Secure Remote Access to Your Industrial Control Center

Published 27 October 2020 - ID G00729470 - 15 min read
By Analysts Wam Voster, Katell Thielemann

Initiatives: Technology, Information and Resilience Risk and 2 more

The control center in asset-intensive industries is a secure area with access limited to essential operators only. A growing need for operators to control these systems remotely to ensure continuity of operations requires that SRM leaders secure remote access to their production environments.

Overview

Key Challenges

- Most of the systems in asset-intensive industries that are managed via industrial control centers were never architected with remote access in mind. They are also composed of a mix of old, retrofitted or new protocols, communications technologies, or segmentation profiles and lack authentication standards.

- Systems like the human-machine interface (HMI) are hardened and have limited capabilities compared to the “regular” endpoints in IT.

- Control room operators working remotely increase the chance for adversaries to gain unauthorized access to connected operations technology (OT) systems and cause physical damage.

Recommendations

Security and risk management (SRM) leaders in asset-intensive industries responsible for technology, information and resilience risk should:

- Architect networks for IT and OT with secure remote connections in mind, and tightly control and manage these connections with permissions and auditing where this is not possible to remove them due to contractual obligations.

- Deploy proper endpoint management for the remote engineers by examining the option of providing company-owned and -managed devices to these employees.

- Develop appropriate policies and an awareness campaign tailored to employees who access systems remotely.
Introduction

The cyber-physical systems (CPS) that support critical infrastructure industries, such as manufacturing, water, transportation or energy, are highly dependent on OT- and IT-based systems for their command and control. While a dependence on legacy industrial control protocols still exists, most of these systems have migrated to other communication technologies via IT/OT convergence. As a result, common communications protocols like TCP/IP and standards like Windows and Linux have replaced the diverse and disparate proprietary mechanics of OT environments. Virtual private networks (VPNs) are commonly used to access these CPS remotely. Unfortunately, security researchers have also shown concerning vulnerabilities in VPNs used to access systems remotely. Newly deployed operational technologies have accelerated these trends (see Figure 1).

Figure 1: OT Systems Evolution

As 2020 has demonstrated, resilience to everything from weather events to global pandemics shows that there are a number of use cases where remote access to operational systems such as a human-machine interface of a plant or facility is required. This ranges from process monitoring to remote alarm management. HMIs, for example, are not only used to display machine and process data, they can also be the data concentrator for the plant’s entire automation systems. Similarly, a driver for remote access is often a financial one: Organizations intend to save money by doing maintenance remotely rather than sending an engineer to a remote site.

This research provides guidance for developing secure remote access strategies for organizations that use cyber-physical systems in industrial operational environments. This research can be used...
in developing or updating strategies related to managing remote connectivity between operational assets and their operators.

For the purpose of this research, the concept of remote access is defined as the capability for an organization's users and operators to access its private computing resources, data and systems, which reside inside a physically and/or logically protected network, from external locations that may be considered outside that organization's network.

The access of third parties and original equipment manufacturers (OEMs) directly into Level 2 and below in the Purdue Enterprise Reference Architecture (PERA) model is excluded from the technical discussion, but is included in the awareness and policy discussion.

Remote access security helps to create a secure electronic pathway to grant authorized and authenticated access into a control room of the trusted OT network from a location that would otherwise be considered untrusted, like the home network of a control room operator.

Analysis

Architect Networks for IT and OT With Secure Remote Connections in Mind

Industrial control systems (ICSs) hold valuable data for users on the corporate network. Shipping and production information held in ICSs, for example, can be used to facilitate forecasting in ERP systems. To fully unlock the potential of data in their industrial control systems, organizations connect their corporate IT networks to their plant's OT. This connection, however, introduces new security risks. Effective segregation of IT and OT networks is one of the best ways to reduce the risk of malware and other threats traversing from one network into the other.

Two types of network segregation play a role when protecting OT from attacks:

- Network segregation between different OT networks
- Network segregation between the IT network and the OT network

SRM leaders must ensure every site has its own demilitarized zone (DMZ) to prevent malware infections from spreading from one production facility to another.

The Purdue Enterprise Reference Architecture uses the concept of levels to divide an IT and OT network into logical segments. These levels consist of systems that perform similar functions or have similar requirements (see Figure 2).

Figure 2: IT-OT Architecture
Level 5 is the global corporate IT network.

Level 4 is for office automation, planning, scheduling and reporting at a local level.

Level 3 is usually where the actual operations to manage the plant take place.

Level 2 is similar to Level 3, but limited to a specific part of the plant or of the production process, for example, areas like welding or bleaching.

Level 1 consists of the process control equipment. This is where programmable logic controllers (PLCs) and remote terminal units (RTUs) are found.

Level 0 contains the actual instrumentation and equipment executing the production process, like pumps and welding equipment.
The original Purdue Enterprise Reference Architecture did not cater for a DMZ. That is why an additional level has been introduced between Level 3 and Level 4: Level 3½. Ideally, this level is built with firewalls on both sides, but financial considerations drive some organizations to deploy a single firewall with three segments.

