PATİKA FİNAL CASE

SECURITY ALTERNATİVES SEARCHİNG

SECURITY ALTERNATIVES SEARCHING: KVKK Kapsamında Müşteri Verilerinin Güvenliği ve Erişim Sınırlandırması

Özet: Bu bölüm, KVKK kapsamında müşteri verilerinin korunmasını ve erişim sınırlandırmasını sağlamak için uygulanan çeşitli güvenlik önlemlerini detaylandırır. Amacımız, hassas verilerin güvenliğini sağlamak ve izinsiz erişimlerin önüne geçmektir.

1. **Tabloya Kişi Bazlı Erişim Yetkisi (Role-Based Access Control - RBAC)**

Amaç: Kullanıcıların yalnızca yetkili oldukları verilere erişmesini sağlamak, hassas verilerin maskelenmesini gerçekleştirmek.

- **Yetkilendirme**: Kullanıcıların yalnızca yetkili oldukları verilere erişebilmeleri sağlandı. Veritabanı düzeyinde kullanıcı gruplarına veya bireysel kullanıcılara rol bazlı erişim hakları tanımlandı. Sadece belirli yetkiye sahip kullanıcıların müşteri verilerini görmesi veya güncelleyebilmesi sağlandı.
- **Hassas Verilerin Maskelenmesi**: Kullanıcıların yetkilerine göre verilerin maskelenmesi işlemi gerçekleştirildi. Örneğin, kredi kartı numaralarının yalnızca son dört hanesi gösterildi.
- **Entegrasyon**: RBAC implementasyonu kapsamında, veritabanı düzeyinde kullanıcı rolleri ve izinleri yapılandırıldı. Uygulama seviyesi yetkilendirme kuralları belirlenerek, veri ve işlemlere erişim sınırlandırıldı.
- **Kullanım Alanı Örneği:** Hastane Bilgi Yönetim Sistemleri, doktorların hasta kayıtlarına erişebildiği, diğer personelin ise yalnızca belirli verilere ulaşabildiği sistemler.

Tabloya Kişi Bazlı Erişim Yetkisi (Role-Based Access Control - RBAC)
Bu süreçte, kullanıcıların yalnızca yetkili oldukları verilere erişmesini sağlamak amacıyla Rol Bazlı Erişim Kontrolü (RBAC) uygulandı. Öncelikle, veritabanı düzeyinde kullanıcı grupları ve bireysel kullanıcılar için roller tanımlandı. PostgreSQL veritabanı üzerinde GRANT komutu kullanılarak belirli tablolara veya sütunlara erişim yetkisi verildi. Uygulama seviyesinde ise, kullanıcı rolleri ve yetkileri belirlenerek, her kullanıcı için farklı erişim hakları tanımlandı. Hassas verilerin maskelenmesi de bu süreçte gerçekleştirildi; örneğin, kredi kartı numaralarının yalnızca son dört hanesi gösterildi.

2. **Veri Maskeleme ve Anonimleştirme**

Amaç: Hassas verilerin gizliliğini sağlamak ve kişisel tanımlayıcı bilgilerin (PII) gizliliğini korumak.

- **Veri Maskeleme**: Üretim ortamında hassas verilerin gizliliğini sağlamak için verilerin belirli kısımları maskelendi. Müşteri adları, adresler veya telefon numaraları maskelenmiş olarak gösterildi.
- **Anonimleştirme**: Veri setlerinden kişisel tanımlayıcı bilgilerin (PII) tamamen kaldırılması işlemi tamamlandı.
- **Kullanım Alanı Örneği**: E-Ticaret platformlarında, müşteri verilerinin analiz edilmesi sırasında, müşterilerin kimliklerini korumak amacıyla verilerin anonimleştirilmesi.

Veri Maskeleme ve Anonimleştirme
Hassas verilerin gizliliğini sağlamak amacıyla, veri maskeleme teknikleri kullanıldı. PostgreSQL'de yerleşik veri maskeleme özellikleri kullanılarak, müşteri adları ve adresleri gibi bilgilerin belirli kısımları maskelendi. Ayrıca, anonimleştirme teknikleri kullanılarak veri setlerinden kişisel tanımlayıcı bilgiler kaldırıldı. Bu işlem, verilerin analiz süreçlerinde kullanılmasına olanak tanırken, müşteri gizliliğini koruma altına aldı.

