KVKK'ya (Kişisel Verileri Koruma Kanunu) uyum sağlamak ve müşteri verilerinin güvenliğini sağlamak için özellikle üretim ortamlarında çeşitli güvenlik önlemleri alabilirsiniz. Bu önlemler arasında erişim kontrolü, loglama, veri şifreleme ve güvenli geliştirme uygulamaları bulunur. İşte bu konuda nasıl bir yaklaşım izleyebileceğinize dair öneriler:

1. **Erişim Kontrolü**
   1. **Tablo Bazlı Erişim Kontrolü:**

**Rol Tabanlı Erişim Kontrolü (RBAC):**

Tanım:

Rol Tabanlı Erişim Kontrolü (RBAC), kullanıcıların rollerine göre sistem kaynaklarına erişimini yönetir. Kullanıcılar belirli roller alır ve bu roller aracılığıyla veri tabanı tablolarına, satırlara veya sütunlara erişir.

Uygulama:

Roller ve İzinler: Admin, geliştirici, analist gibi roller tanımlanır ve her rol için belirli erişim izinleri atanır.

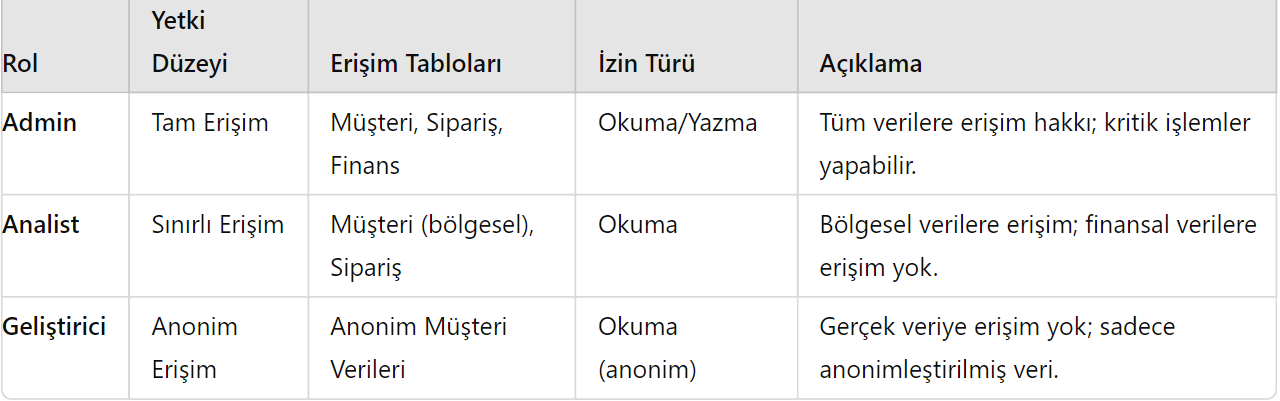
Erişim Sınırlaması: Kullanıcılar, yalnızca rollerine uygun verilere erişebilir (örneğin, geliştirici anonim verilerle, analist bölgesel verilerle sınırlıdır).

Avantajları:

Güvenli: Kullanıcıların yalnızca gerekli verilere erişimini sağlar.

Esnek: Rollerin ve izinlerin kolayca ayarlanmasını sağlar.

Merkezi Yönetim: Erişim kontrolleri merkezi olarak yönetilir.



**Özellik Tabanlı Erişim Kontrolü (ABAC)**:

Tanım:

Özellik Tabanlı Erişim Kontrolü (ABAC), kullanıcıların erişimini, kullanıcı özellikleri (rol, departman, konum) ve verilerin hassasiyeti gibi kriterlere göre yönetir. Bu yaklaşım, daha ayrıntılı ve dinamik erişim kontrolü sağlar.

Uygulama:

Kriterler: Erişim, kullanıcının rolü, departmanı, fiziksel konumu ve veri hassasiyetine göre belirlenir.

