Information Item:
Critical Infrastructure Cybersecurity
Water Sector

Roger Knuteson, Process Computer Manager

Environment Committee: March 9, 2021

METROPOLITAN
COUNCIL

Agenda

- Critical Infrastructure Protection (CIP) Background
- Operational Technology (OT) Cybersecurity
- What Happened at the Oldsmar Florida Water Facility
- How Did This Happened
- Environmental Services OT Cybersecurity Practices
- Continue Current Action Plan

METROPOLITAN COUNCIL

Critical Infrastructure Protection (CIP)

In 1998, President Clinton issued a Presidential Directive PDD 63, the first national policy on critical infrastructure protection creating the framework in which the CIP policy would evolve.

METROPOLITAN COUNCIL

DHS Defined Critical Infrastructure Sectors

Water

Food & Agriculture

Dams

Financial Services

Chemical

Critical Manufacturing

Commercial Facilities

Emergency Services

Transportation

Healthcare

Government Facilities

National Defense

Information Technology

Communications

Nuclear Reactors

Electrical Energy

METROPOLITAN COUNCIL

Water and Wastewater Sector

Safe drinking water is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for preventing disease and protecting the environment. Thus, ensuring the supply of drinking water and wastewater treatment and service is essential to modern life and the Nation's economy.

Why Cybersecurity?

The White House

Office of the Press Secretary

For Immediate Release

February 12, 2013

Executive Order on Improving Critical Infrastructure Cybersecurity

Today, President Obama signed an Executive Order to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with our industry partners.

METROPOLITAN COUNCIL

OT Cybersecurity AWIA S.3021

- America's Water Infrastructure Act of 2018 (AWIA) (129 pages)
- SEC. 2013. references Section 1433 of the Safe Drinking Water Act which was amended to include the following.
- EMERGENCY RESPONSE PLAN.—Each community Drinking Water system serving a population greater than 3,300 shall include an assessment of the physical security and cybersecurity of the system.
- RECORD MAINTENANCE.—Each community Drinking Water system shall maintain a copy of the assessment for 5 years.

METROPOLITAN COUNCIL

What Happened in Oldsmar on 2/5/2021?

- On February 5, 2021, attackers accessed the control system's software at the Oldsmar water-treatment facility in Florida by using remote access to change the setpoint level of sodium hydroxide (lye) dosage in the water from 100 parts per million to 11,100 parts per million.
- The change was immediately detected by a plant operator, who changed the setpoint levels back before the attack had any impact on the system.
- Attacks happened two times that day about five hours apart.
- The attack was reported to the local authorities and the news went national.
- Pinellas County Sheriff's Office, the FBI and the U.S. Secret Service are still working together to investigate exactly what happened in the attack.

METROPOLITAN COUNCIL

How Did This Happen?

- The attackers accessed the Oldsmar water-treatment facility's OT control system via TeamViewer, which is a remote access software.
- All computers used by the facility personnel were connected to the OT control system that used an outdated operating system.
- All computers shared the same password for remote access.
- All computers appeared to be connected directly to the Internet without any type of firewall protection.
- On Feb. 2, just three days before the attack, 3.27 billion unique combinations of cleartext email addresses and passwords were leaked in a database by a cybercrime community. 13 credential pairs linked to the Oldsmar water-treatment facility's OT system were found in that database.

