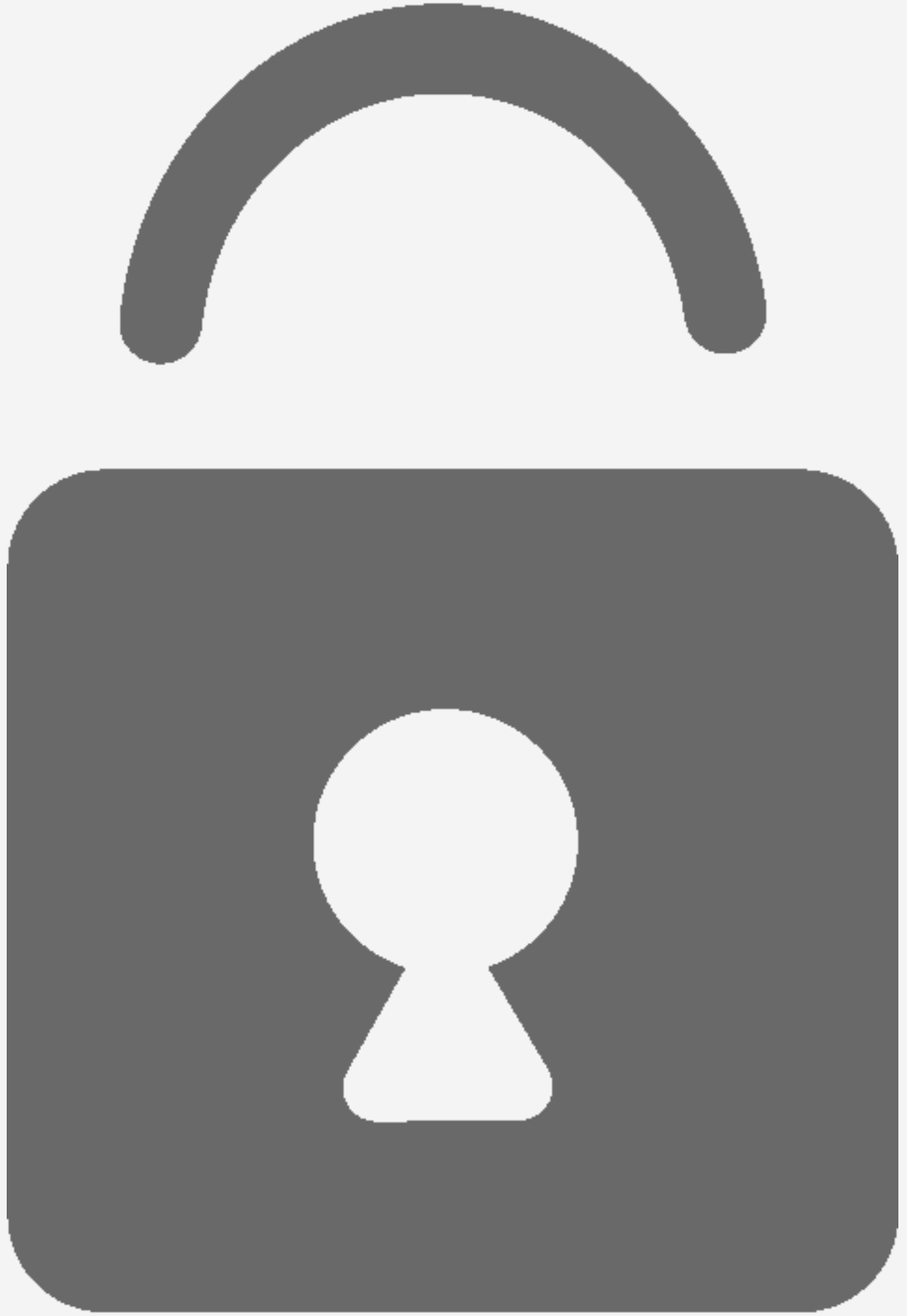
TARİH
28/03/2024

VERİTABANI GÜVENLİĞİ

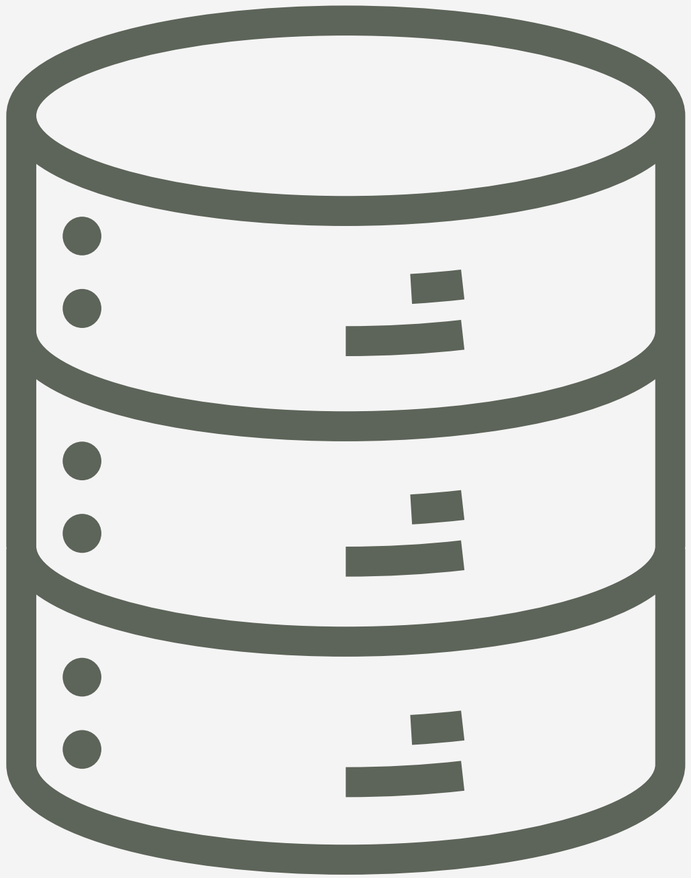
Dilara Ünsal
20360859070
Bilgisayar Mühendisliği 3. Sınıf



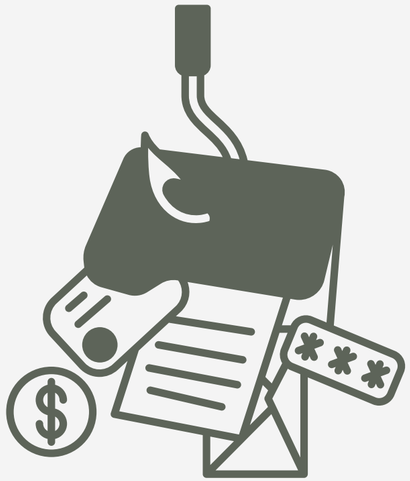
İÇİNDEKİLER

VERİTABANI

Veritabanı genellikle bir bilgisayar sisteminde elektronik olarak depolanan veriden oluşan düzenli bir koleksiyondur.