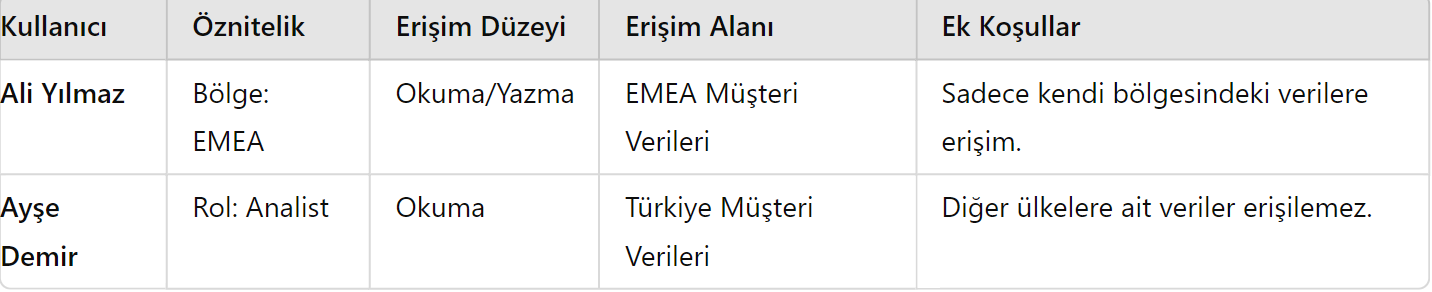
Dinamik Erişim: Kullanıcıların erişim yetkileri, sistemdeki değişikliklere ve veri hassasiyetine göre dinamik olarak ayarlanır.

Avantajları:

Detaylı Kontrol: Erişimi, birden fazla kriter ile ince ayar yaparak yönetir.

Uyumlu: Veri hassasiyetine göre erişimi düzenleyerek güvenliği artırır.

Esnek: Kullanıcı özelliklerine dayalı dinamik erişim sağlar.



* 1. **En Az Ayrıcalık Prensibi:**

Tanım:

Kullanıcılara yalnızca görevlerini yerine getirmek için gerekli minimum erişim seviyesini sağlayın.

Uygulama:

Erişim Kısıtlaması: Kullanıcılara sadece iş görevlerini tamamlamaları için gerekli olan en düşük erişim yetkilerini verin.

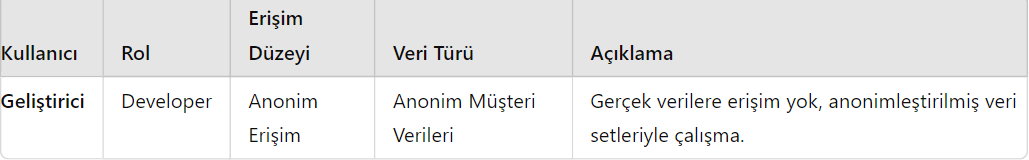
Örnek: Geliştiriciler, üretim verilerine doğrudan erişim yerine anonimleştirilmiş veya sentetik veri setleriyle çalışabilirler.

Avantajları:

Güvenlik: Yetkisiz erişim riskini azaltır.

Veri Koruma: Hassas bilgilerin korunmasına yardımcı olur.

İş Sürekliliği: Erişim gereksinimlerine göre veri güvenliğini sağlar.



* 1. **Veritabanı Düzeyinde Güvenlik:**

**Satır Düzeyinde Güvenlik (RLS**)

**Tanım:**

Kullanıcının rolüne göre veri görünürlüğünü kısıtlamak için satır düzeyinde güvenlik uygulayın.

Uygulama:

Erişim Kısıtlaması: Kullanıcıların yalnızca yetkili oldukları veri satırlarını görmelerini sağlayın.

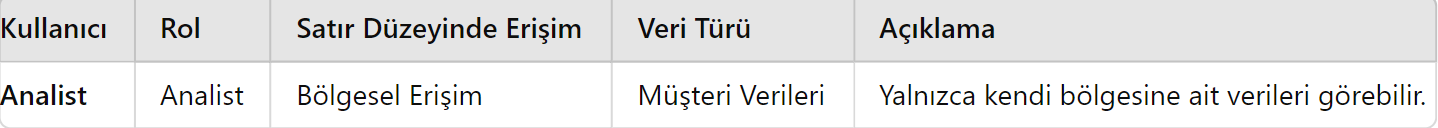
Örnek: Bir analist, yalnızca kendi bölgesi veya departmanıyla ilgili kayıtları görüntüleyebilir.

Avantajları:

Veri Gizliliği: Hassas bilgilerin yetkisiz kullanıcılar tarafından görüntülenmesini önler.

Veri Yönetimi: Verilerin daha düzenli ve kontrol altında tutulmasını sağlar.

