PostgreSQL Güvenlik, PCI-DSS

Fatih Sazan
YTÜ Harita Müh.
Veritabanı Uzmanı
Profelis Bilişim ve Danışmanlık

21 Ekim 2025
Postgres İstanbul'25

Güvenlik Nasıl Sağlanmalı?

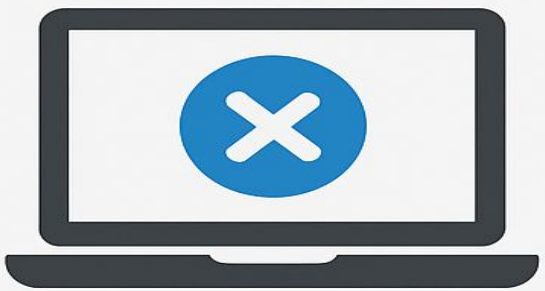
Kaleye girmenin en kolay yolu - kapıdan yürüyerek geçmektir

Veri sızıntı kaynağı

%80 insan !!!

PCI-DSS

HASSAS VERİLERİ KORUMA



İHLALLERİ ÖNLEME

GÜVENLİ ORTAM GÖSTERGESİ

PCI-DSS (Payment Card Industry - Data Security Standard)
(Kartlı Ödeme Sistemleri - Veri Güvenlik Standardı)

PCI Security Standards Council

Güvenli ağ ve sistem kurulumu	1. Güvenli ağ kurulumu ve sürdürülmesi 2. Tüm sistem bileşenlerinde güvenli konfigürasyon
Kart verilerinin korunması	3. Saklanan kart verilerinin korunması 4. Kamuya açık ağlarda kart verilerin şifreli iletimi
Güvenlik açıklarının yönetimi	5. Tüm sistem ve ağların zararlı yazılımlardan korunması 6. Güvenli sistemler ve yazılımların geliştirilmesi
Erişim kontrolü ve yetkilendirme	7. Sistem bileşenleri ve kart verilerine erişimin kısıtlanması 8. Sistem bileşenlerine erişimde kullanıcıların kimlik kontrolü 9. Kart verilerine fiziksel erişimin kısıtlanması
Düzenli izleme ve ağ testleri	10. Sistem bileşenleri ve kart verisine erişimlerin kaydı ve izlenmesi 11. Sistemlerin ve ağların düzenli güvenlik testi
Bilgi güvenliği politikaları	12. Bilgi güvenliğinin kurumsal politikalarla desteklenmesi

1. Güvenli ağ kurulumu ve sürdürülmesi

Ağ

- Ağ Segmenti (Kart verileri özel subnet)
- Jump/Bastion Host

Firewall

- Genel (public) ağdan veritabanı erişimi engelle
- Veritabanı erişimi, sadece belirli sunucular arasında `(HAProxy, pgBouncer, PostgreSQL)`
- Ağ üzerinde iletişimde sadece gerekli portlar açık olmalı `(varsayılan portlar kapalı )`

2. Tüm sistem bileşenlerinde güvenli konfigürasyon

PostgreSQL

- postgres kullanıcısı kullanma ~~parola~~
- superuser tanımla `create role profelis_fatih with superuser`
- sınırla 5432 ve 22 `ufw deny 5432 +  ufw allow from IPx port 5432`
- sınırla gerekli IP adresleri `listen_addresses=IP1,IP2`
- trust/peer kaldır `scram-sha-256 , SSL`
- hba reject postgres `host all postgres 0.0.0.0/0 reject`
- sunucuda sadece veritabanı çalışmalı ~~web sunucu~~

pgAdmin4 tek noktadan erişim

`pgAdmin4 web server, http://...`

Paket sunucusu, Linux / repo server kullanımı

3. Saklanan kart verilerin korunması

Data Encrypt **(data - at - rest - encryption)**

- Disk — Full Disk Encryption (FDE)
- Veritabanı — Transparent Data Encryption (TDE)
- Uygulama — Application Layer Encryption (ALE)

Full Disk Encrypt

- Luks `(dm-crypt), Bitlocker, ...`
- Fiziksel koruma (offline)
- Disk kaybı
- Çalınma

Disk Çalışıyor ise Verilerde Koruma Yok.

