Fundamentals of Utility Cybersecurity

FMEA Energy Connections Conference & Trade Show – November 3, 2021

INTRODUCTION

- Former utility staff (telecommunications, water & electric)
- First NERC CIP auditor in the US
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Director and President Emeritus
- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- Advisor to multiple industrial security product vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

THE HORSESHOE NAIL

- Small doesn't mean lower probability target
- You will be automatically scanned/hacked if vulnerable
- Your resources (data, bandwidth, CPU cycles) = $$$
- Smaller is perceived as less security (easier to hack)
  - 43% of cyberattacks are aimed at small companies
  - Only 14% are prepared to defend themselves
  - 50% - 70% of all ransomware attacks are directed at small companies
- Launch point to larger targets
  - Connectivity
  - Trust relationships

WHAT WORKS FOR S/M UTILITIES?

- Do the “Top Ten” and reduce your risk by 80% or more
- Too many security products to track
- Too many frameworks to follow
- What works in the real world – your Muni world?
- Scientifically proven – ITPI, academic studies
- Operationally proven – CISA/INL, DOE, NERC, empirical
- Real world – 35+ years of experience
- You don’t have to eat the whole elephant at once

1. ASSET INVENTORY

- Not everything, but at least the important stuff
- If you don't know what you have, you can't protect it
- All the other key control areas are based on this
- Start with simple baseline elements
  - Make/model
  - Network and/or or host address
  - OS and/or firmware
  - All other software installed
  - Listening Ports (services)
  - Patches (or patch state; vulnerability)

2. PHASE OUT FRAGILE SYSTEMS

- Legacy systems
- Custom systems
- Unique systems
- That one “application” written by 3 engineers
- Brittle and unreliable hardware
- Borrowed IT used as OT
- Applications that don’t play nice in the tech sandbox
- Applications that are the hardest to update
- Standardization will lower costs/risk and improve uptime

3. ARCHITECT FOR DEFENSE

- You should at least have a firewall between IT/OT
- Specific points for detection and visibility
  - Network boundary
  - Each network segment
  - Critical systems
  - Administrative & engineering systems
- Dependencies on outside systems
- Dependencies on outside business processes
- Intelligent islanding, shear-away networks & “turtle mode”

4. REMOTE ACCESS

- Is anything connected directly to the Internet?
- Remote administration
- Remote operations
- Vendor support
- Consider using a jump host
- Multi-factor authentication
- Monitor and alert

5. RESTRICT ACCESS

- Change all default accounts/passwords
- Unique user accounts wherever you can
- Eliminate shared accounts if possible
  - Where you can't, track who has them
- Principle of least privilege
- Fewest administrator accounts/groups
- Different credentials for OT AD and IT AD
- Remove access ASAP for shared and unique users
- Use LONG (remember-able) passwords, not complex

6. VULNERABILITY MANAGEMENT

- Insecure by design
- First-to-market
- Patching vs. vulnerabilities
- Zero-days, forever-days
- Patching priority
  - Perimeter first, then work inward
  - High-risk systems
- Vulnerability “scanners”
  - Passive vs. active
- Firmware counts too

7. CONTROL CHANGE

- Best defense against both accidents and malice…
- Establish a change control/review board – at least for the critical systems
- Prepare for backing out any change
- Record all changes through baseline tracking
- Test changes, whenever/wherever possible

8. LOGGING AND MONITORING

- Log and monitor as much as you possibly can
- Network monitoring
- System monitoring
- SIEM tools
  - Tuning
  - Monitoring and alerts
  - False positives
  - Integration with other tools
- OT-specific tools exist
- Can integrate with enterprise (most attacks start w/ IT)
- Neighborhood Keeper

9. KEEP IT SIMPLE

- Don’t over-buy security technologies
- Train your staff
- Complexity is the enemy of security
- Reduce technology diversity
  - Standardize tech blueprint (software and hardware)
  - Standardize configurations; control “drift”
- Fewer places for attackers (or problems) to hide
- Reduces attack surface area
- Less expensive through volume purchase
- Easier on supply chain risk

10. RESPONSE AND RECOVERY

- Write down an Incident Response Plan (IRP)
- Keep it simple – something you can follow
- Public Power Incident Response Play Book
- Paper or table-top exercises
- NERC GridEx
- Cyber Mutual Assistance (CMA)
- ICS4ICS
- Practice like it's game day
- Are you sure you can recover?
- Have you actually tried to do it?

BONUS - REGULATION

- Compliance does not equal security
- Often necessary to establish a minimum bar
- Yes, hackers are faster than laws
- You can prescribe action, but not attitude
- “Transient Regulation”
  - NERC CIP
  - Executive Orders
  - National Security Memorandum
  - Insurance
  - Contracts

BONUS - FRAMEWORKS & METRICS

- Where do you start? Is there a playbook?
- Pick one, apply it, and measure to it
- Perfection is the enemy of the good
- Most don't need a gap assessment
  - Attach to existing initiatives, fold in more over time
- Suggest NIST-800-53 and 800-82
  - Fits within NIST Cyber Security Framework
  - Companion to ES-C2M2 (Cybersecurity Capability Maturity Model)
  - Will likely be the US standard for all critical infrastructure(s)
- Consistent measurement to demonstrate progress

BONUS – PEOPLE

- What if you installed 20 new security cameras and no one was watching them?
- Even the best security tool in unskilled hands is a false sense of security
- Break down HR barriers
  - Entry level security talent
  - Higher rates for specific cyber skills or management
- Become a training path & be OK with them leaving
- Encourage conferences and networking for wide relationship connections

SUMMARY – PROVEN TO WORK

- Asset Inventory
- Phase out fragile systems
- Build a network you can defend
- Lock down all remote access
- Restrict user access
- Manage vulnerabilities and patches
- Change control and configuration management
- Monitor as much as possible
- Simplify: fewer security tools, less complexity in systems
- Practice response and recovery like it's game day

CONTACT ME


@PATRICKCMILLER


LINKEDIN.COM/IN/MILLERPATRICKC


PMILLER@AMPERESEC.COM


WWW.AMPERESEC.COM


+15032721414