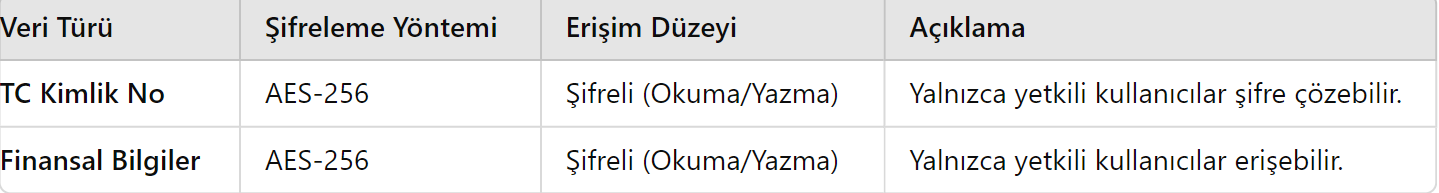
Uyumluluk: Veri erişim politikaları ve yasal gerekliliklerle uyumu destekler.



Sütun Düzeyinde Şifreleme, hassas verilerin güvenliğini sağlamak amacıyla kullanılan bir veri koruma yöntemidir. Bu yaklaşım, özellikle TC Kimlik Numarası, finansal bilgiler ve diğer kritik verilerin bulunduğu sütunları hedef alır. Şifreleme, bu sütunlarda yer alan verilerin yetkisiz erişim durumlarında dahi korunmasını sağlar.

Bu strateji, yalnızca yetkilendirilmiş kullanıcıların ve sistemlerin bu verilere erişimini mümkün kılar, böylece herhangi bir güvenlik ihlali veya veri sızıntısı yaşansa bile şifreli verilerin anlamlandırılması imkânsız hale gelir. Sütun düzeyinde şifreleme, veri güvenliğinin artırılması ve uyumluluk gereksinimlerinin karşılanması açısından kritik bir öneme sahiptir.

Ayrıca, şifreleme süreci performans optimizasyonlarıyla entegre edilerek sistemin verimliliğini etkilemeyecek şekilde uygulanır. Bu sayede hem veri bütünlüğü korunur hem de işletmelerin güvenlik ve yasal uyumluluk gereksinimlerini karşılayarak, kullanıcıların ve müşterilerin bilgilerinin güvenliği sağlanır.

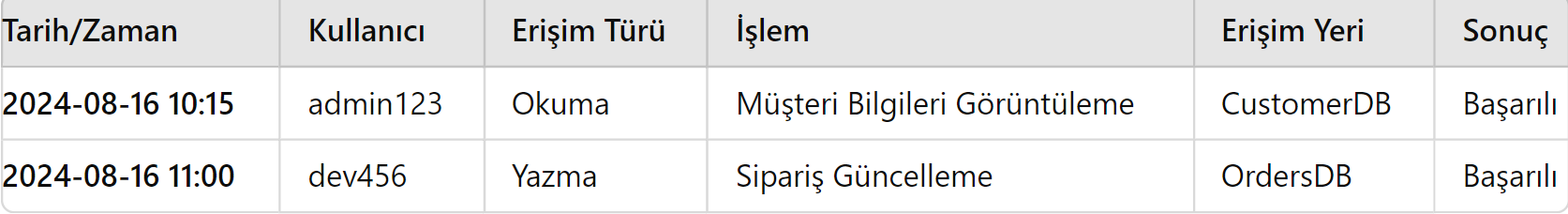


1. **Loglama ve Denetim**
   1. **Loglama:**

Loglama, veri güvenliği ve sistem izlenebilirliği açısından kritik bir süreçtir. Bu süreç, sistemde gerçekleşen tüm erişim ve işlem aktivitelerinin detaylı bir şekilde kaydedilmesini içerir. Özellikle kimlerin hangi verilere eriştiği, hangi işlemlerin gerçekleştirildiği ve bu işlemlerin ne zaman yapıldığı loglama yoluyla belgelenir.

Bu loglar, denetim süreçlerinde ve adli analizlerde vazgeçilmez bir rol oynar. Sistem üzerinde gerçekleşen tüm olayların izini sürmek, güvenlik ihlalleri ve şüpheli aktivitelerin tespit edilmesi açısından önemlidir. Ayrıca, yasal uyumluluk gereksinimlerinin karşılanmasında ve olası sorunların hızlı bir şekilde çözüme kavuşturulmasında loglama verileri kilit bir öneme sahiptir.