3. Saklanan kart verilerin korunması - TDE

```
hexdump -C $PGDATA/base/5/16388
```

```
00001f70  b1 6e 61 72 11 62 6f 79  61 6c c4 b1 00 00 00 00  |.nar.boyal......|
00001f90  03 00 03 00 02 09 18 00  03 00 00 00 0f 74 65 7a  |.............tez|
00001fa0  63 61 6e 0d 64 65 6d 69  72 00 00 00 00 00 00 00  |can.demir.......|
00001fc0  02 00 03 00 02 09 18 00  02 00 00 00 0d 61 79 6c  |.............ayl|
00001fd0  69 6e 0b 67 c3 b6 6b 00  4a 04 00 00 00 00 00 00  |in.g..k.J.......|
00001fe0  00 00 00 00 00 00 00 00  01 00 03 00 02 09 18 00  |................|
00001ff0  01 00 00 00 0d 66 61 74  69 68 07 61 6b 00 00 00  |.....fatih.ak...|
```

Şeffaf veri şifreleme (TDE), verileri **disk**e kaydetmeden önce güvenle şifreler.

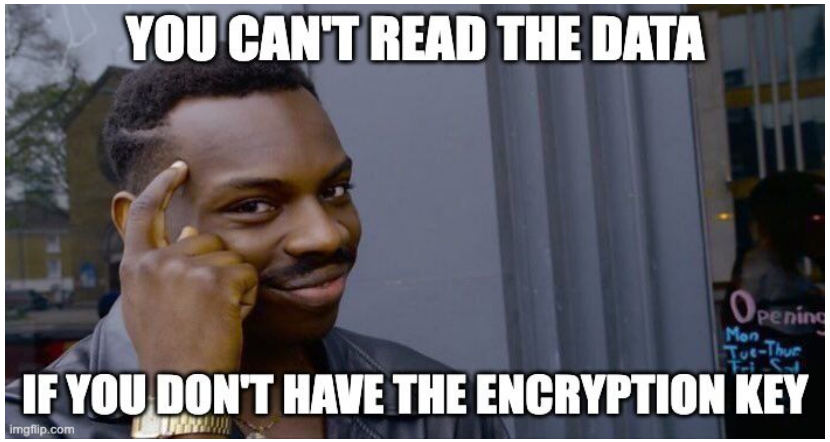
```
hexdump -C $PGDATA/base/5/16388
```

```
00001f70  00 00 00 00 f0 e1 79 01  d3 6a bc 42 a5 95 e8 8b  |......y..j.B....|
00001f90  1e df 30 ad 5f 61 0f 55  6d af f4 79 9b ba 77 69  |..0._a.Um..y..wi|
00001fa0  c6 c7 c5 61 c5 4c f4 a8  00 64 35 af 79 fa e7 fd  |...a.L...d5.y...|
00001fc0  09 a4 07 13 2e c1 76 45  1f ed 03 42 3d d5 1f 8f  |......vE...B=...|
00001fd0  38 3f 87 ad 7c d0 47 79  ed 05 1b 18 34 b6 68 ff  |8?..|.Gy....4.h.|
00001fe0  f6 65 63 4d e2 04 16 bd  3b 8a df 20 22 ff f3 7f  |.ecM....;.. '...|
```

3. Saklanan kart verilerin korunması - TDE

TDE Lisanslı

- CrunchyData
- Cybertec
- EnterpriseDB
- Fujitsu



TDE Lisanssız

- Percona PostgreSQL Community Edition *https://github.com/percona/pg_tde*

- TDE ile base, pg_wal, tablespace disk üzerinde şifreli metin halinde tutulur.
- **Hangi Dosyalar Şifreli Tutuluyor ?**

