# VERİ TABANI GÜVENLİĞİ

VERİ TABANI YÖNETİM SİSTEMLERİ

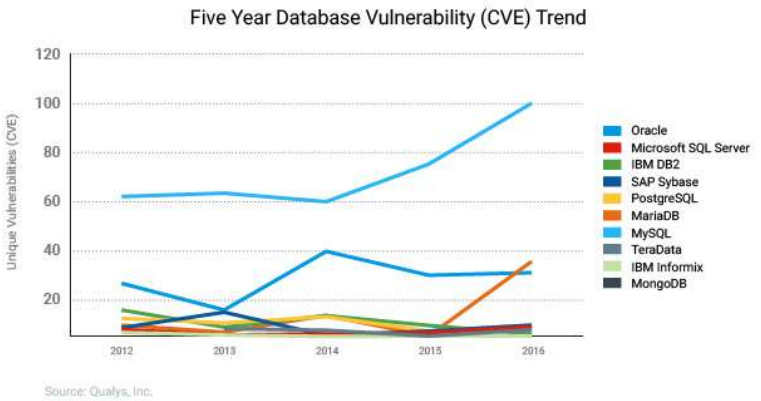
## Veritabanı güvenliği nedir?

Veritabanı güvenliği, veritabanlarını yanlışlıkla oluşan ve kasıtlı tehditlere karşı güvenli hale getirmeye ve korumaya yönelik işlemler, araçlar ve denetimlerdir. Veritabanı güvenliğinin amacı hassas verilerin güvenliğini sağlamak ve veritabanının gizliliğini, kullanılabilirliğini ve bütünlüğünü korumaktır.

Veritabanı güvenliği, veritabanındaki verilerin korunmasına ek olarak veritabanı yönetim sistemi ve ilişkili uygulamaları, sistemleri, fiziksel ve sanal sunucuları ve ağ altyapısını korur.

Kaynak: azure.microsoft.com

Next Generation Security firması tarafından veritabanı güvenliği ile ilgili 2007 yılında yapılan çalışmada 368 bin MS SQL ile 124 bin Oracle veritabanı sunucusunun hiç bir korumaya sahip olmadığı yönünde bir açıklama yapılmıştır.



## Veritabanı Güvenlik Riskleri - I

- Yetkili veritabanı kullanıcıları, Veritabanı yöneticileri, ağ/sistem yöneticileri, yetkisiz kullanıcılar ya da bilgisayar korsanları tarafından yanlış kullanılması veya bu kişiler tarafından yapılan istenmeyen davranışlar (örneğin veri tabanlarındaki kritik verilere, meta verilere veya işlevlere uygun olmayan erişim ya da veritabanı programlarında, yapılarında veya güvenlik konfigürasyonlarında uygun olmayan değişiklikler)
- Zararlı yazılım etkileri, yetkisiz erişim, kişisel ve şahsi verilerinin sızdırılması veya ifşa edilmesi, verilerin ve programların silinmesi veya hasar alması, veritabanına yetkili erişimin kesilmesi veya reddedilmesi, diğer sistemlere yapılan saldırılar ve veritabanı hizmetlerinin beklenmeyen başarısızlıklara neden olan olaylara yol açan zararlı yazılım enfeksiyonları

Kaynak: tr.Wikipedia.org

## Veritabanı Güvenlik Riskleri - II

- Fazla yüklenmeler, performans kısıtlamaları ve kapasite sorunlarından dolayı, yetkili kullanıcıların veritabanlarını amaçlandığı gibi kullanamamaları
- Bilgisayar odasında oluşabilecek yangınlar, seller, aşırı ısınmalar, aydınlatmalar, kaza sonucu sıvı dökülmeleri, statik elektrik boşalmaları, elektronik arızalar/ ekipman arızaları ve eskimeler gibi veritabanı sunucusuna fiziksel hasar veren durumlar
- Veritabanları içerisindeki program açıkları ve tasarım hataları, ilişkili programların ve sistemlerin oluşturduğu çeşitli güvenlik açıkları(örneğin yetkisiz hak artırma), veri kayıpları/ bozulmaları, performans düşüşleri vb.
- Geçersiz veri veya komutların girilmesinden kaynaklanan veri bozulması ve/veya kaybı, veritabanı veya sistem yönetim süreçlerinde yapılan hatalar, sabotaj/kriminal hasar vb.