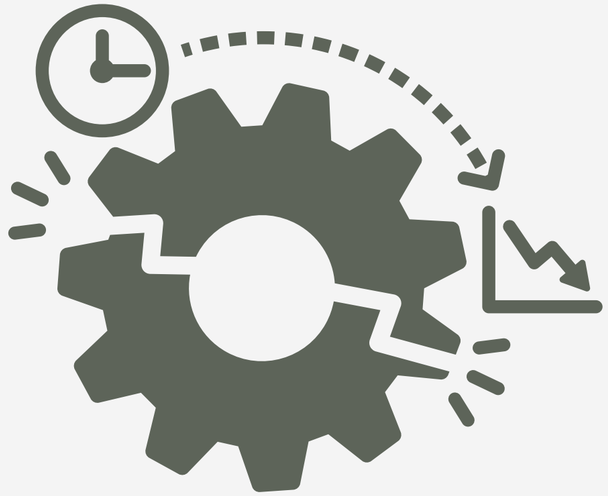


VERİTABANI GÜVENLİĞİ NEDEN ÖNEMLİ?



VERİ HIRSIZLIĞI

Veritabanları, genellikle değerli, gizli ve hassas bilgileri depoladıkları için siber saldırıların ana hedefleridir. Bilgisayar korsanları bu bilgileri kimlikleri çalmak ve yetkisiz satın alımlar yapmak için kullanır.



