YÖNETMELİK

Enerji Piyasası Düzenleme Kurumundan:

Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1- (1) Bu Yönetmeliğin amacı; enerji sektöründe kullanılan endüstriyel kontrol sistemlerinin siber güvenliğini sürekli olarak gelişen ihtiyaç ve tehditlere göre iyileştirmeye, asgari kabul edilebilir güvenlik seviyesini tanımlamaya ve bu kontrol sistemlerinin siber dayanıklılığına, yeterliliğine ve olgunluğuna ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik; elektrik iletim lisansı sahibi, elektrik dağıtım lisansı sahibi, 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), ham petrol iletim lisansı sahibi ile rafinerici lisansı sahibi tüzel kişilerden oluşan kuruluşların endüstriyel kontrol sistemlerinin güvenliğinin ve güvenilirliğinin sağlanmasına ilişkin uygulanacak hükümleri kapsar.

(2) OSB dağıtım lisansı sahipleri ile OSB üretim lisansı sahipleri kapsam dışındadır.

Dayanak

MADDE 3- (1) Bu Yönetmelik; 20/2/2001 tarihli ve 4628 sayılı Enerji Piyasası Düzenleme Kurumunun Teşkilat ve Görevleri Hakkında Kanunun 5 inci, 5/A ve 5/B maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

a) Başkan: Enerji Piyasası Düzenleme Kurumu Başkanını,

b) Bilgi ve İletişim Güvenliği Rehberi: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan ve bünyesinde bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, Devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmeler tarafından uyulması gereken bilgi ve iletişim güvenliği tedbirlerini içeren rehberi,

c) Bilgi ve İletişim Güvenliği Denetim Rehberi: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan ve Bilgi ve İletişim Güvenliği Rehberi çalışmalarının denetim usul ve esaslarını tanımlayan rehberi,

ç) 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 çalışan 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" ve benzeri),

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) Kritik Altyapılar Ulusal Test Yatağı Merkezi: Sakarya Üniversitesi bünyesinde kurulan kritik enerji altyapılarının modellenmesi ve güvenliği ile ilgili koruyucu ve önleyici çözümlerin araştırılması ve geliştirilmesi amacıyla kurulan merkezi,

g) Kurul: Enerji Piyasası Düzenleme Kurulunu,

ğ) Kurum: Enerji Piyasası Düzenleme Kurumunu,

h) Yükümlü kuruluş: 2 nci maddede tanımlanan sorumlu tüzel kişileri,

ifade eder.

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

İKİNCİ BÖLÜM
İlişkili Düzenlemeler, Yetkinlik Modeli Ana Kontrolleri, Yetkinlik Seviyeleri, Sektörel Kritiklik Derecesi Belirleme

İlişkili düzenlemeler

MADDE 5- (1) Yetkinlik modeli, aşağıda listelenen düzenleme ve uyumluluk gereksinimlerini adresler:

a) Bilgi ve İletişim Güvenliği Rehberi: Yükümlü kuruluşlar, bilgi sistemleri altyapı uyumluluğu için Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan bu rehberi referans alır.

b) Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları: Yetkinlik modeli, bu Kurul kararına uyumluluk usul ve esaslarını kapsar.

c) TS ISO/IEC 27001: Yetkinlik modeli kapsamında TS ISO/IEC 27001 uyumluluğunun devamı sağlanır. Modele kapsayıcı ve EKS odaklı yeni kontroller eklenmiştir.

ç) TS EN ISO/IEC 27019: Yetkinlik modeli kapsamına EKS odaklı yeni kontroller eklenmiştir.

d) Enerji sektöründe EKS güvenlik kontrolleri: Yetkinlik modeli kapsamında bu dokümanda yer alan kontroller kapsamlı olarak ele alınır.