Bu nedenle, güvenilir bir loglama altyapısı kurmak, işletmelerin bilgi güvenliği stratejilerinin merkezinde yer almalıdır. Sistemlerin düzenli olarak izlenmesi ve kaydedilen logların analiz edilmesi, işletmelerin risk yönetimi süreçlerini güçlendirmekte ve olası tehditlere karşı proaktif önlemler alınmasını sağlamaktadır.



**Araçlar:**

Merkezi Loglama Çözümleri

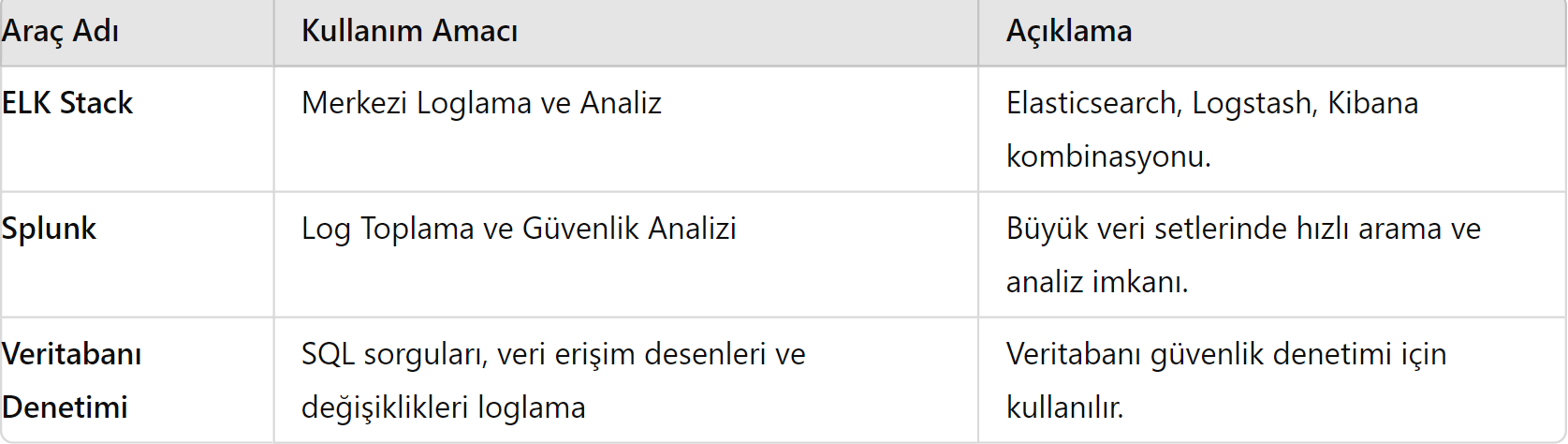
Merkezi loglama çözümleri, çeşitli sistemlerden gelen logların toplanması, depolanması ve analiz edilmesi sürecini etkin bir şekilde yönetmek için kullanılan kritik araçlardır. Bu çözümler, farklı sistemlerden gelen logların merkezi bir noktada toplanmasını sağlayarak, sistem genelinde bütüncül bir izleme ve analiz imkanı sunar.

Bu bağlamda, ELK Stack (Elasticsearch, Logstash, Kibana) ve Splunk gibi araçlar, işletmelerin merkezi log yönetimi ihtiyaçlarını karşılamak için tercih edilen popüler çözümler arasındadır. ELK Stack, log verilerini toplayıp filtrelemek için Logstash'ı, verileri depolamak ve aramak için Elasticsearch'ü, görselleştirme ve analiz için ise Kibana'yı kullanır. Splunk ise, yüksek performanslı log toplama, analiz ve raporlama özellikleri ile dikkat çeker. Bu araçlar sayesinde, log verilerinin analiz edilmesi, olası güvenlik tehditlerinin tespit edilmesi ve sistem performansının optimize edilmesi sağlanır.

Veritabanı Denetimi

Veritabanı denetimi, veri güvenliğini artırmak ve sistem üzerindeki aktiviteleri izlemek amacıyla kullanılan bir diğer önemli süreçtir. Veritabanı denetim özelliklerinin etkinleştirilmesi, veritabanına yapılan tüm SQL sorgularının, veri erişim desenlerinin ve veritabanında gerçekleştirilen değişikliklerin ayrıntılı bir şekilde loglanmasını sağlar.