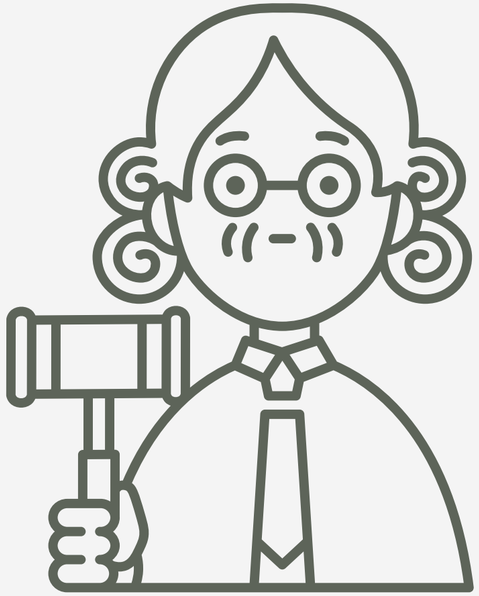
İTİBARININ ZEDELENMESİ

Müşteri bilgilerini tehlikeye atan veritabanı güvenliği sorunları, kuruluşun itibarına zarar verebilir, bu da satışlarda düşüşe ve müşteri kaybıyla sonuçlanabilir.

VERİTABANI GÜVENLİĞİ NEDEN ÖNEMLİ?

GELİR KAYBI

Bir veri ihlali, veritabanı güvenliği sorunları çözülene, sistem tamamen çalışır duruma gelene ve iş sürekliliği yeniden sağlanana kadar iş operasyonlarını ve gelir üretimini durdurabilir veya yavaşlatabilir.



VERİ İHLALİ CEZALARI

Eyalet ve yerel kurumlar, şirketlerin müşteri verilerini korumaması durumunda para cezaları kesilebilir ve bazı durumlarda müşterilere tazminat ödenmesini talep edilebilir.

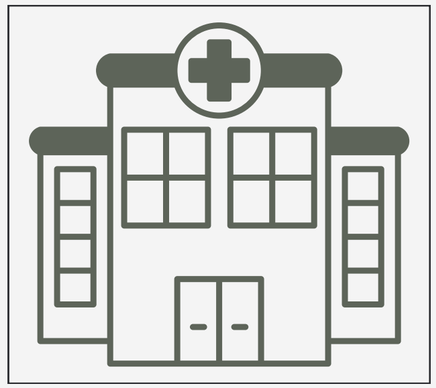
VERİTABANI SALDIRISINA MARUZ KALABİLECEK ALANLAR

Finansal Kurumlar

Bankalar ve diğer finansal kurumlar, büyük miktarda hassas veri barındırdıkları için veritabanı saldırılarına karşı oldukça savunmasızdır.

Hükümet Kurumları

Hükümet kurumları, vatandaşların kişisel bilgileri, ulusal güvenlik bilgileri ve diğer hassas verileri barındıran veritabanlarına sahiptir. Bu nedenle, siber saldırganlar için cazip hedeflerdir.



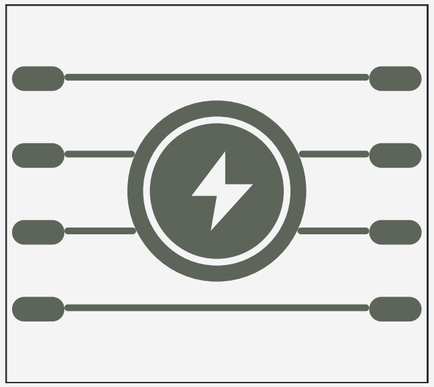
Sağlık Kuruluşları

Hastaneler ve diğer sağlık kuruluşları, hastaların tıbbi kayıtları ve diğer hassas verileri barındıran veritabanlarına sahiptir.

VERİTABANI SALDIRISINA MARUZ KALABİLECEK ALANLAR

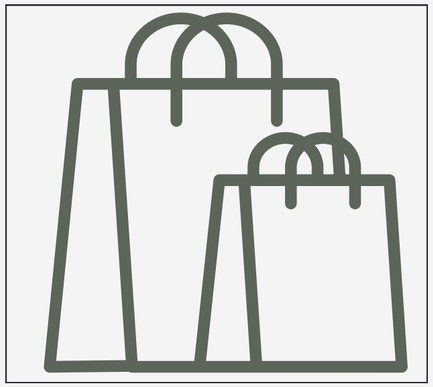
Teknoloji Şirketleri

Teknoloji şirketleri, fikri mülkiyet, araştırma ve geliştirme bilgileri ve müşteri bilgileri gibi hassas verileri barındıran veritabanlarına sahiptir.



Elektrik şebekeleri

Elektrik şebekeleri, SCADA (Gözetleyici Kontrol ve Veri Toplama Sistemi) sistemleri gibi kritik altyapı sistemlerini çalıştırmak için veritabanlarına güvenir.



Perakende Kuruluşları

Perakendeciler, müşterilerin kredi kartı bilgileri, adresleri ve diğer kişisel bilgileri barındıran veritabanlarına sahiptir.

SALDIRI ÖRNEKLERİ

UKRAYNA'YA SİBER SALDIRI (2015)

Saldırının ilk aşamasında, belirli kişileri hedef alan, kötü amaçlı ekler içeren e-postalar aracılığıyla gönderildi.

Saldırının ikinci bölümünde, bilgisayarların sabit disklerinin bazı kısımlarını silip sistemlerin yeniden başlatılmasını engelleyebilen ve sonuçta elektrik kesintilerine yol açan kötü amaçlı yazılımı etkinleştirdi.

Son aşamada, TDoS saldırısı başlatarak arayanların kesintiyi bildirmelerini engelledi.

VERİTABANI GÜVENLİĞİ TEHDİTLERİ

SQL ENJEKSİYONLARI

SQL Injection, bir web uygulamasının güvenlik açığını sömürerek veritabanı üzerinde istenmeyen SQL sorgularının çalıştırılmasına izin veren bir saldırı türüdür.

YETKİ İSTİSMARI VE AŞIRI AYRICALIK

Yetki İstismarı:
Kullanıcılar, veri erişim ayrıcalıklarını yetkisiz amaçlar için kötüye kullanabilirler.
Aşırı Ayrıcalık:
Kullanıcılar, eğer işlevleri gereğinden fazla ayrıcalığa sahipse, bu ayrıcalıklar birey veya hesaplarını ele geçiren saldırganlar tarafından kötüye kullanılabilir.

YETERSİZ KİMLİK DOĞRULAMALARI

Zayıf kimlik doğrulama, sızmak isteyen saldırganların yetkisiz erişim elde etmek için kullandığı brute-force saldırıları ve güvensiz parola depolama gibi zayıf noktaları içerir.

VERİTABANI GÜVENLİĞİ TEHDİTLERİ

KAYIT TUTMA VE DENETİM

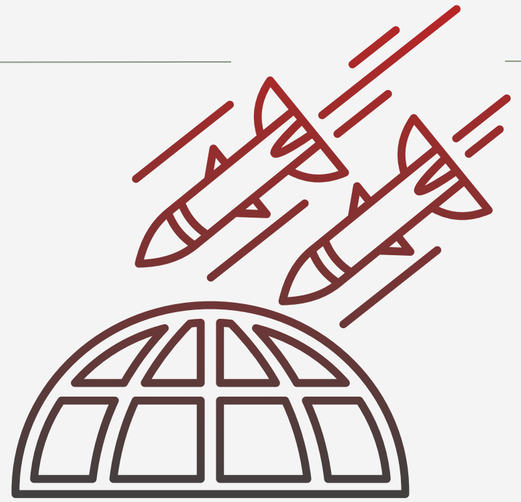
Kayıt tutma ve denetim, kötüye kullanımın önlenmesine ve tespit edilmesine yardımcı olmak ve şüpheli veri ihlallerinin yeterli şekilde araştırılmasını sağlamak için önemlidir.

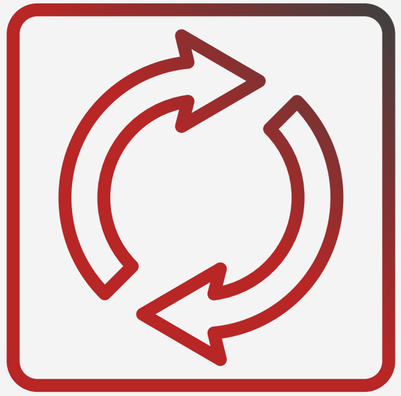
HİZMET REDDİ

Hizmet Reddi (DoS) saldırısı, bir makineyi veya ağı kapatmayı amaçlayan bir saldırıdır, böylece talep edilen servis kullanıcılar tarafından erişilemez hale gelir.

GÜNCELLENMEMİŞ HİZMETLER

Güncel yamaları yapmak, güvenliğinizi kesin olarak sağlamaz; ancak güvenlik açıklarını içeren güncellenmemiş hizmetleri kullanmak, büyük olasılıkla saldırıya maruz kalma riskinizi artırır.





VERİTABANI KORUMA YÖNTEMLERİ

Şifreleme:

Şifreleme, verilerinizi karmaşık algoritmalar kullanarak şifreler, böylece şifre çözme anahtarına sahip olmayan biri için okunamaz hale gelir.

Şifreleme, saldırganlar veritabanına girse bile bilgilerinizi koruyan sanal bir kalkan görevi görür.

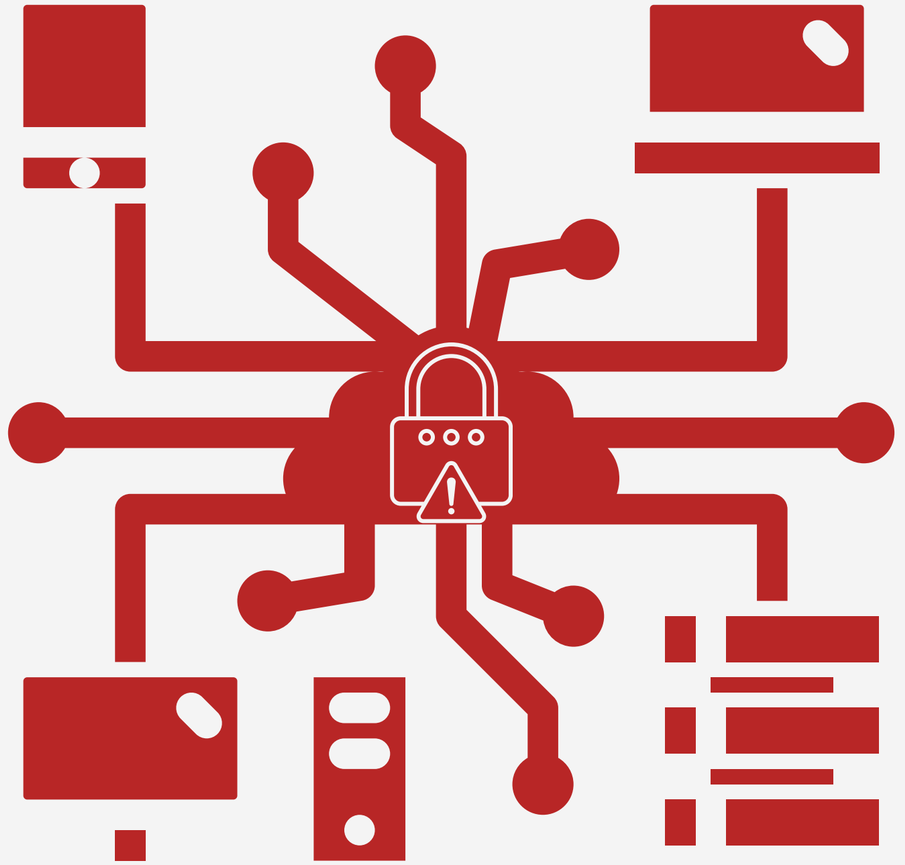
VERİTABANI KORUMA YÖNTEMLERİ

Ağ Güvenliği:

Veritabanları potansiyel bir giriş noktası olabilecek ağın içinde yer alır.

Ağ güvenliği sağlamak için :

- Güvenlik duvarını veritabanı sunucusunun önüne yerleştirilebilir ve yalnızca yetkili trafiğin geçmesine izin verilebilir.
- IDS ve IPS sistemlerini kullanılabilir.
- Uzaktan erişim için VPN kullanılabilir.
- Ağ mikro segmentlere ayırılabilir.

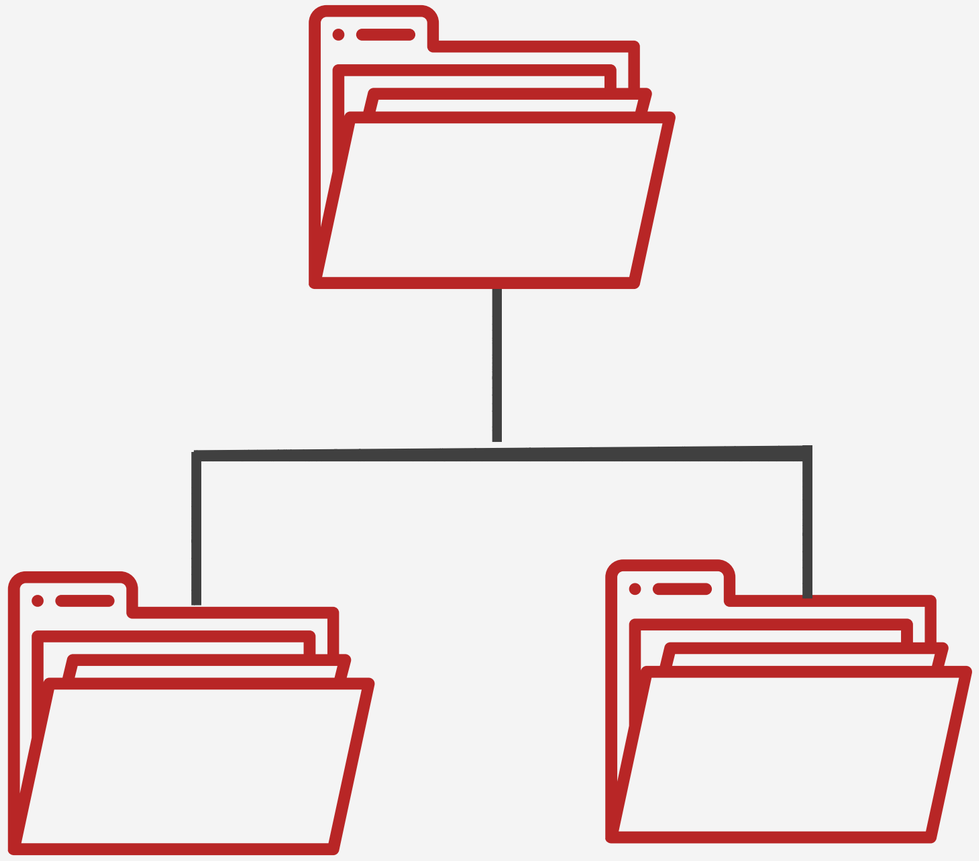


VERİTABANI KORUMA YÖNTEMLERİ

Yedekleme ve Kurtarma:

Veritabanını düzenli olarak yedeklemek, bir felaket, donanım hatası veya yanlışlıkla silme durumunda geri yüklenebilecek yeni bir kopya oluşturur. Bu stratejiyi seçerken dikkat edilmesi gereken hususlar şu şekildedir:

- Veri Yedekleme Sıklığı
- Doğru Yedekleme Türü(Tam, Artımlı, Farklı Yedekleme)
- Uygun bir yedekleme konumu



