IT/Dev CONNECTIONS

Top Down SQL Server Security

Brian Kelley
Data Architect
Truth Solutions

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

About Me

- Database / Infrastructure Architect
- Database Administrator
- SQL Server security columnist / blogger
- IT Auditor

Contact Information

K. Brian Kelley

Email: kbriankelley@acm.org

Twitter: @kbriankelley

Infrastructure/Security Blog: https://truthsolutions.wordpress.com

Personal Development Blog: https://gkdba.wordpress.com

Agenda

- Guiding Principles
- Define the Target and the Value
- Configuration
- Auditing
- Consistency

Guiding Principles & Target Value

Guiding Principles

What should be our guiding principles?

(group activity)

"If you don't have time to do it right, when will you have time to do it over?"

– John Wooden

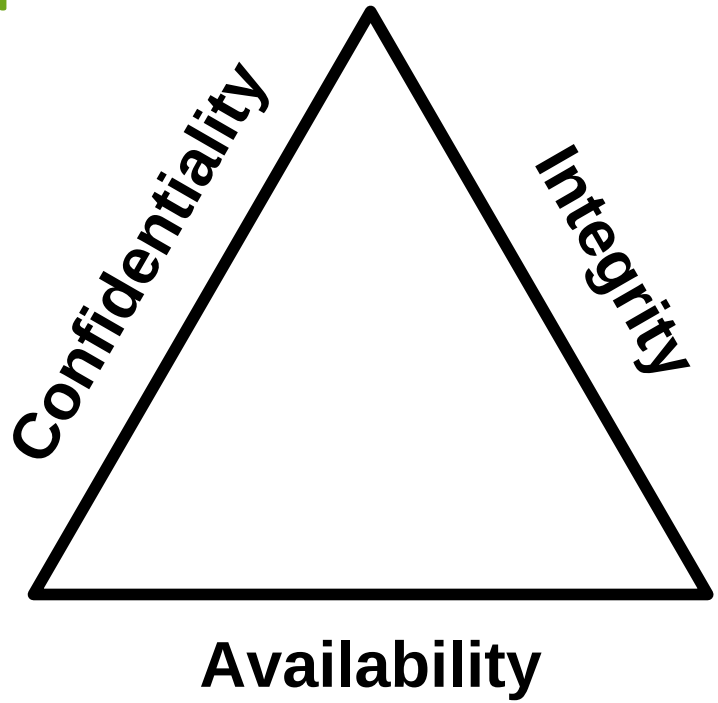
The Minimum

- Principle of Least Privilege
- Minimize Surface Area
- Adherence to C-I-A Triad

Principle of Least Privilege

- Only what's needed. No less, no more.
- Too little and the job doesn't got done.
- Too much, and you've increased your risk!

C-I-A Triad



Target Value

How valuable is the data?

Do you consider lateral movement?

(group activity)

Secure Configuration

Configuration – Surface Area

What are our considerations?

What do we disable?

(group activity)

Surface Area – Three Areas

- Network
- Operating System
- SQL Server itself

SQL Server – specifics

- xp_cmdshell
- CLR
- Remote DAC
- Database Mail

Configuration – OS Level

- Administrators group
- Firewall
- IPSEC policy
- OS Benchmarks?

Configuration – SQL Server

What are the must haves?

What can we automate?

(group activity)

Configuration – SQL Server

- Members of sysadmin
- Cross-Database Ownership Chaining
- Custom Server Roles?
- What else?

Configuration – Databases

What do you look at?

What can we automate?

(group activity)

Configuration - Databases

- Who owns each database?
- Guest account
- Recovery modes
- Database role membership

Auditing

Auditing

What do you need to audit?

What's the best way to do this?

(group activity)

Auditing

- Basic stuff – Failed logins
- Audit object
- Extended Events
- What about traces, Common Criteria, C2 compliance?
- Does the OS or network give us anything?

Automation

Automation

- OS build
- SQL Server install
- SQL Server configuration
- Database configuration

Auditing

What do you do today?

What do you use?

(group activity)

Automating the Whole Cycle

- VM build – Easy to automate hardware
- OS install – “Gold image” to ensure OS
- SQL install – Command-line install options
- SQL Config - Scripts after the install

What We Covered

- Guiding Principles
- Define the Target and the Value
- Configuration
- Auditing
- Consistency

Remaining Questions?

K. Brian Kelley

Email: kbriankelley@acm.org

Twitter: @kbriankelley

Infrastructure/Security Blog: https://truthsolutions.wordpress.com

Personal Development Blog: https://gkdba.wordpress.com