HACKERS WANT YOUR DATA WAREHOUSE – NOW!

HOW HACKERS GET IN

Database hacking is highly favored by hackers due to its financial benefits and easy to exploit vulnerabilities.

A HACKER FIRST GAINS CONTROL OF A DATABASE BY...

1. PASSWORD GUESSING
Just guesses userid and password for access

2. PACKET SNIFFING
Captures packets flowing to and from database server

3. MANIPULATION
Gets data from web url query string from browser request

4. VULNERABILITY EXPLOITATION
Looks for database server with bugs/vulnerabilities

5. SQL INJECTION
A hacker's favorite – runs select query to dump entire database

6. RANSOMWARE
Installs malicious software to block access until paid

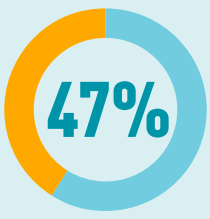
7. PHISHING
Obtains sensitive data in disguise as reputable company

8. SOCIAL ENGINEERING
Deceives individuals into divulging personal information

9. PRIVILEGE ELEVATION
Database servers use roles and rules to control access of a user to a particular database, table or resource in general. A hacker usually inject scripts which try to find out the most generous level of privileges and upon finding one, uses it to create further damage

HOW COMPANIES LEAVE THEIR DATA VULNERABLE

No single industry, country or organization is immune to the risks of overexposed data.



of organizations have at least **1,000 sensitive files** open to every employee.

In data breaches, data warehouses are targeted because they contain high value assets and are usually vulnerable to abuse by insiders and outsiders. While organizations focus on perimeter defenses and chasing threats, **the data itself is left broadly accessible and unmonitored**.

NOT STOPPING THE HACKERS IS COSTLY!

4% or €20m **Potential fines** for General Data Protection Regulation (GDPR) Non-Compliance from May 2018

£122bn 2018 EU GDPR legislation **data breach penalties** for some UK businesses

JAN 2018 **Compliance deadline** for updated EU Payment Services Directive (PSD 2)

$26m **Record fines** levied in 2016 for HIPAA Enforcement

FEB 2018 Effective date for **Payment Card Industry** (PCI) Data Security Standard (PCI DSS 3.2)

DISABLING THE HACKER

Properly configuring firewalls and database policies, and following best practices for the roles and rules by network administrators – the legacy method of protecting database servers at operating system level – is **not sufficient** in the modern world.

- ✓ Go beyond disk encryption and **protect the data itself**
- ✓ Segregate duties for Database Administrator and Security Officer to **ensure those that create data access rules cannot see data**
- ✓ **Establish policies** to ensure all employees only see data in the clear that is needed to perform job function
- ✓ **Achieve compliance** for regulated data, supported by detail audit and reporting

TERADATA CUSTOMERS ARE LEAVING HACKERS EMPTY HANDED

MULTINATIONAL RETAILER protects employee and customer identities enabling analytics for digital lift while complying with FDA regulations

GLOBAL AIR TRAVEL TICKETING DATA PLATFORM protects credit card and personal information of 9.5 billion passengers for regulatory PCI compliance

MULTINATIONAL BANK protected data to ensure restricted access to requesters in respective countries for compliance with EU Cross Border Data Protection Laws

LARGE HEALTHCARE PROVIDER protects HIPAA 18 patient identifiers to mitigate threat vectors while enabling advanced analytics to improve patient outcomes and reduce costs with predictive analytics

GET STARTED TODAY
PROTEGRITY DATA SECURITY FOR TERADATA
PROTECT YOUR DATA IN 90 DAYS – SEE HOW

www.protegrity.com/teradatasolutions

protegrity