



Bilgi ve İletişim Güvenliği Rehberi (BİGR) Uygulama Süreci Danışmanlığı

7545 s. Kanun

Kamu kurumları ve kritik altyapı işletmecileri için BİGR uyum sürecini planlamadan BİGDES raporlamasına kadar uçtan uca yöneten, dokümantasyonu sıfırdan kuran sistematik danışmanlık modeli.

BİGR uyum danışmanlığı

BİGDES

7545 sayılı Siber Güvenlik Kanunu

varlık gruplandırma

EK-C.1 kritiklik derecesi

telafi edici kontrol

KATEGORİ

Uyum ve Sürdürülebilirlik Danışmanlıkları

TİPİK SÜRE

Tipik uyum programı 6-9 ay · Yıllık kontrol ve BİGDES döngüsü süreklidir

KİMLER İÇİN

Kamu kurum ve kuruluşları, kritik altyapı işletmecileri (enerji, elektronik haberleşme, finans, ulaştırma, su yönetimi, kritik kamu hizmetleri) ve bunlara hizmet veren bilişim tedarikçileri.

1 Hizmetin Tanımı

Bu hizmet, 7545 sayılı Siber Güvenlik Kanunu ile değişen yasal çerçevede, kamu kurumları ve kritik altyapı işletmecilerinin BİGR uyum sürecini planlamadan denetim raporlamasına kadar uçtan uca yöneten sistematik bir çözüm ortaklığı ve danışmanlık modelidir. Süreç, sadece bir "rehber uyumu" olmanın ötesine geçerek varlıkların belirlenmesini, risklerin minimize edilmesini ve kurumun Siber Güvenlik Başkanlığı'nın denetim standartlarına tam hazır hâle getirilmesini kapsar.

2 Neden Gereklidir?

6 Temmuz 2019 tarihli Cumhurbaşkanlığı Genelgesi ile başlayan BİGR uyumu, dijital varlıkların güvenliği için yasal bir zorunluluktur. Günümüzde bu zorunluluk, 7545 sayılı Siber Güvenlik Kanunu ile doğrudan Siber Güvenlik Başkanlığı'nın denetim ve yaptırım alanına girmiştir. BİGR süreçlerinin ve BİGDES bildirimlerinin eksik, hatalı veya gecikmeli yapılması; kurumların yüksek tutarlı idari para cezalarıyla karşılaşmasına ve ciddi siber zafiyetlere yol açmasına neden olur.

YAPTIRIM VE RİSK EŞİĞİ

7545 sayılı Kanun m. 16 uyarınca siber güvenlik tedbirlerini almama ve bildirim yükümlülüğüne aykırılık 1.000.000 ₺ - 10.000.000 ₺ idari para cezası ile yaptırıma bağlanmıştır. Menfaat temini veya zarar hâlinde ceza, bu menfaat/zararın üç ilâ beş katı olarak uygulanır.

3 Yasal ve Normatif Dayanak

7545 sayılı Siber Güvenlik Kanunu

2019/12 sayılı Cumhurbaşkanlığı Genelgesi

Bilgi ve İletişim Güvenliği Rehberi

Siber Güvenlik Başkanlığı düzenlemeleri

4 Sağladığı Katma Değer

Yasal güvence ve ceza koruması

7545 sayılı Kanun kapsamında yetkili makamlarca uygulanabilecek ağır idari para cezası ve yaptırım riskleri proaktif olarak ortadan kaldırılır.

Mevcut sistemlerle (ISO 27001) tam entegrasyon

Aynı güvenlik seviyesini gerektiren varlıklar izole edilerek gruplandırılır ve mevcut BGYS envanterinizle mükerrer efor yaratmadan birleştirilir.

Küresel prensiplerle savunma

Güvenlik Temelli Tasarım (Security by Design), Mahremiyet Temelli Tasarım (Privacy by Design), Derinlemesine Savunma (Defence in Depth) ve Asgari Yetki Prensibi gibi küresel yaklaşımlar kurum kültürüne entegre edilir.

Dinamik ve sürekli uyum

Siber güvenlik statik bırakılmaz; varlık değişimleri ve Siber Güvenlik Başkanlığı'nın yeni sürüm güncellemeleri Değişiklik Yönetimi süreciyle anında kurum altyapısına uyarlanır.

