Bloomberg BNA

Privacy and Security Law Report®

Critical Infrastructure

Although reliable data on critical infrastructure attacks is limited, reports appear to support the thesis that there has been an evolution of the cyber-threat landscape, wherein actors aim not just to steal data, but to cause kinetic effect, however, thorough and detailed planning and training can make all the difference when responders are faced with an attack, the authors write.

Stay Out of the Dark!—Dealing With and Responding to Cyberattacks on Critical Infrastructure



By Paul Ferrillo, Randi Singer and Dan Scali

Cyberattacks on industrial control systems have gotten a great deal of publicity in recent weeks—from the dam in Westchester County, N.Y. to the Ukrainian electric grid by the BlackEnergy 3 malware variant.[1] Although reliable data on critical infrastructure attacks is limited, these reports—along with the 2010 Stuxnet malware that degraded Iran's nuclear program and a 2013 attack on a German steel mill—appear to support the thesis that there has been an evolution of the cyber-threat landscape, wherein actors aim not just to steal data, but to cause kinetic effect. Recent public reports indicate that the number of these attacks is rising, and information technology (IT) professionals in the energy, gas and utilities sectors are very concerned their organization may be next.[2]

While not all industrial control systems are critical infrastructure (consider a system that automates the process of milking cows) and not all critical infrastructure is industrial, there is considerable overlap. The term ''critical infrastructure'' applies not only to the electric grid, the energy sector, and the water and dams sector, but also to many other industrial-based activities, including the industrial-defense sector and the critical manufacturing sector (think trains, planes and automo-

[1] *See* John Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, iSight Partners Blog, (Jan. 7, 2016); David Bisson, *BlackEnergy Malware Caused Ukrainian Power Outage, Confirms Researchers*, The State of Security (Jan. 5, 2016).

[2] *See* Corey Bennett, *Critical infrastructure cyberattacks rising, says US official*, The Hill (Jan. 13, 2016); Jim Finkle, U.S. Sees 20% Jump in Cyberattacks on Critical Manufacturers, Claims Journal (Jan. 20, 2016); Eva Hanscom, Survey: Only 35% of Energy Orgs Are Capable of Tracking Threats to OT Networks, The State of Security (Feb 4, 2016).

biles).[3] Critical infrastructure can also include non-industrial sectors with primarily information-based assets, such as the financial services sector, which supplies the investment and working capital for most other sectors and businesses in the U.S.

Cybersecurity issues around critical infrastructure are obviously more complex than a simple IT network, but it need not be a frightening topic. Indeed, it is a topic that all should understand, especially given today's threat environment, which is filled with nation states, criminal and terrorist organizations with the capability and/or aspiration to conduct a broadly destructive attack, such as shutting down power supplies on the eve of a major holiday. These states and organizations have no ''rules of the road,'' just harm that they wish to inflict.

As a prelude to a series of seminars that we will shortly announce on cybersecurity in the critical infrastructure space, we provide this working paper on critical issues to consider when dealing with cybersecurity in this area. We further include advice relating to incident detection and response in order to mitigate the potential effects of a breach. Our goal is to move past the ''fear factor'' of an attack and towards a set of helpful principles that non-cybersecurity experts such as directors, officers and general counsel can consider as part of their cybersecurity risk program.

What's Different About Network Critical Infrastructure For the Industrial Sector?

Unlike the IT network of a retailer or a bank, the IT network and infrastructure of a utility, manufacturer or an oil and gas company may control manufacturing equipment, pumps, tanks, turbines, switches and relays, many of which include legacy systems built long before engineers contemplated remote access from the business network or the Internet. Even some of the more recent industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems were not necessarily developed with Internet connectivity and cybersecurity in mind. These issues are compounded because industrial systems typically have a long lifecycle, necessitating additional connectivity and the integration of commercial off-the-shelf software after the fact to plants, equipment and pipelines to allow them to be remotely-controlled from sometimes faraway locations. In an ever-increasing ''connected world'', these systems are now susceptible to the same security vulnerabilities that have plagued traditional IT networks for years.

The potential damage that can occur while the organization is in the process of containing an incident is significantly higher and potentially more serious in an industrial environment.

Today, control over factory equipment and machinery might be exercised from a company's IT server, which might sit one building over, or from a computer workstation on the factory floor. Digital intruders can attempt to access ICS and SCADA systems from other countries and sites much further away from the industrial plant or facility using a broad attack surface, ranging from malware introduced to the control center floor via removable media like USB, to a spearphishing attack that attempts either to obtain administrative credentials to ICS or to establish an initial foothold on the IT network that can be used to initiate a second-stage attack into more critical ICS networks.

