Technical Paper

IIAR Natural Refrigeration Conference

March 12 – 15, 2023
Long Beach, California

ACKNOWLEDGEMENT

The success of the IIAR Natural Refrigeration Conference is due to the quality of the technical papers in this volume and the labor of its authors. IIAR expresses its deep appreciation to the authors, reviewers, and editors for their contributions to the ammonia refrigeration industry.

ABOUT THIS VOLUME

International Institute of Ammonia Refrigeration
1001 North Fairfax Street, Suite 503
Alexandria, VA 22314

703-312-4200 • info@iiar.org • www.iiar.org

Technical Paper #1

Cybersecurity in Automated Industrial Systems

Josh Symonds, Lead DevOps Engineer
CrossnoKaye

Abstract

The rise of automation brings new cybersecurity threats to heavy industries. Cybersecurity attacks like ransomware, malware, and phishing are becoming commonplace and more sophisticated as they continuously evolve and change. This paper reviews the risks and tactics of the most common classes of attacks and outlines solutions and defense strategies to mitigate Internet attacks that can be easily adopted into automated industrial control systems.

Practical Application

Cybersecurity attacks – ransomware, malware, and phishing – are continuously evolving and changing. However, while it can be frustrating to hit a moving target as industrial control systems become more connected and accessible, it is a target that company leaders cannot afford to miss. Happily, robust solutions and strategies to mitigate Internet attacks are already deployed in other sectors, and these solutions can be adopted into automated industrial control systems.

Introduction

Automation and Internet control of facilities are becoming commonplace in the industrial sector. Plants and grids that previously required manual oversight and teams of skilled engineers can now be controlled from hundreds of miles away by individuals or even automated systems. Automation and connected control offer significant benefits, and this realization has the industrial space moving quickly in this direction. Errors and accidents will become ever rarer as the industry becomes greener, all while costs associated with industrial facilities decrease.

There is, however, a downside to ease of access and control: the threat that bad actors will suborn industrial facilities and the processes used to control them, just as they do other Internet-connected applications. Classes of attacks that in the past were a problem only for Internet applications like Facebook or Twitter could become commonplace in our industrial infrastructure. Imagine the potential losses that could result from a ransomware attack on a large cold-storage facility. Spear phishing that targets operators of electrical grids or industrial equipment and malware attacks on industrial computer systems are other examples of the risks associated with this transformation that has already occurred in multi-billion dollar companies across the industrial sector.

Well-established Internet security protections already exist to mitigate these threats. The industrial space has benefited from a cautious and conservative approach to adopting new technologies, and reasonably so – no one wants the software running electrical grids or refrigeration facilities to have defects when tried-and-true (but older) technologies enjoy the benefits of stability and wide adoption.

A crucial component of this more conservative approach was "air-gapped" systems. Air gapping is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

Twenty years ago, air-gapping was the final word in cybersecurity. Unfortunately, as other sectors have come to realize, unconnected systems have their own vulnerabilities. They are difficult to update and administer, and yet they can still be compromised by clever attackers. In addition, reasserting control over an affected system is extremely difficult (or even impossible). The future requires connection and control, plus security delivered seamlessly at industrial facilities by experts.

The need for connected control systems, and the reality of Internet attacks against those systems, has forced the industrial space to move rapidly to adopt new solutions for these new problems. Fortunately, there are solutions that already work well in other connected industries that the industrial sector can adopt. With proper planning and training, it is possible to create secure systems and processes that are highly resistant to attack, similar to those utilized in social media, finance, healthcare, and government applications.

It behooves us to understand the risks that industrial facilities face from the rise of automation and Internet control. As mentioned, these are broadly the same risks that other sectors of the economy have had to contend with as they have moved towards automation and connection themselves; they are ransomware, malware, phishing, and lack of processes and controls.