Bu denetim süreçleri, veri güvenliği ihlallerinin tespit edilmesi, veri bütünlüğünün korunması ve yasal uyumluluk gereksinimlerinin karşılanması açısından kritik bir rol oynar. Ayrıca, veritabanı aktivitelerinin izlenmesi, performans sorunlarının belirlenmesi ve optimizasyon fırsatlarının değerlendirilmesi için de önemli bir araçtır. Veritabanı denetim özellikleri, sistem yöneticilerine veri erişim desenlerini ve kullanıcı aktivitelerini detaylı bir şekilde analiz etme imkanı sunarak, daha güvenli ve verimli bir veri yönetimi sağlar.

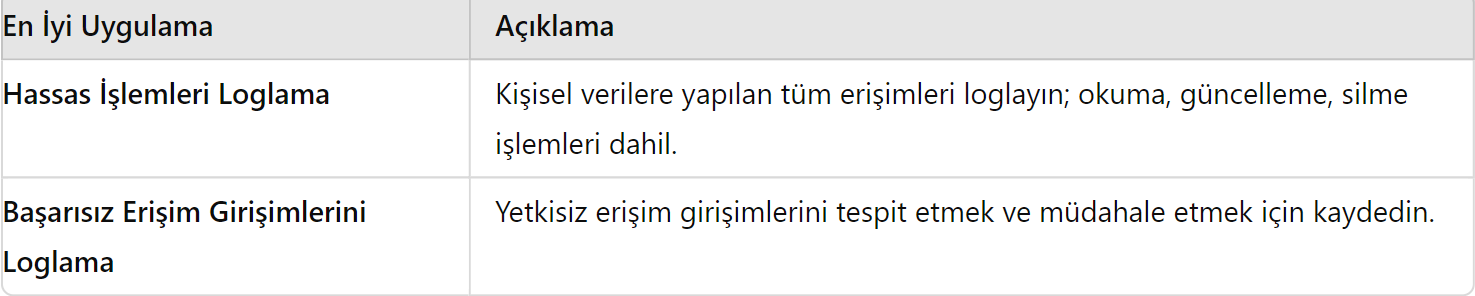


**En İyi Uygulamalar:**

Hassas İşlemleri Loglayın: Kişisel verilere yapılan tüm erişimleri loglayın, okuma, güncelleme, silme işlemleri dahil.

Başarısız Erişim Girişimlerini Loglayın: Veriye erişim başarısızlıklarını kaydederek potansiyel güvenlik ihlallerini tespit edin.

Log Saklama Politikaları: Yasal gerekliliklere uygun log saklama politikaları uygulayarak logların gerekli süre boyunca saklandığından emin olun.



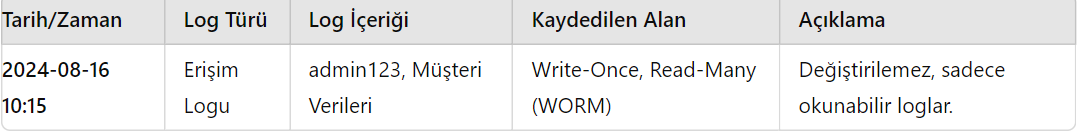
**2.2. Değiştirilemez Loglar:**

Logların WORM Formatında Saklanması

Log verilerinin bütünlüğünü korumak ve güvenilir bir denetim izi sağlamak amacıyla, logların yaz-once, oku-çok (WORM) formatında saklanması kritik bir adım olarak değerlendirilir. WORM formatı, logların ilk yazıldığı andan itibaren değiştirilmesini veya silinmesini önleyerek, güvenlik ve denetim açısından önemli avantajlar sunar.

WORM formatında saklanan loglar, oluşturuldukları andan itibaren herhangi bir manipülasyona karşı korunur, bu da logların güvenilirliğini artırır ve adli analizler için sağlam bir temel oluşturur. Ayrıca, bu yöntem sayesinde logların tarihçesi bozulmadan korunur, bu da uzun süreli denetim ve yasal uyumluluk gereksinimlerinin karşılanmasına yardımcı olur.

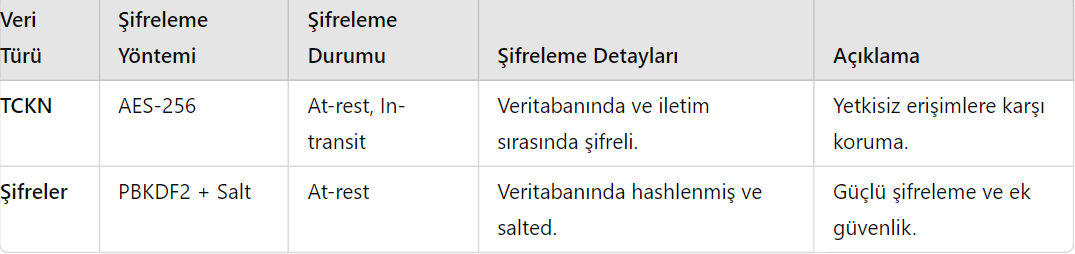
Bu nedenle, logların WORM formatında saklanması, güvenlik politikalarının bir parçası olarak benimsenmeli ve tüm sistemler için standart bir uygulama haline getirilmelidir. Bu yaklaşım, veri bütünlüğünü korurken, olası güvenlik tehditlerine karşı da etkin bir savunma mekanizması sağlar.



1. **Veri Şifreleme ve Hashleme**
   1. **Veri Şifreleme:**

Dinlenme Halinde:

**Veritabanı Şifrelemesi:** Veritabanında depolanan verileri şifrelemek için Şeffaf Veri Şifrelemesi (TDE) gibi teknolojiler kullanılmalıdır.



Dosya Şifrelemesi: Yedekleme dosyaları ve veri ihracı süreçlerinde, veri güvenliğini sağlamak amacıyla tüm dosyalar şifrelenmelidir.

Aktarım Halinde:

TLS/SSL Şifreleme: Uygulama ve veritabanı arasındaki veri iletiminde, veri güvenliğini sağlamak için

TLS/SSL şifreleme protokollerinin kullanılması gerekmektedir.

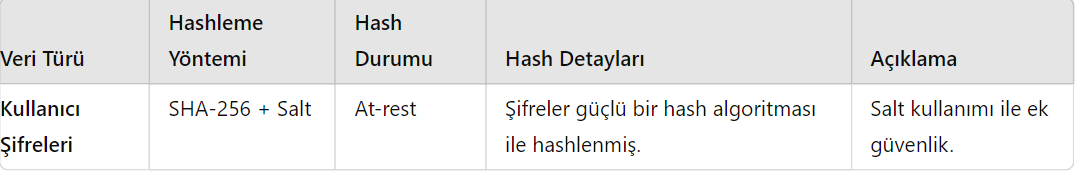
Veri Hashleme:

Amaç: Şifreler ve kişisel tanımlama numaraları (PIN) gibi hassas veriler hashlenerek depolanmalıdır. Bu, veritabanı ihlali durumunda bu bilgilerin kolayca geri alınmasını önler.

Araçlar:

Hashleme Algoritmaları: SHA-256 gibi güçlü hashleme algoritmaları kullanılmalı ve brute-force saldırılarına karşı koruma sağlamak amacıyla tuzlar (salts) ile desteklenmelidir.

HMAC (Hash-based Message Authentication Code): Veri bütünlüğü ve özgünlüğünü sağlamak için HMAC kullanılmalıdır.



* 1. **Anonimleştirme ve Takma Ad Kullanımı:**

Amaç: Geliştiricilerin gerçek müşteri bilgilerini ifşa etmeden, gerçekçi verilerle çalışmalarını sağlamak amacıyla kişisel tanımlayıcı veriler takma adlarla değiştirilmelidir.



Araçlar:

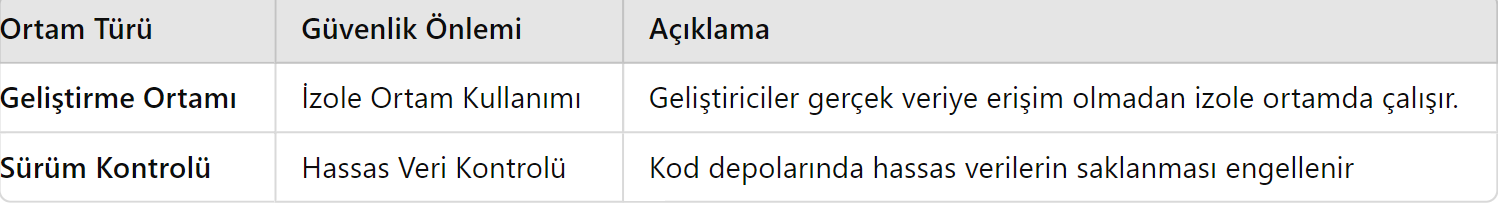
Veri Maskeleme Araçları:

Üretim dışı ortamlarda hassas bilgileri maskelemek için Data Masker veya Delphix gibi veri maskeleme araçları kullanılmalıdır.