Kaynak: tr.Wikipedia.org

Veritabanı güvenliği insan hatasına, yüksek veritabanı ayrıcalıklarına, bilgisayar korsanlarından ve içeriden gelen saldırılara, kötü amaçlı yazılımlara, yedekleme alanının medyaya maruz kalmasına, veritabanı sunucularına yönelik fiziksel zararlara ve eşleşmeyen veya arabelleklerde çok fazla veriye sahip veritabanları gibi savunmasız veritabanlarına karşı koruma sağlamalıdır.


Kaynak: azure.microsoft.com

## Veritabanı güvenliği türleri

1. Ağ Güvenliği
2. Erişim Yönetimi
3. Tehdit Koruması
4. Bilgi Koruması

Kaynak: azure.microsoft.com

## Ağ Güvenliği

- **Güvenlik duvarları** , veritabanı güvenliğinde ilk savunma hattı görevini görür. Mantıksal olarak güvenlik duvarı, ağ trafiğinin ayırıcısı veya kısıtlayıcısıdır. Bunu, kuruluşunuzun veri güvenliği ilkesini zorunlu tutacak şekilde yapılandırabilirsiniz. Güvenlik duvarı kullanırsanız, güvenlik önlemlerinizin odaklanabileceği bir tıkanma noktası sağlayarak işletim sistemi düzeyinde güvenliği artırırsınız.

Kaynak: azure.microsoft.com

## Erişim Yönetimi

- **Kimlik doğrulaması**, kullanıcının doğru kullanıcı kimliği ve parolasını girerek kim olduğunu kanıtlama işlemidir. Bazı güvenlik çözümleri yöneticilerin tek bir merkezi konumda veritabanı kullanıcılarının kimliklerini ve izinlerini merkezi olarak yönetmesine olanak tanır. Bu parola depolamanın en aza indirilmesini içerir ve merkezi parola döndürme ilkelerini sağlar.
- **Yetkilendirme** her kullanıcının belirli veri nesnelerine erişmesine ve verileri okuma fakat değiştirememe, verileri değiştirme fakat silememe veya verileri silme gibi belirli veritabanı işlemlerini gerçekleştirmesine olanak sağlar.
- **Erişim denetimi** veritabanı içindeki bir kullanıcıya izin atayan sistem yöneticisi tarafından yönetilir. İzinler, kullanıcı hesaplarını veritabanı rollerine ekleyerek ve bu rollere veritabanı düzeyinde izinler atayarak en iyi şekilde yönetilir. Örneğin, satır düzeyinde güvenlik (RLS), veritabanı yöneticilerinin kullanıcının kimliği, rol üyelikleri veya sorgu yürütme bağlamını temel alan veri satırlarına okuma ve yazma erişimini kısıtlamasına olanak tanır. RLS, veritabanı içindeki erişim mantığını merkezi hale getirir ve bu da uygulama kodunu basitleştirir ve verilerin yanlışlıkla açığa çıkma riskini azalttır.

Kaynak: azure.microsoft.com

## Tehdit Koruması

- **Denetim** veritabanı etkinliklerini izler ve veritabanı olaylarını bir denetim günlüğüne kaydederek güvenlik standartlarıyla uyumluluğu sürdürmeye yardımcı olur. Böylece devam eden veritabanı etkinliklerini izleyebilir, ayrıca olası tehditleri veya kötüye kullanım ve güvenlik ihlali şüphelerini soruşturmak için geçmiş etkinlikleri analiz edebilir ve araştırabilirsiniz.
- **Tehdit algılama** veritabanına yönelik olası bir güvenlik tehdidini işaret eden anormal veritabanı etkinliklerini ortaya çıkararak şüpheli olaylarla ilgili bilgileri doğrudan yöneticiye sunar

Kaynak: azure.microsoft.com

## Bilgi Koruması

- **Veri şifreleme** hassas verileri alternatif bir biçime dönüştürerek güvenli hale getirir, böylece yalnızca hedeflenen taraflar dosyanın şifresini çözebilir ve özgün biçimine erişebilir. Şifreleme erişim denetimi sorunlarını çözmese de, erişim denetimleri aşıldığında veri kaybını sınırlayarak güvenliği artırır. Örneğin, veritabanı ana bilgisayarı yanlış yapılandırılmışsa ve kötü amaçlı bir kullanıcı kredi kartı numaraları gibi hassas verileri ele geçirirse, bu çalınan bilgiler şifreliyken işe yaramayabilir.
- **Veritabanı yedekleme** verileri ve kurtarma bilgilerin korunması için kritik önemdedir. Bu işlem, düzenli aralıklarla veritabanının ve günlük dosyalarının yedek kopyalarının oluşturulması ve bu kopyaların güvenli bir konumda depolanmasını içerir. Yedekleme dosyası ve kopyası, güvenlik ihlali veya hata durumunda veritabanını geri yüklemek için kullanılabilir.
- **Fiziksel güvenlik** fiziksel sunucu ve donanım bileşenlerine erişimi sıkı bir şekilde sınırlar. Şirket içi veritabanlarına sahip birçok kuruluş, veritabanı sunucusu donanımı ve ağ cihazları için kısıtlı erişime sahip kilitli odalar kullanır. Ayrıca, yedekleme medyasını güvenli bir site dışı konumda depolayarak erişimi sınırlamak da önemlidir

Kaynak: azure.microsoft.com

## Veritabanı Güvenliği Neden Önemlidir?

- Veri Hırsızlığı
- Şirket ve Marka Saygınlığına Zarar
- Gelir Kaybı
- Maliyet Artışı
- Veri İhlali Cezaları

Kaynak: azure.microsoft.com

## Veri Hırsızlığı

Veritabanları genellikle müşteri kayıtları, kredi kartı numaraları, banka hesabı numaraları ve kişisel kimlik numaraları gibi değerli, gizli ve hassas bilgileri depoladığından siber saldırıların başlıca hedefleridir. Korsanlar bu bilgileri, kimlikleri çalmak ve yetkisiz satın almalar yapmak için kullanır.

Kaynak: azure.microsoft.com

## Şirket ve Marka Saygınlığına Zarar

Müşteriler, kişisel verilerini korumayan şirketlerle çalışmaktan çekinir. Müşteri bilgilerini tehlikeye atan veritabanı güvenliği sorunları kuruluşun saygınlığına zarar verebilir ve bu da satışlarda düşüşe ve müşteri erimesine yol açabilir. Bazı işletmeler, saygınlıklarını korumak ve müşteri güvenini yeniden oluşturmak için halkla ilişkiler yatırımlarını artırır ve veri ihlali kurbanı olan müşterilerine ücretsiz kredi izleme sistemleri sunar

Kaynak: azure.microsoft.com

## Gelir Kaybı

Veri ihlali, veritabanı güvenlik sorunları çözülene, sistem yeniden bütünüyle çalışır duruma gelene ve iş sürekliliği tekrar sağlanana kadar iş işlemlerini ve gelir üretmeyi durdurabilir veya yavaşlatabilir.

Kaynak: azure.microsoft.com

## Maliyet Artışı

Rakamlar sektöre göre farklılık gösterse de veri ihlallerinin düzeltmesinin maliyeti yasal ücretler, kurbanlara sunulan destek, verileri kurtarmak ve sistemleri tekrar çalışır hale getirmek için yapılan fazladan harcamalarla birlikte milyonlarca doları bulabilir. Şirketler ayrıca kilitli dosyalarını ve verilerini geri almak için ödeme talep eden korsanlara fidye yazılımı ödemesi de gönderebilir. Birçok işletme bu maliyetlerden sakınmak için sigorta poliçelerine siber güvenlik sigortası ekler

Kaynak: azure.microsoft.com

## Veri İhlali Cezaları

Eyalet ve yerel kurumlar ceza yaptırımında bulunur ve müşteri verilerinin korunmadığı bazı durumlarda şirketlerden müşterilerin zararlarını karşılamasını gerektirir

Kaynak: azure.microsoft.com

## Veritabanı Güvenliği için En İyi Yöntemler

- Veri şifreleme, veritabanı veya uygulama için yalnızca yetkili kullanıcıların kimliğini doğrulama, kullanıcının ilgili veri alt kümesine erişimini sınırlama, etkinliklerin sürekli izlenmesi ve denetlenmesi gibi veritabanının güvenliğini sağlama yollarını ele aldık.
- Veritabanı güvenliği için en iyi yöntemler, tehditlere karşı daha da fazla koruma sağlamak için bu işlevleri güçlendirir.