Ransomware

One of the largest and most dangerous classes of cybersecurity events is ransomware. Ransomware takes connected assets and holds them hostage by encrypting data or control systems and refusing to release the keys used to lock them unless a ransom is paid. (And, just as with most ransoms, whether or not the attacker will liberate the asset after receiving payment is questionable.) In some cases, ransomware attacks have been foiled by clever security teams exploiting flaws in the encryption methods used by attackers – or by government agencies intervening on behalf of the victims. Such defenses are unfortunately unreliable by their very nature.

Cybersecurity experts recommend continuous read-only backups and rapid, well-tested restoration procedures to fully protect against ransomware attacks. Even if a database is encrypted by an attacker, if it can be restored using a point-in-time backup directly before the encryption event, the attacker's efforts are worthless. Similarly, compromised control systems are easily restored if a robust procedure for recovering those systems has been tested and performed prior to an incident. While an attacker might briefly have control, they ultimately have no leverage over the organization they are attempting to ransom.

Of course, these defenses presume an infrastructure that is already highly decentralized across multiple geographic regions and failure zones. Backups are meaningless if attackers can alter or delete them; control system recovery requires a working copy of the control system and a reliable, well-tested procedure to restore it. Plans such as these are real requirements for connected industrial facilities, at least as much as any other on-site safety and control.

Malware

The vectors for ransomware are numerous: a bad PDF downloaded and opened, an unpatched operating system flaw exploited, a compromised USB connected to a running system. Because there are so many potential avenues of delivery, foiling malware in a generalized manner is extremely difficult. Nevertheless, effective anti-malware strategies exist. Reducing attack surfaces as much as possible, applying layers of security and isolation to all outward-facing systems, and implementing real-time observability so that attacks can be perceived and reacted to in their initial stages are all crucial tools in the fight to secure systems from bad software.

Of these, reducing the attack surface is one of the fundamental principles of cybersecurity. A database not accessible from the Internet is inherently more secure than one that is; an operating system with all extraneous software removed is much more desirable than a generic commercial installation. When designing systems that are intended to be connected to the Internet, it is important to consider from the very first steps what should be accessible and what should be firewalled away. Still, even inaccessible systems should be secured. Air-gapping is no guarantee of security. Layers of protection are crucially important so that the failure of one layer does not compromise the entire system.

And one of those layers should certainly be robust anti-malware defense software. Previously termed “anti-virus software,” these tools have evolved into a complicated and predictive suite of processes called “endpoint security” or “monitored detection and response.” In lieu of simply isolating viruses, endpoint security can ensure the integrity of running processes and files, disable the most common vectors malware uses to gain control of systems and provide real-time metrics and real-time responses to controllers continuously monitoring systems.

Observability and control are of the utmost importance to any layered security approach. In the event of total security failure, where an attacker successfully

introduces malware to a running system, operators must know immediately that such a breach has occurred and have robust tools to counter it. The software controlling industrial facilities must not only alert on the penetration of any layer; a knowledgeable security team is required to respond to suspicious events with fine-tuned controls that allow individualized responses on an extremely rapid timeframe.

Phishing

Protecting systems from unauthorized entry is critically important – but what about protecting systems from authorized entry? Sophisticated social media attacks are still some of the most widely used tools to obtain access to secure systems. For example, calling a team member and pretending to be tech support and requesting their password; or giving an operator a nefarious login portal into which they attempt to login. Tragically, even less sophisticated attacks are often successful. Most passwords are still some combination of a single English word or name and two digits (usually a birth year). A simple dictionary attack can frequently brute force a password and allow an attacker authorized entry into a system.

While there are many complicated technical solutions to security, the solution for phishing is a human one. Operators require training and proper tools to defend against these attacks. Password policies requiring strong, unique passwords are a start – even better is supplying employees with password management software that enforces those policies. Multi-factor authentication is a critical tool in preventing an attacker who obtains a login from successfully using it. But nothing beats frequent security seminars with strong and simple messaging. “Never tell your password to anyone” is a maxim that cannot be repeated enough.

