COMBATTING THE INSIDER THREAT

BrianAJackson/iStock

Visibility into a facility's proprietary control system configurations is a prerequisite for cybersecurity | By David Zahn, PAS

"Hell hath no fury like a disgruntled or fired employee scorned."

Not exactly the way the proverb goes, but it is appropriate given the significant rise we are seeing in insider cyber threats. According to IBM's 2016 Cyber Security Intelligence Index report, 44.5 percent of all cyberattacks in 2015 — up from 31.5 percent the previous year — were perpetrated by malicious insiders. An additional 15.5 percent resulted from inadvertent actors.

Process plants are not immune to these attacks. Manufacturing was the second most targeted industry with automotive and chemical as the two most attacked sectors. To cite one incident, a system administrator/IT specialist was fired in early 2014 from the Georgia Pacific Port Hudson paper mill. The fired employee subsequently logged into the plant's computer systems from his home and disrupted production by changing how the paper towel was distributed and quality control systems functioned. He ultimately pled guilty in 2016 to intentionally damaging a protected computer.

The insider threat is a trend that companies in all industries cannot dismiss. The effects of these breaches can negatively impact the reputation and livelihood of a company — or, in an industrial environment, cause damage to plant processes and put people at risk. Insiders benefit from having intimate knowledge of existing cybersecurity safeguards and how best to disrupt plant processes. This ability to affect production underscores a critical vulnerability most process industry companies face today.

Plants often lack sufficient visibility into the systems — distributed control systems, programmable logic controllers and safety instrumented systems — most responsible for generating revenue and keeping employees safe. This lack of visibility means unnecessary risk because unauthorized changes may go undetected. Not surprisingly, it is difficult to secure what you cannot see.

Improving visibility

Gaining visibility into these systems is difficult because identifying changes to ladder logic or recognizing changes to safety system availability means going beyond simply inventorying manufacturer and model. True visibility requires deep configuration data — including input/output cards, firmware and control strategies. The task is made more difficult because these systems are proprietary, which means there are no common protocols, such as Windows Management Instrumentation (WMI) or Simple Network Management Protocol (SNMP), to interrogate for the latest configuration data. The problem of visibility is further exacerbated by a variety of control system manufacturers found in a plant or enterprise.

Many companies settle for gathering data from the workstations, servers, routers and switches sitting in front of the proprietary control systems. In fact, these non-proprietary systems account for only 20 percent of the cyber assets in a process control network and offer only a small portion of the inventory data needed. The other 80 percent come from the proprietary control systems themselves.

In the face of these challenges, when companies inventory control system data, they

only capture basic information — such as manufacturer, model and a handful of other data points. Data is frequently collected by highly paid engineers and recorded in a spreadsheet, which often includes errors and data gaps. Over time, the spreadsheet becomes out of date because manual inventory efforts often lag behind changes in a plant. Most would agree that performing change management against a spreadsheet is challenging at best and does not allow for sufficient unauthorized change detection. With a seven-fold increase in industrial control system cyber incidences since 2010, according to Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), facilities must move beyond the spreadsheet and adopt a more automated approach to proprietary system visibility.

Best practices

How should companies tackle this daunting task? The six steps discussed in this section help address proprietary control system visibility and consequently enable other required cybersecurity best practices.

Collect a detailed inventory

Look for a solution that collects and contextualizes the configuration data found deep within plant control systems. The solution must cover each of the manufacturers found in today's plant and go beyond what is available in the workstation. More than a spreadsheet replacement, this automated inventory management approach spans both proprietary and non-proprietary systems.

"Gaining visibility is difficult because identifying changes to ladder logic or recognizing changes to safety system availability means going beyond simply tracking a manufacturer and model."

Establish a security baseline

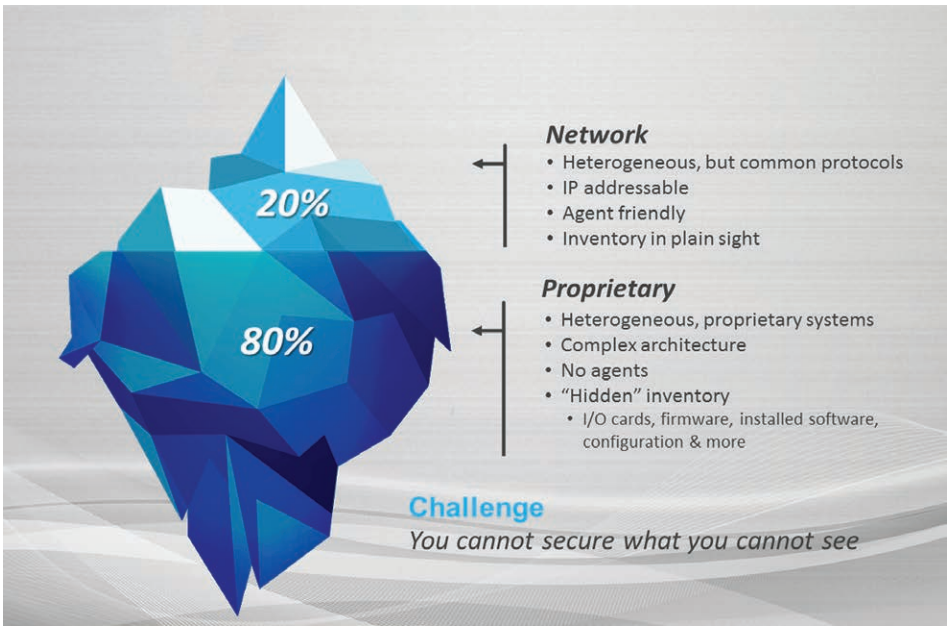
With a comprehensive inventory of configuration data, companies can define which configuration settings require monitoring and reflect a good working state. Baselining is a common practice with non-proprietary systems in which tracking ports and services, for instance, is essential. A similar approach is required for proprietary systems. In addition to being a good cybersecurity practice, having a security baseline conforms to cybersecurity standards and is evidentiary in an audit process.

