KURUL KARARI

Enerji Piyasası Düzenleme Kurumundan:

KURUL KARARI

Karar No: 11956 **Karar Tarihi:** 13/07/2023

Enerji Piyasası Düzenleme Kurulunun 13/07/2023 tarihli toplantısında; aşağıdaki "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın Resmi Gazete'de yayımlanmak üzere Cumhurbaşkanlığına gönderilmesine,

karar verilmiştir.

ENERJİ SEKTÖRÜNDE KULLANILAN ENDÜSTRİYEL KONTROL SİSTEMLERİ İÇİN GÜVENLİK ANALİZ VE TEST USUL VE ESASLARI

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1 – (1) Bu Usul ve Esasların amacı, enerji sektöründe kullanılan endüstriyel kontrol sistemlerinde (EKS) yetkisiz erişim elde edilmesine veya hassas bilgilere ulaşılmasına ve sistem sürekliliğinin aksamasına neden olabilecek güvenlik açıklıklarının sömürülmeden önce tespit edilip giderilmesinin sağlanmasıdır.

Kapsam

MADDE 2 – (1) Bu Usul ve Esaslar aşağıda belirtilen hususlarla sınırlı olmamak kaydıyla:

a) EKS ağının ve mimari yapının incelenmesi analizini,
b) EKS yapılarında görevli personele yönelik sosyal mühendislik testlerini,
c) EKS ağında zafiyet tarama analizini,
ç) EKS ağında zararlı yazılım analizini,
d) EKS kablosuz ağ ve bileşenleri testlerini,
e) EKS ağında sömürü testlerini,

kapsar.

Hukuki dayanak

MADDE 3 – (1) Bu Usul ve Esaslar; 6/6/2023 tarihli ve 32213 sayılı Resmi Gazetede yayımlanan Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliğinin 15 inci maddesinin birinci fıkrasına dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Usul ve Esaslarda geçen;

a) Aktif tarama: Genellikle otomatize edilmiş araçlarla gerçekleştirilen ve ortamda mevcut cihazlara da gerektiğinde erişim sağlanan taramayı,

b) APN: Mobil iletişim altyapısı üzerinde sanal özel ağ kurulmasını sağlayan teknolojiyi,

c) Bilmesi gereken prensibi: Herhangi bir konu veya işi, ancak görev ve sorumlulukları gereği öğrenmekle, incelemekle, gereğini yerine getirmekle ve korumakla sorumlu bulunanların yetkisi düzeyinde bilgi sahibi olması ve nüfuz etmesini,

ç) DKS: EKS'lerin "dağıtık kontrol sistemi" bileşenini,

d) EKS: Endüstriyel Kontrol Sistemlerini,

e) Gömülü Sistem: Bir bilgisayardan farklı olarak, kendisi için önceden özel olarak tanımlanmış görevleri yerine getirmek üzere tasarlanmış, çekirdeği belirli bir sayıda görevi yerine getirmek için programlanan mikroişlemcilerden ya da mikro denetleyicilerden oluşan, üzerinde güncellenebilir yazılımların çalıştığı RTU, PLC, MTU gibi sistemleri,

f) Güvenlik duvarı: EKS'lerin bulunduğu ağı korumaya yönelik konumlandırılan ve erişim kontrolü yapmak için kullanılan bileşeni,

g) HMI: EKS'lerin "insan-makine arayüzü" bileşenini,

ğ) IDS: EKS'lerin bulunduğu ağı korumaya yönelik konumlandırılan "saldırı tespit sistemi" bileşenini,

h) IED: Bir veya birden fazla işlemciye sahip, harici bir kaynaktan veri alma veya gönderme özelliğine sahip akıllı elektronik cihazları,

ı) IP: Internet Protokolünü,

i) IPS: EKS'lerin bulunduğu ağı korumaya yönelik konumlandırılan "saldırı önleme sistemi" bileşenini,

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

k) KBS: Kurumsal Bilişim Sistemlerini,

l) Kurul: Enerji Piyasası Düzenleme Kurulunu,

m) Kuruluş:6/6/2023 tarihli ve 32213 sayılı Resmî Gazetede yayımlanan Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliğinin 2 nci maddesinde tanımlanan sorumlu tüzel kişileri,

n) Kurum: Enerji Piyasası Düzenleme Kurumunu,

o) MTU: EKS'lerin "ana telemetri birimi" bileşenini,

ö) OSI: Açık sistemler bağlantısını,

p) OSINT: Açık kaynak istihbaratını,

r) Pasif tarama: Cihazlara erişim sağlanmadan sadece ağ trafiğinin analizi ile yapılan taramayı,

s) PLC: EKS'lerin "programlanabilir mantık denetleyici" bileşenini,

ş) PERA: Purdue Kurumsal Referans Mimarisini,

t) RF: Radyo frekansını,

u) RTU: EKS'lerin "uzak terminal birimi" bileşenini,

ü) SCADA: EKS'lerin "merkezi denetim ve veri toplama" bileşenini,

v) Sömürü Testi: Bir uygulamada veya sistemdeki bir güvenlik açığından yararlanarak hedef sistem veya uygulama üzerinde yetki elde etme işlemini,

y) Zafiyet tarama: Ağ altyapılarındaki güvenlik açıklarının belirlenmesi ve sınıflandırılması işlemini,

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

aa) VoIP: IP üzerinden video, ses ya da mesaj gönderilmesini,

ifade eder.

