SECURITY ALTERNATIVES SEARCHING

KVKK Kapsamında Müşteri Verilerinin Güvenliği ve Erişim Sınırlandırması

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 sağlanak. Veritabanı düzeyinde kullanıcı gruplarına veya bireysel kullanıcılara rol bazlı erişim hakları tanımlanacak. Sadece belirli yetkiye sahip kullanıcıların müşteri verilerini görmesi veya güncelleyebilmesi sağlanacaktır.
- **Hassas Verilerin Maskelenmesi**: Kullanıcıların yetkilerine göre verilerin maskelenmesi işlemi gerçekleştirilecek.
- **Entegrasyon**: RBAC implementasyonu kapsamında, veritabanı düzeyinde kullanıcı rolleri ve izinleri yapılandırılacaktır. Uygulama seviyesi yetkilendirme kuralları belirlenerek, veri ve işlemlere erişim sınırlandırılacaktır.

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) uygulanacaktır. Öncelikle, veritabanı düzeyinde kullanıcı grupları ve bireysel kullanıcılar için roller tanımlanacak, PostgreSQL veritabanı üzerinde GRANT komutu kullanılarak belirli tablolara veya sütunlara erişim yetkisi verilecek, uygulama seviyesinde ise, kullanıcı rolleri ve yetkileri belirlenerek, her kullanıcı için farklı erişim hakları tanımlanacaktır. Hassas verilerin maskelenmesi de bu süreçte gerçekleştirilecektir.

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 maskelenecektir. Müşteri adları, adresler veya telefon numaraları maskelenmiş olarak gösterilecektir.
- **Anonimleştirme**: Veri setlerinden kişisel tanımlayıcı bilgilerin (PII) tamamen kaldırılması işlemi tamamlanacaktır.

Veri Maskeleme ve Anonimleştirme

Hassas verilerin gizliliğini sağlamak amacıyla, veri maskeleme teknikleri kullanılacaktır, PostgreSQL'de yerleşik veri maskeleme özellikleri kullanılarak, müşteri adları ve adresleri gibi bilgilerin belirli kısımları maskelenecek, ayrıca anonimleştirme teknikleri kullanılarak veri setlerinden kişisel tanımlayıcı bilgiler

kaldırılacaktır. Bu işlem ile, verilerin analiz süreçlerinde kullanılmasına olanak tanırken, müşteri gizliliğini koruma altına almış olacağız.

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 gerçekleştirilecektir. Bu loglar, izinsiz erişimlerin tespit edilmesi ve güvenlik denetimlerinin yapılması için düzenli olarak incelenecektir.
- **Log Analizi ve İzleme**: Logların analizi için otomatik izleme sistemleri kurulup, anormal davranışlar tespit edildiğinde hızlı müdahale sağlanacaktır.

Loglama Uygulaması
Müşteri verilerine erişim hareketlerini izlemek amacıyla detaylı loglama yapılacak, PostgreSQL veritabanında pgaudit eklentisi kullanılarak erişim ve işlem logları tutulacak, log verileri, merkezi bir güvenlik izleme sistemi olan SIEM (Security Information and Event Management) sistemine aktarılacaktır. Bu sistem, logları analiz ederek anormal aktiviteleri tespit edip, güvenlik ihlallerine hızlıca müdahale edilmesini sağlayacaktır.

4. Veritabanı Güvenlik Politikaları

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

- **Şifreleme**: Veritabanında depolanan verilerin şifrelenmesi sağlanacak, özellikle hassas müşteri bilgileri şifrelenerek güvenlik artırılacaktır.
- **Veritabanı Firewall ve Erişim Kontrolleri**: Veritabanına yalnızca yetkili IP adreslerinden erişim sağlanacak şekilde güvenlik duvarı kuralları oluşturulacaktır.

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

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 belirlenip, uygulanacaktır.
- **İhlal Öncesi ve Sonrası Planlama**: Veri ihlalleri için müdahale planı oluşturulacak, veri kurtarma ve hasar tespiti süreçleri belirlenecek ve uygulanacaktır.

Veri İhlali Yönetimi
Veri ihlali durumunda uygulanacak adımlar detaylı bir müdahale planıyla belirlenecek, bu kapsamda, olası bir ihlal durumunda veri kurtarma ve hasar tespiti için süreçler oluşturulaacak, düzenli yedeklemeler yapılarak verilerin güvenliği sağlandı ve olası bir ihlal durumunda hızlıca geri yükleme işlemleri gerçekleştirilecektir. KVKK gereğince veri ihlali bildirim süreçleri hazırlandı ve ihlal durumunda ilgili makamlar ve müşteriler bilgilendirilecektir.

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

Amaç: Hassas verilerin izinsiz kopyalanmasını veya sızdırılmasını önlemek.

- **DLP Araçları**: Veri kaybını önlemek için DLP araçları kullanılacak ve hassas verilerin izinsiz kopyalanması veya dışarı sızdırılması engellenecektir.
- **Ağ İzleme ve Kontrol**: Ağ trafiği analiz edilerek, hassas veri sızdırma girişimleri tespit edilirse engellenecektir.

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 sağlanacaktır. Bu kod, SMS, e-posta veya bir kimlik doğrulama uygulaması üzerinden iletilicektir.
- **Güvenlik Seviyesi:** Şifrenin yanı sıra ikinci bir doğrulama faktörü eklenerek, hesap güvenliği artırılacak bu sayede, kullanıcıların hesaplarına izinsiz girişlerin önüne geçilecektir.

- **Entegrasyon:** 2FA sistemi uygulamanın giriş ekranına entegre edilerek kullanıcı deneyimi bozulmadan, güvenlik seviyesinin artırılması sağlanacaktır. Kullanıcıların 2FA ayarlarını yönetebilmeleri için bir ayarlar menüsü oluşturulacaktır.

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

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