Veri Sızıntısı Müdahale Politikası

Atak Domain Bilgi Teknolojileri A.Ş.

1. Amaç ve kapsam

Bu politika, Atak Domain tarafından işlenen veya saklanan kişisel verilerin, ticari bilgilerin, müşteri verilerinin, teknik logların veya diğer hassas verilerin olası bir **yetkisiz erişim, kayıp, çalınma, ifşa veya bozulma** durumunda uygulanacak tüm prosedürleri tanımlar.

Bu politika aşağıdaki olayları kapsar:

- Kişisel veri sızıntıları
- Müşteri hesabı ihlalleri
- Yetkisiz EPP/API erişimi
- DNS veya domain yönetim hesaplarının ele geçirilmesi
- Sunucu veya veritabanı yetkisiz erişimi
- Kötü amaçlı yazılım kaynaklı veri ihlalleri
- Üçüncü taraf hizmet sağlayıcı kaynaklı ihlaller

Politika, tüm çalışanlar, iş ortakları, bayiler, yükleniciler ve veri işleyen tüm üçüncü taraflar için bağlayıcıdır.

2. Veri sızıntısı tanımı

“Veri sızıntısı” (data breach), aşağıdaki durumlardan herhangi biridir:

- Kişisel verilerin yetkisiz kişilerce erişilmesi
- Verilerin kaybolması, silinmesi veya bozulması
- Verilerin kötü niyetli üçüncü taraflara aktarılması
- Veri bütünlüğünün ve güvenliğinin tehlikeye girmesi
- GDPR kapsamında raporlanması gereken tüm olaylar

3. Veri ihlali tespit yöntemleri

Atak Domain veri ihlallerini aşağıdaki yollarla tespit eder:

- Güvenlik izleme sistemleri (SIEM, IDS/IPS)
- Erişim logları ve API log anormallikleri

- DNS/Domain transfer işlemlerindeki olağandışı hareketler
- SOC/Siber Güvenlik birimi raporları
- Kullanıcı şikayetleri
- Firewall / WAF uyarıları
- DDoS istatistikleri
- Üçüncü taraf güvenlik firmaları veya CERT/CERT-TR bildirimleri

Bu tespitler otomatik veya manuel olabilir.

4. Sızıntı değerlendirme kriterleri

Bir olayın veri sızıntısı olarak değerlendirilmesi için aşağıdaki faktörler analiz edilir:

- Sızan verinin türü (kişisel veri, ödeme verisi, domain hesabı)
- Etkilenen kişi sayısı
- Veri türünün hassasiyeti
- Verinin ifşa edilme, kopyalanma, değiştirilme ihtimali
- Verinin kötü niyetle kullanılıp kullanılmadığı
- Verinin geri alınamaz şekilde kaybolup kaybolmadığı

Kişisel veri ise GDPR 33 ve 34. maddelere göre raporlama yükümlülüğü doğabilir.

5. Veri sızıntısı müdahale süreci

Aşağıdaki 6 aşamalı süreç tüm veri sızıntıları için uygulanır:

5.1. Tespit ve doğrulama

- Olay ilk olarak Cyber Security / DevOps ekibi tarafından kaydedilir.
- Olayın gerçek olup olmadığı doğrulanır.
- Kritik olaylarda olay anı itibarıyla tüm işlemler loglanır.

5.2. İzolasyon

- Etkilenen sistem derhal izole edilir.
- Gerekirse ilgili sunucu karantinaya alınır.
- EPP, API veya müşteri hesabı şifreleri resetlenir.
- Yetkisiz session'lar sonlandırılır.

5.3. Etki analizi

Aşağıdaki sorular yanıtlanır:

- Hangi veriler etkilendi?
- Saldırgan verileri aldı mı yoksa sadece erişim mi sağladı?
- Ne kadar süre boyunca sistem açık kaldı?
- Etkilenen kişi sayısı nedir?
- Sistem bütünlüğü bozuldu mu?

Sonuç "Veri İhlali Etki Raporu"na kaydedilir.

5.4. Düzeltici faaliyet

- Saldırı vektörü kapatılır
- Güvenlik açıkları yamalanır
- Ek güvenlik kontrolü uygulanır
- Etkilenen müşteri hesapları güvenli moda alınır
- DNS/EPP transfer kilitleri etkinleştirilir

5.5. Bildirim

A. Kişisel veri içeriyorsa GDPR ve KVKK kapsamında bildirilir

- GDPR uyarınca **72 saat içinde** ilgili denetim otoritelerine
- Gerekiyorsa ilgili **kullanıcılara**
- TR kişisel veriler için **KVKK 72 saat bildirimi**

B. ICANN gereklilikleri

ICANN RAA 3.18 gereği, güvenlik olaylarında:

- ICANN'e
- İlgili registry'ye
- WHOIS/Proxy kullanılıyorsa talep eden resmi makamlara

bildirim yapılabilir.

C. Diğer bildirimler

- Banka ve ödeme kuruluşları

- Barındırma ortakları
- Güvenlik firmaları
- CERT / USOM / CERT-TR (Türkiye için)

5.6. Kapanış ve raporlama

- Nihai veri ihlali raporu hazırlanır
- Yönetim kuruluna sunulur
- Gerekiyorsa hukuki süreç başlatılır
- Tekrarlamayı önleyici kontroller uygulanır

6. Müşteri bilgilendirme kriterleri

Aşağıdaki durumlarda müşterilere bildirim yapılır:

- Şifre, kimlik bilgileri veya hesap erişim verisi sızdıysa
- Alan adının transfer yetkisi ele geçirildiyse
- DNSSEC anahtarları veya nameserver verisi çalındıysa
- Whois verisi yetkisiz biçimde alındıysa
- Ödeme verileri (token bazlı olsa bile) risk altındaysa

Bildirim içeriği şunları içerir:

- Ne oldu
- Ne zaman oldu
- Hangi bilgiler etkilendi
- Hangi önlemler alındı
- Müşterinin ne yapması gerektiği
- İletişim bilgileri

7. Sızıntı sonrası iyileştirme planı

- Tüm sistemlerin güvenlik denetimi
- Penetrasyon testleri
- Loglama iyileştirmeleri
- MFA zorunluluğu

destek@atakdomain.com atakdomain.com İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR

- API rate-limit artırımı
- Çalışanlara ek güvenlik eğitimi
- Gerekiyorsa mimari değişiklik

8. Üçüncü taraflar ve bayiler

Atak Domain adına veri işleyen tüm **bayiler, reseller'lar, teknik sağlayıcılar, SaaS hizmetleri** şu yükümlülüklere sahiptir:

- Veri sızıntısını **24 saat içinde** Atak Domain'e bildirmek
- Olayla ilgili tüm logları sağlamak
- İşbirliği yapmak
- Veri işleme sözleşmesine (DPA) uymak

9. Sorumluluk sınırları

Atak Domain:

- Müşteri hatalarından (zayıf parola, kimlik avı, cihaz enfeksiyonu)
- Üçüncü taraf eklenti/tema kaynaklı güvenlik açıklarından
- Müşteri sistemlerindeki ihlallerden
- Müşterinin kendisine ait hosting sunucularındaki zafiyetlerden

sorumlu tutulamaz.

10. Politikanın yürürlüğe girmesi ve güncellenmesi

Bu politika yayınlandığı tarihten itibaren geçerlidir.
ICANN, GDPR veya ulusal mevzuatta değişiklik oldukça güncellenebilir.

destek@atakdomain.com
atakdomain.com
İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR