**BİLGİ GÜVENLİĞİ UYGULAMASI: Tehdit Modelleme ve Risk Analizi**

**CIA Üçlemesi (Confidentiality, Integrity, Availability)**

**Gizlilik (Confidentiality):** Bilgiye sadece erişim yetkisi olan kişilerin ulaşabilmesini sağlar. Yetkisiz erişimlerin engellenmesi anlamına gelir.

**Bütünlük (Integrity):** Bilginin bozulmadan, değiştirilmeden ve tahrif edilmeden korunmasını ifade eder. Veri bütünlüğü, bilginin doğru ve güvenilir kalmasını sağlar.

**Erişilebilirlik (Availability):** Bilgiye gerektiğinde, istenilen zamanda ve kesintisiz olarak erişilebilmesini sağlar.

**Tehdit Modelleme Nedir?**

Tehdit modelleme, bir sistem üzerindeki potansiyel güvenlik tehditlerini tanımlamak, bu tehditlerin olası etkilerini değerlendirmek ve uygun güvenlik önlemlerini belirlemek için kullanılan sistematik bir yaklaşımdır.

Tehdit modelleme sürecinde:

1. Sistemin varlıkları (assets) belirlenir
2. Olası tehditler tanımlanır
3. Zafiyetler (vulnerabilities) tespit edilir
4. Risklerin olasılık ve etki düzeyleri değerlendirilir
5. Önlemler planlanır

**Risk Analizi**

Risk = Olasılık x Etki

Risk analizi, bir tehdide maruz kalma olasılığını ve bu tehdide maruz kalmanın yaratacağı etkiyi ölçerek risk skorunun belirlenmesidir.

**Olasılık (1-5) Değerlendirme Kriterleri:**

1. Çok Düşük: Tehdide maruz kalma ihtimali çok düşük, neredeyse hiç yok
2. Düşük: Tehdide maruz kalma ihtimali düşük, nadiren gerçekleşir
3. Orta: Tehdide maruz kalma ihtimali orta düzeyde, zaman zaman gerçekleşebilir
4. Yüksek: Tehdide maruz kalma ihtimali yüksek, sıklıkla gerçekleşir
5. Çok Yüksek: Tehdide maruz kalma ihtimali çok yüksek, neredeyse kesin

**Etki (1-5) Değerlendirme Kriterleri:**

1. Çok Düşük: Etkisi çok az, kolayca telafi edilebilir
2. Düşük: Etkisi sınırlı, kısa sürede düzeltilebilir
3. Orta: Etkisi önemli, düzeltilmesi zaman ve kaynak gerektirir
4. Yüksek: Etkisi ciddi, önemli kayıp veya zararlar oluşturur
5. Çok Yüksek: Etkisi yıkıcı, felaket seviyesinde zararlara yol açar

**Risk Skoru Değerlendirmesi:**

* 1-5: Düşük risk - Normal izleme yeterli
* 6-10: Orta risk - Dikkatli izleme ve bazı önlemler gerekli
* 11-15: Yüksek risk - Acil önlemler ve özel dikkat gerekli
* 16-25: Çok yüksek risk - Derhal müdahale edilmeli

**ÖRNEK UYGULAMA: OKUL KÜTÜPHANE SİSTEMİ**

**Senaryo:** Okulumuzun kütüphane bilgi sistemi var. Bu sistemde öğrencilerin kişisel bilgileri, ödünç alınan kitaplar ve kitap envanteri bulunuyor. Sistem, internet üzerinden erişilebiliyor ve öğrenciler kitap rezervasyonu yapabiliyor.

