WATCH OUT FOR THE RABBITS

This is not a vendor presentation
Poll...
AGENDA

- Top 10 Security Controls
- Correlation of Controls with current buzzwords
- Questions
- Audience participation is welcomed
- Wrap up at 11:50 so you can get a good place in line for lunch

Photograph: Andrew Linscott/Alamy
TOP 10 SECURITY CONTROLS
1. COMPETENT SECURITY PROFESSIONALS

- Someone who understands risk mitigation vs. security
- Someone who understands business vs. a piece of technology
- Continuing education is essential (the real security awareness program)
2. INCIDENT RESPONSE CAPABILITY

- What are you going to do when something unexpected happens?

- Have a plan and procedures for
  - Business Continuity
  - Disaster Recovery
  - Breaches
  - Data Recovery

- How will you lead everyone?
3. [ROLE-BASED] ACCESS CONTROL

- Give only needed access
- Physical security is included
- Ensure strong procedures are in place for terminations and job/department changes
- Perform local and network account reviews
4. KNOW WHAT/WHERE YOUR ASSETS ARE

- Software & Hardware Inventory

- No such thing as the “crown jewels”
  - However, a risk based approach is wise

- Data at rest and how it’s transported
5. SYSTEM CONFIGURATION

- Vulnerability Management
- System Hardening
- Base image before things go live
6. SECURE DEVELOPMENT LIFECYCLIES

- Software

- System

- Ensure you are inserted into projects throughout the organization

- Sanitization / Destruction must be observed
7. ALERTING/CORRELATION OF EVENTS

- Hundreds of system emails a day (hour) is pointless

- Set up a triage as alerts come in
  - Prioritize them to aide the confusion

- Takes a lot of time and a dedicated resource
8. RISK ASSESSMENTS & GAP ANALYSIS

- Requires that Asset Management and Data Management be in a mature state

- Requires senior leadership to determine risk appetite
  - Determines true gaps (or not)
9. PHYSICAL & ENVIRONMENTAL SECURITY

- Something that techies often forget or don’t follow up on

- Requires behavioral analysis of employees and the environment
10. ATTESTATION, AUDIT, AND/OR PENETRATION TESTING

- Verify your program, controls

- Address the “yeah but’s”
SECURITY PROFESSIONALS...
WHAT THE WORLD THINKS WE DO
WHAT MY WIFE THINKS I DO
Don't you know I'm a DEVELOPER?
APPLYING THESE PRINCIPLES
HACKERS / HACKTIVISM
Hackers / Hactivism

Analysis

- They try to
  - Steal stuff
  - Deface stuff
  - Piggyback off of your environment to do other stuff

Mitigating Controls

- System hardening
- Alerting (Monitoring)
- Pen Testing/Scanning
I’M A LITTLE TIRED OF “APT”
APT’S CONTINUED

trojan rabbit
ADVANCED PERSISTENT THREAT (APT)

- It’s advanced
- It’s persistent
- It’s a threat to your organization
APT’S - MITIGATION

- ALL of the Top 10

- Alerting

- Competent security professionals to identify “goofy” things

- Baseline of infrastructure

- ***Incident Response Procedures***
HEARTBLEED

Analysis

- OpenSSL provides SSL and TLS protection for email and browsing
- The bug allows an attacker to read memory and steal
  - secret keys for X.509 certs
  - user names/passwords
  - and stuff...

Mitigating Controls

- Asset Management
- Secure Configurations
- Competent Sec. Professionals who don’t panic
  - Also who can assign a realistic risk rating so the business understands
- Alerting for the aftermath
0-DAY

Analysis
- Unknown Vulns
- Hack Wednesday

Mitigation
- Incident Response
- Patch/Vulnerability Management
MOBILE / BYOD

Analysis
- Device is not in the direct control of I.T. (outside the boundary)
- Cannot control a personal device

Mitigating Controls
- Understand what the business purpose is
- Understand what data they need access to
- Invest in a MDM/container
BIG SECURITY DATA
Isn’t that the same as SIEM?
CLOUD, CLOUD, AND MORE CLOUD
CLOUD

RUN AWAY!

RUN AWAY!!
< < INSERT PRODUCT > >
NEXTGEN <<INSERT PRODUCT NAME>>

- I am your king.
- I didn’t vote for you.
NEXTGEN <<INSERT PRODUCT NAME>>

I told them we already got one

*snicker*
DEFENSE IN DEPTH VS. EXPENSE IN DEPTH
ENOUGH SAID?

My level of sarcasm has reached a dangerous level where even I don't know if I'm kidding or not.
RECAP
Top 10
1. Competent Security Professionals
2. Incident Response
3. Role-Based Access Control
4. Asset Management
5. System Configuration
6. Secure Development Lifecycles
7. Alerting/Correlating Events
8. Risk Management & Gap Analysis
9. Physical & Environmental
10. Attestation/Audit/Pen Testing
QUESTIONS?

ASK QUESTIONS Please
Feel free to contact me with any follow up questions:

Mat Wilcek
- Mwilcek@Gmail.com