1. **Güvenli Geliştirme Uygulamaları**
   1. **Geliştirme Ortamı:**

İzole Geliştirme Ortamları: Geliştiriciler, üretim verilerine doğrudan erişim sağlamadan izole ortamlarda çalışmalıdır. Bu ortamda anonimleştirilmiş veya sentetik veriler kullanılmalıdır.

Sürüm Kontrolü: Hassas verilerin kod depolarında ifşa edilmediğinden emin olmak için uygun erişim kontrolleriyle sürüm kontrol sistemleri (örn. Git) kullanılmalıdır.



**4.2. Sürekli Güvenlik Testi:**

Rapor Özeti: Müşteri Verilerinin KVKK'ya Uygun Olarak Korunması

Bu rapor, müşteri verilerini Kişisel Verilerin Korunması Kanunu'na (KVKK) uyumlu bir şekilde korumak için izlenmesi gereken stratejileri ve önlemleri kapsamaktadır. Aşağıda, bu stratejiler çeşitli başlıklar altında özetlenmiştir:

1. Erişim Kontrolü

Rol Tabanlı Erişim Kontrolü (RBAC): Erişim haklarını kullanıcı rollerine göre sınırlandırarak, yalnızca gerekli bilgilerin yetkilendirilmiş personel tarafından erişilmesini sağlayın.

2. Loglama

Merkezi Loglama Çözümleri: ELK Stack veya Splunk gibi araçlar kullanılarak, farklı sistemlerden logların merkezi bir yerde toplanması ve analiz edilmesi sağlanmalıdır.

Veritabanı Denetimi: SQL sorguları, veri erişim desenleri ve veritabanında yapılan değişikliklerin izlenmesi amacıyla veritabanı denetim özellikleri etkinleştirilmelidir.

WORM Formatında Saklama: Logların değiştirilememesi için yaz-once, oku-çok (WORM) formatında saklanması gereklidir.

1. Şifreleme

Sütun Düzeyinde Şifreleme: TC Kimlik Numarası ve finansal bilgiler gibi hassas veriler şifrelenmelidir. Bu sayede, yetkisiz erişim olsa bile veriler korunmuş olur.

1. Güvenli Geliştirme Uygulamaları

Statik Uygulama Güvenlik Testi (SAST): Geliştirme sırasında kodun güvenlik açıkları açısından taranması gereklidir.

Dinamik Uygulama Güvenlik Testi (DAST): Çalışan uygulamanın özellikle veri işleme konularında güvenlik açıkları açısından test edilmesi önemlidir.

1. İzleme ve Müdahale

Gerçek Zamanlı İzleme: Şüpheli etkinliklerin hızlı tespiti için veritabanı erişimi ve uygulama davranışları gerçek zamanlı olarak izlenmelidir.

Araçlar:

Gizli Giriş Tespit Sistemleri (IDS): Yetkisiz erişim girişimlerini tespit ederek uyarılar üretir.

SIEM: Logları analiz ederek olayları birleştirir ve altyapı genelinde tehditlere karşı koruma sağlar.

Olay Müdahale Planı: Veri ihlalleri durumunda etkili bir şekilde müdahale edebilmek için, olay müdahale planının geliştirilmesi ve düzenli olarak güncellenmesi gereklidir.

Sonuç

Müşteri verilerinin KVKK'ya uyumlu olarak korunması, erişim kontrolü, loglama, şifreleme, güvenli geliştirme uygulamaları ve sürekli izleme gibi güvenlik önlemlerinin bir kombinasyonunu gerektirir. Rol tabanlı erişim kontrollerinin uygulanması, hassas verilerin şifrelenmesi, kritik bilgilerin hashlenerek saklanması ve detaylı logların tutulması önemlidir. Ayrıca, geliştiricilerin anonimleştirilmiş verilerle izole ortamlarda çalışmasını sağlamak ve sürekli güvenlik testi yapmak, müşteri verilerinin etkili bir şekilde korunmasına yardımcı olur.