Similarly, creating channels to report breaches and respond to them rapidly is an unfortunate necessity. A company’s security team needs to be accessible and responsive. Creating open lines of communication between employees and security is

an excellent first step to reporting incidents, but even people outside companies need a verifiable and secure way to report security flaws. A simple bug bounty program can be a surprisingly effective tool to turn potential attackers into responsible reporters, and a security incident into a closed avenue of attack.

Process and Controls

Robust backups; layers of anti-malware software; an excellent security training program. What good are these strategies if they are not used? How can one say that an expensive security system is functioning properly when an employee leaves a door ajar, uses an operating system that has not been hardened properly, or receives a file with an unapproved email program? The ideal security program must prevent process failures due to a lack of documentation, training, and standardization.

Processes and controls are an often overlooked component of a complete security story that is as crucial as anti-malware software. There are multiple security organizations and guidance frameworks that organizations can use to audit their security controls – and even better, the output of these frameworks is robust documentation and training materials that employees can use to do their jobs safely and effectively.

For a company following the path of standardization and controls, a third-party auditor is a vital business partner. Being able to prove compliance, both to external clients and internal security teams, multiplies the effectiveness of an investment in cybersecurity. Conversely, an expensive security program without standardized processes and controls is as useless as a bank with a backdoor into its vault.

Most process frameworks require vendors to be audited carefully, which is a task everyone – but especially industrial facilities – must take extremely seriously. Vendors with connections to facility controls or sensitive data can be backdoored or suborned

to gain access to those resources; ensuring that vendors are strongly compliant with a well-known security framework that they consistently maintain is a prerequisite to a strong vendor relationship.

As a starting point, at the very least, a vendor should:

- Have an information security program that includes policies that, upon signing an NDA, they should be happy to disclose
- Use two-factor authentication internally and provide it externally for all client-facing resources
- Be SOC2 Compliant (or another equivalent framework)
- Train employees annually on cybersecurity threats

Evidence of these controls is a very strong indicator the vendor in question takes security seriously enough to be trusted with industrial systems.

Cybersecurity attacks – ransomware, malware, and phishing – are continuously evolving and changing. While it can be frustrating to hit a moving target, as industrial control systems become more connected and accessible, it is a target they cannot afford to miss. Happily, robust solutions and strategies to mitigate Internet attacks are already deployed in other sectors; said solutions can be easily adopted into automated industrial control systems.

In the end, however, the effectiveness of these solutions is limited by how uniformly they are implemented. Proper Internet security, standardization, and control are now every bit as important as any other industrial safety tool. By looking to other sectors of the economy that have been transformed by Internet connectivity and accessibility, industrial solutions can find a path to the efficiencies promised by remote control and automated systems that are still safe and secure.

Conclusion

Within our industry, much discussion rightfully focuses on equipment capability, energy efficiency, product load, and the right Insurance policy. However, our discussions must now expand to include an understanding of the new tools and processes needed as we move into the future. Cyber-secure cloud control platforms is now a reality in the industrial sector. As companies begin to embrace these solutions it's important to know exactly what's important:

1. Make sure these platforms are controlled and managed via a SOC2-compliant secure development process.
2. Use secure remote access and provide a secure login provider via Single Sign-On.
3. Keep all clients siloed from each other.
4. Provide control via a facility-located local dashboard in case there's a loss of Internet connectivity or cloud downtime.
5. Make sure a server-side agent is validating control commands.
6. Create role-based access control for operators and users. Operators can have different levels of access, from "read-only" all the way to total control "admin."
7. Log all commands from operators/users to create a chain of accountability.
8. Use full-disk encryption and encrypted communications.
9. Make sure the platform is continuously logging, auditing metrics, and alerting.

Knowing how to move forward during this period can be somewhat daunting, but it's necessary.

Notes:

Notes: