Advancing Automation

Cutting Edge Cybersecurity

May 2018

Volume IX

Automation.com

Introduction

Last year, Automation.com introduced the first of the Cybersecurity series of Advancing Automation eBooks. Unfortunately, during that intervening time cyber threats have continued to evolve and even the biggest businesses are struggling to cope. Big names like Facebook, Equifax and Yahoo have all experienced breeches over the last year, and reminded the industrial world how vital it is to stay up-to-date and informed on all the latest trends and technologies that can protect industrial facility. That's why Automation.com has compiled a new edition of our Cybersecurity eBook to deliver the necessary information needed to ensure the strongest possible safeguards for any facility and facilitate future planning to keep one step ahead of the next cyberattack

With valuable insights for both managers and floor personnel, IT and OT, new and experienced professionals, this eBook series continues to keep you securely on the cutting-edge.

Table of Contents

Implementing DHS Best Practices to Secure Industrial Control Systems

by: Scott Coleman,
Owl Cyber Defense Solutions, LLC

Implementing DHS Best Practices to Secure Industrial Control Systems

By: Scott Coleman
Director of Product Management and Marketing
Owl Cyber Defense Solutions, LLC

Modern advancements in industrial control systems (ICS) enable marked improvements in efficiency, production, reliability, and safety, all through increased use of "smart" assets and digital communications. However, this has led to a dependency on communication technology that is seemingly at odds with the ever increasing pressure to enhance cybersecurity in ICS networks.

To better balance the need for communication and security in OT networks, and to determine how best to secure them, it's important to recognize the reasons behind each of their connections. The two primary reasons that organizations provide data paths into or out of their OT networks are:

- To provide information to remote users outside the OT network (production data, SIEM, files, historians, monitoring/maintenance information, etc.)

or

- To allow for remote command and control by users outside the OT network (error remediation, system adjustments, etc.)

To this end, the US Department of Homeland Security, in conjunction with the FBI and NSA, has released recommended best practices that any organization can use to help secure their ICSs:

1. Map and identify all external connections within the OT network architecture

Until you have accurately mapped the network, there is no way of assuring that all points of entry into the OT network are secured, including connections to other networks within your organization. Therefore it is vital to take the time to thoroughly assess, map, and understand the literal ins and outs of your OT network, whether it is performed internally or by a respected third party. This mapping often proves incredibly useful not just for securing ICSs, but also for any number of cybersecurity or operational projects you may consider.

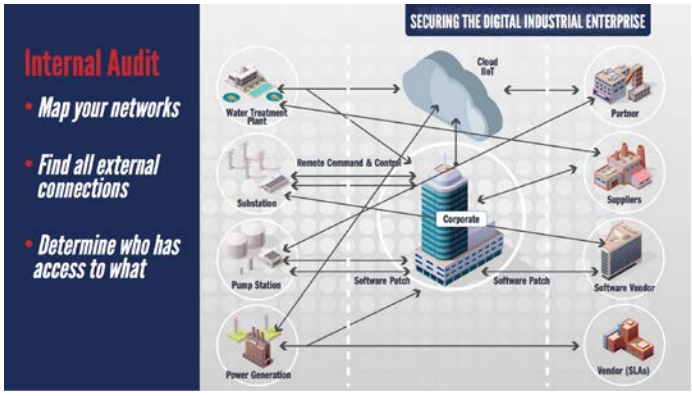

Figure 1: *Map out your network architecture*

2. Reduce the attack surface of your OT network

No matter what the purpose or number of authorized users, it's very important to recognize that each external connection is a potential attack vector for cyberthreats both into and out of your OT network. In order to reduce the attack surface of the OT network, you must first reduce the number of connections to an as-needed or as-authorized basis only.

The DHS recommends that organizations, "Isolate ICS networks from any untrusted networks, espe-

cially the Internet. Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function."

Further, the DHS suggests the logical use of network segmentation to restrict and further control communication paths. "This can stop adversaries from expanding their access, while letting the normal system communications continue to operate. Enclaving limits possible damage, as compromised systems cannot be used to reach and contaminate systems in other enclaves. Containment provided by enclaving also makes incident cleanup significantly less costly."

Consolidating, limiting, or eliminating any unnecessary external connections and services makes it easier to monitor and defend those fewer remaining points of entry into (and exit from) your OT network. Segmenting your networks can also cut off malware proliferation before it finds its way throughout your organization.

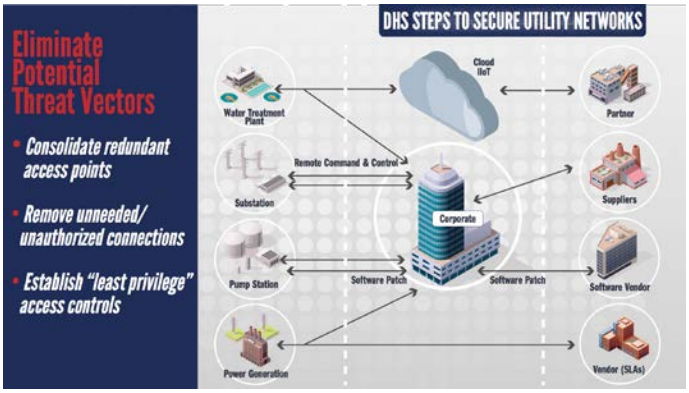

Figure 2: *Reduce network attack surface*

3. If any of the remaining external connections are for monitoring purposes only, convert them to one-way connections

Many times it is thought that the only way to perform remote monitoring is to allow remote access into the network to gather data for monitoring. However pushing or replicating data (historians, databases, SIEM) out to the IT network has proven to be a secure way of getting data into the hands of end-users.

