Process Solutions

White Paper

Easing the Cyber Stress

Abstract

Security awareness is on the rise, but translating that awareness into action can be a very daunting experience. A manufacturer can end up stalled because they lack direction in where to begin or which best practices to follow. This is where managed industrial cyber security services can open the door to a secure environment. Managed security services in an industrial environment takes the uncertainty, complication and effort of industrial cyber security off the task list of process control engineers and puts it into the hands of process control security experts.

Table of Contents

Managed Industrial Cyber Security Services Boosts Process Uptime 3

Attack Vectors All Around 4

Awareness Elevates 5

Managed Change is Inevitable 6

Cost Factor 6

Managed Industrial Security Services Takeaway 6

HQ Needs to Know 7

Conclusion 7

Background

In this day of targeted attacks that can focus on any manufacturing enterprise, a solid industrial cyber security program is critical to ensuring availability. A system outage due to a virus infection or other cyber incident is unacceptable.

On top of that, the direct consequences of an attack could result in unplanned downtime, loss of product or impaired quality, manipulation of data, unauthorized use of systems, damaged reputation, and harm to personnel and monetary damages.

Utilizing managed security services in an industrial environment enables continued uptime because these providers assess, design, implement, and continuously monitor security for control environments. In addition, they provide a proactive defense with continuous monitoring and analysis of the system. As a result, the manufacturer can focus on keeping the process operational and making more product.

The goal of a managed industrial services program is to:

- Deliver services with a secure encrypted connection with two-factor authentication
- Protection management that provides tested and approved patches and anti-malware definitions
- Continuous monitoring and alerting, which provides 24/7 monitoring of system, network and cyber security performance and automated alerting against thresholds
- Intelligence reporting that delivers insights into the operation and security status of distributed control system (DCS) components and the process control network (PCN)
- Perimeter and intrusion management, which offers firewall support and intrusion protection system (IPS) implementation and management

Managed Industrial Cyber Security Services Boosts Process Uptime

Getting started with industrial cyber security solutions and programs can be overwhelming. People often end up stalled because they lack direction in where to begin or which best practices to follow. This is one area where managed industrial cyber security services can assist. Managed security services in an industrial environment takes the uncertainty, complication and effort of industrial cyber security off the task list of process control engineers and puts it into the hands of process control security experts.

One hundred percent uptime is the goal of any automation environment and a solid industrial cyber security program is critical to ensuring availability. A system outage due to a virus infection or other cyber incident is unacceptable.

Utilizing managed security services in an industrial environment enables continued uptime because these providers assess, design, implement, and continuously monitor security for control environments. In addition, they provide a proactive defense with continuous monitoring and analysis of the system. As a result, the manufacturer can focus on keeping the process operational and making more product.

Understanding security is not the same for every company. Implementing an industrial cyber security solution is not a cookie-cutter initiative where all organizations get the same products and services, but rather it is a true integration program. With managed industrial security services, each organization gets an engineered solution, not a one-sized fits all program.

While companies question why they should spend resources when they have never suffered a cyber incident, the truth is, organizations often don’t know they suffered an attack. In serious attacks the direct consequences could be substantial, including:

- Unplanned downtime
- Loss of product or impaired quality
- Manipulation of data
- Unauthorized use of systems
- Damaged reputation
- Harm to personnel
- Monetary damages

Attack Vectors All Around

There are plenty of new and sophisticated attacks hitting industry from the outside, like advanced persistent threats (APTs), including malware, viruses and Trojans. These threats are dynamic, ever-changing and the attack code is readily available. In addition, there is the issue of an accidental, or malicious inside attack.

For most process control environments, the insider threat is more prevalent and dangerous than the outside attack. Most environments have some type of firewall in place, so attackers must go through the corporate firewall and then the process control firewall to infiltrate. If proper configurations are in place this could be difficult.

A more plausible scenario could be someone on the plant floor, such as an employee or contractor. They could plug in a USB and that is the beginning of a security problem. Or possibly someone with elevated privileges getting on the system and then accidentally causing a problem--like changing a configuration parameter or the name of a software program resulting in an outage.

