Sully Station Solutions

Securing ICS Endpoints

Pressure is mounting for operations technology (OT) teams to lock down their industrial control systems (ICSs) against cyberthreats. International events like the Stuxnet attack against Iran's nuclear program and the BlackEnergy attack against Ukraine's electric grid have focused attention on the vulnerability of critical infrastructure control systems. Behind the headlines is the sobering reality that securing ICS equipment in the whack-a-mole world of rapidly evolving cyberthreats is a costly and challenging endeavor.

Historically, ICS security has relied on a combination of firewalls and the so-called air gap. Firewalls provide a perimeter protection, denying bad actors access to the network. The air gap, referring to the lack of connectivity for an ICS device, limits the ability of a cyber intruder to do mischief should they defeat the firewall. This two-pronged firewall and air gap security strategy has proven to be inadequate and the emphasis for ICS protection has now expanded to include securing the endpoints.

Broadly speaking, endpoints are defined as any devices connected to the network. From the perspective of the information layers of the network, endpoint devices include desktops, laptops, cellphones, printers and routers. When the hunt for endpoints opens to the operational layers, the number and types of devices grows considerably. Examples of OT endpoints include programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, safety instrumented systems (SISs), remote terminal units (RTUs), intelligent electronic devices (IEDs), and human machine interfaces (HMI).

There are, of course, numerous challenges that arise in the operational layers of the network. These systems can be highly complex. The control systems are frequently proprietary, and in any but the smallest plants are likely to be from multiple vendors. OT endpoints are also often legacy devices, designed long before cyberthreats were a known issue, and never intended to be interconnected as they are today.

As the OT and IT worlds converge, threats to the ICS network are looking more and more like threats to the information network, with viruses, phishing exploits, malware and even ransomware figuring heavily. Hackers are demonstrating a good deal of sophistication in their approach, along with a willingness to work multilayered exploits over an extended period to accomplish their goals.

Consider the 2015 Ukraine power grid attack which was executed in two distinct phases over six months or more. The first phase began with a targeted spear phishing attack in which IT staff at multiple power distribution companies received official looking e-mails with a Microsoft Word document attachment. The Word documents were infected with the BlackEnergy trojan, a bit of malware that traces back to

2007. Recipients were prompted to run a macro to open the attachments. The IT staffers complied and turned BlackEnergy loose, giving the hackers broad access across the information layer of Ukraine's power infrastructure.

Having gained access to the network, the hackers moved into phase two of the attack and sought to penetrate the firewalled SCADA network. Methodically combing through the servers and devices to which they did have access, the hackers eventually were able to harvest account information, including passwords, for the VPN accounts used by staff to access the SCADA network and the grid's substation controllers. Beyond the firewall there was no endpoint protection. The hackers were able to replace the firmware on serial-to-Ethernet converters at more than a dozen substations with their own code.

On December 23, 2015 the hackers began systematically opening circuit breakers across the grid, one-by-one bringing the substations offline, and turning off the lights for hundreds of thousands of customers. With the rewritten firmware in place, power company staff were unable to close the circuit breakers and restore power. Although power was restored in just six hours, the damage was lasting. Operations were hampered for months after the attack, during which time workers were forced to operate the hacked breakers manually.

Although the threats and challenges of ICS security are daunting, there is some good news. Many traditional industrial security frameworks and standards are applicable to ICS, and a growing body of work dedicated to ICS security exists to help organizations put improved process in place. Some of the most useful and important of these frameworks and standards are NIST SP800-82, ANSI/ISA99 IEC-62443, the NIST Cyber Security Framework, NERC CIP and IEC 61850.

The CIS Critical Security Controls is a set of 20 security measures developed by leading international security organizations including the United States Department of Defense, United Kingdom's Centre for the Protection of National Infrastructure (CPNI), the United States National Security Agency (NSA), and the SANS Institute. Although designed for IT networks with Internet exposure, many ICS professionals are finding the controls very useful for OT application as well.

Two great strengths of the controls are their relative simplicity and their effectiveness. It has been estimated that simply by implementing the first five controls an organization can reduce its exposure by 85%. For more information on the CIS Critical Security Controls and other cybersecurity best practices see the Center for Internet Security website at www.cisecurity.org.

It is urgent that those with OT infrastructure responsibility take steps to secure the endpoints of their ICS systems. The following high-level actions may be helpful in establishing the scope of a security improvement initiative:

- Establish a base and know what you have. Maintain an accurate, living inventory of all hardware and software.
- Secure all network and Internet connections to the control systems, being sure to include wireless and remote access. Minimize connectivity whenever possible and tightly control authorization for connectivity.
- Understand and document the configurations for your OT network. Secure and harden the configurations of endpoints and control systems.

- Put in place continuous, real time monitoring of all endpoint and control systems and investigate any changes or unusual access patterns.
- Develop and improve security policies and procedures. Train all personnel on the policies, procedures and cybersecurity best practices.