(2) Bu Usul ve Esaslarda geçen ve birinci fıkrada yer almayan tanım ve kısaltmalar için ilgili mevzuatta geçen tanım ve kısaltmalar esas alınır.

İKİNCİ BÖLÜM
Güvenlik Analiz ve Test Metodolojisi

EKS ağının ve mimari yapının incelenmesi analizi

MADDE 5 – (1) Bu analizde EKS'nin bulunduğu mevcut ağ yapısı incelenerek güvenlik pratikleri açısından değerlendirilmesi sağlanır. Bu amaçla, incelenen yapıların mantıksal topolojisi, uzak saha bağlantılarını da içerecek şekilde analizi gerçekleştiren kişi tarafından oluşturulur. Eğer kuruluş tarafından bir topoloji bilgisi sağlanır ise, bunun güncel olup olmadığı ve mevcut durumu yansıtıp yansıtmadığı doğrulanır. Yapılan analiz ile EKS'yi oluşturan IP'ye sahip MTU, RTU, HMI, SCADA/DKS sunucu, yönlendirici, anahtar gibi bileşenlerin ağ üzerindeki konumları belirlenir. Analiz sonucunda, ilgili bileşenlerin topolojideki konumlarına istinaden EKS'leri etkileyebilecek, erişilebilirlik, bütünlük ve gizlilik açılarından tehdit unsuru oluşturan riskler bulgu olarak ortaya konulur.

(2) EKS ağının ve mimari yapının incelenmesi aşağıdaki başlıkların detaylı analizini ve raporlamasını içerir:

a) Topoloji analizi,

b) Konfigürasyon analizi,

c) EKS sınır güvenliği analizi,

ç) Erişim analizi,

d) Diğer analizler:

1) Yetkili hesap yönetimi,

2) Kurum altyapısındaki varlıkların konumlandırılması,

3) İnternete erişebilen varlıklar,

4) İnternetten erişilebilen varlıklar,

5) SSL kullanımı,

6) İş sürekliliği analizi.

(3) EKS ağının ve mimari yapının incelenmesi çalışmaları, bu altyapıya hâkim kuruluş personeli ile soru-cevap şeklinde ve altyapıda OSI 3 üncü katmanda çalışmakta olan ağ ve güvenlik cihazlarının yapılandırmalarını ve erişim politikalarını inceleyerek gerçekleştirilir. Bu kapsamda yapılması öngörülen analizlerin detayları konu başlıklarına göre aşağıdaki gibidir:

a) Topoloji Analizi: Topoloji analizi çalışması sırasında EKS altyapısında çalışmakta olan ve IP adresine sahip sunucu, ağ bileşenleri, güvenlik bileşenleri ve MTU, RTU, HMI, PLC gibi saha ekipmanları soru-cevap ya da saha incelemesi ile belirlenir. Belirlenen ağ cihazlarından OSI 3 üncü katmanda çalışmakta olanların yapılandırmalarını incelemek için, ara yüz bağlantısı sağlanır ve yapılandırma çıktısı temin edilir. Elde edilen verilerle mevcut altyapının topoloji çizimi sağlanır. Mevcut topolojiye göre EKS altyapısı için yüksek erişilebilirlik olmaması durumu, IDS/IPS bulunmaması gibi riskli konular bulgu olarak raporlanır.

b)Konfigürasyon Analizi: Konfigürasyon analizi çalışması sırasında kritik öneme sahip omurga anahtarı, güvenlik duvarı, IDS/IPS gibi ağ ve güvenlik cihazlarının yapılandırmaları incelenerek bu sistemlerin yedekliliği, güvenlik duvarının SSL denetimi yapması ve segmentasyon gibi konular değerlendirilir. Mevcut altyapıda rutin işleyişin aksamasına sebebiyet verebilecek yedeklilik yapılandırmasının eksik/yanlış olması, ağdaki diğer sistemlere sıçrama riskini minimize edecek segmentasyon yapılandırmasının olup olmaması gibi riskli konular bulgu olarak ortaya konur.

c)EKS Sınır Güvenliği Analizi: Bu analiz ile EKS altyapısını tehdit eden unsurların EKS altyapısına etki etmeden önce engellenebilmesi adına alınan;

1) İş ihtiyacı olan güvensiz servislerin güvenli olan alternatifleri ile değiştirilmesi,

2) EKS ağında, internete hizmet veren sistemlerin bulundurulmaması,

3) EKS ve KBS ağlarında IDS/IPS sistemlerinin mevcudiyeti,

4) 802.1x ile bağlantı kontrolü yapılması,

konuları denetlenir ve riskli konular bulgu olarak raporlanır.

