.

infosec 716 meetup

OT Security in Public Utilities

About Me:

Currently titled IT Manager. how did i get here?

- started out in a kitchen. this is a great place to learn composure, stress management, incident response, planning, and so many other skills.
- Accidented into Water.

Dug holes. Cleaned sewers. Rebuilt pumps. drove a truck full of tools around and learned all the good places to eat.

I also learned how water gets to your house and where it goes when youre done dirtying it up. I was hooked. Turns out, working for the city public works is really great. stable, benefits, education. EDUCATION.

"Good at Computers"

i took so many classes. why not? they were free. learned about automation. microwave radios. built some HMIs. migrated from Novell to Active Directory one day because why not? Elbows deep in every system because nobody was telling me no. a magic time.

What is a Public Utility?

There are lots of different types of Public Utilities. Water, Power, Gas, and transport agencies enjoy some level of monopoly status in exchange for providing necessary public services at a reasonable cost. They can be co-op, municipal, or state run.

A Special District is a local government outside the jurisdiction of the cities and counties it serves. They have an elected board of directors and basically make their own rules. This is important for several reasons, not least of which is that the usual rules for how an organization handles information security generally do not apply. They operate as a quasi state entity, with powers granted by the state constitution. Special districts are funded through tax assessments, rates, and bond measures.

https://calafco.org/resources/lafco-procedures-special-districts/water-management

Seems Critical...

NERC? nope

PCI-DSS? not usually

DOD? lol

Most public utilities i have had contact with, especially water/wastewater, are just winging it. Most dont have a CISO or equivalent. Almost none have a SOC. (MWD Exception)

Duties as Assigned

For the most part, water utilities have a handful of SCADA programmers and a network administrator or two who are tasked with keeping the systems operating. Many outsource their business IT function and rely on the manufacturer or integrator for ICS support. If they are lucky they have a manager who supports investment in information security and sponsors the effort with leadership.

This, more than anything IMO is why events like Oldsmar happen. Just like in the private sector, getting popped is often what it takes for agencies to pay attention.

Why are Industrial Control Systems special?

We typically have the usual variety of weird tech in our facilities; modbus, Ethernet/IP, devicenet, CIP, OPC. In the context of water and wastewater, ICS is critical to public health goals. Poop on the street is yucky. Poisoned drinking water is deadly.

Some common challenges:

- Vision
- Leadership
- Funding
- Skills and Capabilities
- Procurement/Engineering (black boxes)

We have lots of guides though!

- Trusty old NIST 800-53 (general) and 800-82 (ICS)
  - Cybersecurity Framework | NIST
- EPA
  - https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector
  - https://www.epa.gov/newsreleases/epa-announces-action-plan-accelerate-cyber-resilience-water-sector

- Center for Internet Security
  - https://www.cisecurity.org/insights/white-papers/cis-controls-implementation-guide-for-industrial-control-systems
- American Water Works Association
  - https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance

Case Study: Wastewater Treatment

Goal

- Availability
- Compliance (the environmental kind!)
- Reliability
- Standardization

Approach

Operational Excellence

- SCADA/OT Standards.
- Commitment to Reliability
- Adequate Staffing
- Appropriate tooling (shoutout security onion!)

OT Security Hearts Operations

- CIS Implementation group 1 "The Basics"
- Change Management
- Log everything. (Sysmon. Windows Event Forwarding, SNMP) Automation vendors are all hot on Digital Transformation lately too- more logs!
- **Incident response plan. practice with operations**. (shoutout ICS4ICS)

Hot Takes (Yes, And...)

- Its okay to scan ICS devices for vulnerabilities.
- Its okay to upgrade systems.(CIP Secure, machine authentication)
- Patching is fine.

Get Help

MS-ISAC: https://www.cisecurity.org/ms-isac

Water-ISAC: https://www.waterisac.org/

DHS/CISA: https://www.cisa.gov/cyber-assessments

CIS ALBERT: https://www.cisecurity.org/services/albert-network-monitoring

Incident Response Retainers- high value

A Plea

we need you. your community needs you. Water and other utilities are not particularly special. but they are important.

Revision #14
Created 15 February 2023 04:06:37 by Nolan
Updated 15 February 2023 19:01:08 by Nolan