Again the DHS recommends "If one-way communication can accomplish a task, use optical separation ("data diode"). … Where possible, implement 'monitoring only' access enforced by data diodes." Data diodes are one-way transfer devices that allow operational data to exit the organization for monitoring or use by a remote user, without opening a potential entry point or attack vector into the OT network.

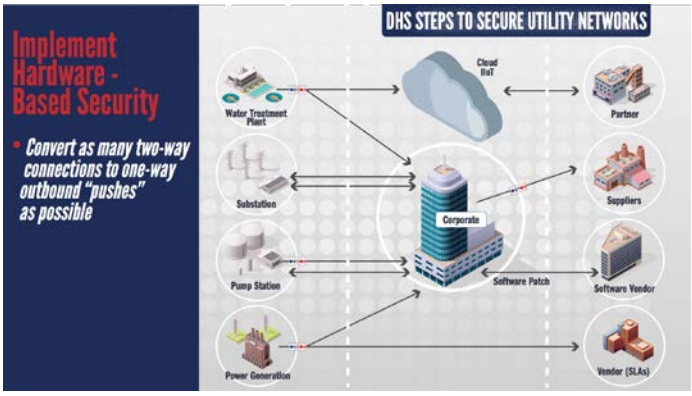

Figure 3: *One-way connection out*

4. If data transfers into the OT network are required (software updates, patches, etc.), convert as many as possible to one-way connections

Despite the desire to lock down the network and keep all threats out, data files, usually in the form of a software patch or update from a vendor, often need to be transferred into OT networks. With a locked down network this is typically achieved with some kind of portable media (thumb drive, laptop, etc.). However, this runs the significant risk of infecting the network when something other than the software update exists on the media. As the DHS notes, "ICS-CERT responded to a Stuxnet infection at a power generation facility. The root cause of the infection was a vendor laptop."

The DHS recommends that organizations, "Get updates from authenticated vendor sites. Validate the authenticity of downloads. Insist that vendors digitally sign updates, and/or publish hashes via an out-of-bound communications path, and use these to authenticate. Don't load updates from unverified sources." Data diodes can simplify this process for secure inbound transfers by utilizing a manifest and hash code verification to ensure the correct and unmodified file is transferred, including matching

the file provided by the vendor on their website or portal. Any file or software that doesn't appear on the manifest or have a matching hash code is placed in quarantine and is never transferred to the OT network.

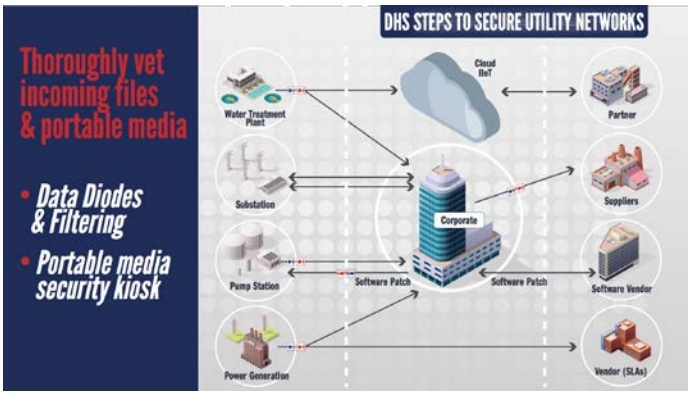

Figure 4: *One-way connection in*

5. Lock down any remaining two-way connections with defense in depth

Most likely, some business or support operations are going to require a two-way external connection. Whether it's for remote command and control, error remediation, or some other critical purpose, it's not always possible to eliminate two-way external connections completely, but it's vital that these remaining connections be heavily controlled.

"Limit any accesses that remain," says the DHS. "Some adversaries are effective at gaining remote access into control systems, finding obscure access vectors, even 'hidden back doors' intentionally created by system operators. Remove such accesses wherever possible, especially modems as these are fundamentally insecure. … If bidirectional communication is necessary, then use a single open port over a restricted network path." This can be accomplished through a highly secured firewall, or a specialized bilateral data diode implementation, using one data diode for each direction in and out of the network.

In addition, the DHS advises against any kind of persistent connections, especially from third parties (or the Internet) – "Do not allow remote persistent vendor connections into the control network."

Bottom line, make sure all external connections are limited in capability, restricted in their paths, and if possible, only exist for a limited amount of time.

