Setting the Standard for Automation™

WHITE PAPER

The Industrial Cybersecurity Problem

By Eric Byres, PE
Chief Technology Officer
Tofino Security
A Belden Brand

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Until recently, the reasons for securing Supervisory Control and Data Acquisition (SCADA) or Industrial Control Systems (ICS) weren't always that compelling. Certainly, companies had to deal with inadvertent network incidents and the occasional insider-threat in their production environment. But for most, the risk of an externally driven cyber-attack against ICS was considered minimal. Then in 2010, we witnessed the overnight emergence of global cyber attacks against key industries, such as energy, chemicals and manufacturing.

The trigger for this new reality was the discovery of the Stuxnet worm. This destructive malware was successfully introduced into an apparently "air-gapped" nuclear facility with the intent to destroy an industrial process. It used multiple methods to infiltrate the target site, the most famous of which was the use of a USB key.

The exposure of Stuxnet had multiple effects:

1. **Security researchers turned their attention to industrial systems.**

   Stuxnet's fame drew the attention of security researchers and hackers to the existence of industrial systems and devices. It also made it clear how insecure they really were. In 2011, more ICS vulnerabilities were made public (many including exploit software freely available on the internet) than in the entire previous decade. In 2012, there were even more vulnerabilities. 2013 shows every sign of breaking records again.

2. **New advanced persistent threats targeting industry began to emerge.**

   Stuxnet wasn't the first advanced persistent threat (APT), but it was the first to focus on industry. As well, it was so well dissected by security experts that it became an "APTs for Dummies" cookbook on how to write attacks that target industrial companies.

   Most recent APTs have focused on industrial espionage to steal business information from the energy and chemicals industries. Others, like Shamoon (which was not all that "advanced" or "persistent"), have been successful at destroying very large computer systems in the oil and gas industry.

   APTs are difficult to detect: they can hide and collect data for years. The losses resulting from them are financial- and reputation-related, rather than being safety or environmental incidents. Critical infrastructure, such as financial services, has been dealing with APTs for years, but they are new to the industrial space.

   Expect to see many more APTs discovered in the coming years. If we don't see more, it is likely due to the fact that we haven't found them, not that they don't exist. Industrial-focused APTs are clearly effective for their creators, so they won't likely stop creating them.

3. **Low-grade cyber "warfare" went mainstream.**

   Stuxnet has been widely attributed to a joint U.S./Israeli project to destroy Iran's uranium enrichment program. Its existence has given tacit approval to other nations and political groups to use cyber-attacks as a form of undeclared warfare. Most recently, we have seen large scale cyber attacks on South Korea that have been attributed to North Korea.

   If you have critical industrial facilities in any politically sensitive region (such as the U.S., the Middle East, or the Far East), now is the time to renew your industrial cybersecurity efforts.

Industrial Control Networks are a Challenge to Secure

Industrial networks used to run on proprietary networks, used proprietary equipment, and were isolated from business networks and the internet. This was the era of "security by obscurity" and "security by air gap."

Over the last decade, however, industrial networks have been migrating from proprietary systems to commercial off-the-shelf technology like Ethernet, TCP/IP, and Windows. Keeping a modern industrial system running requires a constant stream of updates from the outside world. The result is that the industrial floor has become a hotbed of communications activity and is no longer isolated.

Furthermore, devices such as Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCS) were designed with a focus on reliability and safety, rather than security. This makes many of them, particularly older units, easy to exploit.

Since industrial networks are often required to run 24/7/365 and withstand hazardous environments, many security policies are never deployed; operational necessities and safety regulations overrule them. Even traditional IT security strategies, such as patching, are often impossible due to conflicting industry-specific regulations.

Add it up: vital networks with millions of hard-to-secure nodes, interconnected with enterprise networks and the internet, running 24/7/365 in heavily regulated environments with safety concerns, and the focus of the smartest security researchers and government warfare hacking programs in the world. It's a lot to contend with.

The Perfect Storm for the Attacker

Today, industrial security is clearly a game with the advantage going to the attacker: millions of decades-old systems that were never designed to be secure, increasing connectivity of SCADA and ICS, and a growing library of free tools and techniques to attack SCADA and ICS.

A successful attack on an industrial network could mean production losses, significant safety or environmental issues, or the theft of intellectual property, including information obtained from the enterprise network. Indeed, the industrial network could be the simplest backdoor to your enterprise network.

What Can be Done?