Identify vulnerabilities

With a comprehensive inventory, recognizing vulnerabilities becomes a straightforward exercise. Vulnerabilities published by ICS-CERT provide information that a simple, automated query can use to identify everywhere those issues exist. This capability allows for more informed decision-making on whether and when to mitigate the risk.

Manage configuration changes

Unauthorized change detection is not only a good cybersecurity best practice but a requirement for most standards. A comprehensive inventory and baseline provide the building blocks to monitor for any changes.



Hidden cyber assets create risks. Graphic courtesy of PAS

Automated workflows initiate incident response protocols based on asset risk levels when change is detected based on asset risk levels. In the end, this capability creates electronic bread crumbs that support management and audit processes.

Close the loop on patch management

Many companies rely on plants to identify Microsoft patches and make implementation or mitigation decisions. Few have a real-time view into the applicability and status of patches in the plant environment. As patches and manufacturer approval bulletins are published, personnel should automatically and centrally track patch status through the testing, implementation and mitigation phases. Unlike an IT patch process, this approach focuses only on automating the work processes behind operational technology patch management.

Verify backup & recovery

When all else fails, a robust backup and recovery capability is essential. On-site and offsite backups of all critical systems — both proprietary and non-proprietary — mean a quicker return to production if a malicious attack or inadvertent engineering change gets through. A backup process tied to an inventory management process is the most efficient approach to achieving recover goals.

3 examples

Taking the six steps detailed in the section above reduces risks to a process and ultimately increases asset reliability and plant safety. How do these steps apply to real-world cybersecurity scenarios? Three scenarios are discussed in which having a rich inventory hardens cybersecurity within a plant.

Unauthorized control strategy change

A plant turnaround is occurring, and scores of facility and third-party engineers are onsite in support of the turnaround activities. A process control engineer makes an unauthorized change to the control strategy of a critical control system. The change may result from a simple engineering mistake or because a third-party engineer introduces malicious code from his compromised lap-

top. How likely is a company to detect this unauthorized change — by an authorized user no less — and drive appropriate remediating, auditable actions?

The solution is to collect and contextualize inventory data including control strategies from all critical cyber assets — both proprietary and non-proprietary. Based on a security baseline, the facility should monitor for unauthorized change and initiate a response protocol commensurate with process risk. Finally, the team should automatically track the change that restores the control system to the proper configuration verifying that the necessary mitigation steps were taken.

Published vulnerability impact identification

ICS-CERT published a critical vulnerability in early 2015 concerning multiple models and versions of a certain manufacturer's transmitter. This transmitter notably works across all control system brands and is not typically captured in manual or non-proprietary inventory efforts. How easily will the cybersecurity team answer a question on enterprise-wide exposure to this vulnerability?

A simple query will immediately identify every inventoried control system that has this transmitter. An inventory that spans the heterogeneous, proprietary control systems across the entire enterprise will provide complete results. Further, an automated policy can look for instances in the future when that same transmitter is reintroduced — possibly from a spares inventory.

Closed-loop patch management

Microsoft publishes a patch that is approved by the control system manufacturer. The patch is deemed critical and additional security controls are required to mitigate risk if not implemented. How easily can personnel identify the affected systems and whether the patch or security controls are implemented?

A comprehensive inventory enables automated identification of which manufacturer-approved patches apply to which systems. Workflow automation drives patch processes, capturing all steps for internal and external audit purposes.

Detailed inventory required

According to ICS-CERT's 2014 Industrial Control Systems Assessments Overview and Analysis, effective physical and environmental protection requires a detailed inventory that spans all operational hardware and software components. This is not news to cybersecurity personnel responsible for corporate networks, but it is a relatively new concept for personnel managing or securing the proprietary control systems responsible for processes. Getting inventory right means gaining visibility into both the proprietary and non-proprietary systems with configuration detail that protects the plant from malicious attack or inadvertent change.

Although few details of such attacks are published, companies that have experienced compromised control systems from malicious insiders or inadvertent actors may have avoided downtime or financial loss with a more comprehensive inventory that included proprietary control system configuration information. With this data, they could have detected change more quickly and understood the optimal path to recovery. This is an object lesson for the process industries as the scorn of a disgruntled or fired employee is something all may suffer one day. PR

David Zahn is the chief marketing officer and the general manager of the Cybersecurity Business Unit at PAS. He has more than 24 years of enterprise software and services experience within startup and high-growth companies in the oil and gas and information technology industries. Most recently, he served as vice president of marketing at FuelQuest and vice president of marketing at Avalara. Zahn holds a bachelor's degree in economics and managerial studies from Rice University as well as an Master of Business Administration from the University of Texas – McCombs School of Business.

PAS
www.pas.com

As seen in the September 2016 issue of *Processing* magazine.