While the actual impact of an attack on ICS will be highly dependent on the industrial process in question, as well as the specific organization under attack and the attacker's intentions, at least the following business impact scenarios should be considered as part of a robust enterprise risk management process:

- *Unsafe conditions*: An attacker who compromises a control system may be able to manipulate the process in a manner that causes unsafe conditions, particularly in cases where a Safety Instrumented System (SIS) is not in place or if the SIS itself is compromised or incorrectly implemented to mitigate a cyber-attack scenario.
- *Damage to equipment*: An attacker with access to a control system and knowledge of an industrial process can make changes that could result in physical damage. Examples could include tripping breakers or shedding load in the power grid or over-spinning a turbine until it fails.
- *Disruption of revenue stream or reliable operations*: In cases where operators have lost view or control of the industrial process, operations will be impaired or may need to be shut down altogether. If the data on the control room screen does not match what's going on in the real world, operators could make poor decisions that result in further confusion, disruption or consequence.
- *Regulatory fines*: Many industrial processes are regulated. Companies that rely on historical process data to demonstrate compliance to financial or environmental regulations could be required to pause operations if they cannot produce required data , or could face penalties if they later discover that they have been reporting incorrect data altered by an attacker.
- *Financial integrity & confidentiality*: Some industrial data may be used downstream in financial statements or may influence financial markets. Consider a scenario where pipeline meter data is used to calculate how much of a product was sold at a particular time. If this data is incorrect, it could impact financial statements. If this data is silently collected and monitored by an attacker, the attacker could use this information to make sure-to-win bets on energy prices.
- *Intellectual property loss*: Although the availability and integrity of ICS are typically of primary concern, ICS networks or engineering laptops may contain proprietary information, trade secret, confidential technical information, or other sensitive data.

[3] *See* U.S. Department of Homeland Security, ''Critical Infrastructure Sectors.''

  PVLR ISSN 1538-3423

Protecting the Industrial Control System Cybersecurity Network

Given the potential attack surface on an industrial control system computer network, no single solution can provide certainty that the either the network or the ICS will never be breached; rather, a holistic approach is necessary. Here are some of the methods that many companies use in the first instance to protect their network and ICS devices:

- *Reduce the attack surface/entry points to the ICS*: Savvy organizations establish ICS architectures that are capable of being defended. The more entry points to the ICS network, the more ability there is to find a way to enter the ICS and do harm. Consider whether or not ICS can be logically separated or isolated from the corporate network or the Internet through firewalls or other segmentation techniques to frustrate attackers.

- *Establish appropriate access controls*: Attackers frequently steal administrative credentials. Multifactor authentication is a technical control that frustrates the attacker's ability access the network with a stolen username/password alone and then move laterally to escalate administrative privileges to allow direct access to ICS. Another good practice is to establish separate authentication domains for the corporate network and the ICS network. Finally, any vendor access to your ICS network should be controlled, managed and audited as appropriate.[4]

- *Deliver employee training and awareness programs*: As we now know, the Ukraine power grid attack may have started from a socially-engineered spearphishing attack which carried with it a macro containing malware. Employees need to understand that ''clicking on the link'' could have significant consequences, including but not limited to delivering targeted malware or ransomware.[5] There are also other hardware techniques to isolate, sandbox or block suspicious e-mails that have potential deleterious attachments.

- *Regular patching*: Finally, although patching is much more difficult in an ICS environment, prepared organizations do establish some reasonable strategy and interval (for example, quarterly) for patching servers, computer workstations on the plant floor, and engineering laptops to reduce the risk that a known vulnerability creates a vector into your ICS network. Application whitelisting technology can help mitigate the risks of missing patches between regularly scheduled maintenance and patching windows. One recent reported noted that ''through the end of 2014, more than 85 percent of all ICS vulnerabilities have been disclosed since 2011—the year following the discovery of Stuxnet. The Open Source Vulnerability database currently tracks a total of 1069 ICS vulnerabilities, with 98 added so far in 2015 (as of 5/22/15). . . . Based on first half data, the total number of vulnerabilities targeting ICS should exceed 150 for the fifth straight year.''[6] These vulnerabilities are increasingly being weaponized by attackers, as evidenced by analysis of the Havex and BlackEnergy3 malware families.

Incident Detection and Incident Response for Critical Infrastructure

Incident detection and incident response programs for organizations with critical ICS must also consider technical scenarios that extend beyond a typical IT environment. Among the technical challenges associated with incident detection and response in ICS are:

1. *Cultural resistance*: In some organizations, there is a difference in philosophy between IT and operations technology (OT) staff. In many ICS environments, the idea is ''If it works, don't touch it.'' Unfortunately, due to the operational executive's desire to generally leave well enough alone, many industrial facilities do not have a mature cybersecurity strategy or incident detection capabilities. One expert recently noted that, ''The plant manager will not let you mess around with all of those digital systems and reboot. . . Incident response is very difficult and very challenging in a cyber-physical environment. Nobody has procedures for it.''[7]

2. *Heterogeneous environment*: Unlike IT environments where Microsoft Windows platforms dominate, along with a few others common operating systems like Mac OS and Unix or Linux variants, small ICS environments can have dozens of embedded platforms and ICS software packages from a variety of vendors. ICS systems also use different communication protocols than are used in the IT space. Performing accurate incident detection or forensics requires detailed knowledge of all of the technology deployed in the ICS environment.

