Profelis EDB

PostgreSQL Güvenlik Kontrol Listenizde Bulunması Gereken 5 Nokta

Verilerin güvenliğini sağlamak, kuruluşların başarısı için olduğu kadar müşterilerin güvenliği için de kritik bir öneme sahiptir. Bu infografik, bir PostgreSQL veritabanının güvenliğini sağlamak ve korumak için neler yapılabileceğine dair bazı öneriler sunmaktadır.
Aşağıdaki 5 nokta; fiziksel güvenlik, ağ güvenliği, ana bilgisayar erişim kontrolü, veritabanı erişim yönetimi ve veri güvenliği konularını kapsamaktadır.

1 Erişimin Güvenli Hale Getirilmesi

- **Fiziksel Erişim**
  Güvenli tesis, CCTV İzleme, Kilitleme rafları
- **Bağlanma (Unix Etki Alanı / TCP/IP)**
  Uzaktan bağlantı, doğrudan uzaktan saldırıların güvenliğini sağlama
- **Güvenlik Duvarı (Yerel/Bulut)**
  Bağlantı portlarına yetkisiz erişim, gelen ve giden kurallar
- **Veri Aktarımını Şifreleme**
  Ağ üzerinden trafiğin şifrelenmesi

2 Kimlik Doğrulamanın Güvenliğinin Sağlanması

- **pg_hba.conf Trust**
  Herhangi bir kimlik doğrulaması olmadan yapılan sunucu bağlantısı, dikkatli kullanılmalı.
- **pg_hba.conf Peer & Indent**
  Temel işletim sistemi tarafından kimlik doğrulama
- **pg_hba.conf Md5 vs. SCRAM**
  Ağın dinlenmesini önleyin ve karıştırılmış parolaları sunucuda saklayın
- **pg_hba.conf LDAP vs. Kerberos**
  Single Sign-On (SSO) sistemlerinin uygulanması
- **pg_hba.conf TLC Certificates**
  Ağ üzerinden Postgres sunucusuna bağlanması gereken otomatik sistemlerin kimliğini doğrulayın
- **authentication_timeout**
  Sunucu bağlantıyı kapatmadan önce izin verilen maksimum kimlik doğrulama süresini tanımlayın
- **Auth_delay**
  Kaba kuvvet saldırılarını kısıtlayın

3 Rollerin Güvence Altına Alınması

- **Parola Karmaşıklığı**
  C Development veya harici kimlik hizmeti kullanmayın
- **Parola Profelleri**
  Kullanıcıların güçlü parolalar kullanmasını sağlayın
- **SET ROLE**
  Bir rol oluştururken NOINHERIT anahtar sözcüğünü kullanmayın
- **İzleme Rolleri**
  Sistemi izlemek için kullanılan rollere belirli ayrıcalıklar verin

4 Veri Erişim Denetimi

- **ACLs**
  Bireysel oturum açma rolleri için ayrıcalık yönetimini basitleştirmek için grup rollerinden yararlanın
- **GRANT & REVOKE**
  Grup rollerine çalışmak için gereken minimum ayrıcalık düzeyini verin
- **RLS (Row Level Security) (Satır Düzeyinde Güvenlik)**
  Bir tablodaki satırların görünürlüğünü belirli rollerle sınırlayan politikalar tanımlayın
- **Görüntüleme**
  Öncelikle tablolardan seçim yapma yeteneğini kısıtlayın ve bunun yerine verilere geçerli görünümlerden erişme zorunluluğu getirin
- **Güvenlik Bariyerler**
  Fonksiyonun gizli satırları asla görmemesini sağlayın
- **Güvenlik Tanımlayıcı Fonksiyonlar**
  Bu görevleri doğrudan kendi başlarına gerçekleştiremeyen rollere özel işlevler tanımlayın
- **Veri Çıkarma**
  Kullanıcılardan belirli hassas bilgileri gizleyin

5 Şifrelemenin Güvenliğinin Sağlanması

- **Pgcrypto**
  Veritabanı tasarım mantığının bir parçası olarak kullanılabilen şifreleme ve hashing için SQL fonksiyonları
- **Anahtar Yönetimi**
  Anahtarları veritabanından ve uygulamadan ayrı olarak güvenli bir hizmette saklayın
- **Dosya Sistemi ve Disk**
  Çalışmayan donanıma yönelik fiziksel saldırılara karşı koruma sağlayın

Bu infografik, PostgreSQL dağıtımınızın güvenliğini baştan sona değerlendirmenizde size yardımcı olacak kapsamlı bir genel bakış niteliğindedir.