ç) Erişim Analizi: Erişim analizi çalışması sonucu KBS ve EKS ağları arasındaki erişimlerin durumu ortaya konur. Bu çalışma esnasında;

1) EKS ağında kamu ve hizmet sağlayıcıların erişimleri gibi zorunlu olarak sağlanması gereken bağlantıların uygun şekilde yapılandırılmış olması,

2) EKS ağı ile kuruluşta çalışan kullanıcıların e-posta alma-gönderme, kurumsal sistemlere erişim, dosya sunucusuna erişim, İnternet erişimi gibi kurumsal işlemlerini gerçekleştirdikleri bilgisayarların/tabletlerin/telefonların bulunduğu ağ arasında kontrol edilen ve tanımlanmış izleme gibi erişimlerin haricinde bir erişimin olmaması,

3) Mevcut erişim izinlerinin bilmesi gereken prensibine uygunluğu,

gibi konular denetlenir.

d) Diğer Analizler:

1) Yetkili Hesap Yönetimi: Yetkili hesap yönetimi konusunda gerçekleştirilen analiz çalışması ile EKS'de kullanılmakta olan hesapların yetkilendirmesinin nasıl yapıldığı, parola yönetimi ve bilmesi gereken prensibinin uygulanıp uygulanmadığının denetimi gerçekleştirilir.

2) Kuruluş Altyapısındaki Varlıkların Konumlandırılması: Kuruluş altyapısındaki varlıkların konumlandırılması incelenirken PERA, NIST SP800-82r2 ve SANS Secure Architecture for Industrial Control Systems dokümanlarında belirtilen en iyi uygulama örneklerine uygun ve/veya IEC-62443 standartlarına uyumlu ağ segmentasyonu yapılıp yapılmadığı denetlenir.

3) İnternete Erişebilen Varlıklar: EKS altyapısında İnternete erişebilen varlıkların bulunup bulunmadığı incelenir, varsa gerekliliklerinin sorgulanması ile birlikte İnternete erişimlerin hangi izinlerle gerçekleştiği ortaya konur.

4) İnternetten Erişilebilen Varlıklar: EKS altyapısında İnternetten erişilebilen varlıkların bulunup bulunmadığı incelenir, varsa gerekliliklerinin sorgulanması ile birlikte ne amaçla ve hangi izinlerle erişildiği belirlenir.

5) SSL Kullanımı: EKS altyapısında kullanıcı arayüzlerinin şifre ile korunup korunmadığı ve bunların SSL üzerinden hizmet verip vermediği belirlenir.

6) İş Sürekliliği Analizi: İş sürekliliği analiz çalışmasıyla kuruluşun mevcut EKS altyapısındaki bileşenlerden herhangi birinde sorun yaşanması durumunda rutin işleyişin aksamamasını sağlayacak önlemlerin alınıp alınmadığı belirlenir. Güvenlik ve ağ cihazlarında problem olması durumunda fiziksel bir yedeğinin olup olmadığı ve yapılandırma yedeklerinin düzenli olarak alınıp alınmadığı kontrol edilir.

(4) Bu analiz çalışması kapsamında, bir kontrol listesi üzerinden hareket edilmesi önerilir. Bu liste yukarıdaki analiz yöntemlerinin gereksinimlerini kapsayacak şekilde hazırlanmalı ve herhangi bir gereksinimin gözden kaçmasını önlemek için takip edilmelidir. Bunun yanında, ağ ve güvenlik cihazları üzerinde konfigürasyon incelemeleri, temin edilecek IP bazlı envanter listesi, ağ topolojisi, ilgililere sorulacak soruların bulunduğu soru listeleri ve güvenlik duvarı analiz yazılımı gibi otomatik analiz araçları kullanılabilir.

EKS yapılarında görevli personele yönelik sosyal mühendislik testleri

MADDE 6 – (1) Sosyal mühendislik testleri ile, EKS ağına erişim yetkisi olan personelin güvenlik davranışları ve farkındalık seviyeleri analiz edilir.

