



Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli (SGYM) Bağımsız Denetim Hizmeti

EPDK / EBİS

EPDK SGYM Yönetmeliği kapsamında, yetkilendirilmiş bağımsız denetçilerle yürütülen; EBİS üzerinden EPDK'ya sunulmaya hazır resmî sektörel denetim raporu üreten OT/EKS denetimi.

SGYM denetimi

EPDK bağımsız sektörel denetim

EBİS bildirim

SGYM seviye 1 2 3

EKS denetimi

OT güvenlik denetimi

KATEGORİ

Denetim Hizmetleri

TİPİK SÜRE

Kritiklik seviyesine göre asgari 2-3 gün saha denetimi + uzaktan inceleme · Toplam 3-6 hafta

KİMLER İÇİN

Elektrik dağıtım, doğal gaz dağıtım, elektrik üretim, rafineri ve iletim faaliyeti yürüten; A, B veya C kritiklik sınıfında yer alan EPDK lisans sahibi kuruluşlar.

1 Hizmetin Tanımı

Bu hizmet, EPDK tarafından 6 Haziran 2023 tarihinde yayımlanan "Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği" kapsamında; enerji sektörü kuruluşlarının endüstriyel kontrol sistemleri (EKS) ve operasyonel teknoloji (OT) altyapılarının yetkilendirilmiş bağımsız denetçiler tarafından incelenmesi sürecidir. Hizmet, "sıfırdan değerlendirme" yaklaşımıyla SGYM'nin öngördüğü 10'dan fazla ana kontrol başlığının mevcut risk ve gereklilikler temelinde yeniden analiz edilmesini ve kuruluşun zorunlu yetkinlik seviyelerine (Seviye 1, 2, 3) uygunluğunun EPDK standartlarında denetlenerek raporlanmasını kapsar.

2 Neden Gereklidir?

EPDK Yönetmeliği ve 7545 sayılı Siber Güvenlik Kanunu gereğince, kritik altyapı işletmecisi olan enerji kuruluşlarının SGYM uyumluluklarını yetkilendirilmiş bağımsız denetim firmaları aracılığıyla belgelendirmeleri yasal bir zorunluluktur. Ayrıca kuruluşun kritiklik sınıfına (A, B, C) bağlı olarak EBİS üzerinden EPDK'ya sunulması gereken seviye bildirimlerinin ardından, resmî takvime göre en geç 12 ay içinde Bağımsız Sektörel Denetim Raporlarının kuruma iletilmesi gerekmektedir. Zamanında ve usulüne uygun yapılmayan denetimler ağır yaptırımlara ve idari para cezalarına yol açabilmektedir.

YAPTIRIM VE RİSK EŞİĞİ

Seviye bildiriminin ardından 12 aylık yasal süre içinde denetim raporunun sunulmaması idari yaptırım ve lisans süreçlerinde risk doğurur; 7545 sayılı Kanun kapsamındaki denetim yükümlülüğü aykırılıkları ayrıca cezalandırılır.

3 Yasal ve Normatif Dayanak

EPDK SGYM Yönetmeliği — 6 Haziran 2023

7545 sayılı Siber Güvenlik Kanunu

SGYM Denetim Rehberi

ISO/IEC 27019

IEC 62443

NIST SP 800-82

4 Sağladığı Katma Değer

Hukuki katkı

7545 sayılı Kanun ve 6 Haziran 2023 tarihli EPDK SGYM Yönetmeliği uyarınca bağımsız sektörel denetim yükümlülüğü eksiksiz yerine getirilerek, ağır idari yaptırım ve lisans durdurma riskleri ortadan kaldırılır.

Operasyonel katkı

Bağımsız bir gözle yapılan değerlendirme, EKS ve OT ağlarındaki kör noktaları tespit ederek ISO 27019, IEC 62443 ve NIST SP 800-82 gibi uluslararası standartlara uyum durumunuzu şeffaf biçimde ortaya koyar.

Yönetsel katkı

Üst yönetime kurumun siber güvenlik olgunluk seviyesine dair tarafsız bir fotoğraf sunulur. "Kısmen Uyum" ve "Uyumsuz" maddeler netleştirilerek teknoloji, süreç ve insan kaynağı yatırımları için objektif bir karar destek mekanizması sağlanır.

5 Hizmet Kapsamı ve Metodoloji

Genel bakış: SEVIYE 1 Temel Yetkinlik Asgari kontrol seti • C sınıfı SEVIYE 2 Yönetilen Yetkinlik Ölçülen ve izlenen süreçler • B sınıfı SEVIYE 3 İleri Yetkinlik Optimize edilen, kanıtlanan • A sınıfı

AŞAMA 1

Açılış Toplantısı ve Kapsamın Belirlenmesi

OT ağı sınırları, uzak bağlantılar, tedarikçi süreçleri, yardımcı tesisler ve haberleşen tüm sistemlerin yönetmelik beklentilerine göre (Tam Uyum, Kısmen Uyum, Uyumsuz, Kapsam Dışı) bütüncül değerlendirme kapsamının çizilmesi.