**CIA Üçlemesi Değerlendirme Örneği**

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| **Gizlilik (Confidentiality)** | Öğrenci bilgilerinin yetkisiz kişilerce görüntülenmesi | Kişisel veri ihlali, öğrenci mahremiyetinin zarar görmesi | Güçlü şifreler, kullanıcı yetkilendirme sistemi, oturum zaman aşımı |
| **Bütünlük (Integrity)** | Kitap kayıtlarının yanlışlıkla veya kötü niyetle değiştirilmesi veya silinmesi | Kitap envanterinde tutarsızlık, kayıp kitaplar | Veri değişiklik günlükleri, yetki sınırlandırma, düzenli veri doğrulama |
| **Erişilebilirlik (Availability)** | Sistemin çalışmaması, sunucu arızası | Kitap ödünç alma/verme işlemlerinin yapılamaması | Düzenli yedekleme, yedek sunucu, basit kağıt tabanlı yedek sistem |

**Risk Analizi Örneği**

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
| **Şifre hırsızlığı** | 3 (Orta) | 4 (Yüksek) | 12 (Yüksek Risk) | Çift faktörlü kimlik doğrulama, düzenli şifre değiştirme zorunluluğu, şifre politikası |
| **Sunucu arızası** | 2 (Düşük) | 3 (Orta) | 6 (Orta Risk) | Düzenli bakım, yedek donanım, bulut yedekleme |
| **Veritabanına SQL enjeksiyon saldırısı** | 2 (Düşük) | 5 (Çok Yüksek) | 10 (Orta Risk) | Güvenli kodlama, parametreli sorgular, düzenli güvenlik testleri |

**UYGULAMA**

**Senaryo 1: E-Ticaret Şirketi Veri Güvenliği**

**Senaryo Özeti:** Bir e-ticaret şirketi, kullanıcılarının ad, soyad, adres, telefon numarası ve ödeme bilgilerini içeren bir veritabanına sahiptir. Web sitesi üzerinden kredi kartı ile ödeme kabul etmektedir. Son zamanlarda kimlik avı saldırıları ve siber tehditlerin arttığını fark etmiştir. Şirketin güvenliğini artırmak için bir tehdit modeli oluşturulacaktır.

**Referans Olaylar:** Equifax veri ihlali (2017), Target veri sızıntısı (2013)

**Görev 1: CIA Üçlemesini Değerlendirme**

Aşağıdaki tabloyu tamamlayınız. Güvenlik ilkesi, tehdit, potansiyel sonuç ve önerilen önlem sütunlarını, gizlilik, bütünlük, erişilebilirlik satırları için doldurunuz.

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| **Gizlilik (Confidentiality)** |  |  |  |
| **Bütünlük (Integrity)** |  |  |  |
| **Erişilebilirlik (Availability)** |  |  |  |

**Görev 2: Risk Analizi**

Senaryo için en az 3 farklı tehdit belirleyerek aşağıdaki risk analizi tablosunu doldurunuz.

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Senaryo 2: Hastane Bilgi Sistemi Güvenliği**

**Senaryo Özeti:** Bir hastane, hastaların tıbbi kayıtlarını, kişisel bilgilerini ve tedavi geçmişlerini saklayan bir bilgi sistemine sahiptir. Hastane personeli, doktorlar ve hemşireler bu sisteme farklı yetki seviyelerinde erişebilmektedir. Hasta gizliliği yasaları gereği (KVKK, GDPR, HIPAA vb.) verilerin korunması yasal bir zorunluluktur.

**Referans Olay:** Anthem sağlık sigortası veri ihlali (2015)

**Görev 1: CIA Üçlemesini Değerlendirme**

Aşağıdaki tabloyu tamamlayınız. Güvenlik ilkesi, tehdit, potansiyel sonuç ve önerilen önlem sütunlarını, gizlilik, bütünlük, erişilebilirlik satırları için doldurunuz.

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| **Gizlilik (Confidentiality)** |  |  |  |
| **Bütünlük (Integrity)** |  |  |  |
| **Erişilebilirlik (Availability)** |  |  |  |

**Görev 2: Risk Analizi**

Senaryo için en az 3 farklı tehdit belirleyerek aşağıdaki risk analizi tablosunu doldurunuz.

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Senaryo 3: Finansal Kurum Güvenliği**

**Senaryo Özeti:** Bir banka, müşterilerinin hesap bilgileri, kredi kartı detayları, kişisel bilgiler ve işlem geçmişlerini tutan kritik sistemlere sahiptir. Ayrıca çevrimiçi bankacılık hizmetleri de sunmaktadır. Son dönemde finans sektöründe siber saldırıların arttığı gözlemlenmiştir.

