Building a Strong Foundation

Hudson Valley Cybersecurity Workshop

Paul Chauvet
Why is this guy blathering on here?
Tech can fix it all!

• “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.” - Bruce Schneier
Where to start?
What is being threatened?

[Diagram showing a triangle with the words "Integrity," "Availability," and "Confidentiality" on the sides, and "Information Security" at the bottom.]
Security Foundation

- Asset Inventory
- Authentication
- Backups
- Network Segmentation
- Patching/Vulnerability Management
- Training & Awareness
- Assessment
Asset Inventory

- Hardware & Software
- Should be a *continuous/active* process
- Essential for risk management and asset classification
- 800-171 – 3.4.1
Google: Security Keys Neutralized Employee Phishing

Google has not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical Security Keys in place of passwords and one-time codes, the company told KrebsOnSecurity.

Security Keys are inexpensive USB-based devices that offer an alternative approach to two-factor authentication (2FA), which requires the user to log in to a Web site using something they know (the password) and something they have (e.g., a mobile device).

A Google spokesperson said Security Keys now form the basis of all account access at Google.

“We have had no reported or confirmed account takeovers since implementing security keys at Google,” the spokesperson said. “Users might be asked to authenticate using their security key for many different apps/reasons. It all depends on the sensitivity of the app and the risk of the user at that point in time.”
Login Request

Acme Corp
Acme Web App

rsanchez
10.35.40.116
Ann Arbor, MI, US

January 16, 2018, 5:11 PM

[Image of an authentication request]

[Image of a YubiKey]

[Image of a clock showing 123 456]
Authentication

- Multifactor Authentication
- Something you have – and something you know
- 800-171 3.5.3 – *Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.*
This is not a (real) backup...
Backups

• Follow 3-2-1 rule
  – At least 3 copies of data
  – Store 2 copies on different media
  – Store 1 copy offsite

• The systems being backed up should not be able to reach back to the backup system to change the backups.

• Test backups regularly!!!
SHODAN

12,651

TOTAL RESULTS

TOP COUNTRIES

195.70.113.180
195-70-113-180.stat.salzburg-online.at
Hotel Kaprunerhof
Added on 2018-07-24 14:10:22 GMT
Austria, Salzburg
Details
honeypot

Reserved for operating system:
Serial number of memory card: SD 217C9210
Location designation of a module:
Manufacturer and profile of a CPU module:
Module type: CPU 315-2 PN/DP
PLC name: SIMATIC 300(1)
Module: 6ES7 315-2EH14-0AB0 v.0.1
Plant identification:
OEM ID of a module:
Module name: ...

61.90.63.12
ppp-61-90-63-12.revip.asianet.co.th
Network Segmentation

- Ensure your non-public assets are not accessible from the Internet (without VPN).
- Segment critical assets internally.
- Lack of segmentation and/or public Internet visibility the cause of major breaches.
“Both the human deployment of the patch and the scanning deployment did not work,” Equifax CEO Richard Smith told Congress. “The protocol was followed.”

“The human error was that the individual who’s responsible for communicating in the organization to apply the patch, did not,”

Quotes courtesy – TheVerge.com:
Patch/Vulnerability Management

• Have a process in place to ensure systems are patched.
• Have a way of verifying this (software, periodic review, etc.).
• Use compensating controls for systems which cannot be patched.
Security Training & Awareness

• Need basic training so people know and can recognize the risks.
• Ideally have simulated phishing to enhance training.
Assessment

• Qualified assessment of risk and vulnerabilities needed.
• Use outside resources if you don’t have sufficient internal staffing.
Where to go for help?

• MTEC
• NIST MEP
• Manufacturing sector ISACs
CMMI Staged Representation - 5 Maturity Levels

- **Initial (Level 1)**: Processes are unpredictable, poorly controlled, reactive.
- **Managed (Level 2)**: Processes are planned, documented, performed, monitored, and controlled at the project level. Often reactive.
- **Defined (Level 3)**: Processes are well characterized and understood. Processes, standards, procedures, tools, etc. are defined at the organizational (Organization X) level. Proactive.
- **Quantitatively Managed (Level 4)**: Processes are controlled using statistical and other quantitative techniques.
- **Optimizing (Level 5)**: Process performance continually improved through incremental and innovative technological improvements.

Process Maturity

Slide 6 of 13
• Questions?
  Comments?
  Rotten Fruit to throw at the speaker?