5 Hizmet Kapsamı ve Metodoloji

AŞAMA 1

Planlama – Stratejik Yol Haritası

Ağ, sistem, uygulama, IoT, taşınabilir ortam, fiziksel mekân ve personel gibi varlık gruplarının belirlenmesi. Gizlilik, Bütünlük ve Erişilebilirlik (CIA) ilkeleri doğrultusunda EK-C.1 Anket Formu kullanılarak kritiklik derecelerinin (Derece 1, 2, 3) tespiti ve eksiklikleri (Tamamen, Kısmen, Hiç) gösteren Mevcut Durum (Boşluk) Analizinin yapılması.

AŞAMA 2

Uygulama ve Dokümantasyon

Planlanan tedbirlerin kurum personeliyle birlikte hayata geçirilmesi, teknik şartnamelerde yerli ve millî ürün tercihinde destek sağlanması ve Rehber'e uygun tüm doküman, politika ve prosedür setlerinin uçtan uca / sıfırdan hazırlanması.

AŞAMA 3

Kontrol ve Denetim Yönetimi

BİGR kapsamında yılda en az bir kez yapılması zorunlu olan denetim sürecinin yönetilmesi ve elde edilen sonuçların (EK-A, B, E, F, H formları dâhil) resmî BİGDES sistemine eksiksiz ve hatasız yüklenmesinin sağlanması.

AŞAMA 4

Değişiklik Yönetimi – Süreklilik

Yeni sistemlerin devreye alınması, varlık kritiklik seviyelerinin değişmesi ve Rehber güncellemelerine göre uyum planının sürekli revize edilmesi.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ BİGR Varlık Grupları Envanteri ve EK-C.1 Kritiklik Derecelendirme Analizleri
- ✓ Mevcut Durum / Boşluk (Gap) Analizi Raporu ve Uygulama Yol Haritası
- ✓ Teknik olarak uygulanamayan tedbirler için EK-C.5 Telif Edici Kontroller Çerçevesi
- ✓ Kuruma özel BİGR idari ve teknik tedbirler dokümantasyon seti (politika, prosedür, form)
- ✓ BİGDES sistemine yüklenmeye hazır resmî kontrol formları (EK-A, B, E, F, H)

HEDEFLenen ÇIKTI / BAŞARI KRİTERİ

- ✓ 7545 sayılı Kanun'un ve Cumhurbaşkanlığı Genelgesi'nin gerektirdiği yasal BİGR yükümlülükleri, idari para cezası riski olmaksızın hukuki ve operasyonel seviyede eksiksiz tamamlanmış olur.
- ✓ Zorunlu denetim süreçleri ve BİGDES bildirimleri hiçbir belirsizlik yaşanmadan, hatasız formlarla Siber Güvenlik Başkanlığı standartlarına uygun şekilde tamamlanır.
- ✓ Güvenlik ve mahremiyet temelli tasarımı içselleştirmiş, siber tehditlere ve veri sızıntılarına karşı dirençli, millî güvenlik beklentilerini karşılayan bir BT altyapısı elde edilir.

- ✓ Personel yetkinlik artırıcı BİGR eğitim ve çalıştay raporları

7 Sık Sorulan Sorular

ISO 27001 belgemiz var, yine de BİGR uyumu gerekli mi?

Evet. ISO 27001 gönüllü bir yönetim sistemi standardı, BİGR ise kapsamdaki kurumlar için yasal bir yükümlülüktür. Ancak iki çalışma büyük ölçüde ortak envanter ve risk tabanı üzerinde birleştirilebilir; bu, eforun ve maliyetin belirgin biçimde düşürülmesini sağlar.

Bir tedbiri teknik olarak uygulayamıyoruz, ne olacak?

Rehber bu durum için telafi edici kontrol mekanizmasını öngörür. EK-C.5 çerçevesinde gerekçe, alternatif kontrol ve artık risk kayıt altına alınır; böylece uyumsuzluk değil yönetilen bir istisna doğar.

BİGRES yüklemesini biz mi yapacağız?

Yükleme kurumun resmî sorumluluğundadır; biz formların içeriğini denetime hazır biçimde üretir, doğrular ve yükleme sürecine refakat ederiz.

8 Etiketler

BİGR uyum danışmanlığı

BİGRES

7545 sayılı Siber Güvenlik Kanunu

varlık gruplandırma

EK-C.1 kritiklik derecesi

telafi edici kontrol

Siber Güvenlik Başkanlığı

kritik altyapı

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.