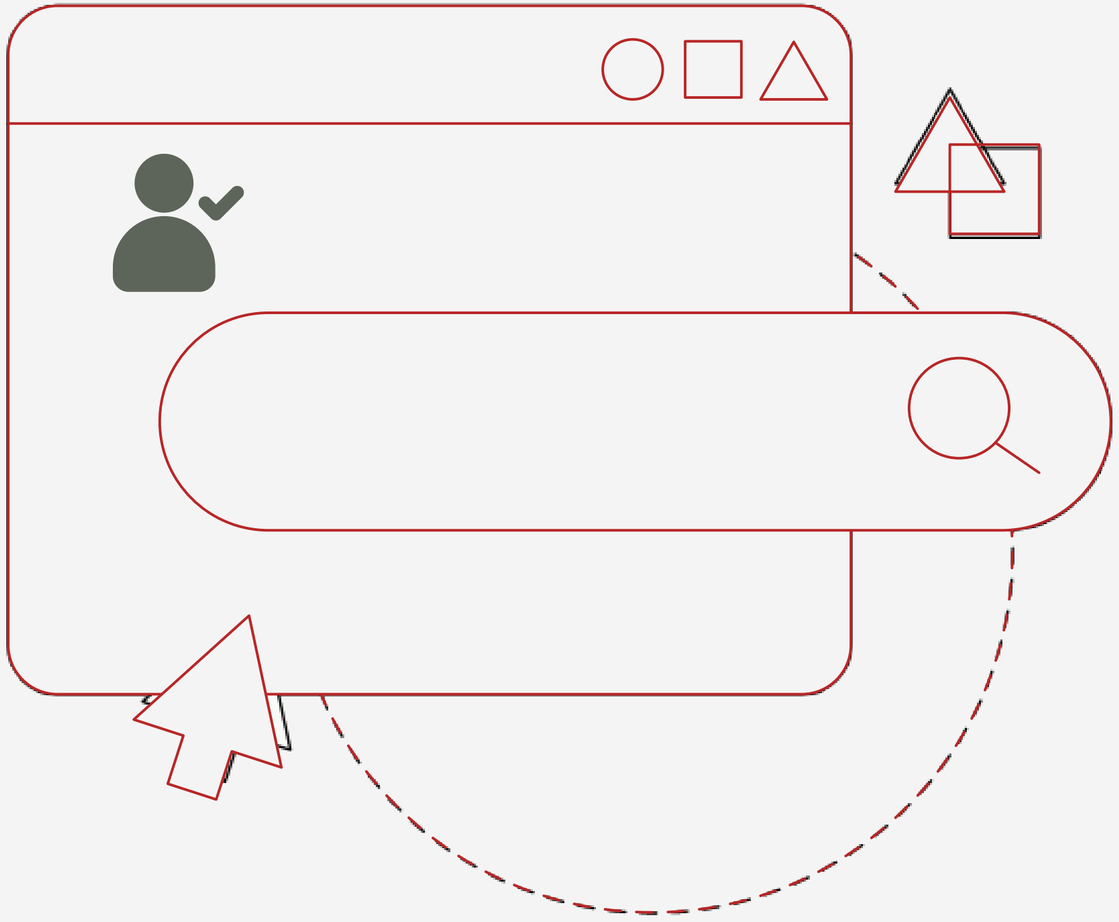
VERİTABANI KORUMA YÖNTEMLERİ

Erişim Kontrolü:

Erişim kontrolü, kimlerin veritabanına erişebileceğini ve eriştiklerinde verilerle ne yapabileceklerini belirler.

Bu, kullanıcı hesapları oluşturmayı, uygun izinler vermeyi ve güçlü kimlik doğrulama önlemleri uygulamayı içerir.

En az ayrıcalık ilkesi burada kilit faktördür kullanıcılara görevlerini yerine getirmek için gereken minimum erişim seviyesi verilmelidir.