(2) EKS yapılarında görev yapan personele yönelik yapılacak olan sosyal mühendislik testi siyah kutu veya beyaz kutu olarak uygulanabilir. Uygulanacak yönteme göre test kapsamı belirlenir. Kuruluş tarafından siyah kutu testi istenildiği takdirde, testi gerçekleştirecek ekip kuruluş personeline ait bilgileri pasif tarama yöntemleriyle araştırıp kuruluşun bilgisi dâhilinde kapsamı belirler. Beyaz kutu olması halinde test kapsamı kuruluş tarafından belirlenip testi gerçekleştirecek ekibe verilir.

(3) EKS yapılarında görevli personele yönelik yapılacak sosyal mühendislik testleri aşağıdaki yöntemler kullanılarak gerçekleştirilir:

a) Siyah Kutu: Siyah kutu yöntemiyle gerçekleştirilecek olan sosyal mühendislik testinde, testi gerçekleştirecek kişi kurumdan daha önceden kapsam bilgisi almadan OSINT

araçları ile kuruluşa özel saldırı vektörlerini geliştirmek amacıyla e-posta adreslerini, telefon numaralarını ve fiziksel güvenlik kontrolleri ile ilgili bilgileri toplar. Bu bilgilerin kullanımı ve uygulanacak senaryolar kuruluş yetkilisinin onayına sunulur.

b) Beyaz Kutu: Beyaz kutu yöntemiyle gerçekleştirilecek sosyal mühendislik testinde kuruluş tarafından, testi gerçekleştirecek kişiye, kapsam dâhilindeki personelin telefon numaraları, e-posta adresleri ve fiziksel lokasyon bilgileri verilir. Bu bilgilerin kullanımı ve uygulanacak senaryolar kuruluş yetkilisinin onayına sunulur.

(4) EKS'lere yönelik gerçekleştirilecek sosyal mühendislik testlerinde OSINT araçları kullanılarak kuruluş ve kuruluş personeline ait bilgiler toplanır. Toplanan bilgiler sosyal mühendislik testi gerçekleştirmek amacıyla kullanılır.

(5) Toplanan bilgiler doğrultusunda kuruluş personelinin farkındalık seviyesini tespit etmeye yönelik oltalama testi gerçekleştirilir. Bu test gerçekleştirilirken, zararlı eklenti barındıran e-posta veya sahte web sitelerine yapılan yönlendirmelerle hassas kuruluş bilgileri veya operasyonel bilgilerin toplanması gibi farklı yöntemler kullanılabilir. Testler kapsamında, 7/4/2016 tarihli ve 29677 sayılı Resmi Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu'na aykırı olarak değerlendirilebilecek kişisel veriler alınmamalıdır.

(6) Kuruluş personeline yönelik sesle oltalama testinde hassas personel bilgileri ele geçirilmeye çalışılır. Test, telefon numaralarını taklit ederek veya farklı bir kimlik bilgisiyle aranarak gerçekleştirilir. Test kapsamında VoIP, cep telefonu veya dâhili hatlar gibi farklı erişim kanalları kullanılır.

(7) Fiziksel güvenlik değerlendirmesinde, kuruluşların fiziksel güvenlik kontrolleri çeşitli atlatma teknikleri kullanılarak yerinde denetlenir ve kuruluşun iyileştirme yapması gereken alanlar belirlenir. Fiziksel güvenlik testinde;

a) Video gözetimi,

b) İzole alanlara erişim,

c) Güvenlik görevlilerinin kuruluşun inisiyatifinde olacak şekilde atlatılması/kandırılması,

test edilir.

(8) Test edilecek şirket politikaları asgari olarak:

a) Yabancılara/misafirlere yönelik uygulamalar,

b) Kilit, şifre ve biyometrik sistemler gibi geçiş kontrollerinin etkinliği,

c) Çöpe atılan kritik bilgilerin elde edilmesi,

ç) Taşınabilir donanımların kullanımına yönelik çalışanların farkındalığı,

konularından oluşur.

EKS ağında zafiyet tarama analizi

MADDE 7 – (1) Kuruluşun EKS ağındaki bileşenlere yönelik zafiyet taramasının pasif tarama yöntemleriyle gerçekleştirilmesi esastır. Teknik olarak pasif tarama yapılamaması durumunda ise bu maddede belirtilen uygun aktif tarama yöntemlerinden biri kullanılır. Yapılan tarama sonrasında keşfedilen zafiyetlerin doğrulaması ve bu zafiyetlerin sömürülmesi sonucu oluşabilecek etkilerin değerlendirilmesi yapılır. Tespit edilen zafiyetler aynı zamanda sömürü testlerinde saldırı yöntemlerinin belirlenmesi için kullanılır.