Yetkinlik modeli ana kontrol başlıkları

MADDE 6- (1) Yetkinlik modeli, enerji alt sektörleri özelinde farklılık göstermekle birlikte aşağıda listelenen başlıklardan oluşur:

a) Endüstriyel ağ güvenliği; endüstriyel altyapılar için yerel ağ güvenliği, geniş alan ağı güvenliği, iletişim güvenliği, protokol güvenliği, kablosuz ağ güvenliği, entegrasyon güvenliği kontrollerini içerir.

b) Endüstriyel istemci ve sunucu güvenliği; endüstriyel altyapıda yer alan tüm istemci ve sunuculara ilişkin mantıksal ve fiziksel güvenlik kontrollerini içerir.

c) Endüstriyel tehdit ve zafiyet yönetimi; endüstriyel altyapılarda uygulanan tehdit ve zafiyet yönetimi kontrollerini içerir.

ç) Endüstriyel siber güvenlik risk yönetimi; endüstriyel altyapının dinamiklerine uygun endüstriyel siber güvenlik risk yönetimi kontrollerini içerir.

d) Endüstriyel varlık, değişim ve konfigürasyon yönetimi; endüstriyel altyapılarda bulunan varlıkların yönetimi, bileşenlerin değişim ve konfigürasyon yönetimi kontrollerini içerir.

e) Endüstriyel kimlik ve erişim yönetimi; endüstriyel altyapıda bulunan bileşenler için kimlik ve erişim yönetimi kontrollerini içerir.

f) Endüstriyel olay yönetimi ve süreklilik; endüstriyel siber güvenlik olay yönetimi, süreklilik, yedekleme ve yedeklilik kontrollerini içerir.

g) Akıllı cihaz güvenliği; sayaç ve nesnelerin interneti teknolojisinin kullanıldığı endüstriyel altyapılar için güvenlik kontrollerini içerir.

ğ) Endüstriyel operasyon güvenliği; endüstriyel operasyon güvenliğine yönelik kontrolleri içerir.

h) İnsan kaynakları güvenliği; kritik enerji altyapılarında çalışan tüm personel için istihdam öncesi, sırası ve sonrasında uygulanması gereken kontrolleri içerir.

ı) Fiziksel güvenlik; endüstriyel altyapıların sektörlerine uygun, dağıtık veya tekil yapıdaki fiziksel ortamların güvenlik kontrollerini içerir.

i) Tedarikçi yönetimi; endüstriyel altyapılar için teknoloji, insan ve altyapı tedarikçilerine ilişkin siber güvenlik kontrollerini içerir.

j) PLC güvenliği; PLC güvenliğine ilişkin güvenlik kontrollerini içerir.

(2) Her bir ana kontrol başlığı kendi içerisinde alt kontrol başlıklarına bölünerek ele alınır.

Yetkinlik seviyeleri

MADDE 7- (1) Yetkinlik modeli kapsamında üç temel yetkinlik seviyesi bulunmakta olup yükümlü kuruluşların sahip olmaları gereken yetkinlik seviyesi, Kurum tarafından belirlenen sektörel kritiklik dereceleri ile tespit edilir. Her bir seviye için açıklamalar aşağıdaki şekildedir:

a) Seviye 1: Giriş seviyesi kontroller, bu seviyede yer alır. İlgili kontrollerin hali hazırda uygulandığı ya da kolayca uygulanabileceği değerlendirilen maddeler bu seviyede toplanır. Bu seviyede yer alan maddeleri, hedeflenen tamamlama süresinde uygulamak zorunludur.

b) Seviye 2: İkinci aşama kontroller, bu seviyede yer alır. İlgili kontrollerin uygulanabilmesi için yükümlü kuruluş sistemlerinde veya süreçlerinde değişiklik yapılmasını gerektiren maddeler bu seviyede toplanır. Bu seviyede yer alan maddeleri, hedeflenen tamamlama süresinde uygulamak zorunludur.

c) Seviye 3: Üçüncü seviye kontroller, bu seviyede yer alır. Bu seviyede yer alan kontroller yeni bir projelendirme ya da uzun soluklu değişim gerektirir. Bu seviyede yer alan maddeleri, hedeflenen tamamlama süresinde uygulamak zorunludur.

ç) Ek kontrol: Zorluk derecesi yüksek ya da uygulanması faydalı olabileceği değerlendirilen kontroller, bu seviyede toplanmış olup uygulanması zorunlu değildir.