In the end, a manufacturer needs the defenses to fight off any kind of attack.

Thus the need to transition from a static, reactionary security to a continuous security program – one with an infrastructure and methodology that supports the ISA99/IEC 62443 concepts of zones and conduits, authentication, security logging, input validation and system integrity checks.

The goal of a managed industrial services program is to provide:

- Deliver services with a secure encrypted connection with two-factor authentication
- Protection management that provides tested and approved patches and anti-malware definitions
- Continuous monitoring and alerting, which provides 24/7 monitoring of system, network and cyber security performance and automated alerting against thresholds
- Intelligence reporting that delivers insights into the operation and security status of distributed control system (DCS) components and the process control network (PCN)
- Perimeter and intrusion management, which offers firewall support and intrusion protection system (IPS) implementation and management

Managed Industrial
Cyber Security Services

Secure Connection
Protection Management
Continuous Monitoring and Alerting
Intelligence Reporting
Perimeter and Intrusion Management

Awareness Elevates

Attack awareness continues to rise as one survey by BAE Systems Applied Intelligence found that 53% of U.S. companies now regard the cyber attack threat one of their top three business risks[1].

That report echoes the warning from the World Economic Forum that cyber attacks are among the five biggest threats facing the world this year. That research detailed concerns and opinion around security and indicates a strong demand for greater intelligence about the nature of new cyber threats and a better understanding of business vulnerability.

Another survey by the SANS Institute, a private U.S. company that specializes in information security and cyber security training, points out a majority of organizations now operate under the assumption their network already suffered a compromise[2], or will soon suffer an attack.

With that heightened awareness of the inevitability of an attack, enterprises still remain vulnerable to all manner of cyber assaults, according to Hewlett-Packard's annual Cyber Risk Report. Configuration issues and widespread use of antiquated technologies are among the main threats to large organizations, the HP report said[3] .

While awareness is a step in the right direction, showing the dollars and cents effect illustrates the bottom line value of an industrial security program.

That is because the cleanup and resolution of a breach takes an average time of one month to complete and it costs a large organization $20,000 per day to remediate, according to a new Ponemon Institute report.

To add it all up, the price tag for a data breach now at $639,462, the Ponemon report found[4]. That's an increase of 23 percent over 2013, said Larry Ponemon, chairman and founder of the Ponemon Institute, whose 2014 Global Report on the Cost of Cyber Crime is an annual look showing what organizations end up paying after a breach.

The average cost of cybercrime per company in the U.S. was $12.7 million this year, according to the Ponemon report. Globally, the mean annualized cost for the surveyed organizations was $7.6 million per year, ranging from $0.5 million to $61 million per company.

With costs of breaches continuing to rise, companies struggle to keep their networks secure against rapidly evolving, and more sophisticated cyber threats.

Despite the rising complexity in the technological and regulatory landscapes, companies still typically rely on outdated methods to keep data secure, according to new research from Frost & Sullivan. By investing in several point products, businesses are finding the process to maintain these solutions to be unmanageable, the report said.

[1] Attacks a Top Risk, After Target Hack, ISSSource, February 25, 2014
[2] Awareness Awakening: Firms Assume Compromise, ISSSource, February 25, 2014
[3] HP Cyber Risk Report 2013
[4] Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis, Ponemon Institute, May 5, 2014

Managed Change is Inevitable

There are engineers and operators that have been doing process control for a long time and in the past their environment has been completely isolated from any, and all, other networks in the company. The reality is at least 90 percent of manufacturers don't have that anymore. Whether they realize it or not, the plant floor has connectivity. Either through a firewall, or a gateway to the business networks, there is connectivity because the people in the corporate offices need to monitor what is going on inside those networks.

In addition, outside third parties need to enter systems for activities like monitoring for environmental or compliance issues. So, there is plenty of connectivity outside of the process control environment and engineers executing real-time process control often don't understand that. Process engineers believe their environments are completely isolated, but attackers and accidental incidents can infect what they have today.

