Security İşlemleri

Problem

Müşterilere ait verilere erişimi KVKK kapsamında sınırlandırmanız gerekmektedir. Üretim ortamında herhangi bir erişime ait iz bırakmak adına ne gibi alternatifler kullanabilir veya güvenliği sağlarsınız (Tabloya kişi bazlı erişim yetkisi, loglama uygulaması vs.)

Çözüm

Kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi gibi problemlerin önüne geçmek için 2016 senesinde Kişisel Verileri Koruma Kanunu çıkarılmıştır. Araç kiralama uygulamasında da müşteri verilerinin korunması gerekmektedir. Dış kaynaklı tehditlere karşı koruma sağlanmasının yanı sıra, uygulama geliştiricileri tarafından yapılabilecek suistimallerin de önüne geçilmelidir. Geliştiricilerin üretim ortamındaki uygulamada yaptıkları işlemler kayıt altına alınmalı ve sonradan izlenebilir olmalıdır. Ayrıca müşteri verilerinin yer aldığı veri tabanına erişim sırasında çeşitli kısıtlamalar konulmalı ve veri tabanı noktasında karşılaşılabilecek yetkisiz girişler engellenmelidir. Bütün bu istekleri gerçekleştirmek için aşağıda listelenen adımlar gerçekleştirilebilir.

1. Kişi Bazlı Erişimin Yetkilendirilmesi

Uygulama geliştiricilerine verilecek roller sayesinde yetkisiz erişimlerin önüne geçilebilir. Rol Tabanlı Erişim Kontrolü (RBAC) mekanizması tasarlanarak, geliştiricilerin sadece gerekli olduğu durumlarda müşteri verilerine erişebilmesine ve geliştiricilerin rollerine göre müşteri verilerinin sadece ihtiyaç duyulan kısmına erişim sağlamasına onay verilebilir. Şayet veri tabanındaki müşteri verilerine erişim konusunda daha katı bir yol izlenmek isteniyorsa kişi bazlı erişim izinleri oluşturulabilir. Örnek vermek gerekirse, sadece belli geliştiriciler müşteri verilerinin bir kısmına erişim sağlayabilir. Ayrıca uygulamanın geliştirilme sürecinde, sadece belirli müşterilerin verilerine erişim sağlanarak, diğer müşterilerin verilerinin erişimine engel olunabilir.

2. İzin ve Onay Süreçleri

Geliştiricilerin müşteri verilerine erişimi konusunda eklenebilecek kısıtlardan biri de onay süreçleri sonucunda müşteri verilerine erişim sağlanması yöntemidir. Geliştirici firmadaki bir üst yetkili veya bizzat müşterinin onayı olmadan müşterinin verilerine erişilememesi şeklinde

bir kısıt konularak, müşteri verilerinin gizliliğinin korunması sağlanabilir. Ayrıca verilen bu onay, kalıcı bir onay olmak yerine, sadece işlem süresince kullanılabilecek bir geçici onay da olabilir. Veyahut belirli bir süre ile kısıtlanan erişim onayı tanımlanarak, erişim süresi dolduktan sonra geliştiricilerin müşteri verilerine erişimi kısıtlanabilir.

Üretim ortamındaki müşteri verilerinin güçlü şifreleme teknikleri kullanılarak korunmaya alınması da geliştirici kaynaklı oluşabilecek problemlerin önüne geçmek için kullanılabilecek önemli bir yöntemdir. Bu yöntem kullanıldığı zaman, geliştirici erişim iznine sahip olsa bile, verilerin anlamlı bir şekline erişebilmesi için şifre çözücü anahtara ihtiyaç duyacağından dolayı, geliştirici kaynaklı veri sızıntılarının önüne geçilebilmektedir.

3. Geliştirici Ortamı ve Üretim Ortamının Ayrılması

Uygulamanın geliştirilmesi sürecinde geliştiricilerin müşteri verilerine erişememesi için eklenebilecek mekanizmalardan biri, geliştirme yapılan ortam ile müşteri verilerinin yer aldığı üretim ortamını ayırmaktır. Bir örnekle açıklamak gerekirse, uygulamanın geliştirildiği ve test edildiği ortamlarda anonimleştirilmiş veya maskelenmiş veri setleri kullanılarak gerçek müşteri verilerine erişim kısıtlanabilir. Bu sayede geliştiriciler ve test mühendisleri – müşteri verilerine erişmeye gerek duymadan – güvenle uygulamanın üretim sürecinde yer alabilirler.

4. Loglama ve İzleme Yöntemleri

Uygulama geliştiricilerinin müşteri verilerinin yer aldığı veri tabanını kullanarak yaptıkları işlemlerin tamamı detaylı bir şekilde kayıt altına alınarak, loglama mekanizması kurulabilir. Bu log kayıtlarında geliştiriciye ait bilgiler, verilere erişim zamanı, erişilen verilerin türü, veri tabanı üzerinde yapılan işlemler gibi kayıtlar yer almalıdır. Ayrıca geliştirilecek bir log uygulaması aracılığıyla, log kayıtları üzerindeki anormal veya yetkisiz erişimleri tespit eden bir sistem kurulmalıdır. Bu sistem aracılığıyla anormal veya yetkisiz işlemler otomatik olarak belirlenebilir ve uyarı verilebilir.

Müşteri verilerinin log kayıtlarında da korunması amacıyla, veri maskeleme teknikleri kullanılarak, müşteri verilerinin kısmen görüntülenebildiği log kayıtları oluşturulabilir.

Erişim log kayıtlarının periyodik olarak denetlenmesi de güvenlik ihlallerini tespit etmek için kullanılabilecek yöntemlerden biridir. Bu noktada log kayıtları kullanılarak detaylı güvenlik raporları oluşturulabilir ve geliştiricilerin üretim ortamlarını kullanım alışkanlıklarına dair detaylı veriler çıkarılabilir.