The use of the DMZ allows a controlled flow of network traffic. This applies to interactive sessions and machine-to-machine traffic in both directions. Examples include:

- Real-time data from warehousing systems in OT to the ERP systems in IT to enable automated replenishment orders (machine to machine).

- Plant supervisors in the IT network accessing plant information (PI) systems in the OT network for initiatives like process improvement, quality control and predictive maintenance (interactive).

Once the proper network segmentation with a DMZ has been established between the office domain and the production domain, it becomes clear that the value of this segmentation would be seriously diminished if direct external connection into the OT network were to be introduced. As a rule of thumb, all connections into the OT network should go through the DMZ. This includes the connections from remote workers. Unfortunately, OEM connectivity is often required for remote support, diagnosis, warranty and data collection as part of contractual obligation. As such, these connections cannot all be eliminated, but rather will need to be strictly documented, authorized, monitored and managed. A service provider for OT systems with remote access to a large number of facilities in the energy and utilities industry was hacked a number of years ago. Hackers accessed project information related to its OASyS SCADA system. If that attack had not been detected in time, this could have meant these attackers would use the OT service provider as a stepping stone and have remote access to a large number of players in national critical infrastructure.

In special circumstances, like a pandemic, it seems attractive to connect operators directly to the HMIs and engineering workstations from their home working location. This is a fast and convenient way to allow for social distancing while operating the plant at the same time. This would, however, bypass the controls implemented in the DMZ, and attackers would most likely identify this weakness before you do.

Although analog modems are still used in older facilities, these unmanaged connections pose a serious security risk.

The International Electrotechnical Commission (IEC) 62443 standard presents the use of a jump server as a best practice for a remote connection. Typically, a jump server is a hardened computer to manage devices in a separate security zone. A hardened system is a system where all unnecessary software and services, including games, are removed as part of the hardening process. The jump server is placed within the DMZ and configured with strong authentication (e.g., utilizing two-factor authentication).
To provide remote access to the control center, the architecture shown in Figure 3 is recommended. The operator connects to the existing VPN infrastructure using his (company-provided) endpoint (see the Deploy Proper Endpoint Management for the Remote Engineers section for more details). Multifactor authentication (MFA) should be used to establish the connection to the corporate network. Subsequently, the connection traverses the corporate network to the jump server in the DMZ, Level 3½. To connect to the jump server, MFA should be used again; however, this time a different method should be used. This is to prevent attackers from accessing the control center in the unlikely event the companywide MFA method is compromised. As an example, the remote connection to the corporate network uses smart cards or hardware tokens as the additional factor, and the connection to the jump server requires the use of an out-of-band smartphone one-time password. This is also the realm where privileged access management solutions can be deployed. Access to the control center is without a doubt a form of privileged access.

SRM leaders should ensure that monitoring is set up for both the VPN remote access as well as for the connections to the jump server. Using a security information and event management (SIEM) infrastructure allows for the correlation of the events in the VPN and the jump server to ensure the detection of suspicious events, traffic patterns, access or behavior. Existing incident response procedures may need to be reviewed and amended to ensure these use cases are addressed with the appropriate priority.

Deploy Proper Endpoint Management for the Remote Engineers
Physical worksites such as control rooms and operations floors provide inherent security benefits by restricting physical and cyber access to OT. When the control room is extended into the home location of the operators additional controls are required.

The use of privately owned hardware and software allows for a rapid deployment of remote access when needed. It does, however, mean that SRM leaders lose control over the endpoint used for remote access to their OT environment. The recommendation, therefore, is that only corporate-owned and -managed devices are used when connecting remotely to the corporate and operational networks. SRM leaders should minimize the trust in uncontrolled environments, like the home situation of their remote workers. This uncontrolled environment extends beyond the actual endpoint and should include the private wireless network as well. Providing the remote working engineers with a company-owned router with a built-in wireless access point (WAP) has many advantages:

- Media Access Control (MAC) address filtering can be set up such that only the corporate endpoint can connect to the WAP.
- Port (range) forwarding can be disabled, further reducing the options for adversaries to connect remotely to a system in the engineer’s home-working location. Port forwarding enables any external traffic to be routed to an endpoint based on the port number.
- Universal Plug and Play (UPnP) can be disabled. UPnP allows hosts on the internal network that are using UPnP-capable operating systems to automatically configure the router to allow traffic from the external network to access the corresponding internal network resource.

The network address translation (NAT) in the router is insufficient for anything but a “casual attack," even though most broadband routers/firewalls are designed not to permit any unsolicited packets from an external host to be delivered to an internal host. Also, by default, most broadband routers for home use are delivered taking the approach of “permit all outbound, block only.” This is obviously done with the nontechnical consumer in mind. This setup therefore saves technical support costs for the broadband router vendor. The built-in firewall (if any) may not be sufficient to do intrusion detection or intrusion prevention based on packet content. If that is the case, an additional firewall may be desirable at the remote worker's home location. A small office/home office (SOHO) device that blocks incoming data and potentially even employs deep packet inspection (DPI) can identify whether the network traffic is indeed the appropriate traffic or whether it should be discarded.

SRM leaders must ensure that the actual remote endpoints are included when patches are deployed. Unpatched vulnerabilities are one of the top drivers of data breaches for a reason: They are an easy target. In 2017, the Equifax breach exposed personal data for more than 143 million Americans. That breach could have been prevented with proper patch deployment according to the Committee on Homeland Security and Governmental Affairs. In this case, a patch was available months prior to the Equifax attack. Any adversary will attempt to compromise the remote
workstation of the remote-working operators as soon as they discover a vulnerability. Therefore, the implementation of vulnerability scanning on remote workstations to know which essential services may be exposed to adversaries is vital.

Likewise, the use of local admin rights on the remote workstation should be removed. For a properly managed device, the use of local admin by the end user is unnecessary. 1

Another benefit of company-managed devices is that these machines can be “hardened.” The hardening of an endpoint refers to a collection of techniques and best practices to reduce the attack surface. Activities like removing or disabling nonessential software, drivers, services, file sharing and functionality help to reduce the attack surface as these may act as back doors to the endpoint. Obviously SRM leaders should ensure that endpoint protection platform (EPP) or endpoint detection and response (EDR) capabilities are deployed and operational in the endpoints with remote OT access.

Last but not least, logins and sessions should be logged and monitored so that suspicious behavior can be detected rapidly should a device or a session be compromised. SRM leaders should also ensure that remote access sessions are automatically terminated when the session is idle for too long.

**Develop Appropriate Policies and an Awareness Campaign Tailored to Employees Who Access Systems Remotely**

While remote working may be effective to slow the spread of pandemics, it does create security challenges that can be different than for on-premises work. In a period of working remotely, some operators may experience social and professional isolation compared with the time they worked in the control center. Those feelings of loneliness will likely be worse now, as “social distancing” measures cut workers off from their in-person social support systems outside of work as well. Consequently, working in a nonwork environment may result in remote workers being less vigilant when it comes to security.

One of the major risks remote operators will face, especially in this time of both dramatic change and an environment of urgency, is social engineering attacks. Social engineering is a psychological attack where attackers trick or fool their victims into making a mistake, which will be made easier during a time of change and confusion.

SRM leaders must create a targeted and tailored awareness campaign for the operators working from home. They should ensure the remote operators are trained about what social engineering is, how to spot the most common indicators of a social engineering attack, and what to do when they spot one.

It is key to focus on not just email phishing attacks but also other methods of the adversaries, including phone calls, texting and even social media messages.
SRM leaders should also include phishing tactics in their tailored awareness campaign. Remind the operators working from home to be suspicious of emails from unknown sources, and explicitly advise not to open file attachments or click on links. The fact that attackers will seek to take advantage of the current confusion will need to be very clear in the messaging. This is required to make sure the remote operators know to be suspicious of any email that asks for credentials.

It is key to keep operational security teams well-staffed to ensure remote operators have ready access to contact information for the security team to whom they can report security incidents.

SRM leaders should review their current information security policies to determine if there are any established security controls for remote access to company information systems. If no relevant policies exist, this is a good moment to establish the guidelines to address remote access to the company OT control center. A clear definition of roles and responsibilities, not just for the remote operators, but also for their line managers is one of the key sections in the policy. The provision of a company device (see the Deploy Proper Endpoint Management for the Remote Engineers section) means that the security policy can prohibit other members of the same household from using this company resource. A statement to lock the screen when leaving the machine unattended is therefore also required in the policy. As with the human-machine interface in the physical control center, access to the internet from the company-provided device for remote operation of the process should be technically controlled or prohibited in the policy.

SRM leaders must ensure that the “scope” section of their policy explicitly includes the control center operators working remotely. In case one of the multifactor authentication methods involves the use of smart cards, a clear statement that the smart card may not be left in the computer is required. Also, in other cases, mention should be made that the second authentication factor should not be stored or kept with the device that is used for remote access to the industrial control center. The physical security in private homes does not match the level of security control in place to enter the control center. The policy should also ensure that the number of failed logins from remote operators is restricted to prevent brute forcing. The connection should use strong encryption.

SRM leaders should also include a “rapid disconnection” method in the policy to quickly disconnect a remote operator in case suspicious activities are detected. However, this should be done with safety of the process in mind.

Last but not least, SRM leaders should be extra cautious when lateral movement in the OT environment is detected in a period that remote connections are established.

Evidence

1 Researchers Analyze Entry Points, Vectors for Manufacturing System Attacks, Security Week.

Recommended by the Authors

Solving the Challenges of Modern Remote Access
How COVID-19 Has Changed Business Continuity Management

Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus (COVID-19) Outbreak by Focusing on These 7 Areas

Guide Contract Management With the EaaS Customer Bill of Rights

Key Considerations for Implementing a Work From Home Program and Reducing Risk

Recommended For You

GDPR Is Starting to Get Teeth

Getting Serious About Insider Threats

How Disinformation-as-a-Service Affects You

FedRAMP Demystified

Supported Control Implementation for the Public Cloud (Pfizer)

Supporting Initiatives

- Technology, Information and Resilience Risk

- Coronavirus (COVID-19) Resource Center

- Security and Risk Management Leaders

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see “Guiding Principles on Independence and Objectivity.”