(2) Her bir seviyede yer alan kontrollerin uygulanması için hedeflenen tamamlama süresi; enerji alt sektörlerine göre farklılık göstermekte olup bu Yönetmelik eklerinde yer alan sektörel yetkinlik modeli dokümanlarında açıklanır.

(3) Üç yıllık periyotlarda, Kurum tarafından yapılacak güncellemeler ile kontrol maddeleri ve kontrol maddeleri için tespit edilen yetkinlik seviyeleri değiştirilebilir.

Sektörel kritiklik derecesi belirleme

MADDE 8- (1) Yükümlü kuruluşların zorunlu olarak gerçekleştirmeleri gereken kontrol maddeleri belirlenirken aşağıdaki tablolarda yer alan sınıflandırma kullanılır:

Sektör	Asgari Seviye	Kritiklik Derecesi
Elektrik Dağıtım	Seviye 2	Yükümlü kuruluşa özel
Doğal Gaz Dağıtım	Seviye 1	Yükümlü kuruluşa özel

Kritiklik Derecesi	Açıklama	Asgari Seviye
A Sınıfı	İlgili sektörde kritiklik derecesi en yüksek olan yükümlü kuruluşların sınıfını ifade eder.	Seviye 3
B Sınıfı	İlgili sektörde kritiklik derecesi orta olan yükümlü kuruluşların sınıfını ifade eder.	Seviye 2
C Sınıfı	İlgili sektörde kritiklik derecesi beklenen seviyede olan yükümlü kuruluşların sınıfını ifade eder.	Seviye 1

(2) Birinci fıkrada yer alan tablolardaki sınıflandırma, sektörün asgari yetkinlik seviyesi ve sektörde yer alan yükümlü kuruluşların kritiklik derecesinden oluşur. Asgari seviye parametresi, sektörel olarak belirlenmekte olup yükümlü kuruluşlar bu seviyeye uyumlu hareket eder. Kritiklik derecesi ise Kurumca çeşitli parametreler kullanılarak belirlenmekte olup belirlenen kritiklik derecelerine göre uygulanan asgari kontrol maddelerine yeni kontroller eklenebilir.

(3) Sektörlerin kritiklik derecelendirmesinde kullanılan parametreler, Kurum tarafından üç yıllık periyotlarda güncellenebilir, bu periyotların sonunda yapılan değerlendirmelerde yükümlü kuruluşların kritiklik dereceleri değişebilir.

ÜÇÜNCÜ BÖLÜM
Yetkinlik Modeli Uygulama, Uyumluluk ve Denetim

Uygulama

MADDE 9- (1) Yetkinlik modeli uygulama yükümlülüğü, Kurum tarafından kritiklik dereceleri belirlenip yükümlü kuruluşlara tebliğ edildiğinde başlar.

(2) Yükümlü kuruluşlar, kritiklik dereceleri ve sektörleri özelinde hazırlanmış olan yetkinlik modeli asgari seviye kontrolleri kapsamında yükümlülüklerini gerçekleştirir.

(3) Yükümlü kuruluşlar, hedeflenen tamamlama süresinde uygulamakla yükümlü oldukları kontrolleri değerlendirirken aşağıda yer alan uyum sınıflandırmasını kullanır.

a) Tam uyum: Yetkinlik modeli kapsamında yer alan ana kontrol başlıklarında bulunan her bir kontrol maddesine ilişkin gereksinimin modelde yazıldığı şekilde karşılanması durumudur.

b) Kısmen uyum: Yetkinlik modeli kapsamında yer alan ana kontrol başlıklarında bulunan her bir kontrol maddesine ilişkin gereksinimin tam olarak karşılanamadığı, geçici ya da iyileştirici önlemlerin uygulandığı durumdur.

c) Uyumsuz: Yetkinlik modeli kapsamında yer alan ana kontrol başlıklarında bulunan her bir kontrol maddesine ilişkin gereksinimin hiçbir şekilde karşılanamadığı durumdur.