(2) Kuruluşta aktif zafiyet tarama;

a) Duruş yapılabilen EKS'lerde duruş esnasında,

b) Parçalı duruş yapılabilen EKS'lerde sadece duruş yapılan EKS'ler üzerinde,

c) Duruş yapılamayan EKS'lerde, enerji talebinin düşük olduğu dönemlerde EKS'leri en az etkileyecek şekilde,

ç) Yukarıdaki seçenekler değerlendirilemiyor ise, testin neden olabileceği riskler detaylı olarak analiz edildikten sonra uygun görülen bir ortamda,

yapılır.

(3) Test yaptıracak kuruluşların, EKS'de kullanılan tüm bileşenlerin aynı yazılım sürümleri ve yapılandırma ayarlarıyla birlikte var olacağı bir test yatağı hazırlaması canlı

ortamda mevcut olan zafiyetlerin belirlenmesi açısından fayda sağlar. Test yatağının canlı ortam ile uyumluluğu testi gerçekleştirecek uzman tarafından doğrulanır.

(4) Kuruluşun belirtilen koşullarda test yatağı bulunuyorsa bu ortamda aktif zafiyet tarama yöntemiyle gerçekleştirilir. Aksi durumda zafiyet taraması canlı ortamda pasif tarama yöntemiyle gerçekleştirilir. EKS bileşenleri arasında seri haberleşme teknolojileri mevcut ise ve EKS ağı içerisinde seri haberleşme ortamından TCP/IP haberleşme ortamına geçişi sağlayan dönüştürücü varsa bu sistem üzerinden güvenlik testi gerçekleştirilir.

(5) EKS üzerinde zafiyet taraması sırasında dikkat edilmesi gereken hususlar aşağıdaki gibidir:

a) Taranan cihazın işlevinin bozulmayacağından veya bu cihazın kaybının rutin işleyişi etkilemeyeceğinden emin olunmalıdır.

b) Herhangi bir olumsuzluk durumunda teste tabi bileşenin, hızlı bir şekilde eski haline geri döndürülmesi için gerekli hazırlıklar ve planlar yapılmış olmalıdır. Söz konusu durumlar için acil durum eylem planının hazırlanmamış olması mevcut bir zafiyet olarak değerlendirilmelidir.

c) Taranacak sistem yedekli değil ise, yapılacak olan zafiyet tarama işlemi risk teşkil etmeyecek şekilde sınırlandırılmalıdır.

(6) Zafiyet taramasında kullanılacak araç, içerisinde endüstriyel protokollerin ve uygulamaların, EKS ağında bulunan işletim sistemlerinin zafiyetlerini tespit edebilecek özellikler barındırır.

(7) Zafiyet tarama aracı ile bütün bir IP bloğu taraması yapılmaksızın taraması yapılacak olan cihazların IP adresleri tekil olarak tanımlanır ve uygun parametre ile taranır. Parametrelerin seçimi iki farklı yaklaşımla gerçekleştirilir:

a) Açık portların belirlenmesi için port taraması gerçekleştirilir. Tespit edilen bulgulara göre uygun tarama yöntemi ile teste devam edilir. Port taraması yapılırken sisteme zarar vermeyecek parametreler seçilir.

b) Sunucu hakkında kuruluş tarafından verilecek bilgiye göre uygun parametrelerle teste devam edilir.

(8) Servis dışı bırakma ve kaba kuvvet gibi tehlikeli sayılabilecek yöntemler kullanılmamalıdır.

EKS ağında zararlı yazılım analizi

MADDE 8 – (1) Zararlı yazılım analizi ile EKS ağında oluşan trafik analiz edilerek zararlı yazılım kaynaklı herhangi bir iletişimin mevcut bulunup bulunmadığı tespit edilir. Bu tür bir iletişimin tespiti durumunda, anormal trafiğin kaynağı ve EKS bileşenlerine etkisi incelenir.

(2) Bu analiz EKS ağı trafiğinin aynalanabildiği sistemler üzerinde uygulanır. EKS ağı trafiğinin aynalanamadığı ortamlarda işletim sistemi seviyesinde zararlı yazılım tespiti yapılır.

(3) EKS ağı trafiği üzerinde zararlı yazılımın tespit edilebilmesi için yapılacak analiz, EKS ağında mevcut yönlendirici veya anahtarlar üzerinden port aynalaması yapılarak gerçekleştirilir. Port aynalama için elverişli olmayan ortamlarda işletim sistemi seviyesinde, taşınabilir bellek üzerinden kurulum yapmaksızın çalıştırılabilen zararlı yazılım tespit araçları ile zararlı yazılımlar tespit edilir. Gerekli görüldüğü durumlarda zararlı yazılım analizi teknikleri ile zararlı olarak tespit edilen içeriğin EKS bileşenlerine olan etkileri incelenir.

(4) Zararlı yazılım analizi kapsamında imzası henüz bilinmeyen yeni zararlılar veya kurumları hedef alarak hazırlanmış olan gelişmiş kalıcı tehdit saldırılarının da tespit edilip engellenmesi hedeflenir.

