CONFRONTING THE ENEMY WITHIN

By Gary Olsen and Marcel Davidson - LDS Church

UTOUG – Fall Symposium 2015

AGENDA

- Biography
- Introduction
- Awareness
- Attitude
- Next Steps
- Q&A

BIOGRAPHY

- Database Professionals - Security Focus

INTRODUCTION

- Why are you here today?
- Our goal is for you to leave a different person
- A change of perception when it comes to database security

QUESTIONS

- As an I/T professional, how well do you sleep at night?
- Do you have a top notch security team that keeps the bad guys out?
- Why should the database administrator be worried, if it's not their job?
- Do you have enough to high priorities to worry about, that security is an 'B','C','D', … priority?

CASE STUDY

- One of these is not like the other?

CASE STUDY

- One of these is not like the other?
- Target, Sony, Home Depot, U. S. Office of Personnel Management (OPM)

U.S. OFFICE OF PERSONNEL MANAGEMENT

- ~22 million personnel records, including security clearance info and references from families and friends
- ~1.1 million fingerprints, financial/health records and username/passwords
- Traced to the Chinese government
- Disclosure months afterwards - citing enormous, outdated systems (2015)
- Hackers had access for ~year

CASE STUDY CONTINUED (OPM)

- Stolen login credentials of contractor
- CIA personnel shielded?
- Check names on rosters of U.S Embassies!
- Breach discovered by newly installed cyber security software
- CIO targeted to resign, when her initiative helped discover the breach in an organization seen as lacking a security strategy.
- "There are certainly some people I would like to see given the boot for not paying attention to cyber security, but the CIO is not one of them." Anonymous Source

CASE STUDY CONTINUED (OPM)

- What was the impact of this breach?
  - Personal details of federal employees and their friends and family members
  - Compromised Agents (loss of life?)
  - Targets "who might be susceptible to pressure or inducements to engage in espionage."
- How would you fill if you were seen as one of those that didn't think a security strategy was necessary?
- Are you a friend or enemy of your organization?

INTROSPECTION

- Can I say with confidence that I am a part of the solution and not the problem?
- Do I see others as the problem or don't see that there is a problem?
- Is this because of my attitude and or lack of awareness regarding security?

AWARENESS VS ATTITUDE

AWARENESS

- Easier to fix
- Framework (Basic Training)
  - Confidentiality, Integrity, Availability (CIA)
  - Speak the speak – Vocabulary between groups
  - Impact – Ponemon
  - RISK Model – Probability of an adverse event

RISK CALCULATION

- ***RISK*** = *Threat* x *Vulnerability* x *Impact*
  - ***Threat***: Source of danger
  - ***Vulnerability***: Weakness
  - ***Impact***: Measure of damage (data asset)
- Independent variables

REDUCING RISK

- RISK = Threat x Vulnerability x Impact
  - Reduce ***Threat***
    - Difficult (you don't control)
  - Reduce ***Vulnerability***
    - Your ***best*** (only) option
  - Reduce ***Impact***
    - Difficult (you don't control)

ACTION PLAN

- Start with proven practices

ACTION PLAN

- Start with proven practices
- Critical Security Controls - Top N (CSC)

CRITICAL SECURITY CONTROLS

1. *Inventory of Authorized and Unauthorized Devices*
2. *Inventory of Authorized and Unauthorized Software*
3. *Secure Configurations for Hardware and Software*
4. *Continuous Vulnerability Assessment and Remediation*
5. *Malware Defenses*
6. *Application Software Security*

.

.

17. Data Protection

Source: SANS.ORG, ***Critical Security Controls***

PRIORITY

"Possibly the biggest … continued lack of attention—by businesses and consumers alike—[are] updates, patches, password security, security alerts, default configurations, and other easy but critical ways to secure cyber and physical assets. This is not news to the security industry; we have banged this drum for decades, and yet these remain the most likely vectors for successful attacks."

Source: McAfee Labs, "***Threats Report***" August, 2015

AUSTRALIA - TOP 4 STRATEGIES (CONTROLS)

1. Application Whitelisting
2. Application (database) Patching
3. O/S patching
4. Minimize administrative privileges

Source: http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

ACTION PLAN

- Start with proven practices
- Critical Security Controls - Top N (CSC)
- Eat the elephant in small bites

ACTION PLAN

- Start with proven practices
- Critical Security Controls - Top N (CSC)
- Eat the elephant in small bites
- Not so hard no one will want to use

ACTION PLAN

- Start with proven practices
- Critical Security Controls - Top N (CSC)
- Eat the elephant in small bites
- Not so hard no one will want to use
- Don’t re-create the wheel

RESOURCES

- Security Technical Implementation Guides (STIGS)
- CIS Benchmarks
- Peers / Security Team
  - May already have best practices unique for your environment

ATTITUDE

How well do you sleep at night?

Remember:

Confidentiality

Integrity

Availability

STATE OF COMPROMISE

"In 2020, enterprise systems will be in a state of continuous compromise. They will be unable to prevent advanced targeted attacks from gaining foothold on their systems…The majority of information security spending will shift to rapid detection and response capabilities."

Source: Gartner, "***Prevention Is Futile in 2020**: Protect Information Via Pervasive Monitoring and Collective Intelligence,"* May, 2013

ATTITUDE

- Difference between compliance and being security conscious
  - High Value Targets (HVT) - Spear phishing!
  - At some institutions, fired if you forget to lock your work station. (No 2nd chances)
  - Remember U. S. Office of Personnel Management example

POSITIVE ATTITUDE

- Peers
  - Rogue - Adversarial, Resistant or Inadvertent? (all of us - make mistakes. What is our response?)
  - Be firm, but diplomatic (Not too hard or distasteful)
  - Have a solid case to present on why it's important
  - If necessary, work with your manager to help shape/adjust attitude

POSITIVE ATTITUDE

- Management
  - Help understand the realities
    - FUD / PTSD
    - Ponemon Estimates
    - Reputational Estimates
    - Use RISK Formula

POSITIVE ATTITUDE

- Auditors
  - Do they see you as a partner, or an adversary?
  - They can be you ~~best~~ friend or your worse enemy

WHERE DO I GO FROM HERE?

- *Education / Training (Beyond Boot Camp)*
- *Subscribe to news feeds*
- *Get involved with user groups*
- Develop a plan of action for your organization, including a marketing campaign

REFERENCE

Top 20 Critical Security Controls: https://www.sans.org/critical-security-controls/

Australia Top 4 Strategies: http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

STIGS: http://iase.disa.mil/stigs/Pages/index.aspx

CIS Benchmarks: https://benchmarks.cisecurity.org/downloads/benchmarks/

Oracle Database Security
http://www.oracle.com/us/products/database/security/resources/index.html

www.darkreading.com

www.sans.org

www.ponemon.org

www.owasp.org/index.php/Main_Page

CONCLUSION

- How is your comfort now pertaining to security?
- Are you leaving a different person?
- Has your perception changed when it comes to database security?

QUESTIONS?

EVALUATE THIS SESSION

https://www.surveymonkey.com/r/UTOUGSessionEvals

Session Evaluation Number: 19