AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

MFG201

Industrial OT security best practices at Amazon

Shane Thoney
Senior Manager
Fulfillment, Transportation, and Delivery Security
Amazon Web Services

Steve Blackwell
WW Tech Leader
Manufacturing
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

AWS golden OT security rules

Security best practices at Amazon

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Golden rules for OT security

Asset inventory

Maintain an asset inventory of all connected assets. Categorize them by safety, criticality, patchability, design for air-gapped environments, etc. Create a network architecture showing interconnection between assets and their relationships.

Cyber security risk assessment

Conduct a cyber security risk assessment. Prioritize and group assets into security zones and tighten the trust boundary using micro network segmentation, firewalls, and unidirectional security gateways. Isolate or disconnect insecure assets from the network.

Patch management

Prioritize and implement OT- and IIoT-specific patch management, and software and firmware update mechanisms. Check software integrity and ensure safety and availability of production systems.

Antivirus

Deploy antivirus/antimalware after consultation with equipment vendors. Create a mechanism to discover vulnerabilities and their potential impact to systems.

Auditing and monitoring

Deploy security auditing and monitoring mechanisms across OT and IIoT. Create an incident response playbook and automate aspects of containing events and returning to a known good state.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Golden rules for OT security

Identity and access management

Provision modern IIoT devices and systems with unique identities and credentials. Apply authentication and access control mechanisms.

Encrypt protocols

When ever possible, use cryptographic network protocols for data, monitoring, administration, provisioning, and deployments. Convert unsecure protocols into standardized secure protocols as close to the source as possible.

Encrypt data

Secure manufacturing data at the edge and in the cloud by encrypting data at rest, in transit, and in use. Create mechanisms for secure data sharing, governance, and sovereignty.

Secure network topology

Harden internet connected resources. Place Edge Gateway in a secure network zone. Establish secure connections to cloud services and secure remote access to on-premises resources.

BCP and DR

Create a business continuity and recovery plan, including a plan for cybersecurity testing.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security best practices at Amazon

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security best practices at Amazon

Golden rules are still golden

The same practices apply, but there are a few additional things you may want to consider.

Can you decouple your OT from your central networks?

Challenging to airgap entirely, but does that robot arm really need to be attached to the same networks as your online lunch menu?

Isolate your safety systems

Safety systems are designed to keep risks to an acceptable level. Keeping them isolated reduces their exposure to tampering.

Test your safety systems

Create a schedule and plan for testing these systems, or consider making it part of the system maintenance routine.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security best practices at Amazon

Sensitive communications should be encrypted, even if your PLC needs some help to do so

OT equipment does not always have the ability or capacity to protect the data. In those cases, consider external devices that can protect the data in flight.

Bastion hosts are your friend

When you have to connect into your OT environment, bastion hosts give you a known good platform with more advanced security capabilities than your controller likely has.

Use as secure of operation mode as possible, and monitor for state changes

Avoid using run remote for devices that do not require it. If a device goes from run to program, was there a change record.

Use a historian and mine the data

Why did this conveyance execute a HALT? Was that planned?

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security best practices at Amazon

Use safety signatures

This will help identify changes to the safety configuration as well as be a record of when there is a variance from a known validated configuration.

Password-protect your HMIs

While HMIs should not be able to do things outside the bounds of the configuration protecting them prevents mishaps.

Reach out instead of reaching in

Prefer sending data out of your OT environment to a known destination rather than having an external source connecting into the OT environment.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Shane Thoney

Steve Blackwell

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.