(5) Zararlı yazılım analizinin gerçekleştirilmesi için, EKS bileşenlerini ve protokollerini destekleyen zararlı yazılım tespit ve analiz araçlarının kullanılması tercih sebebidir. Bu araçların kullanımı, test yapılacak ortamın kullanılacak yöntemlerde belirtildiği üzere zararlı yazılım tespiti için elverişli olup olmamasına göre belirlenir. Elverişli olan ortamlarda port aynalama yöntemiyle ağ trafiğinin kopyasını alarak ağ trafiği üzerinde zararlı yazılım tespit ve analizi yapan araçlar kullanılır. Elverişli olmayan ortamlarda taşınabilir bellek üzerinden kurulum yapmaksızın çalıştırılabilen zararlı yazılım tespit araçları kullanılır.

EKS kablosuz ağ ve bileşenleri testleri

MADDE 9 – (1) Kablosuz EKS ağları ve kablosuz ağ bileşenleri ile bu ağlar üzerinden haberleşen uygulamaların güvenliği analiz edilir.

(2) Kablosuz ağ testlerinin amacı, kablosuz ağa yetkisiz erişim imkanı olup olmadığının ve ağdaki trafik üzerinde manipülasyon yapılıp yapılamayacağının değerlendirilmesidir. EKS bileşenlerinin bağlı olabileceği kablosuz ağların şifreleme ve anahtar güvenliği, APN yapısı kullanılıyorsa bu sistemlerin güvenlik seviyeleri ve sahte erişim noktaları açılarak kullanıcıların veya operatörlerin tepkileri ölçülür. Bu kapsamda aşağıda belirtilen testler yapılır:

a) 802.11x, 802.15.1 ve 802.15.4 güvenlik testleri,

b) Mobil ağ iletişiminin güvenlik testleri,

c) APN güvenlik testleri,

ç) RF (Radyo Frekans) iletişiminin güvenlik testleri.

(3) Kablosuz ağ keşif çalışmalarının amacı, kuruluş yerleşkesinde bilinen veya bilinmeyen kablosuz ağ erişim noktalarının tespit edilmesidir. Bu kapsamda aşağıdaki özellikler belirlenmeye çalışılır:

a) 802.11x güvenlik testleri kapsamında:

1) Kullanıcı denetimleri,

2) Çevresel tehdit analizleri,

3) Yetkilendirme saldırıları,

4) Erişim noktası hizmeti veren cihazların denetlenmesi,

5) Kablosuz ağ güvenlik çözümlerinin denetlenmesi.

b) 802.15.1 ve 802.15.4 güvenlik testleri kapsamında:

1) İlgili cihazın bileşenlerinin tespit edilmesi,

2) İlgili cihaz hakkında yetkili ve yetkisiz bir şekilde toplanabilecek bilgilerin kontrol edilmesi,

3) İlgili cihazın kullandığı yetkilendirme tipinin test edilmesi,

4) İlgili cihazın kullandığı şifreleme yönteminin test edilmesi.

c) Mobil ağ iletişiminin güvenlik testleri kapsamında:

1) İlgili cihazın bileşenlerinin tespit edilmesi,

2) İlgili cihaz hakkında yetkili ve yetkisiz bir şekilde toplanabilecek bilgilerin kontrol edilmesi,

3) İlgili cihazın mobil ağ iletişimini sağlamak amacı ile kullandığı SIM kartın test edilmesi,

4) İlgili cihazın mobil ağ iletişiminin yayın bozma saldırılarına karşı tepkilerinin ölçülmesi,

5) İlgili cihazın mobil ağ araya girme saldırılarına karşı tepkilerinin ölçülmesi ve elde edilebilecek bilgilerin incelenmesi.

ç) APN güvenlik testleri kapsamında:

1) Kuruluşun vereceği izinler doğrultusunda APN bulutuna dâhil edilmesi,

2) APN bulutuna bağlı cihazların tespit edilmesi,

3) APN bulutundaki cihazların haberleşme protokollerinin tespit edilmesi ve zafiyetlerinin raporlanması.

d) RF iletişimin güvenlik testleri kapsamında:

1) İlgili cihazın bileşenlerinin tespit edilmesi,

2) İlgili cihaz hakkında yetkili ve yetkisiz bir şekilde toplanabilecek bilgilerin kontrol edilmesi,

3) İlgili cihazın RF iletişiminin tekrarlanabilirliğinin test edilmesi,

4) İlgili cihazın RF iletişiminin yayın bozma saldırılarına karşı tepkilerinin ölçülmesi,

5) İlgili cihazın RF araya girme saldırılarına karşı tepkilerinin ölçülmesi ve elde edilebilecek bilgilerin incelenmesi.

