The Devil Wears SQL: The Most Powerful Person in the Company

May 17th, 2019
IIA & ISACA Tech Conference
"Truth is, no one can do what I do"
Protecting The Perimeter
Traditional Security Controls

Internal Network

Office

App Controls

Intrusion Prevention

Load Balancing

Firewall

Remote Access Portal

VPN

Internet

Multi-Factor Authentication

Virus/Malware/Spam Protection

Client/Customer/Partner

Web Content Controls

The Data
So I am fully protected…

“There are two kinds of big companies in the United States. There are those who’ve been hacked… and those who don’t know they’ve been hacked.”
- James Comey (October 2014)
Cost and Benefit Analysis

COST OF BREACH

- Equifax
  - 143m
  - $275m

- Yahoo!
  - 3 billion
  - $350m

- Target
  - 110 m
  - $300m

- Home Depot
  - 56m
  - $179m

- Uber
  - 57m
  - $148m

COST OF COMPLIANCE
Traditional Security Is Out of Fashion
Traditional Security Is Out of Fashion

- Insiders bypass the perimeter and compromise your data
- Malware leverages unsuspecting users
- Applications and data moving to the cloud
Traditional Security Is Out of Fashion

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD

DATA
Traditional Security Is Out of Fashion

Hackers breach applications effectively
Social Engineering
AI/RPA/Automation/IoT
The Database
Peeling the Layers: 3-tier architecture
Peeling the Layers: 3-tier architecture

PRESENTATION LAYER
- Sends content to browsers in the form of HTML/JS/CSS
- Presents information formatted for viewing
- Translates keystrokes/mouse and other interaction
Peeling the Layers: 3-tier architecture

APPLICATION LAYER
- Processes all business logic
- Validates accuracy of actions and executions
- Maintains and executes user basic controls
Peeling the Layers: 3-tier architecture

DATA LAYER
- Maintains all application data
- Provides data as requested by application layer
- Generally controls access to data and interaction
# The Power of the DBMS

## Data Principles
- Data Redundancy
- Data Consistency
- Data Integrity
- Concurrency

## Safeguards
- Privacy
- Security
- Data Sharing Rules
- Standards Enforcement

## Convenience
- Search Capability
- Backup and Recovery
- Powerful User Language
- Ease of App Development
The Different SQL Statements

- **DDL**
  - CREATE
  - ALTER
  - DROP
- **DML**
  - INSERT
  - UPDATE
  - DELETE
- **DCL**
  - GRANT
  - REVOKE
- **TCL**
  - COMMIT
  - ROLLBACK
Sarbanes-Oxley

- General Ledger
- Accounts Receivable
- Accounts Payable
- Inventories
- Reconciliations
HIPAA

- Health Visits
- Diagnostics
- Employee Records
- Scanned Documents
GDPR/CCPA – Personal Information

- Names
- E-mails
- Phone Numbers
- Social Security Numbers
- Social Media Accounts
- Passwords
Social Media

- Posts
- Pictures
- Videos
- Relationships
- Personal Information
Introducing the Most Powerful Person in the Company
What can the Database Administrator do?
Can it possibly get worse?
The devil is in the details…
I already have enough controls
Change Management

Limitations:
• Generally DBAs are provided scripts when pushing to Production
• Stored Procedure activity is not “pre-compiled” and therefore DBAs have full view of code
User Access Reviews

**Limitations:**

- Performed at a point in time
- Generally focused on application users. DBAs already have full access
- Generally omits needs to segregate database “Super Users”
The Legend of Audit Trail

Limitations:

• DBAs have full access to turn on/off as needed
• DBAs may have full access to modify or delete
• Consume significant amount of resources from the DBMS
• Considerable amount of information. Hard to use when needed
Business Controls

Limitations:

• These controls generally happen at the front-end
• Database activity may be modified behind-the-scenes
• Controls rely on integrity of data being used
What are the options?
Control the Access – Use Case # 1

- Change Management Solution

- Developer makes changes
- Informs that change is ready

- QA validates and approves
- Staging Server is ready to publish

- Staging tool uses a system account to log into the DB server
- Changes are pushed without human intervention
Control the Access – Use Case #2

• Segregate Access as Needed

• DBA has an account specific for business needs (e.g., provision access, update data, troubleshoot)
• Segregate access based on functions
• Users that provision access
• Users access based on database/application need
• Keep the “Super User” account password saved and protected
• Only use these accounts for emergency purposes
Privileged Access Management Solutions

- Password Management
- Shared Accounts
- Privileged Access Controls
- System/Service Accounts
- Access Request Approval Workflow
- Limit Access as Needed
Privileged Access Management

- Privilege Elevation
- Delegated Privileged Role
- Multi-Factor Authentication
- Time-Based Role Assignment
Privileged Access Management

- Session Recording
- Auditing and Monitoring

Audit and Monitoring

- Real-Time Alerting
- Combine with Ticketing tools
Database Activity Monitoring Solutions

Preventive Safeguard
Database Activity Monitoring Solutions

Preventive Safeguard
Database Activity Monitoring Solutions

Detective Safeguard
Database Activity Monitoring

DATA ACCESS CRITERIA

- Who?
- What?
- How?
- When?
- How much?
- How often?