**Referans Olay:** JPMorgan Chase veri ihlali (2014)

**Görev 1: CIA Üçlemesini Değerlendirme**

Aşağıdaki tabloyu tamamlayınız. Güvenlik ilkesi, tehdit, potansiyel sonuç ve önerilen önlem sütunlarını, gizlilik, bütünlük, erişilebilirlik satırları için doldurunuz.

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| **Gizlilik (Confidentiality)** |  |  |  |
| **Bütünlük (Integrity)** |  |  |  |
| **Erişilebilirlik (Availability)** |  |  |  |

**Görev 2: Risk Analizi**

Senaryo için en az 3 farklı tehdit belirleyerek aşağıdaki risk analizi tablosunu doldurunuz.

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**ÖNERİLER VE İPUÇLARI**

Tehdit modellemesi ve risk analizi yaparken aşağıdaki hususlara dikkat ediniz:

1. **Gerçekçi tehditler belirleyin:** Senaryoya uygun, gerçek dünyada karşılaşılabilecek tehditler seçin.
2. **Olasılık ve etki değerlendirmelerinde tutarlı olun:** Benzer tehditler için benzer değerlendirmeler yapın.
3. **Önlemlerin uygulanabilir olmasına dikkat edin:** Önerdiğiniz güvenlik önlemlerinin pratik ve maliyet-etkin olmasına özen gösterin.
4. **Sektörel düzenlemeleri göz önünde bulundurun:** Her sektörün kendine özgü güvenlik gereksinimleri ve yasal yükümlülükleri vardır.

**ÖRNEK CEVAPLAR**

**Senaryo 1: E-Ticaret Şirketi Veri Güvenliği**

**CIA Üçlemesi Değerlendirmesi**

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| Gizlilik (Confidentiality) | Kimlik avı (phishing) saldırıları, veri sızıntısı | Müşteri kişisel ve finansal bilgilerinin çalınması, müşteri güven kaybı, yasal yaptırımlar | Çift faktörlü kimlik doğrulama (2FA), veri şifreleme, personel eğitimi, güvenli erişim politikaları |
| Bütünlük (Integrity) | Veri manipülasyonu, yetkisiz değişiklikler, SQL enjeksiyon saldırıları | Fiyat manipülasyonu, stok bilgilerinde hata, ödeme işlemlerinde tutarsızlık | Veri doğrulama mekanizmaları, parametre temizleme, veritabanı yetkilendirme kontrolü, veri giriş validasyonu |
| Erişilebilirlik (Availability) | DDoS saldırıları, sunucu arızaları, altyapı sorunları | Web sitesi erişilemezliği, satış kaybı, müşteri memnuniyetsizliği | Yedekli sistemler, yük dengeleme, DDoS koruma servisleri, bulut altyapısı, düzenli yedekleme planları |

**Risk Analizi**

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
| Kimlik avı (phishing) saldırıları | 4 | 5 | 20 | Personel eğitimi, e-posta filtreleme, anti-phishing araçları, çift faktörlü kimlik doğrulama |
| Ödeme bilgilerinin ele geçirilmesi | 3 | 5 | 15 | PCI DSS standartlarının uygulanması, kredi kartı bilgilerinin tokenizasyonu, SSL/TLS kullanımı |
| DDoS saldırıları | 4 | 4 | 16 | DDoS koruma servisleri, CDN kullanımı, trafik analizi, acil durum planı |
| SQL enjeksiyon saldırıları | 3 | 4 | 12 | Web uygulama güvenlik duvarı (WAF), güvenli kodlama pratikleri, düzenli güvenlik testleri |

**Senaryo 2: Hastane Bilgi Sistemi Güvenliği**

**CIA Üçlemesi Değerlendirmesi**

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| Gizlilik (Confidentiality) | Yetkisiz veri erişimi, sosyal mühendislik, içeriden tehditler | Hasta mahremiyetinin ihlali, yasal sorumluluk, kurumsal itibar kaybı | Rol bazlı erişim kontrolü, veri şifreleme, erişim günlükleri, veri sınıflandırma |
| Bütünlük (Integrity) | Tıbbi kayıtlarda yetkisiz değişiklik, veri girişi hataları, kötü amaçlı yazılımlar | Yanlış teşhis/tedavi riskleri, hasta güvenliği tehlikeleri, sigorta/fatura sorunları | Dijital imzalar, versiyon kontrolü, değişiklik günlükleri, kayıt doğrulama |
| Erişilebilirlik (Availability) | Sistem kesintileri, siber saldırılar, donanım arızaları, fidye yazılımları | Kritik hasta verilerine erişememe, acil durum müdahalelerinde gecikmeler | Yedekli sistemler, düzenli yedekleme, felaket kurtarma planı, kesintisiz güç kaynağı |

**Risk Analizi**

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
| Hasta verilerinin sızması | 3 | 5 | 15 | Veri şifreleme, erişim kontrolü, veri sınıflandırma, düzenli güvenlik denetimleri |
| Fidye yazılımı saldırısı | 4 | 5 | 20 | Düzenli yedekleme, güvenlik yamalarının zamanında uygulanması, personel eğitimi, güvenli e-posta uygulamaları |
| İçeriden veri hırsızlığı | 2 | 5 | 10 | Ayrıcalıklı hesap yönetimi, erişim günlükleri, davranış analizi, çıkış prosedürleri |
| Sistem kesintisi | 3 | 4 | 12 | Yedekli sistemler, otomatik failover mekanizmaları, düzenli bakım planlaması |

**Senaryo 3: Finansal Kurum Güvenliği**

**CIA Üçlemesi Değerlendirmesi**

| **Güvenlik İlkesi** | **Tehdit** | **Potansiyel Sonuç** | **Önerilen Önlem** |
| --- | --- | --- | --- |
| Gizlilik (Confidentiality) | Veri ihlalleri, hedefli saldırılar (APT), müşteri bilgilerinin çalınması | Müşteri bilgilerinin çalınması, finansal kayıplar, yasal yaptırımlar, itibar kaybı | Çok katmanlı şifreleme, güçlü kimlik doğrulama, ağ segmentasyonu, veri kaybı önleme (DLP) sistemleri |
| Bütünlük (Integrity) | Finansal verilerde tahrifat, işlem manipülasyonu, yetkisiz transferler | Finansal kayıplar, düzenleyici cezalar, müşteri güven kaybı | İşlem doğrulama, anormal davranış tespiti, çok imzalı onay süreçleri, dijital imzalar |
| Erişilebilirlik (Availability) | Sistem kesintileri, DDoS saldırıları, altyapı sorunları | Finansal hizmetlerde kesinti, müşteri memnuniyetsizliği, itibar kaybı | Yüksek erişilebilirlik mimarisi, coğrafi olarak dağıtılmış veri merkezleri, felaket kurtarma planı |

**Risk Analizi**

| **Tehdit** | **Olasılık (1-5)** | **Etki (1-5)** | **Risk Skoru (Olasılık x Etki)** | **Önerilen Önlem** |
| --- | --- | --- | --- | --- |
| Hedefli siber saldırılar (APT) | 4 | 5 | 20 | Gelişmiş tehdit koruması, güvenlik operasyon merkezi (SOC), tehdit istihbaratı, düzenli penetrasyon testleri |
| Çevrimiçi bankacılık dolandırıcılığı | 5 | 4 | 20 | İşlem doğrulama, davranışsal analiz, müşteri eğitimi, anormal işlem algılama |
| Sistem kesintileri | 3 | 5 | 15 | Yedekli sistemler, yük dengeleme, iş sürekliliği planlaması, düzenli kapasite planlaması |
| İçeriden hırsızlık/dolandırıcılık | 2 | 5 | 10 | Görevlerin ayrılması ilkesi, çift onay gerektiren işlemler, kullanıcı davranış analizi, iç denetim |