KATEGORİ 3 · DENETİM HİZMETLERİ

Bağımsız Tedarikçi Siber Güvenlik Denetim Hizmeti

Tedarik Zinciri

Tedarikçi ve alt yüklenicilerin bilgi güvenliği olgunluğunu risk odaklı sınıflandırma (tiering) ile denetleyen; "çalışılabilirlik kararı"na temel oluşturan nicel skorlu bağımsız denetim.

tedarikçi denetimi · tedarik zinciri güvenliği · third party risk management · NIST CSF 2.0 · veri işleyen denetimi · tedarikçi risk skorlama

KATEGORİ
Denetim Hizmetleri

TİPİK SÜRE
Tedarikçi başına Tip A: 2–5 gün · Tip B: 3–7 gün · Tip C: 1–3 gün

KİMLER İÇİN
Kritik hizmetlerini dış kaynağa devretmiş kurumlar; bulut, yazılım geliştirme, çağrı merkezi, bakım-onarım ve saha hizmeti tedarikçileriyle çalışan tüm organizasyonlar; satın alma ve sözleşme yenileme kararı alacak yönetimler.

1 Hizmetin Tanımı

Bu hizmet, kurumunuza hizmet veren tedarikçilerin, alt yüklenicilerin ve iş ortaklarının bilgi güvenliği olgunluk seviyelerinin ISO 27001, NIST CSF v2.0 ve KVKK standartları çerçevesinde yetkilendirilmiş bağımsız denetçiler tarafından incelenmesi sürecidir. Hizmet, "Risk Odaklı Sınıflandırma (Tiering)" yaklaşımıyla; tedarikçinin işlediği verinin hassasiyeti ve erişim yetkilerine göre 5 temel ana kontrol başlığının (GRC, teknik güvenlik, operasyonel güvenlik vb.) analiz edilmesini ve güvenlik seviyesinin denetlenerek raporlanmasını kapsar.

2 Neden Gereklidir?

Günümüzün karmaşık siber tehdit ortamında kurumların güvenliği, sadece kendi aldıkları önlemlerle değil; birlikte çalıştıkları tedarikçi ağının güvenlik seviyesiyle de doğrudan bağlantılıdır. Tedarikçi tarafında yaşanabilecek bir veri ihlali veya hizmet kesintisi, doğrudan kurumunuzu etkileme potansiyeline sahiptir. Bağımsız tedarikçi denetimleri, sözleşmesel ve yasal güvenlik yükümlülüklerinin tedarikçi tarafından gerçekten yerine getirilip getirilmediğini doğrulamak için kritik bir zorunluluktur.

YAPTIRIM VE RİSK EŞİĞİ

Veri işleyen üzerinden gerçekleşen ihlallerde sorumluluk veri sorumlusundadır; KVKK veri güvenliği yükümlülüğü ihlali 2026 yılı için 256.357 ₺ – 17.092.242 ₺ idari para cezasına konudur.

3 Yasal ve Normatif Dayanak

- **6698 sayılı KVKK — veri işleyeni denetleme yükümlülüğü**
- **ISO/IEC 27001 A.5.19–A.5.23**
- **NIST CSF v2.0**
- **Bilgi ve İletişim Güvenliği Rehberi — tedarikçi güvenliği**

4 Sağladığı Katma Değer

Hukuki katkı

KVKK başta olmak üzere yasal regülasyonlar çerçevesinde kuruma düşen "veri işleyenleri denetleme" yükümlülüğü bağımsız bir gözle yerine getirilerek olası hukuki ve idari yaptırım riskleri minimize edilir.

Operasyonel katkı

Bağımsız bir gözle yapılan değerlendirme, tedarikçilerinizin bilgi güvenliği altyapısındaki kör noktaları tespit ederek uluslararası standartlara uyum durumlarını şeffaf biçimde ortaya koyar ve hizmet kalitesini artırır.

Yönetsel katkı

Yapılandırılmış raporlar (çalışılabilirlik kararı vb.) ile üst yönetime tedarikçi ilişkisinin risk durumu hakkında tarafsız bir fotoğraf sunulur; stratejik satın alma ve sözleşme yenileme süreçleri için objektif bir karar destek mekanizması sağlanır.

5 Hizmet Kapsamı ve Metodoloji

Genel bakış: RISK ODAKLI SINIFLANDIRMA (TIERING) TIP A Yerinde Denetim Kritik tedarikçi · saha mülakat ve fiziksel kontrol TIP B Uzaktan Denetim Önemli tedarikçi · dokümantasyon ve kanıt incelemesi TIP C Beyan Esaslı Standart tedarikçi · soru seti ve öz değerlendirme

AŞAMA 1

Tedarikçi Sınıflandırması ve Kapsam Belirleme

Tedarikçilerin veri hassasiyeti, erişim yetkisi ve iş etkisine göre (Kritik, Önemli, Standart) sınıflandırılması ve uygulanacak denetim yönteminin (Tip A yerinde, Tip B uzaktan, Tip C beyan) belirlenmesi.

AŞAMA 2

Soru Seti ve Dokümantasyon İncelemesi (Tip B ve C)

Politika, prosedür ve bilgi güvenliği süreç dokümantasyonlarının uzaktan veya soru seti üzerinden analiz edilmesi ve standartlara uygunluğunun doğrulanması.

AŞAMA 3

Yerinde (Saha) Kontroller ve Teknik İncelemeler (Tip A)

Kritik tedarikçiler için uzmanlarımız tarafından bizzat sahada gerçekleştirilen mülakatlar, fiziksel güvenlik (veri merkezi, ofis) ve teknik güvenlik kontrolleri.

AŞAMA 4

Teknik İnceleme ve Güvenli Örnekleme

Log yönetimi, ağ güvenliği (VLAN, güvenlik duvarı), kimlik yönetimi (MFA) ve yedekleme sistemlerinin (BCP/DR) teknik standartlar çerçevesinde incelenmesi.

AŞAMA 5

Mutabakat, Puanlama ve Kapanış

Tespit edilen eksikliklerin "Acil", "Yüksek", "Orta" ve "Düşük" seviyelerinde nicel skorlarla derecelendirilerek kuruluşa sunulması.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ Teknik Detay Raporu ve Çözüm Planı — her bulgunun nicel skorla derecelendirildiği, iş etkilerinin açıklandığı ve uygulanabilir teknik çözüm adımlarını içeren detaylı yol haritası
- ✓ Yönetici Özeti — tedarikçinin genel risk skorunu ve en kritik zafiyetlerini içeren, çalışılabilirlik kararına destek sağlayacak özet rapor
- ✓ Denetim kriterleri, metodoloji, bulgular ve tavsiyeleri içeren yapılandırılmış rapor seti

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Tedarikçi zincirinden kaynaklanabilecek siber güvenlik ve veri ihlali riskleri, bağımsız ve uzman bir denetim süreciyle objektif olarak tespit edilir.
- ✓ Tedarikçilerle çalışmaya devam edip etmeme veya sözleşme şartlarını revize etme konusunda net kanıtlara dayanan stratejik kararlar alınabilir.
- ✓ Tedarikçi altyapılarındaki güvenlik boşlukları şeffaf ve ölçülebilir biçimde kayıt altına alınır ve kapatılması için net bir iyileştirme planı tedarikçiye sunulur.

7 Sık Sorulan Sorular

Tedarikçimiz denetimi kabul etmezse ne olur?

Denetim hakkı, sözleşmelerin veri işleyen maddelerine yazılması gereken temel bir haktır. Reddedilmesi başlı başına bir risk göstergesidir ve çalışılabilirlik kararında dikkate alınmalıdır.

Tüm tedarikçileri denetlemek zorunda mıyız?

Hayır. Risk odaklı sınıflandırma (tiering) ile kritik tedarikçilere yerinde denetim, diğerlerine uzaktan veya beyan esaslı denetim uygulanır. Amaç kapsamı değil, riski kapsamaktır.

Rapor tedarikçiyle paylaşılıyor mu?

Teknik detay raporu, bulguların kapatılabilmesi için tedarikçinin BT ve güvenlik ekipleriyle paylaşılmak üzere tasarlanmıştır; yönetici özeti ise kurumunuzun karar mekanizmasına yöneliktir.

8 Etiketler

tedarikçi denetimi · tedarik zinciri güvenliği · third party risk management · NIST CSF 2.0 · veri işleyen denetimi · tedarikçi risk skorlama · çalışılabilirlik kararı · vendor tiering

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.