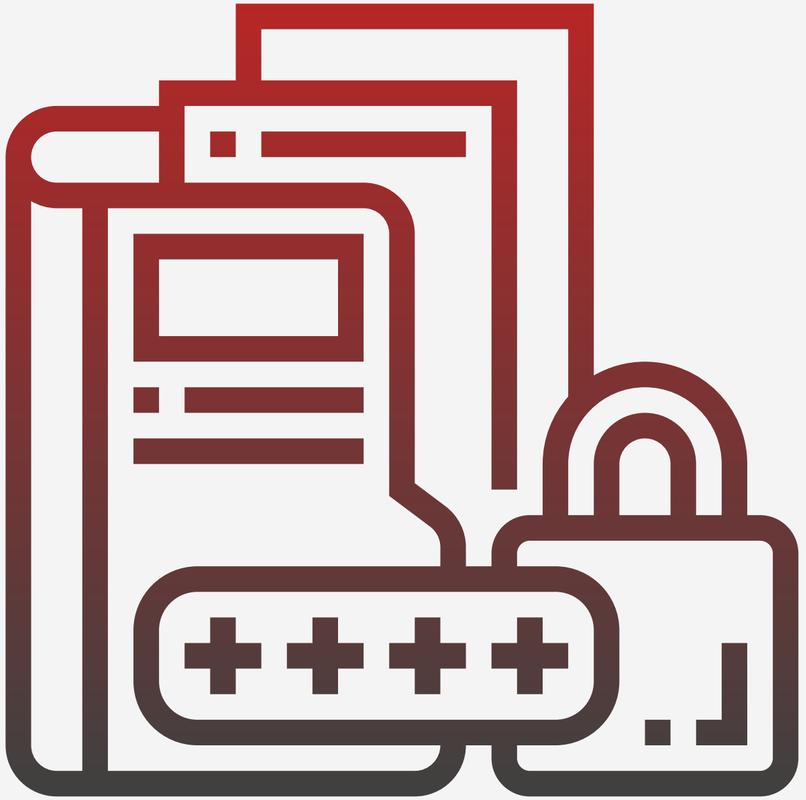
VERİTABANI KORUMA YÖNTEMLERİ

Veri Maskeleme:

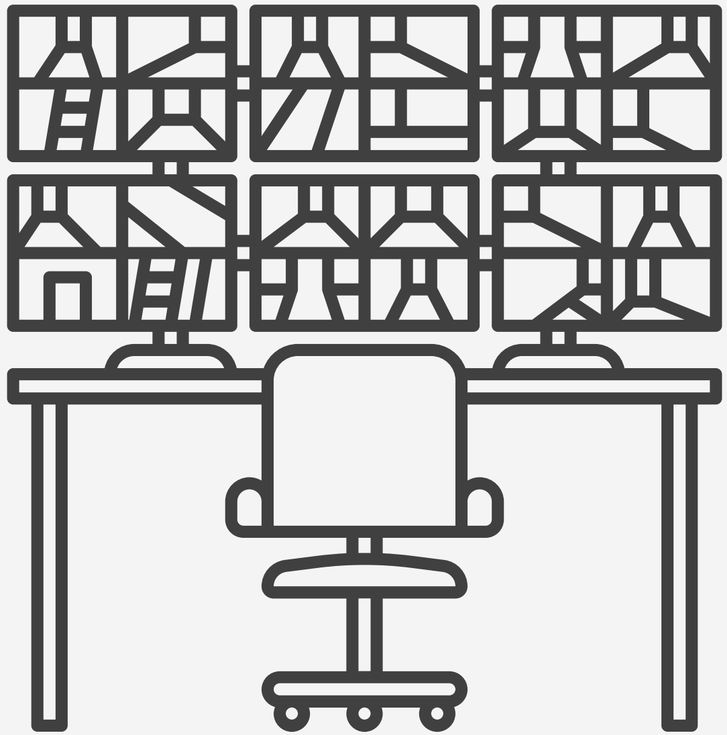
Veri maskeleme, gizli bilgileri değiştirerek bir kuruluşun verilerinin sahte sürümlerini oluşturma işlemidir.

Şifreleme verileri kodlamak için algoritmalar kullanırken, veri maskeleme gerçek verileri benzer ancak sahte verilerle değiştirmeyi içerir.

Veriler maskelendikten sonra orijinal veri kümesine erişmeden tersine mühendislik yapamaz veya orijinal veri değerlerine geri dönemezsiniz.



VERİTABANI KORUMA YÖNTEMLERİ



Fiziksel Güvenlik:

Tehditlerin çoğu dijital olsa da fiziksel güvenlik ihmal edilmemelidir.

Bu, veritabanınızın bulunduğu fiziksel sunucuları güvence altına almayı içerir.

Yetkisiz personelin erişimini kısıtlayın, güvenlik kameraları yerleştirin ve donanım arızalarını önlemek için optimum sıcaklık ve nemi koruyun.

Kaynakça

- Preeti Sharma, Monika, Database Security: Attacks and Techniques, International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 7, Dec-2016.
- AWS- Veri Maskeleme
- Microsoft Azure- What is database security?
- Martin Pill Citp-Database Attacks

SORULAR

Teşekkürler