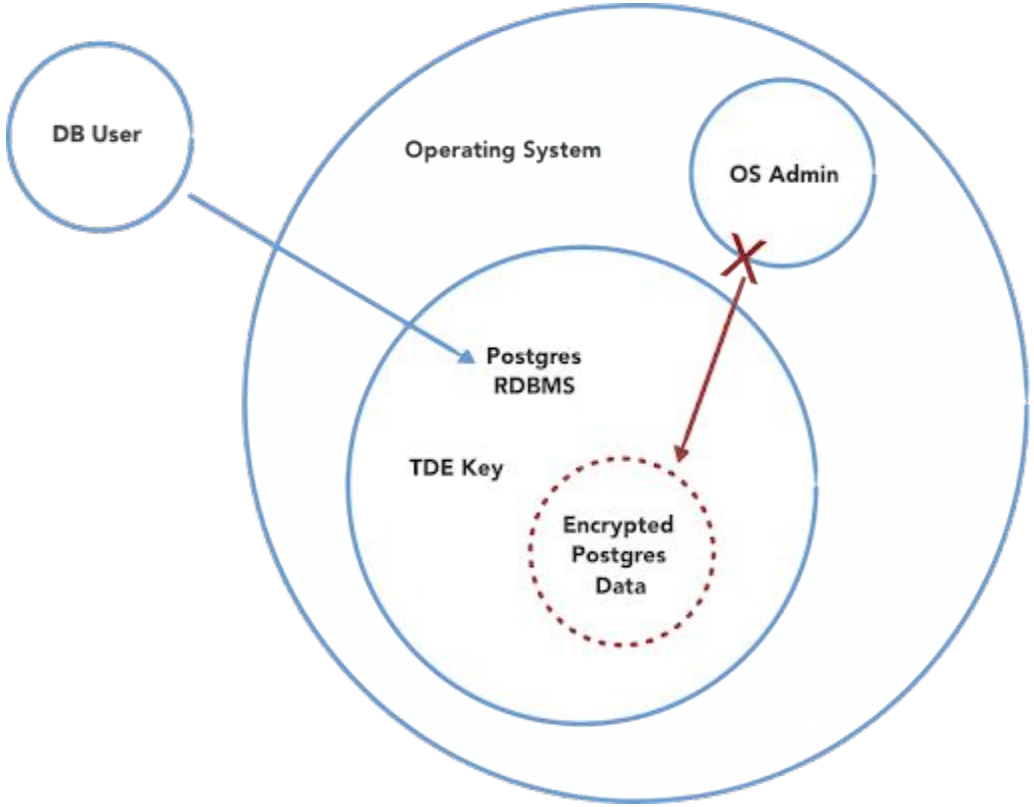
  Sorgular work_mem değerini aştığında oluşturulan geçici dosyalar şifrelenmez/koruma dışı
- “pg_ctl start” komutu ek parametre tde_key
- TDE anahtarı kaybında - sizin içinde **VERİ ULAŞILMAZ OLUR.**

3. Saklanan kart verilerinin korunması - TDE

Veritabanı dosyaları tamamı / bir kısmı veri ihlal olmasına **KARŞI KORUYOR.**

Veritabanı içinde hassas **VERİ ULAŞIR DURUMDA**.

PCI-DSS, 2025 mart geçerli
“veri kaydedildiği yerde açık (düz metin) şekilde görüntülenemez”
yoruma kapalı güncellendi.



FDE , TDE artık yeterli görünmüyor.