(4) EKS kablosuz ağ ve bileşenleri testlerinde, güvenlik ortamında sahte kablosuz yerel ağlar tespit etmek için saldırı tespit ve önleme sensörleri, tarayıcılar gibi araçlar kullanılır. Kablosuz yerel ağları tespit etmek için kablosuz ağ kartları ve test araçları bulunan bir veya daha fazla taşınabilir bilgisayar kullanılır.

EKS ağında sömürü testleri

MADDE 10 – (1) EKS ağında sömürü testleri analiz ve test çalışmasının son adımıdır. Sömürü testlerinin uygulanması için kuruluşun onayı ve uygun şartları sağlaması, testlere dair ön şartların belirlenerek kuruluş tarafından testi yapan firmaya yazılı olarak sunulması gerekmektedir.

(2) Bu testler 3 alt aşamadan oluşur:

a) EKS ağında çalışan bilinen işletim sistemlerine sömürü testleri

1) EKS'nin yönetimi amacıyla kullanılan sunuculardaki işletim sistemlerinin sömürü testlerinin canlı ortamda gerçekleştirilmesi önerilmez. Tespit edilen zafiyetlerin sömürü testi, yükümlü kuruluşun sağlayacağı test yatağında veya canlı ortamı etkilemeyeceği bir sistem üzerinde gerçekleştirilir.

2) İşletim sistemlerinin sömürü testlerini gerçekleştirecek araçlar KBS'lerde sömürü testleri için kullanılan zafiyet sömürü araçları ile aynıdır. Kullanılan işletim sistemleri üzerinde tespit edilen zafiyetler ticari veya açık kaynak kodlu ilgili araçlarla test edilir.

b) EKS ağında çalışan bilinen uygulamalara sömürü testleri

1) Kuruluş tarafından kapsama dâhil edilen veya test sırasında tespit edilen uygulamalar statik ve dinamik olarak test edilir. İlgili uygulamalara, İnternet ortamından veya KBS ağından testin gerçekleştirilmesi gerekir. Yapılan sömürü testi sonucunda zafiyet barındıran uygulamalara erişim ve yetki kontrolü sağlanır. Canlı ortamda yapılan sömürü testi, ilgili uygulamada bazı değişikliklere sebebiyet verebileceğinden risk teşkil etmekte olup, söz konusu testin test yatağı üzerinde gerçekleştirilmesi tavsiye edilir.

2) EKS veya gerektiğinde KBS uygulamalarına özel geliştirilmiş zafiyet sömürü araçları kullanılır.

c) EKS ağında çalışan gömülü sistemlere yönelik sömürü testleri

1) EKS ağı üzerinde ilk katmanda yer alan PLC, RTU, IED gibi bileşenlere yönelik daha önce tespit edilen zafiyetlerin sömürü testleri gerçekleştirilir. Bu aşamada birkaç farklı yöntem kullanılabilir. Söz konusu test, EKS ağı içerisindeki tüm bileşenlerin işletim sistemi, yazılım ve donanım sürümlerinin aynı olması koşulu ile sağlanacak test yatağında gerçekleştirilir. Test yatağı olmaması durumunda yapılacak testler bu Usul ve Esasların 7 nci maddesinin ikinci fıkrasında belirtilen koşullar göz önüne alınarak gerçekleştirilir.

2) Testin bu aşamasında KBS ve EKS için geliştirilmiş zafiyet sömürü testi araçları veya otomatize olmayan teknikler kullanılır. Söz konusu sömürü testi ticari veya açık kaynak kodlu ilgili araçlarla gerçekleştirilir.

Uygulama

MADDE 11- (1) İşletmeye yeni başlayacak olan kuruluşlar faaliyete geçtikten sonra on sekiz ay içerisinde, bu Usul ve Esaslarda tanımlanan güvenlik analiz ve test metodolojisi uyarınca testleri yaptırırlar.

(2) Testler en geç üç yılda bir tekrarlanır.

(3) Teste tabi kuruluş test esnasında envanterinde bulunan EKS bileşenlerine hâkim en az bir uzman personel ve test sürecine refakat edecek bir personel bulundurur.

Güvenlik analiz ve test sonuçlarının takibi

MADDE 12 – (1) Kuruluşlar güvenlik analiz ve testleri sonucu tespit edilen bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri ve bunların yer aldığı rapordaki önerileri dikkate alarak, kendi yönetim kurullarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planını uygular. Güvenlik analizi ve testi sonuçlarının yer aldığı rapor, tamamlanmasının ardından talep edildiği takdirde Kuruma sunulmak üzere saklanır.

(2) Bulgu önem dereceleri beş kategoride ele alınır. Acil, kritik, yüksek, orta ve düşük şeklinde olan kategorilere ilişkin açıklamalar aşağıdaki tabloda yer almaktadır:

Bulgu Önem Derecesi	**Açıklama**
Acil	Niteliksiz saldırgan tarafından kuruluşun dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından kuruluşun dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Kuruluşun dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

(3) Kapsam bölümünde belirtilen başlıkların her biri altında raporlanacak bulguların sunuş biçimi aşağıda yer alan tabloda belirtilmektedir:

Bulgu Referans No	Rapordaki her bulguyu tekil olarak niteleyen harf/rakam dizisi
Bulgu Adı	Bulguyu özet olarak ifade eden tanımlayıcı isim
Önem Derecesi	Bulgunun, aynı maddenin ikinci fıkrasında yer verilen önem derecesi
Etkisi	Bulguda yer verilen açıklığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel sonuç
Kullanılan Yöntem	Bulguya erişimde kullanılan yöntem
Araçlar	Bulguya erişirken kullanılan araçlar
Kullanıcı Profili	Bulguya hangi kullanıcı profili ile erişildiği bilgisi
Erişim Noktası	İnternet, intranet veya spesifik bir ağ segmenti
Bulgunun Tespit Edildiği Bileşen(ler)	Bulgunun tespit edildiği bileşeni niteleyen IP adresi, URL, sistem, servis, sunucu veya varlık adı gibi bilgiler
Bulgu Açıklaması	Bulgunun detaylı açıklaması
Çözüm Önerisi	Bulgunun giderilmesi için testi gerçekleştiren firma tarafından yapılacak çözüm önerisi

Güvenlik analiz ve testlerini yapacak firma/kuruluş ve personelinde aranacak yetkinlikler

MADDE 13 – (1) Güvenlik analiz ve testlerini yapacak firma/kuruluşta aranacak yetkinlikler aşağıda belirtilmiştir:

a) TS 13638 sayılı yeterlilik belgesinin olması,

b) ISO/IEC 27001 belgesinin olması.

(2) Güvenlik analiz ve testlerini yapacak firma/kuruluş personelinde aranacak yetkinlikler aşağıda belirtilmiştir:

a) GICSP sertifikasına sahip olmak ve EKS mimarisi, çalışma prensipleri ve iletişim protokolleri ile ilgili üretici veya üreticilerin yetkilendirdiği firmalardan, eğitim içeriği ve katılım belgesi ibraz edilecek şekilde eğitim almış olmak,

b) *Kritik Altyapılar Ulusal Test Yatağı Merkezi tarafından verilen EKS eğitimleri sonrası başarı sertifikasına sahip olmak,*

c) Ağ güvenliği konusunda uluslararası kabul görmüş kuruluşlardan alınmış Comptia Security+, GSEC, CND, SSCP, CISSP, CNSS vb. sertifikalardan en az birine sahip olmak,

ç) CEH, OSCP, ICS/SCADA Cybersecurity, en az Sertifikalı Sızma Testi Uzmanı seviyesinde olmak üzere TSE Ağ ve Sistem Altyapısı Sızma Testi Uzmanı, GPEN'den en az ikisine sahip olmak,

d) Bu fıkranın (a) ve (b) bentlerinden en az birisini sağlamak.

(3) Kuruluşun güvenlik analiz ve testlerini, bu maddenin ikinci fıkrasında belirtilen yetkinliklere sahip personeli tarafından yapılmak istenmesi durumunda; bu maddenin birinci fıkrasının (a) bendinde yer alan yeterlilik belgesi aranmaz.

(4) Güvenlik analiz ve testlerini yapan personelin en az altı ay güvenlik analiz ve testlerini yapan firmada/kuruluşta çalışıyor olması gerekir.

(5) Güvenlik analizi ve testlerini gerçekleştirecek firma ile kuruluş arasında gizlilik sözleşmesi yapılır.

ÜÇÜNCÜ BÖLÜM
Çeşitli ve Son Hükümler

Yürürlükten kaldırılan düzenleme ve atıflar

MADDE 14 – (1) 3/5/2019 tarihli ve 30763 sayılı Resmî Gazetede yayımlanan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları yürürlükten kaldırılmıştır.

(2) Mevzuatta, birinci fıkra ile yürürlükten kaldırılan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esaslarına yapılan atıflar bu Usul ve Esaslara yapılmış sayılır.

Geçiş süreci

GEÇİCİ MADDE 1 – (1) Bu Usul ve Esasların yürürlüğe girdiği tarihten itibaren yirmi dört ay içerisinde EKS üzerinde güvenlik analizleri ve testleri yaptırılır.

Yürürlük

MADDE 15 – (1) Bu Usul ve Esaslar yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 16 – (1) Bu Usul ve Esasları Enerji Piyasası Düzenleme Kurumu Başkanı yürütür.