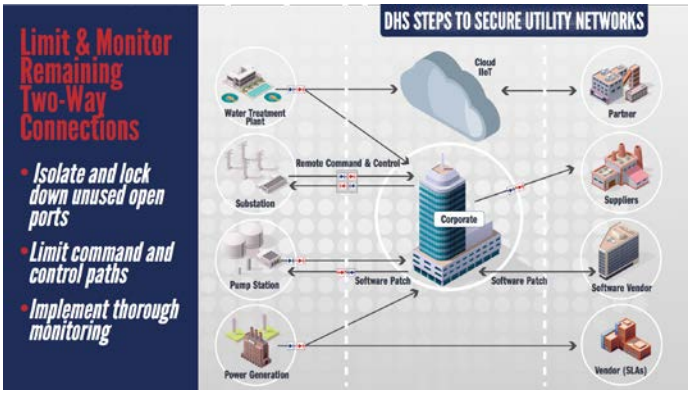

Figure 5: *Limit & Monitor Remaining Connections*

Defense in Depth

As part of a layered, "defense in depth" cybersecurity strategy for ICS communications, a variety of tools are employed, from role-based access controls, multi-factor authentication, whitelisting, and more. Beyond these baseline tools, the two major transfer technologies used to control access points within OT networks, firewalls (software-based) and data diodes (hardware-based) provide the strongest means to secure ICS communications. Yet it's important to point out the fundamental differences and reasons for using both of these tools, either together or separately, and in different situations, to increase the security of your ICS systems.

Software solutions, such as firewalls, are highly versatile cybersecurity tools that can be augmented with a number of security information and event management (SIEM) capabilities, from intrusion detection to deep packet inspection. They are ideal for those connections which must be two-way in order for business operations to function properly. However, they are also inherently vulnerable to configuration changes, bugs, and they will always require regular updates (or replacement) to stop new and emerging threats.

Hardware-enforced solutions utilize physical components to prevent access to secured networks. For instance, data diodes contain specialized circuitry

that only allows data to flow in one direction. The sending circuit is incapable of receiving data, and the receiving circuit is incapable of sending data. For this reason, hardware-based transfer solutions cannot be hacked, and when used to transfer data out of an OT network, cannot be used as a threat vector back into the network.

These fundamental differences represent a sliding scale of access vs. risk, reinforcing the basic concept of reducing risk wherever possible. For example, US military cross domain deployments and nuclear power plants utilize one-way connections with data diodes to transfer data one-way between networks of different security levels, while software solutions cannot be used in these cases, as the risk they present is too high and unnecessary. On the other hand, commercial businesses may have vital two-way connections in their operations, in which case well-configured firewalls can be useful to restrict access, or used in conjunction with a bilateral data diode solution for added security.

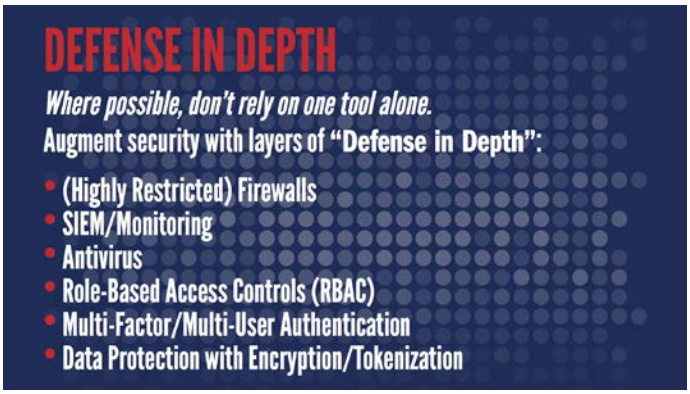

Figure 6: *Defense in Depth*

Keep in Mind

So in summary, the DHS advises that organizations reduce the number of connections to ICS networks, use hardware-enforced one-way transfers where possible to limit exposure, anticipate one-way transfers may have to be made both **into** and **out** of OT networks based on business needs, and for those two-way connections that cannot be eliminated, limit their capability, their communication paths, and the amount of time they are connected.

While defending the perimeter may have fallen out of vogue recently in favor of intrusion detection, advanced biometric authentication, and other measures, keeping intruders out is still one of the best methods to prevent damage to or hijacking of critical systems. Following these five concrete steps from the DHS can help to dramatically improve the cybersecurity of industrial control systems with minimal disruption to normal business operations.

For more information about Owl Cyber Defense and data diode cybersecurity, visit www.owlcyberdefense.com.

ABOUT THE AUTHOR

Scott Coleman has 25+ years of experience working in high tech as a Programmer, Product Manager and now Director of Product Management & Marketing for Owl Cyber Defense. His breadth of experience includes healthcare, telecom, and cybersecurity, for both private and public sectors. He is a published author and an invited speaker at many conferences.

IT'S TIME TO GET PHYSICAL
DON'T LEAVE YOUR SECURITY TO CHANCE

Owl Data Diode Cybersecurity Can Help

Physically-enforced cybersecurity for the strongest protection from cyber threats. Data diode technology secures industrial control system networks and devices from all external attacks, including malware, ransomware, and advanced persistent threats.

In a world gone software, harden your defenses with *Owl Cyber Defense.*

@owlcyberdefense
www.owlcyberdefense.com

OWL
CYBER DEFENSE