Kaynak: azure.microsoft.com

## Veritabanı Sağlamlaştırma

Veritabanı sunucusunu güvenli hale getirme veya "sağlamlaştırma", güvenlik açıklarına karşı ağ ve işletim sistemi güvenliğini birleştirir ve korsanların sisteme erişimini zorlaştırır. Veritabanı sağlamlaştırma için en iyi yöntemler veritabanı platformunun türüne göre değişiklik gösterir. Yaygın adımlardan bazıları parola korumasını ve erişim denetimlerini güçlendirme, ağ trafiğinin güvenliğini sağlama ve veritabanındaki hassas alanları şifrelemedir.

Kaynak: azure.microsoft.com

## Kapsamlı Veri Şifreleme

Bu özellikler, veri şifrelemesini güçlendirerek kuruluşların verilerini güvenli hale getirmesini ve yönetmeliklere uyum sağlamasını kolaylaştırır:

- Her zaman şifrelenmiş veriler aktarım sırasında, bellekte, diskte ve hatta sorgu işleme sırasında çalınmalara karşı yerleşik koruma sunar.
- Saydam veri şifrelemesi, depolanan verileri (bekleyen veriler) şifreleyerek kötü amaçlı çevrimdışı etkinlik tehdidine karşı koruma sağlar. Saydam veri şifrelemesi özelliği bekleme sırasında veritabanını, ilişkili yedekleri ve işlem günlüğü dosyalarını uygulamada değişiklik gerektirmeden gerçek zamanlı olarak şifreleyip şifresini çözer

Kaynak: azure.microsoft.com

## Gelişmiş Tehdit Koruması

Gelişmiş Tehdit Koruması, veritabanlarına erişmeye veya onları kötüye kullanmaya yönelik olağandışı ve zararlı olabilecek girişimlerin algılanması için günlükleri analiz eder. SQL ekleme, olası veri sızıntısı ve deneme yanılma saldırıları gibi şüpheli etkinlikler için veya ayrıcalık yükseltme ve kimlik bilgilerinin ihlali gibi erişim desenlerindeki anomaliler için uyarılar oluşturulur.

Kaynak: azure.microsoft.com

## Ayrı Kimlik Doğrulama Hesapları

En iyi yöntem olarak, kullanıcıların ve uygulamaların kimlik doğrulaması için ayrı hesaplar kullanmaları gerekir. Bu şekilde kullanıcılara ve uygulamalara verilen izinler sınırlanır ve kötü amaçlı etkinlik risklerini azalır.

Özellikle uygulama kodunun SQL ekleme saldırısına karşı savunmasız olduğu durumlarda çok önemlidir

Kaynak: azure.microsoft.com

## En Az Ayrıcalık İlkesi

Bilgi güvenliği en az ayrıcalık ilkesi , kullanıcıların ve uygulamaların yalnızca işlerini yapmak için gereken verilere ve işlemlere erişim izni verilmesi gerektiğini ifade eder.

Bu en iyi yöntem, uygulamanın saldırı yüzeyini azaltmaya ve bir güvenlik ihlali oluşursa etkisini (sızıntı çapı) azaltmaya yardımcı olur.

Kaynak: azure.microsoft.com

## “Sıfır Güven” Güvenlik Modeli

Veritabanı güvenliğine yönelik en iyi yöntemler, kuruluşunuzun tamamını korumak için platformlar ve bulutlar arasında birlikte çalışan  kapsamlı güvenlik yaklaşımının  bir parçası olmalıdır. Sıfır Güven modeli kişileri, cihazları, uygulamaları ve verileri nerede bulunurlarsa bulunsunlar korumak için kimlikleri ve cihaz uyumluluğunu her erişim isteğinde doğrular.

Sıfır Güven modeli şirket güvenlik duvarının arkasında her şeyin güvenli olduğunu varsaymak yerine olası bir ihlal durumunu göz önünde bulundurarak her isteği açık bir ağdan gelmiş gibi doğrular. İsteğin kaynağı veya hangi kaynağa eriştiği fark etmeksizin, Sıfır Güven "asla güvenme, her zaman doğrula" ilkesini izler.

Kaynak: azure.microsoft.com