AŞAMA 2

Uzaktan Denetim Faaliyetleri

Politika, prosedür, yönerge ve süreç dokümantasyonlarının güvenli paylaşım platformları (hash doğrulamalı) üzerinden uzaktan analiz edilmesi ve SGYM kontrollerine uygunluğunun doğrulanması.

AŞAMA 3

Yerinde (Saha) Kontroller ve Teknik İncelemeler

SGYM Yönetmeliği m. 11'e haiz, Kritik Altyapılar Ulusal Test Yatağı Merkezi sertifikalı uzmanlarımız tarafından canlı sistemler üzerinden fiziksel ve teknik güvenlik kontrollerinin yapılması. Kritiklik seviyesine göre asgari 2 veya 3 günlük saha denetimi.

AŞAMA 4

Teknik İnceleme ve Güvenli Örneklemeler

Ağ cihazı, sunucu/istemci ve güvenlik sistemleri loglarının kuruluşa ait yetkili personel aracılığıyla doğrudan erişim olmadan, canlı ekranlar üzerinden incelenmesi. Dağıtık yapılarda varlık sayısının karekökü (en fazla 5) kuralına uygun metodolojik örneklemeler yapılması.

AŞAMA 5

Mutabakat ve Kapanış Toplantısı

Tespit edilen "Tam Uyum", "Kısmen Uyum", "Uyumsuz" ve "Kapsam Dışı" bulguların kuruluşa sunulması ve resmi mutabakat belgesinin hazırlanması ve imzalanması.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ EPDK SGYM Bağımsız Sektörel Denetim Raporu – EBİS aracılığıyla EPDK'ya sunulmaya hazır, resmî EPDK formatında
- ✓ Resmî Denetim Mutabakat Belgesi – denetim tarihleri, değerlendirilen madde sayıları, örnekleme gerekçeleri ve yasal uyumluluk beyanlarını (danışmanlık/denetim ayrılığı, veri saklanmaması kuralı) içeren tutanak
- ✓ Yönetici Özeti Sunumu – üst yönetim için hazırlanmış durum tespit özeti

HEDEFLenen ÇIKTI / BAŞARI KRİTERİ

- ✓ EPDK SGYM Yönetmeliği (Üçüncü Bölüm, m. 10) uyarınca zorunlu olan bağımsız sektörel denetim süreci, resmî yetkili ve sertifikalı bir kurum aracılığıyla eksiksiz tamamlanır.
- ✓ EPDK'nın resmî bildirim yükümlülükleri hatasız ve zamanında yerine getirilerek cezai müeyyidelerden uzak durulur.
- ✓ Siber güvenlik olgunluğu (Seviye 1, 2 veya 3) şeffaf, ölçülebilir ve kanıtlanabilir biçimde kayıt altına alınır; iç süreçler ulusal ve küresel standartlara göre doğrulanır.

7 Sık Sorulan Sorular

Seviye bildirimimizi yaptık, denetim için ne kadar süremiz var?

Resmî takvime göre seviye bildiriminin ardından en geç 12 ay içinde bağımsız sektörel denetim raporunun kuruma iletilmesi gerekir. Planlamanın erken başlatılması, bulgu kapatma için manevra alanı bırakır.

Denetçiler sistemlerimize doğrudan erişecek mi?

Hayır. Log ve konfigürasyon incelemeleri, kuruluşa ait yetkili personel aracılığıyla canlı ekranlar üzerinden yürütülür; denetim ekibi doğrudan erişim talep etmez ve veri saklamaz.

Tüm sahalarımız denetlenecek mi?

Dağıtık yapılarda varlık sayısının karekökü (en fazla 5) kuralına uygun metodolojik örnekleme uygulanır; örneklem gerekçeleri mutabakat belgesinde kayıt altına alınır.

8 Etiketler

SGYM denetimi

EPDK bağımsız sektörel denetim

EBİS bildirim

SGYM seviye 1 2 3

EKS denetimi

OT güvenlik denetimi

kritiklik sınıfı A B C

enerji sektörü denetim

Bu hizmet, tam hizmet kataloğunun bir parçasıdır. Diğer 11 hizmet ve bütüncül paketler hakkında bilgi için Genel Broşür'e başvurabilirsiniz. Bu doküman bilgilendirme amaçlıdır; hukuki mütalaa veya taahhüt niteliği taşımaz.