3. *Validation of software placed on ICS devices*: Technical approaches that require new software (i.e. agents) be introduced into ICS will typically require validation by the ICS software or hardware vendor (for example, Siemens AG, General Electric Co., Honeywell International Inc., ABB Ltd., Schneider Electric SE, Yokogawa Electric Corp.) which takes time in the best case scenario, but may be impossible in the worst case. Some ven-

[4] See Daryk Rowland, *Combating cyber risk in the supply chain*, SC Magazine (Nov. 14, 2014). The critical vendor issue is well known both in the retail community and in the critical infrastructure community. This article further notes that ''the recent Dragonfly/Energetic Bear hack of U.S. and European energy companies began with a spearphishing campaign against senior employees in energy sector companies. Those senior employees took the bait and enabled the hackers to compromise legitimate software used by industrial control system (ICS) manufacturers, inserting malware into software updates sent from the ICS manufacturers to their clients.''

[5] *See* Darlene Storm, No, Israel's power grid wasn't hacked, but ransomware hit Israel's Electric Authority, Computer World (Jan. 27, 2016)

[6] *See* SCADAhacker Cybersecurity for Critical Infrastructure.

[7] *See* Kelly Jackson Higgins, *How Incident Response Fails In Industrial Control System Networks* Information Week (Jan. 28, 2016).

dors will even void the ICS warranty if unauthorized security software is installed. It can be challenging to place security software such as anti-virus, anti-malware or other investigative technology in the ICS environment.

4. *Notification by physical consequence*: In cases where data is stolen from an organization, the victim is typically notified by law enforcement or another external party who discovers a copy of the data on the Internet, underground forum or an attacker's server. The victim then starts an investigation into how the data was obtained and exfiltrated. In the ICS world, the first indication of compromise could be equipment failure, damage or some other physical consequence.

Incident Detection

Targeted ICS incidents, as we understand them today, are by nature low frequency, high-impact events. Perhaps the most important indicator of a compromise is when things look and feel abnormal. It is important for both system operator and IT professional to understand what the normal state of their facility is so that anomalies become readily apparent.

Strategies that work for incident detection in ICS environments typically focus on deploying network-level technology and collecting logs generated by ICS technologies. For example:

- Deploying network sensors to collect and monitor all traffic;
- Deploying intrusion detection systems (IDS) between the Corporate IT and ICS networks;
- Collecting log files from all deployed ICS technology and any cyber security technology in place such as anti-virus, firewalls, IDS, etc.; and
- Deploying security software on ICS hosts after performing appropriate validation.

If your organization has a Security Operations Center (SOC), the technical information collected from the ICS should be routed to the security experts there so that they have visibility into ICS and can continually monitor and respond to potential incidents quickly.

One final note about incident detection. We would urge those in charge of critical infrastructure networks to perform regular vulnerability and red/blue team assessments to determine if, when and how an attack could occur. Any assessments that might harden the defense posture of an ICS system should be considered. Given the potential operational risks associated with security testing, organizations should ensure that the assessment team has experience in ICS environments and should establish acceptable rules of engagement prior to the assessment.

Incident Response Tactics

In many respects, an incident response plan for critical infrastructure follows an accepted course: (a) have a plan to respond to various identifiable incidents that could arise in an ICS environment; (b) have a team to investigate; and (c) deal with the incident and practice those plans quarterly to make sure that every person on the team knows his or her role.

But the potential damage that can occur while the organization is in the process of containing an incident is significantly higher and potentially more serious in an industrial environment. For instance, an organization might choose to contain an attacker in a retail environment by disabling compromised accounts. We don't want to understate the potential loss of data, intellectual property, or revenue in that scenario, but it is of a different order of magnitude when an industrial control system is compromised and risks include damage to equipment or other physical assets, disruption of critical infrastructure such as water or power, or even safety concerns including the potential for loss of life. An industrial control system needs containment procedures that include a procedure for placing the industrial process into a safe state.

Prepared organizations establish detailed technical incident response procedures well before an incident occurs. They start by establishing cybersecurity points of contact at every industrial facility and agreeing upon roles, responsibilities and handoffs between IT Security and Operations personnel. Next, they develop playbooks for common scenarios such as containing commodity malware on ICS. They pre-deploy tools and technologies that will reduce incident response cycle time and train points of contact on how to use them. They upgrade their infrastructure to be resilient and recoverable—taking regular and complete backups of the environment and establishing redundant architectures for failover in the event of impaired operations due to a cyber security incident. They also periodically stress-test their incident response procedures with tabletop exercises that bring together technical personnel from IT and OT along with executives and role-play various incident response scenarios.

The Ukrainian power grid attack was a stark reminder that critical infrastructure attacks must be considered a constant threat to both our physical and business environment. With the trickle-down theory of cybercrime, more and more attackers will have tools that could one day turn of the lights. Through proper architecture networks and by segmentation and micro-segmentation solutions, attacks can hopefully be lessened and contained before they spread throughout an ICS network.

And, as always, thorough and detailed planning and training can make all the difference when responders are faced with an attack.

  PVLR ISSN 1538-3423

PVLR ISSN 1538-3423