavi etmek, yükümlü kuruluşların bilgi güvenliği seviyesini artırmak, EKS'ler üzerinde olası diğer risklerin gerçekleşme olasılığını azaltmak amacıyla uygulanması önerilen kontrolleri tanımlamaktadır. Bu kontrollerin belirlenmesinde Kurul yetkili olup kontroller Kurum tarafından belirtilen bir veya birden fazla riski tedavi etmek için kullanılabilir.

(2) Kurul tarafından tanımlı kontroller öneri mahiyetinde olup, yükümlü kuruluş sorumluluğunda olmak kaydıyla değiştirilerek veya ekleme yapılmak suretiyle uygulanabilir.

(3) Kontroller Kurul tarafından belirlenip Kurum internet sitesi ana sayfasında yayımlanır.

ÜÇÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Bildirimlerin yapılışı

MADDE 11 - (1) Yükümlü kuruluşların bu Yönetmelik kapsamındaki yükümlülüklerini içeren bildirimler Enerji Piyasası Bildirim Yönetmeliği kapsamında, bildirim yükümlülük tablolarında tanımlanır, yükümlü kuruluşlarca Enerji Piyasası Bildirim Sistemi aracılığı ile Kuruma gönderilir.

(2) Bildirimlerin yapılabilmesi için, Kurum tarafından ilave yöntemler belirlenebilir.

Denetim

MADDE 12 - (1) Kurum, yükümlü kuruluşların bu Yönetmelikte belirtilen yükümlülüklerini yerine getirip getirmediğini re'sen veya şikâyet üzerine denetler veya denetlettirir.

(2) Yapılacak denetimlerin usul ve esaslarını belirlemeye Kurul yetkilidir.

Yaptırımlar

MADDE 13 – (1) Kanunda ve bu Yönetmelikte belirlenen süreler içerisinde yerine getirilmemiş yükümlülükler hakkında, Kurumca durumun tespiti halinde ilgisine göre 14/3/2013 tarihli ve 6446 sayılı Elektrik Piyasası Kanununun 16 ncı, 18/4/2001 tarihli ve 4646 sayılı Doğal Gaz Piyasası Kanunu (Elektrik Piyasası Kanununda Değişiklik Yapılması ve Doğal Gaz Piyasası Hakkında Kanun)'nun 9 uncu, 4/12/2003 tarihli ve 5015 sayılı Petrol Piyasası Kanununun 19 ve 20 nci maddeleri hükümleri uygulanır.

Geçiş süreci

GEÇİCİ MADDE 1 – (1) Yükümlü kuruluşlar 2017 yılı için bu Yönetmelik kapsamındaki sorumluluklarından EKS tanıma ve EKS risk değerlendirmesi formlarını içeren bildirimi Yönetmeliğin yürürlüğe girdiği tarihte Kuruma göndermekle yükümlüdür.

(2) EKS envanter formunu içeren bildirim, Yönetmeliğin yürürlüğe girdiği tarihte kuruluşların sistemlerinde hazır bulundurulur.

Yürürlük

MADDE 14 – (1) Bu Yönetmelik yayımı tarihinden itibaren 2 ay sonra yürürlüğe girer.

Yürütme

MADDE 15 – (1) Bu Yönetmelik hükümlerini Enerji Piyasası Düzenleme Kurumu Başkanı yürütür.