

ÖRNEK 1: Nicel Risk Analizi

Problem Metni

www.hbmacit.com şirketinin elinde 3 farklı ana dijital varlık bulunsun:

1. Müşteri Kredi Kartı ve Kişisel Veri Veritabanı
2. Şirketin Blog Sitesi (Ürün satılmayan, sadece duyuru yapılan site)
3. E-Ticaret Satış / Ödeme Altyapısı (Web & Mobil Uygulama)

Bu 3 varlığı nitel olarak değerleyelim.

Cevap

Varlık	Gizlilik (C) Veri sızarsa?	Bütünlük (I) Veri bozulursa?	Erişebilirlik (A) Sistem çökerse?	Toplam kritiklik skoru
Müşteri Kredi Kartı ve Kişisel Veri Veritabanı	5/5 (KVKK cezaları)	4/5 (Kart bilgisi bozuldu, ödeme alınamaz)	1/5 (Veri sızmadığı sürece problem olmaz)	5/5
Şirketin Blog Sitesi	1/5 (Zaten kamuya açık)	2/5 (Yedekleri mevcut, hemen düzeltilir)	2/5 (Satışlar etkilenmez)	2/5
E-Ticaret Satış / Ödeme Altyapısı	2/5 (Burada anlık ödeme bilgileri var, hassas veri değil)	5/5 (1000TL olan ürün sepette 1TL görünürse ciddi maddi zarar oluşur)	5/5 (Kısa süre bile çökerse müşteriler başka siteye kaçır)	5/5

ÖRNEK 2: Kuantitatif Risk Analizi (SLE ve ALE Hesabı)

Problem Metni

www.hbmacit.com e-ticaret şirketinin ana ödeme ve sipariş veritabanı sunucusu ile ilgili finansal veriler ve risk tahminleri aşağıda verilmiştir:

Varlık Değeri (AV - Asset Value): Sunucunun donanım değeri, üzerindeki lisanslar ve veritabanı altyapısının toplam değeri 2.000.000 TL'dir.

Saldırı Senaryosu (Ransomware / Fidyeci Yazılım): Şirket veritabanının bir fidyeci yazılım saldırısına uğraması durumunda, veri kurtarma, sistemlerin temizlenmesi ve operasyonel aksama nedeniyle varlığın %60'ının zarar göreceği (EF=0.60) öngörülmektedir.

Tehdit Gerçekleşme Sıklığı (ARO - Annualized Rate of Occurrence): Geçmiş siber tehdit istatistikleri ve sektör raporlarına göre, bu tür bir fidyeci yazılım saldırısının şirkette 5 yılda 1 kez gerçekleşeceği tahmin edilmektedir.

Güvenlik firması, bu sunucuyu fidyeci yazılımlara karşı tam koruma sağlayacak bir EDR (Endpoint Detection and Response) yazılım çözümünü yıllık 150.000 TL lisans bedeliyle sunmaktadır.

Soru 1. Bu fidyeci yazılım saldırısı için Tek Bir Olaydaki Tahmini Kaybı (SLE) hesaplayınız.

Soru 2. Saldırının şirket için Yıllık Tahmini Kaybını (ALE) hesaplayınız.

Soru 3. Karar / Değerlendirme: Şirket yönetimi yıllık 150.000 TL değerindeki EDR güvenlik yatırımını yapmalı mıdır? Neden? (Net Risk Önleme Oranı / ROI açısından gerekçelendiriniz).

Cevap 1.: SLE, tek bir siber olayın gerçekleşmesi durumunda ortaya çıkacak toplam finansal kayıptır.

$$SLE = AV \times EF = 2.000.000 \times 0,60 = 1.200.000 \text{ TL}$$

Şirket tek bir ransomware saldırısı yediğinde doğrudan ve dolaylı olarak 1.200.000 TL kaybedecektir.

Cevap 2.: ALE, tehdidin bir yıl içerisindeki ortalama maliyet beklentisidir.

$$ALE = SLE \times ARO = 1.200.000 \times 0,20 = 240.000 \text{ TL / Yıl}$$

Bu risk önlenmediği sürece şirkete yıllık ortalama maliyeti 240.000 TL'dir.

Cevap 3. Güvenlik önleminin finansal olarak mantıklı olup olmadığını anlamak için Güvenlik Maliyeti ile Yıllık Tahmini Kayıp (ALE) karşılaştırılır:

$$\begin{aligned} \text{Yıllık Risk Maliyeti (ALE)} &= 240.000 \text{ TL} \\ \text{Yıllık Güvenlik Çözümü Maliyeti (C)} &= 150.000 \text{ TL} \\ ALE - C &= 90.000 \text{ TL} \end{aligned}$$

Karar: Yatırım yapılmalıdır. Çünkü güvenlik yazılımının yıllık maliyeti (150.000 TL), önlediği yıllık risk maliyetinden (240.000 TL) düşüktür. Şirket bu yatırımı yaparak riskini bertaraf etmekle kalmaz, uzun vadede yıllık ortalama 90.000 TL finansal kazanç (tasarruf) sağlar.

ÖRNEK 3: Hastane Bilgi Yönetim Sistemi Nicel ve Nitel Varlık Değerleme ve Risk Analizi

“hbmecit Hastanesi”, günde binlerce hastaya hizmet veren orta ölçekli bir özel hastanedir. Hastanenin kritik operasyonlarını yürüten ana dijital varlığı "Hastane Bilgi Yönetim Sistemi (HBYS) Sunucu ve veritabanı altyapısıdır. Siber güvenlik ekibi, bu sistem üzerinde hem nitel hem de nicel bir varlık değerlendirme çalışması yapacaktır.