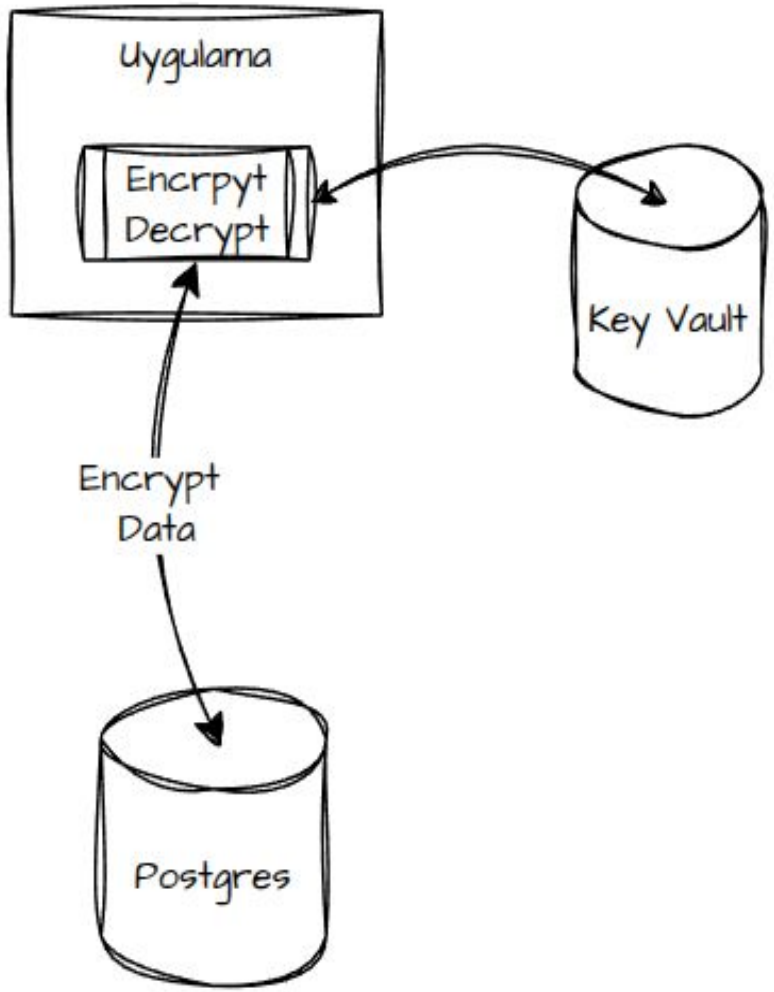
Veritabanına gelmeden Şifreli / Encrypt olmalı.

3. Saklanan kart verilerin korunması - ALE

Application Layer Encrypt (ALE)

- Veriyi kaydetmeden önce, Uygulama katmanında **ŞİFRELE**
- 31 mart 2025 PCI-DSS zorunlu
- Veri saklandığı yerde okunamaz

- İki katmanlı yaklaşım
- Key Vault gereksinimi
- **Anahtar yok ise , Veri anlamsız.**



id	name	email
104	dba4c62c282c…	78996706ff294962a a10447e98c2b274
105	6d99dbbd8d93…	843d99b30b394265 a921d2121f3de374
206	2c3fda3fcfe84…	fbd71be3c3dc4c5db 13c2dbcfe0d5775

3. Saklanan kart verilerin korunması - ALE

pgcrypto

- Postgres üzerinde Encrpyt / Decrypt

```
SELECT pgp_sym_encrypt('verim
güvende', 'secret_key');
-[ RECORD 1
]---+-----------------------------------------------
---------------------------------------------------
---------------------------------------------------
---------
pgp_sym_encrypt |
\xc30d0407030204121edc93ad3b5370d23f0104b567b3a09
571563da4e3eb85a0d5503343298556dd1a0ed6b0dc0ee02a
8a3d7b81696a7d0fb5d01344fa0272cc76c537b9cc3adcecd
dbbcc4bda8a196a
```

```
LOG:  statement: SELECT
pgp_sym_encrypt('verim güvende',
'secret_key');
```

- Kart veri işlemlerin log takibi (PCI - DSS)
- Yazılım katmanında güçlü kripto (şifreleme) kütüphane kullanımı

4. Kamuya açık ağlarda kart verilerin şifreli iletimi

TLS / SSL

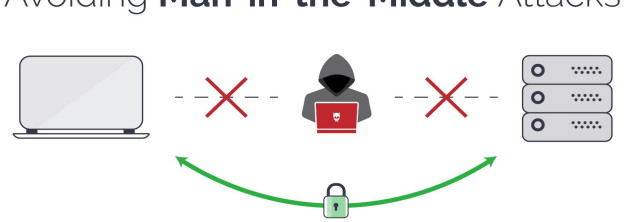
- Scram-sha-256 parola doğrulama. Veri iletimi şifrelenmez / korumaz **(man-in-the-middle)**
- Postgres **ile veri akışının olduğu** Uygulama, Replication, pgBackrest, Barman, Haproxy, pgBouncer
- pg_hba.conf scram-sha-256 yerine
  hostssl all all IP cert clientcert=verify-full

SSL bağlantı modu

- İstemci (client) , sslmode=~~prefer~~ (varsayılan)
  ,**(man-in-the-middle)**
- sslmode = verify-full

https://www.postgresql.org/docs/current/libpq-ssl.html#LIBPQ-SSL-PROTECTION

```
import psycopg2
conn_params = {
    'dbname': 'your_database',
    'user': 'your_username',
    'password': 'your_password',
    'host': 'your_host',
    'port': 'your_port',
   # or 'verify-ca', 'verify-full'
    'sslmode': 'require',
   # Required for 'verify-ca' and 'verify-full'
    'sslrootcert': '/path/to/ca_certificate.crt',
   # Optional, required for mutual authentication
    'sslcert': '/path/to/client_certificate.crt',
   # Optional, required for mutual authentication
    'sslkey': '/path/to/client_key.key'
}
```



5. Tüm sistem ve ağların zararlı yazılımlardan korunması

- Veri hırsızlığı genellikle aynı ağı paylaşan cihazlar üzerinde gerçekleşir
- Kötü amaçlı yazılımlar, veritabanı dosyalarından ziyade erişim bilgilerini hedefler
- Kötü amaçlı yazılımların hedefinde olan sistemler üzerinde Antivirüs yazılımı kullan, güncel tut ve düzenli tarama yap **(PCI - DSS)**

6. Güvenli Sistemler ve Yazılımların Geliştirilmesi

Güvenli Yazılım Geliştirme

- Dev / Test ortamı
- ~~Sql injection~~ Güvenli Uygulama geliştir

PostgreSQL Güvenlik Yamalarını UYGULA

- Güvenlik yamalarını takipte ol mail abone
  pgsql-announce
- Minor sürüm yol haritasına göre iş planı
  https://www.postgresql.org/developer/roadmap

Kullanım ömrü biten (EOL) Postgres kullanma

- Ana sürüm (Major) yükseltme

PostgreSQL Global Development Group, yaklaşık olarak **yılda bir kez** yeni özellikler içeren yeni bir **ANA sürüm yayınlar**. Her ana sürüm, en az **üç ayda bir "küçük sürüm"** olarak adlandırdığımız sürümlerde yayınlanan hata düzeltmeleri ve gerekirse güvenlik düzeltmeleri alır. Küçük sürüm takvimi hakkında daha fazla bilgi için, küçük sürüm yol haritasını inceleyebilirsiniz.

Sürüm ekibi, kritik bir hata veya güvenlik düzeltmesinin düzenli olarak planlanan küçük sürümün yayınlanmasını beklemek için çok **önemli** olduğuna karar verirse, **küçük sürüm yol haritası dışında bir sürüm yayınlayabilir**.

PostgreSQL Global Development Group, **ana sürümü ilk yayınlanmasından** itibaren **5 yıl** boyunca **destekler**. Bundan sonra, son küçük sürüm yayınlanır ve yazılım artık desteklenmez (**kullanım ömrü sona erer**).

Sürüm	Minor Vers	Destek	İlk Sürüm	Son Sürüm
17	17.6	Evet	26 Eylül 2024	8 Kasım 2029
16	16.10	Evet	14 Eylül 2023	9 Kasım 2028
15	15.14	Evet	13 Ekim 2022	11 Kasım 2027
14	14.19	Evet	30 Eylül 2021	12 Kasım 2026
13	**13.22**	**Evet**	**24 Eylül 2020**	**13 Kasım 2025**
12	12.22	HAYIR	3 Ekim 2019	21 Kasım 2024

7. Sistem bileşenleri ve kart verilerine erişimin kısıtlanması

Rol tabanlı erişim kontrolü (RBAC)

- app_role, crm_role, report_role ,pg_read_all_data ,pg_write_all_data
  - `GRANT insert,update on table card_data to app_role;`
  - `GRANT select (id,mail) on table users to report_role;`
- Anonim rol kullanımı engelle, kullanıcı adresleyecek şekilde tanım
  - `CREATE ROLE report_role WITH NOLOGIN;`
  - `ALTER ROLE report_role to profelis_eylem_kaya;`
  - `ALTER ROLE postgres with NOLOGIN;`
  - `CREATE ROLE profelis_fatih_sazan with SUPERUSER;`

En az ayrıcalık (Least Privilege)

- Kullanıcı için gereken minimum izin
  - `revoke all on database db_payment from public;`
  - `revoke all on database db_log from public;`
  - `grant connect on database db_log to role_log;`
- RLS (satır bazlı güvenlik), view, veri maskeleme

8. Sistem bileşenlerine erişimde kullanıcıların kimlik kontrolü

Çok faktörlü kimlik doğrulama (MFA)

- Otomatik işvel yürüten Uygulama (app_user vb .) ve Sistem kullanıcı (replication vb .) dışındaki erişimde MFA (password + 2.yöntem) zorunlu
- PostgreSQL MFA özelliği ver.18
- MFA Kimlik Doğrulama için ldap vb …

Parolada Güçlü Politika

- Postgres bu özellik bulunmamakta
- credcheck, password_profile

Defined Approach Requirements
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.
Customized Approach Objective
A guessed password/passphrase cannot be verified by either an online or offline brute force attack.

PostgreSQL, LDAP entegrasyonu = MFA + Password Policy

8. Sistem bileşenlerine erişimde kullanıcıların kimlik kontrolü

Parola Tanımında Dikkat

- Create role / alter role kullanmak tehlikeli
- Kullanıcılar üzerinde yapılan değişiklikler loglanmalı (PCI-DSS)

```
create role profelis with password 'güçlü_parola';

LOG:  statement: create role profelis with password 'güçlü_parola';
```

Parola Tanımında Güvenli Yol

- `/password` güçlü_parola
- `create role  with login password`

```
‘SCRAM-SHA-256$4096:E8Tm8I7G8MeCByfzi/y6qg==$moIr3CCfJf8iZlGwHxV9q/fDYHC/oatX4vngDlXJ1Ck=:D2A
bpxrgCDOPFH41noxQoUCXPhyqbAjLFrIWqcu40Vw=’

 LOG:  statement: ALTER USER "profelis_fatih_sazan" PASSWORD
‘SCRAM-SHA-256$4096:E8Tm8I7G8MeCByfzi/y6qg==$moIr3CCfJf8iZlGwHxV9q/fDYHC/oatX4vngDlXJ1Ck=:D2A
bpxrgCDOPFH41noxQoUCXPhyqbAjLFrIWqcu40Vw=’
```

9. Kart verilerine fiziksel erişimin kısıtlanması

Fiziksel erişimde uyulması gereken maddeler

10. Sistem bileşenleri ve kart verisine erişimlerin kaydı ve izlenmesi

Postgres LOG

Topla

- log_statement = ’ALL’ , pgAudit
- Veritabanı kullanıcı (create,alter ..) , Superuser yetkilendirme
- Kart verisi üzerinde DDL, DML, Select
- Log kişi özelinde takip edilebilir
- Log kaydı hassas veri gözükmemeli

Sakla

- Tüm Sistem logları merkezi SIEM (Wazuh, ELK, log360 vb.) üzerinde tut
- En az 12 ay sakla, 3 aya anında erişim sağla

11. Sistemlerin ve ağların düzenli güvenlik testi

Güvenliği sadece kurma, test et!

12. Bilgi güvenliğinin kurumsal politikalarla desteklenmesi

Kurum içi Güvenlik bilinci oluşturma , Eğitimler ile destekleme

Güvenlik = 80% İnsan + Süreç + 20% teknoloji

PostgreSQL Güvenlik, PCI-DSS

Teşekkürler – Soru & Cevap

PCI Security Standards Council

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf