KATEGORİ 2 · BÜTÜNCÜL PAKETLER

Enerji Sektörüne Özel Siber Güvenlik, Kurumsal Olgunluk ve Sürdürülebilirlik Paketi

Enerji / EPDK

Holding ve grup şirketlerinin 7545 sayılı Kanun, EPDK mevzuatı, BİGR, SGYM, ISO 27001, IEC 62443 ve ISO 42001 yükümlülüklerini tek potada eriten; IT ve OT'yi birlikte yöneten entegre GRC programı.

enerji siber güvenlik danışmanlığı · EPDK uyum · SGYM · BİGR · IEC 62443 · OT SCADA güvenliği

KATEGORİ
Bütüncül Paketler

TİPİK SÜRE
12 ay ve üzeri · Çoklu şirket yapısına göre ölçeklenir

KİMLER İÇİN
Enerji holdingleri ve grup şirketleri; elektrik/doğal gaz dağıtım ve üretim lisansı sahipleri; rafineri ve iletim operatörleri; birden fazla tesis ve tüzel kişilik yöneten yapılar.

1 Hizmetin Tanımı

Bu hizmet, enerji sektöründe faaliyet gösteren holdinglerin ve grup şirketlerinin karşı karşıya olduğu karmaşık regülasyon (7545 sayılı Kanun, EPDK mevzuatları) ve standart (BİGR, SGYM, ISO 27001, IEC 62443, ISO 42001 vb.) yükümlülüklerini tek bir potada eriterek konsolide eden bütünleşik bir danışmanlık ve yönetişim modelidir. Çevik proje yönetimi prensipleriyle hareket ederek riskleri önceden öngören, ekiplere metodolojik yön gösteren ve know-how transferi gerçekleştiren proaktif bir çözüm ortaklığıdır.

2 Neden Gereklidir?

Kritik altyapı işletmecisi olan enerji kuruluşları; Siber Güvenlik Başkanlığı'nın ulusal vizyonu, 7545 sayılı Kanun'un yasal bağlayıcılığı ve EPDK'nın ağır yaptırımlar içeren ikincil mevzuatları ile her zamankinden daha sıkı bir denetim kıskacındadır. IT için BİGR, OT için SGYM ve IEC 62443, veri gizliliği için KVKK gibi birbirinden farklı regülasyonlar süreç karmaşasına ve efor mükerrerliğine neden olmaktadır. Bu çok başlı yapıyı şemsiye bir GRC modeliyle birleştirmek, operasyonel ve itibar sürekliliği için kaçınılmaz bir gerekliliktir.

> **YAPTIRIM VE RİSK EŞİĞİ**
> EPDK yaptırımları lisans süreçlerini doğrudan etkileyebilmekte; 7545 sayılı Kanun kapsamındaki idari para cezaları 10.000.000 ₺'ye kadar uygulanabilmektedir. Menfaat veya zarar hâlinde ceza üç ilâ beş katına çıkar.

3 Yasal ve Normatif Dayanak

- 7545 sayılı Siber Güvenlik Kanunu
- EPDK SGYM Yönetmeliği
- EKS Güvenlik Usul ve Esasları
- Bilgi ve İletişim Güvenliği Rehberi
- ISO/IEC 27019
- IEC 62443
- 6698 sayılı KVKK

4 Sağladığı Katma Değer

Operasyonel verimlilik (konsolidasyon)

BİGR, SGYM, IEC 62443, ISO 27001 ve KVKK gereksinimleri birbiriyle uyumlandırılarak tekil varlık envanteri ve konsolide risk kütükleri oluşturulur; kurum ekiplerinin mükerrer iş yapmasının önüne geçilir ve maliyet optimizasyonu sağlanır.

Yönetsel ve stratejik vizyon (GRC)

Holding geneli regülasyon ve yapay zekâ (ISO 42001) yönetişim komitelerinin kurulmasına rehberlik edilerek, yönetim kurulu raporlamaları ve KPI'lar aracılığıyla süreçlerin üst yönetim tarafından şeffaf biçimde izlenmesi sağlanır.

Hukuki ve regülatif güvence

7545 sayılı Kanun ve EPDK mevzuatlarındaki değişiklikler proaktif olarak takip edilir; olası EPDK veya Kurul incelemelerinde hukuki ve teknik refakat sağlanarak idari yaptırım riskleri minimize edilir.

Teknik proaktiflik ve dayanıklılık

Sızma testleri, siber tatbikatlar, SOME aktif saha desteği, tehdit avcılığı ve böcek taraması gibi operasyonel güvenlik hizmetleriyle zafiyetler sömürülmeden önce tespit edilir ve kurumun siber kriz müdahale kasları güçlendirilir.

5 Hizmet Kapsamı ve Metodoloji

Genel bakış: TEK ÇATI Enerji Sektörü Entegre GRC Programı BİGR EPDK SGYM IEC 62443 ISO 27001/27019 ISO 42001 KVKK SONUÇ Tekil varlık envanteri · konsolide risk kütüğü · ortak politika seti · tek KPI panosu

MODÜL 1

Regülasyon Uyumu ve Stratejik Yönetişim (GRC)

Enerji mevzuatı takibi (7545 sayılı Kanun, EPDK vb.), etki analizleri ve olası incelemelerde hukuki/teknik süreç refakati. Holding geneli şemsiye komite (GRC, sürdürülebilirlik, yapay zekâ yönetişimi) kurulumuna metodolojik rehberlik. Farklı standartları kapsayan bütüncül politikaların ve KPI'ların tanımlanması. Stratejik yol haritası oluşturma ve çoklu şirket yapısına uygun GRC yazılımı seçimi ile entegrasyon danışmanlığı.

MODÜL 2

Risk Yönetimi ve Denetim

ISO 42001 YZ Yönetim Sistemi danışmanlığı (model risk değerlendirmesi). IT ve OT/EKS (Zone & Conduit mimarisi) için BİGR, ISO ve SGYM standartlarında konsolide tekil varlık envanteri ve risk kütüğü oluşturulması, risk analizi çalıştaylarının yönetimi. EPDK, SGYM ve BİGR iç/dış denetim hazırlık refakati, ön denetimler ve iç tetkikler. Kritik sistem tedarikçilerinin kurum adına resmî standartlara göre denetlenmesi ve düzeltici faaliyet planlarına destek.

MODÜL 3

Siber Güvenlik Operasyonları ve İş Sürekliliği

IT ve OT (SGYM/IEC 62443) ortamları için İş Sürekliliği (BCP/DRP) ve olay/ihlal kök neden analizi süreçlerine rehberlik. IT (BİGR) ve OT/SCADA ortamlarına yönelik detaylı yetkisiz erişim/sızma testleri ve zafiyet analizi. Güvenlik teknolojilerinin IEC 62443 Savunma Derinliği mimarisine uygunluğu konusunda mimari danışmanlık. Kriz anlarında SOME ekiplerine aktif saha desteği (koordinasyon ve adli bilişim analizi) ve kritik sunucular ile OT uç noktalarında tehdit avcılığı. Siber tatbikatların yönetimi ve kontrol odalarında böcek tarama hizmeti.

MODÜL 4

Sürdürülebilirlik, İletişim ve Kültür

Kurumsal iletişim ekiplerine kamuoyu ve regülatör beklentilerini yönetme (PR) stratejilerinde rehberlik. Yılda iki kez oltalama/sosyal mühendislik tatbikatları. Yönetim kurulu ve üst yönetime özel BİGR/SGYM konsolide olgunluk raporlamaları. Kurum ihtiyacına özel eğitimler: tüm çalışanlara BG/KVKK; üst yönetime GRC/Yapay Zekâ Yönetişimi; teknik ekiplere BİGR uyumlu SOME ve SGYM/IEC 62443 esaslı OT/SCADA güvenliği.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ Entegre varlık envanteri, konsolide risk kütüğü ve bütüncül güvenlik politikaları dokümanları
- ✓ Tedarikçi denetim raporları, GAP (fark) analizi ve iç tetkik raporları
- ✓ Detaylı EKS/OT ve IT sızma testi raporu ile tehdit avcılığı (Compromise Assessment) bulguları
- ✓ Yönetim kurulu bilgilendirme sunumları ve siber tatbikat sonuç/gelişim raporu
- ✓ Yönetici (C-Level) raporları ile GRC komite kurulum / çalışma esasları çerçevesi
- ✓ Eğitim katılım/başarı sertifikaları ve sosyal mühendislik test raporları

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ IT, OT (EKS) ve KVKK gibi birbirinden farklı regülatif dikey yükümlülükler, karmaşadan arındırılmış, entegre ve sürdürülebilir bir yönetişim şemsiyesi altında toplanır.
- ✓ Olası denetim (Siber Güvenlik Başkanlığı, EPDK) ve siber kriz anlarında refleksif değil; önceden planlanmış, hukuki ve teknik altyapısı sağlam proaktif bir savunma mekanizması işler.
- ✓ Teknoloji ve insan kaynağı yatırımları, birbirini tekrar eden regülasyonlar için parçalı yapılmak yerine maliyet ve zaman verimliliğini maksimize eden ortak hedeflere kanalize edilir.

7 Sık Sorulan Sorular

Grup şirketlerimizin her biri ayrı ayrı mı ele alınıyor?

Hayır. Model, holding düzeyinde tek bir politika ve risk çatısı kurar; şirket düzeyinde ise yalnızca yerel farklılıklar (lisans türü, tesis yapısı) için ek katman uygulanır. Konsolidasyonun maliyet avantajı buradan doğar.

EPDK incelemesi gelirse ne oluyor?

Hizmet, inceleme süreçlerinde hukuki ve teknik refakat içerir; talep edilen kayıtların derlenmesi, savunma metinlerinin teknik altyapısının hazırlanması ve toplantı refakati kapsamdadır.

Böcek tarama hizmeti neden bu pakette?

Kontrol odaları ve yönetim kurulu toplantı alanları, fiziksel dinleme riski taşıyan yüksek değerli hedeflerdir. Bu risk, siber savunmanın gözden kaçan fiziksel ayağıdır.

8 Etiketler

enerji siber güvenlik danışmanlığı · EPDK uyum · SGYM · BİGR · IEC 62443 · OT SCADA güvenliği · holding GRC · böcek tarama · kritik altyapı · adli bilişim

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.