METROPOLITAN COUNCIL

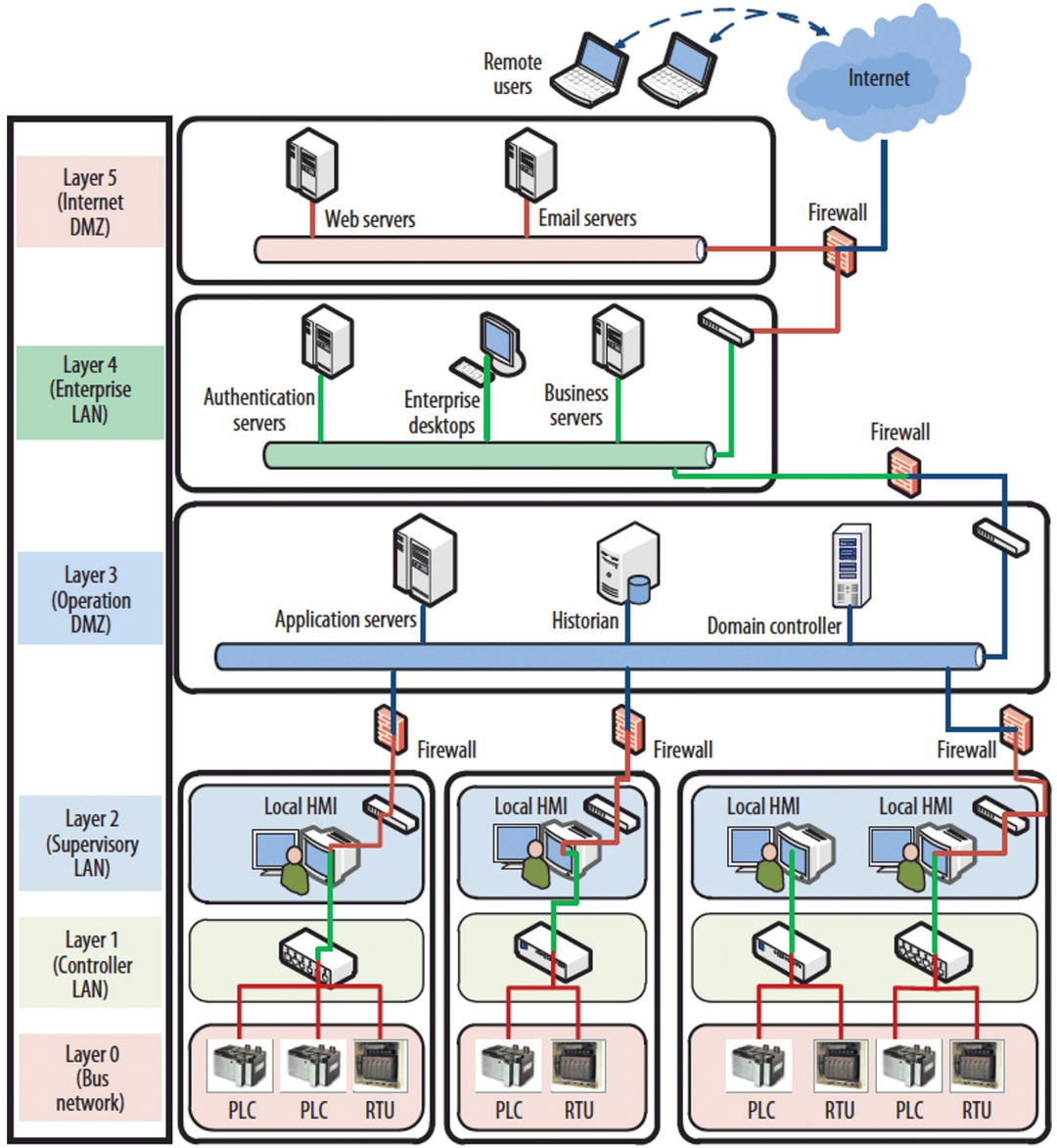
ES OT Cybersecurity Practices

- Restrict remote connections to OT systems that allow physical control and manipulation of equipment.
- Use read-only connected devices to monitor OT systems remotely.
- Firewalls used to implement the Purdue defense in depth network model.
- Keep all computers, devices, and applications patched and up-to-date.
- Use Multi-Factor authentication with unique user accounts and strong passwords.
- Only use secure (Trusted) networks with virtual private network (VPN).
- Block internet connections to the OT system, allow only short-term exception.
- Engineering controls restrict or “clamp” setpoint values of process equipment, other interlocks, permissive and alarms provide additional safeguards.

METROPOLITAN COUNCIL

OT Network Firewalls

Firewalls are used to implement the Purdue model which uses the concept of zones to subdivide Enterprise and ICS networks into logical segments (Defense in Depth strategy) comprised of systems that perform similar functions or have similar requirements. Level 4 and 5 is where corporate IT network infrastructure systems and applications exist.



IEEE Computer Society

CISA releases 3 Industrial Control Systems Advisories

ICS-CERT <ics-cert@ncas.us-cert.gov>
To Knuteson, Roger
1:34 PM
Retention Policy METC-Inbox183Days (6 months) Expires 8/25/2021

You are subscribed to Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Advisories for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

CISA releases 3 Industrial Control Systems Advisories

02/23/2021 10:00 AM EDT

ICS-CERT has released the following 3 advisories today, February 23, 2021. Click on the links below for more detailed information on these Industrial Control Systems vulnerabilities.

Rockwell Automation FactoryTalk Services Platform

This advisory contains mitigations for a Use of Password Hash with Insufficient Computational Effort vulnerability in the Rockwell Automation FactoryTalk Services Platform.

Advantech BB-ESWGP506-2SFP-T

This advisory contains mitigations for a Use of Hard-coded Credentials vulnerability in Advantech BB-ESWGP506-2SFP-T industrial ethernet switches.

Advantech Spectre RT Industrial Routers

This advisory contains mitigations for Improper Neutralization of Input During Web Page Generation, Cleartext Transmission of Sensitive Information, Improper Restriction of Excessive Authentication Attempts, Use of a Broken or Risky Cryptographic Algorithm, and Use of Platform-Dependent Third-party Components vulnerabilities in Advantech Spectre RT Industrial Routers.

Stay Up to Date

- Monitor communications from State and Federal agencies for security advisories.
- Keep up with trade journals.
- Track OT manufactures new technology advancements.
- Partner with other Water Sector utilities.
- Engage with local and national user groups.

METROPOLITAN COUNCIL

Continue Current Action Plan

- Conduct DHS evaluations and act on the findings.
- Follow NIST 800.82r2 OT Cybersecurity Guidelines.
- Support sufficient staff levels and training.
- Support OT system hardware and software upgrade budgeting.
- Keep documentation secure and updated.
- Ensure resilient and operational OT systems per plant.
- Optimize what we already have.
- Continuously improve the ES OT system cybersecurity posture.
- Promote Cybersecurity Awareness.

METROPOLITAN COUNCIL

Questions

Roger Knuteson
Process Computer Manager
651-602-8240
Roger.Knuteson@metc.state.mn.us

METROPOLITAN COUNCIL