Sistem ve Varlık Bilgileri

Varlık Tanımı: HBYS Veritabanı ve Hasta Tıbbi Kayıtları Sunucusu.

Varlık Değeri (AV - Asset Value): Sunucu donanımları, HBYS yazılım lisansları ve veri entegrasyon altyapısının toplam yeniden kurulum maliyeti 4.000.000 TL'dir.

Risk ve Tehdit Senaryosu

Hastanenin HBYS altyapısının bir fidye yazılımı ile şifrelenmesi ve hasta tıbbi verilerinin (KVKK kapsamındaki özel nitelikli kişisel veriler) sızdırılması senaryosu incelenmektedir:

Hasar Oranı (EF - Exposure Factor): Saldırı gerçekleştiğinde; sistemlerin durması, tıbbi cihaz entegrasyonlarının kopması, acil servis kilitlenmesi ve yasal KVKK cezaları nedeniyle varlığın %75'inin ($EF = 0,75$) zarar göreceği öngörülmektedir.

Tehdit Gerçekleşme Sıklığı (ARO - Annualized Rate of Occurrence): Sağlık sektöründeki güncel istatistiklere ve mevcut zaafiyet taramalarına göre, bu tür bir fidyeci yazılım/veri ihlali saldırısının bu hastanede 4 yılda 1 kez gerçekleşeceği tahmin edilmektedir.

Önerilen Güvenlik Önlemi

Güvenlik danışmanlığı firması, hastaneye bu riski %100'e yakın oranla engelleyecek Yedekli Veri Merkezi, Anlık Şifrelenmiş Ağ Mimarisi ve Yedekleme (DRP) çözümünü yıllık 600.000 TL lisans ve bakım bedeliyle önermektedir.

Soru 1. HBYS Veritabanı varlığını CIA Triad kriterlerine göre 1 (Düşük) ile 5 (Kritik) arasında puanlayınız. Puanlama gerekçelerinizi sağlık sektörü dinamiklerine göre açıklayınız.

Soru 2. Bu fidye yazılımı saldırısı için Tek Bir Olaydaki Tahmini Kaybı (SLE) hesaplayınız.

Saldırının hastane için Yıllık Tahmini Kaybını (ALE) hesaplayınız.

Soru 3. Hastane yönetimi yıllık 600.000 TL maliyeti olan güvenlik çözümünü satın almalı mıdır? Yapacağınız finansal analizle (Yıllık Net Tasarruf) yanıtınızı gerekçelendiriniz.

Cevap 1. HBYS veritabanının CIA Triad açısından değerlendirilmesi:

Gizlilik (Confidentiality) 5/5 (Kritik) Hasta teşhisleri, tahliller ve kişisel veriler KVKK kapsamında özel nitelikli kişisel veridir. Veri sızması durumunda devasa cezalar ve itibar kaybı oluşur.

Bütünlük (Integrity) 5/5 (Kritik) Hasta kan grubu, alerji veya dozaj bilgilerinin bozulması/değişmesi doğrudan hasta ölümüne yol açabilir.

Erişilebilirlik (Availability) 5/5 (Kritik) Sistem çöktüğünde ameliyatlar, acil müdahaleler ve ilaç yazımları durur. İnsan hayatı doğrudan riske girer.

$$\text{Nitel değer} = \max(C, I, A) = 5$$

HBYS, hastanenin kalbidir. Her üç güvenlik boyutunda da en yüksek skor olan 5'i almıştır. Bu durum, sisteme koşulsuz olarak en yüksek güvenlik önceliklerinin tanınması gerektiğini gösterir.

Cevap 2.

$$SLE = AV \times EF = 4.000.000 \times 0,75 = 3.000.000 \text{ TL}$$

Hastane bu saldırıyı 1 kez yaşadığında, doğrudan ve dolaylı olarak toplam 3.000.000 TL kayıp yaşayacaktır.

Cevap 3.

$$ALE = SLE \times ARO = 3.000.000TL \times 0,25 = 750.000TL/yıl$$

Bu risk önlenmediği takdirde, hastanenin bilançosuna yıllık yansıyan ortalama finansal risk yükü 750.000 TL'dir. Güvenlik yatırımının finansal olarak mantıklı olup olmadığını anlamak için Önlenebilir Yıllık Risk (ALE) ile Güvenlik Çözümünün Yıllık Maliyeti (C) karşılaştırılır:

$$Yıllık Net Finansal Kazanç = ALE - C = 750.000 - 600.000 = 150.000 TL / yıl$$

Sonuç: Evet, önlem satın alınmalıdır.

Nitel Açıdan: HBYS'nin CIA skoru 5/5 (Kritik)'tir. Veri bütünlüğünün bozulması hasta hayatını riske atacağından bu risk kabul edilemez.

Nicel Açıdan: Güvenlik çözümünün yıllık maliyeti (600.000 TL), sistemin yıllık risk maliyetinden (750.000 TL) daha düşüktür. Hastane bu yatırımı yaparak hem hastalarının hayatını ve verilerini korumuş olur hem de finansal olarak yılda ortalama 150.000 TL net tasarruf sağlar.