Air Force Materiel Command

AFMC Cyber Hygiene Short Course Overview

Tim Ewart

HQ AFMC A3/6
Cyberspace Operations
Technical Director

Background

- **Problem Statement**
  Human error contribute significantly to cybersecurity breaches

- **One (of many) Solutions**
  Train workforce of cyber dangers

- **Example of AFMC Cyber Hygiene Training Effort**

Weapon System Cyber Defense

Q: When is a wall not a defense?

- **Traditional IT has strong defenses**
  - Network monitoring, auditing, logging
  - Automatic software updates and patches
  - Authenticated users, no admin privileges
- **Platform IT is often treated like a tool**
  - Weaker defenses due to standalone nature
  - Relies on border defenses for protection
- **Air Gaps used as a border defense**
  - Relies on proper media handling procedures
  - Used incorrectly, it's like a direct network connection

A: When it's unmanned or when you leave the door open

Controlling Data Transfer Risks

- **Verify data**
  - Only use data from known sources
  - ALWAYS virus scan media before use
  - Virus scan on an independent system
  - Encryption, digital signatures if possible
- **One-way transfers** are safest
  - Use read-only media when possible
  - Do not reuse writeable media
  - Prevents adversary C2 to your systems
  - Controls data exfiltration

Never network an air-gapped system!

Limitations of Virus Scanning

- **Virus scanning is a defensive measure**
  - **Can identify known malware (likely nuisance variety)**
  - **Inadequate against targeted malware**
  - **Does not stop zero-day attacks**
  - **Insufficient as the only solution – reactive only**
- **Relies on being run on a clean, hardened system**
  - **Virus scan results on an infected system can't be trusted**
  - **If media being scanned infects you first, you lose**
- **Shows whether good cyber hygiene is practiced**

You can only stop the malware you know about.

Cyber Hygiene

- **Computers are like your body**
  - **Can only be kept healthy through proper hygiene**
- **Defensive measures on the computer are not enough – you are the first line of defense**
- **Think *Defense-in-Depth***
- **Don't trust the computer to keep itself safe**
- **Be suspicious of anything that touches a computer electronically**

Defense-in-Depth	
Process:	Policies, Procedures, T.O.s, Safe Cyber Practices
People:	Training, Awareness, Alertness
Physical:	Gates, Guards, Guns
Network:	Perimeter Defenses, Air Gaps
Computer:	Anti-Virus, Software Patching, Hardened Configurations
Device:	One-way/Read-only Media for Transfers, Authorized Media

Basic Cyber Hygiene

- **Don’t use maintenance computers for:**
  - **Charging personal electronics**
  - **Personal work**
  - **Surfing the web**
  - **Playing games, watching movies, or listening to music**
  - **File sharing or backups**
  - **Anything not mission-related**

But this is obvious and almost no one does this
(but almost no one isn’t the same as no one…)

Summary of Recommendations

- **Don’t trust a computer to protect itself**
  - Know the attack paths and common adversary methods
  - Question any physical or electronic connection
- **Think carefully about data crossing an air gap**
  - Move data in one direction using read-only media
  - Don’t inadvertently create a network path for attackers
- **Scan media on a dedicated scanning station**
  - Always scan media before it touches a flightline computer
- **Use maintenance computers for one purpose only**
  - Don’t reconfigure hardware or alter software baseline
  - Don’t use for non-mission functions

What is the Air Force Doing?

- **Addressing causal factors**
  - **TCTOs to fix identified weaknesses**
    - Turn off known vulnerabilities due to misconfiguration
  - **TO edits to correct inaccuracies**
    - Clearly identify authorized systems and devices
  - **Cyber hygiene training for MX personnel**
    - Policies being addressed, accountability being introduced
  - **Authorizing additional protections**
    - Working with Program Offices and Authorizing Officials (AO) to develop and approve solutions
  - **Planning for future hardened systems**
    - Acquisition, migration

Questions