Clearing up the misconception of Internet connectivity and allowing a third-party service center access to the network can be a challenge. However, a managed industrial security program provides a very secure way for the user to control delivery of software and antivirus updates and patches.

Alternatively, if a manufacturer tries to connect to the Internet themselves for updates, or if engineers not versed in security bring updates on an USB drive, these can be more dangerous to the environment than using a third-party managed secure connection.

The software found on the Internet can have viruses – and who knows where the laptop has been? Managed industrial services experts will test and verify all updates and then send software updates over a secured connection for the process control network. As a result, it will be free of viruses and it will be the correct version of software for the network.

While there is fear about remote connectivity with engineers saying, "Someone from the outside will be able to connect to my environment and do anything they want," a secure encrypted connection with two-factor authentication can resolve those concerns. A secure connection means it is a dedicated private communication from the process control network to the isolated managed security facility. The user is in complete control of the connection as far as who connects, when they connect, and what traffic is allowed to flow. Having all communication flow through a single, high security channel is much more secure than allowing multiple connection solutions or using portable media or devices.

Secure Connection Architecture

- SSL Encrypted, Certificate Authenticated Tunnel
- Initiated by site's Secure Service Node
- Connect to Managed Security Service Center Only
- Tunnel through corporate network provides additional security
- Relay Server isolates PCN from Corporate Network
- Restricts end nodes from sending or receiving data out of PCN

Cost Factor

A managed security service is not a new idea. Corporate IT environments have been doing this for a long time and have achieved great cost benefits. The cost for managed industrial services ends up being about one fourth the price of a single onsite engineer. If a company were to employ security services by itself, it would need, depending on the size of the network, two or three people dedicated to the program.

When you really look at it, the crown jewels in any organization are the process control environment. If there is any unplanned downtime, cash can begin draining like water through a sieve. Therefore, the most critical component in their infrastructure requires a secure environment.

Managed Industrial Security Services Takeaway

- Connection between service center and facility totally encrypted all the way through
- All sessions end up logged; recorded sessions so you can see everything an engineer did

- When auditors and compliance people come in, you can show them the logging and recording
- Local personnel are in control of everything
- Two-factor authentication is used for any allowed remote connectivity

HQ Needs to Know

Awareness is continuing to grow to the point where everyone from the plant floor up to the boardroom recognizes an insecure environment is a clear and present danger.

The board is going to ask questions about the process control environment security regarding compliance and adherence to regulations. The managed industrial services program can provide a plan, answering those questions before they are asked.

In addition, in this litigious age, having a solid and cost effective security plan will show the board and stockholders you invested in keeping the organization secure. It shows a strong level of corporate diligence.

However, industrial cyber security is a complex problem that cripples most organizations from the start of planning.

With that in mind C-level executives and board members are beginning to understand they need to develop stronger, more comprehensive plans for incident response. A managed security service in an industrial environment is a vital move to reduce a breach that will damage the corporate image, or incur losses. A risk-free decision considering the alternative.

Conclusion

At Honeywell, we are committed to providing cyber security solutions, technology and services that help the process and critical infrastructure sectors defend the availability, reliability and safety of their operations.

Honeywell's portfolio of end-to-end solutions enables industrial facilities to improve their cyber security posture and provide on-going threat management. They are enabled by advanced technology, and include the training of people and application of the operational process controls necessary to ensure effectiveness.

Our industrial cyber security solutions leverage Honeywell's long history in plant safety and proven know-how in process control environments. Having delivered hundreds of industrial cyber security projects globally, Honeywell's team of certified experts provide consultation and solutions across verticals such as Oil & Gas; Chemicals; Refining and Petrochemicals; Energy and Power; and Minerals, Mining and Metals.

Honeywell's Managed Industrial Cyber Security Services offering packages the services needed to reduce the risk of security breaches. Our solutions manage the essential elements of your process control infrastructure into one comprehensive solution.

For More Information
Learn more about Honeywell's Industrial
Cyber Security Services visit our website
www.becybersecure.com or contact your
Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell Control Systems Ltd, Honeywell
House Skimped Hill Lane Bracknell RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

WP-14-19-ENG
November 2014

Honeywell