ç) Kapsam dışı: Yetkinlik modeli kapsamında yer alan alt kontrol başlıklarında birbirine alternatif olabilecek teknoloji veya yöntem bulunması durumunda yükümlü kuruluşta mevcut bulunan teknoloji ve yönteme uygun kontrollerin uygulanması, diğer alternatif teknoloji ve yöntemlere ilişkin kontrol maddelerinin kapsam dışı bırakılması durumudur.

(4) Yükümlü kuruluşlar, yükümlü oldukları kontrol maddelerine hedeflenen tamamlama süresi sonunda tam uyumlu olmak zorundadır.

(5) Kontrollerin uygulanmasında hedeflenen tamamlama süresi, aşağıda adları belirtilen sektörler özelinde hazırlanan ve Ek-1 ile Ek-2'de yer alan yetkinlik modeli dokümanlarında açıklanır:

a) Elektrik Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri.

b) Doğal Gaz Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri.

Uyumluluk ve denetim

MADDE 10- (1) Yükümlü kuruluşların yetkinlik modeline uyumluluğu üç aşamada gerçekleştirilir. Bu aşamalar şunlardır:

a) Öz denetim/fark analizi: Öz denetimler, yükümlü kuruluşların ilgili kontrol maddelerini kendi iç kaynakları ile denetlemesi sürecidir. Bu aşama, bir fark analizi olarak değerlendirilir. Bu sürecin, yükümlülüklerin başlamasından itibaren üç ay içerisinde tamamlanması gerekir.

b) Sektörel denetim: Sektörel denetimler, Kurumun bu Yönetmelik kapsamında belirlediği şartlara uyan firma ve personeli tarafından gerçekleştirilen çalışmalardır. Bu çalışmalar, bağımsız denetim olarak değerlendirilir.

c) Kurum denetimleri: Kurumun; öz kaynakları ile denetçi firmaları ve yükümlü kuruluşları denetlediği çalışmalardır. Bu çalışmalar çapraz denetim ya da kontrol denetimi olarak değerlendirilir. Kurum, bu denetimleri süreç içerisinde her zaman yapabilir.

(2) Yükümlü kuruluşlar, öz denetim/fark analizini tamamladıktan sonra en geç bir ay içerisinde Kuruma raporlarını Enerji Piyasası Bildirim Sistemi aracılığı ile iletir.

(3) Yükümlü kuruluşlar, her bir yetkinlik seviyesinde yer alan kontroller için; tanımlanan uygulama süreleri sonunda Kuruma ilerleme raporlarını enerji piyasası bildirim sistemi aracılığı ile iletir.

(4) Yetkilendirilmiş denetim firmaları, sektörel denetimleri yetkinlik modeline uygun seviye süreçlerinin tamamlanmasından itibaren on iki ay içerisinde yaparak, denetim raporlarını en geç bir ay içerisinde Kuruma enerji piyasası bildirim sistemi aracılığı ile iletir.

(5) Yükümlü kuruluşlar, belirlenen asgari yetkinlik seviyesine ulaşmalarının ardından bu Yönetmelik eklerinde sektörler özelinde hazırlanan yetkinlik modeli dokümanlarında yer alan hedeflenen tamamlama süresi periyotlarında, sektörel denetimlerini tekrarlamak zorundadır.

(6) Yükümlü kuruluşlar, öz denetim/fark analizi çalışmaları esnasında danışmanlık hizmeti almaları durumunda sektörel denetimi, danışmanlık hizmeti aldıkları firma ile gerçekleştiremez. Danışmanlık ve sektörel denetim hizmetleri, alt yüklenici kullanmak suretiyle de gerçekleştirilemez.

(7) Sektörel denetim, aynı firma ile üst üste en fazla üç kez gerçekleştirilebilir.

Denetçi firma ve personelinde aranacak yetkinlikler

MADDE 11- (1) Bilgi ve İletişim Güvenliği Denetim Rehberinde hizmet alımı ile oluşturulan denetim ekibi için belirlenen kriterlere ek olarak, yetkinlik modeli denetimlerini yapacak firma personelinde Kritik Altyapılar Ulusal Test Yatağı Merkezi tarafından verilen EKS eğitimleri sonrası başarı sertifikası aranır.

Denetçi firmanın yetki başvurusu sırasında Kuruma sunması gereken bilgi ve belgeler

MADDE 12- (1) Yetkinlik modeli denetimi faaliyetinde bulunmak isteyen firmaların, taleplerini başvuru dilekçesi ile Kuruma iletmeleri gerekir. Kuruma verilecek başvuru dilekçesine 11 inci maddede belirtilen bilgi ve belgeler eklenir.

Denetim yapma yetkisinin verilmesi

MADDE 13- (1) Yetkinlik modeli denetimi yapmak üzere Kuruma başvuruda bulunan firmalar, 12 nci maddede belirtilen bilgi ve belgeler çerçevesinde Kurum tarafından değerlendirilir. Mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından yapılacak değerlendirme sonucunda denetim faaliyetlerini yürütebilecek yeterliliğe sahip olduklarının tespit edilmesi halinde firmaya, denetim yapma yetki sertifikası verilir ve bu firma yetkinlik modeli denetim kuruluşları listesine eklenir.

(2) Yetki başvurularının değerlendirilmesi sürecinde, Kurum tarafından gerekli görülmesi halinde ilave bilgi ve belgeler talep edilebilir. Talep edilen bilgi ve belgeler yetkinin verilmesine ilişkin değerlendirmelerde dikkate alınır.

(3) Bu Yönetmelik kapsamında denetim yapma yetkisinin alınmasını sağlayan unsurların devamlılığı esastır. Kurum gerekli gördüğü durumlarda bu unsurların varlığını her zaman kontrol edebilir.

(4) Bu Yönetmelik kapsamında denetim yapma yetkisi verilen firmaların unvanları, Kurumun internet sitesinde yayımlanır.

Denetim yapma yetkisinin kaldırılması

MADDE 14- (1) Denetçi firma, 12 nci maddesi kapsamında sahip olması gereken nitelikleri gösterir bilgi ve belgeleri altı aylık periyotlarda Kuruma resmî olarak iletmekle yükümlüdür.

(2) Denetçi firma, 12 nci madde kapsamında sahip olması gereken niteliklerin bir veya birkaçını kaybetmesi durumunda en geç bir hafta içerisinde Kurumu resmî olarak bilgilendirir. Söz konusu bilgilendirmenin süresi içinde yapılmadığının tespiti durumunda ilgili firmanın denetim yapma yetkisi sona erdirilir ve tespitin yapıldığı tarihten itibaren ilgili firma üç yıl süre ile denetçi firma yetkisi alamaz.

(3) Denetçi firmanın Kurum tarafından istenilen bilgi ve belgeleri, Kuruma vermemesi halinde denetim yapma yetkisi sona erdirilir.

(4) Firma, denetim yetkisinin sona erdirilmesinin ardından yeniden yetki talebinde bulunursa 12 nci ve 13 üncü madde hükümleri uygulanır.

(5) Bu Yönetmelik kapsamında denetim yapma yetkisi sona erdirilen firmaların unvanları Kurumun internet sitesinde yayımlanır.

DÖRDÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Düzenlemeler

MADDE 15- (1) Yükümlü kuruluşların EKS'lere yönelik risklerinin tespiti için yaptırdıkları güvenlik analizi ve testlerinin usul ve esaslarını belirlemeye Kurul yetkilidir.

(2) Enerji sektöründe EKS güvenlik kontrolleri, Kurul tarafından belirlenip Kurum internet sitesinde yayımlanır.

Yürürlükten kaldırılan yönetmelik ve atıflar

MADDE 16- (1) 13/7/2017 tarihli ve 30123 sayılı Resmî Gazete'de yayımlanan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği yürürlükten kaldırılmıştır.

(2) Mevzuatta, birinci fıkra ile yürürlükten kaldırılan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliğine yapılan atıflar bu Yönetmeliğe yapılmış sayılır.

Yürürlük

MADDE 17- (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 18- (1) Bu Yönetmelik hükümlerini Enerji Piyasası Düzenleme Kurumu Başkanı yürütür.

Ekleri için tıklayınız