It's evident then that there's no simple solution to securing our critical infrastructure. The process is going to take a lot of time and effort, as well as some very careful planning. A combination of three strategies – policy and technologies designed for industrial security, best practices, and a focused effort – is effective in mitigating the risk of attacks on industrial systems.

Understand that Industrial Risks and Objectives Are Different

It is important to understand that the security risks and requirements in an ICS system can be considerably different from that of an IT system. This can result in very different strategies and technologies being needed to secure a manufacturing system. For example, in a typical IT security strategy the primary focus is on confidentiality and the necessary access controls needed to achieve that. On the other hand, security in ICS is primarily concerned with maintaining the integrity and availability of all system components. Therefore, technologies such as encryption may be viewed as counterproductive on the plant floor, as they can make troubleshooting network issues more complex, thus reducing overall systems availability.

This isn't to say that IT security solutions are bad for industrial systems. In fact, studies at major oil companies have shown that 90% of all IT security policies work well for industrial process control. The answer lies in clearly understanding how operational assumptions and needs differ from those of the IT world and then modifying the IT security practices to use them properly in our world. This takes close cooperation and teamwork from both IT and process control staffs, rather than blind dependence on IT security procedures.

As well, control systems have unusual operating systems and applications, such as VXWorks or RSLogix, that differ significantly from typical IT operating systems and applications. This means that many of the tried-and-true IT security solutions will not function correctly or, assuming they do run, will interfere with the process systems.

A good example of this was reported at an ISA Industrial Security Conference in 2004. When an emergency shutdown system on a boiler failed to operate correctly, investigators discovered that anti-virus software had been installed on the computer used to configure the safety system. This software blocked the proper operation of the safety system, putting the entire plant at risk. There was nothing wrong with the safety system or the anti-virus software on their own, but together they made a life-threatening combination.

Thus it is important to look at technology solutions that are designed specifically for the plant floor. These will be optimized to meet the performance, safety and security needs of real time systems.

Follow Proven Best Practices for ICS/SCADA Security

No matter what industry you are in, it is important that your controls and IT staff be familiar with industrial security standards, such as the ISA/IEC-62443 series.

To learn about industrial security, a good place to start is "7 Steps to ICS and SCADA Security." This was developed in partnership between Tofino Security and exida, and condenses the ISA security standards and best practice documents into an easy-to-follow process:

1. Assess existing systems: Understand risk and prioritize vulnerabilities
2. Document policies and procedures: Determine position regarding ICS and develop company-specific policies
3. Train personnel and contractors: Develop and institute policy awareness and training programs
4. Segment the control system network: Create distinct network segments and isolate critical parts of the system using a "zone and conduit" model
5. Control access to the system: Provide physical and logistical access controls to both your zones and equipment
6. Harden the components of the system: Lock down the functionality of components
7. Monitor and maintain the system: Update antivirus signatures, install patches, and monitor the system for suspicious activity

Focus on the Crown Jewels

Every control system has one or more asset(s) that would seriously impact production, safety, or the environment if successfully attacked. Your control engineers know what really matters to the operation. If those assets are aggressively protected, the chance of a truly serious cyber incident is massively reduced.

Another tool in securing an industrial control infrastructure that isn't to be overlooked is teamwork. IT and engineering teams need to work together within organizations, as all industry participants must work together to ensure that best practices are in place, and that innovative advances to security are developed and deployed. Whether your organization is a critical infrastructure provider or your enterprise has one or more industrial networks, securing these systems has never been more important.

Regardless of the pain points involved, investing in industrial network security is not only responsible, but also necessary for any mission critical application. The profitability, reliability and safety of both your company and customers depend on it.

Resources

ISA99/IEC62443 Standards
www.isa.org/isa99

#1 ICS and SCADA Security Myth: Protection by Air Gap
http://www.tofinosecurity.com/blog/1-ics-and-scada-security-myth-protection-air-gap

Air Gaps won't Stop Stuxnet's Children
http://www.tofinosecurity.com/blog/air-gaps-won%E2%80%99t-stop-stuxnet%E2%80%99s-children

Byres, Eric, "Using ISA/IEC 62433 Standards to Improve Control System Security"
http://web.tofinosecurity.com/download-the-white-paper-using-ansi-/-isa-99-standards-to-improve-control-system-security/

Byres, Eric and Cusimano, John "7 Steps to ICS and SCADA Security"
http://web.tofinosecurity.com/download-7-steps/

International Society of Automation
67 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
PHONE +1 919-549-8411
FAX +1 919-549-8288
EMAIL info@isa.org
www.isa.org

EP83-2556-1113