3. **Loglama Uygulaması**

Amaç: Kullanıcıların veri erişim hareketlerini izlemek ve izinsiz erişimleri tespit etmek.

- **Erişim Loglama**: Hangi kullanıcıların hangi verilere ne zaman eriştiği konusunda detaylı loglama işlemi gerçekleştirildi. Bu loglar, izinsiz erişimlerin tespit edilmesi ve güvenlik denetimlerinin yapılması için düzenli olarak incelendi.
- **Log Analizi ve İzleme**: Logların analizi için otomatik izleme sistemleri kuruldu ve anormal davranışlar tespit edildiğinde hızlı müdahale sağlandı.
- **Kullanım Alanı Örneği**: Banka veritabanlarına yapılan her erişimin loglanması ve bu logların düzenli olarak denetlenmesi.

Loglama Uygulaması
Müşteri verilerine erişim hareketlerini izlemek amacıyla detaylı loglama yapıldı. PostgreSQL veritabanında pgaudit eklentisi kullanılarak erişim ve işlem logları tutuldu. Log verileri, merkezi bir güvenlik izleme sistemi olan SIEM (Security Information and Event Management) sistemine aktarıldı. Bu sistem, logları analiz ederek anormal aktiviteleri tespit etti ve güvenlik ihlallerine hızlıca müdahale edilmesini sağladı.

4. **Veritabanı Güvenlik Politikaları**

Amaç: Veritabanında depolanan verilerin güvenliğini artırmak ve izinsiz erişimleri engellemek.

- **Şifreleme**: Veritabanında depolanan verilerin şifrelenmesi sağlandı. Özellikle hassas müşteri bilgileri şifrelenerek güvenlik artırıldı.
- **Veritabanı Firewall ve Erişim Kontrolleri**: Veritabanına yalnızca yetkili IP adreslerinden erişim sağlanacak şekilde güvenlik duvarı kuralları oluşturuldu.
- **Kullanım Alanı Örneği:** Hasta bilgilerinin şifrelenmesi ve yalnızca yetkili sağlık personelinin bu verilere erişebilmesi.

Veritabanı Güvenlik Politikaları
Veritabanı güvenliğini artırmak için şifreleme yöntemleri kullanıldı. PostgreSQL'in pgcrypto modülüyle müşteri verileri şifrelenerek depolandı. Veritabanı erişimi yalnızca belirli IP adreslerinden veya VPN üzerinden yapılabilecek şekilde güvenlik duvarlarıyla kontrol altına alındı. Ayrıca, veritabanı güvenlik denetimleri düzenli olarak gerçekleştirildi ve penetrasyon testleri ile güvenlik açıkları tespit edilerek giderildi.

5. **Veri İhlali Yönetimi**

Amaç: Veri ihlali durumlarında etkili bir müdahale ve bilgilendirme süreci oluşturmak.

- **Veri İhlali Bildirimi**: KVKK gereğince, bir veri ihlali durumunda ilgili makamları ve etkilenen bireyleri zamanında bilgilendirme süreci belirlendi ve uygulandı.
- **İhlal Öncesi ve Sonrası Planlama**: Veri ihlalleri için müdahale planı oluşturuldu. Veri kurtarma ve hasar tespiti süreçleri belirlendi ve uygulandı.
- **Kullanım Alanı Örneği**: Müşteri verilerinin çalınması durumunda, hızlı bir şekilde müşteri bilgilendirmesi ve hasar kontrolü yapılması.

Veri İhlali Yönetimi
Veri ihlali durumunda uygulanacak adımlar detaylı bir müdahale planıyla belirlendi. Bu kapsamda, olası bir ihlal durumunda veri kurtarma ve hasar tespiti için süreçler oluşturuldu. Düzenli yedeklemeler yapılarak verilerin güvenliği sağlandı ve olası bir ihlal durumunda hızlıca geri yükleme işlemleri gerçekleştirildi. KVKK gereğince veri ihlali bildirim süreçleri hazırlandı ve ihlal durumunda ilgili makamlar ve müşteriler bilgilendirildi.

6. **Veri Kaybı Önleme (Data Loss Prevention - DLP)**

Amaç: Hassas verilerin izinsiz kopyalanmasını veya sızdırılmasını önlemek.

- **DLP Araçları**: Veri kaybını önlemek için DLP araçları kullanıldı ve hassas verilerin izinsiz kopyalanması veya dışarı sızdırılması engellendi.
- **Ağ İzleme ve Kontrol**: Ağ trafiği analiz edilerek, hassas veri sızdırma girişimleri tespit edildi ve engellendi.
- **Kullanım Alanı Örneği**: Kredi kartı bilgileri gibi hassas verilerin izinsiz olarak dışarı sızdırılmasını engellemek için DLP çözümleri kullanımı.

Veri Kaybı Önleme (Data Loss Prevention - DLP)
DLP araçları kullanılarak verilerin izinsiz kopyalanmasını veya sızdırılmasını önleyici önlemler alındı. Ayrıca, ağ trafiği izleme ve kontrol sistemleri kurularak, hassas veri sızdırma girişimleri tespit edilip engellendi. Bu amaçla kullanılan DLP yazılımı, veritabanı ve ağ trafiği üzerinde izleme yaparak hassas verilerin izinsiz olarak dışarı çıkmasını engelledi.

7. **İki Aşamalı Kimlik Doğrulama (Two Factor Authentication – 2FA)**

Amaç: Hesap güvenliğini artırmak ve izinsiz girişleri önlemek.

- **Doğrulama Süreci:** Kullanıcıların hesaplarına giriş yaparken yalnızca şifre ile değil, ek olarak bir doğrulama kodu kullanmaları sağlandı. Bu kod, SMS, e-posta veya bir kimlik doğrulama uygulaması üzerinden iletildi.
- **Güvenlik Seviyesi:** Şifrenin yanı sıra ikinci bir doğrulama faktörü eklenerek, hesap güvenliği artırıldı. Bu sayede, kullanıcıların hesaplarına izinsiz girişlerin önüne geçildi.
- **Entegrasyon:** 2FA sistemi uygulamanın giriş ekranına entegre edildi. Kullanıcı deneyimi bozulmadan, güvenlik seviyesinin artırılması sağlandı. Kullanıcıların 2FA ayarlarını yönetebilmeleri için bir ayarlar menüsü oluşturuldu.
- **Kullanım Alanı Örneği**: Bankacılık uygulamaları gibi yüksek güvenlik gerektiren platformlar.

İki Faktörlü Kimlik Doğrulama (Two-Factor Authentication - 2FA)

İki faktörlü kimlik doğrulama (2FA) uygulanarak, kullanıcı hesaplarına girişte ek güvenlik önlemleri alındı. Kullanıcılar, şifrelerini girdikten sonra ikinci bir doğrulama faktörü olarak SMS, e-posta veya kimlik doğrulama uygulamaları aracılığıyla gönderilen bir kodu girmek zorunda bırakıldı. Bu yöntem, hesap güvenliğini artırarak izinsiz erişimlerin önüne geçilmesini sağladı. 2FA sistemi, uygulamanın giriş ekranına entegre edildi ve kullanıcıların bu özelliği kolayca yönetebilmeleri için ayarlar menüsünde gerekli düzenlemeler yapıldı.

8. **Ek Olarak Önerilen Etkili Yöntemler**

Amaç: Güvenlik önlemlerini daha da güçlendirmek ve sistemin güvenliğini artırmak.

Bu süreçte yapılabilecek ek güvenlik yöntemleri arasında SIEM sistemleri entegrasyonu ve düzenli penetrasyon testleri yer aldı. SIEM sistemleri, tüm güvenlik olaylarını merkezi bir noktada toplayarak analiz etti ve anormal aktiviteleri tespit etti. Düzenli penetrasyon testleri yapılarak sistemdeki güvenlik açıkları tespit edilip kapatıldı. Kullanım alanlarına SIEM sistemleri için büyük ölçekli kurumsal ağlar ve veri merkezleri, penetrasyon testleri ve güvenlik denetimleri için de herhangi bir hassas veri işleyen kurum ve kuruluşlar verilebilir.