SIEMENS
Ingenuity for life

White Paper

Safeguarding operational technology against cyber threats in a NERC CIP environment

Anomaly-based Intrusion Detection System provides early warning of cyber threats

Cybersecurity breaches have made headlines for years as their impacts on data privacy have come to light. In the past, cybersecurity failures typically have involved the penetration of Information Technology (IT) networks and the theft of intellectual property, government secrets or consumers' personally identifiable information.

Recent headlines, however, reflect a new, potentially ominous twist to cybersecurity breaches. Hackers are now targeting Industrial Control Systems (ICSs) based on Operational Technologies (OT) and OT-based networks.

Operators across numerous industry verticals migrate their ICS networks from serial communications to Internet Protocol (IP)-based communications. This process allows for integration of OT and IT networks and significant enhancements to remote monitoring, remote control, performance, reliability and other operational advantages.

In an increasingly networked world, however, these advantages come with distinct threats and risks to ICSs that must be addressed and managed. This is particularly true of ICSs at the heart of critical infrastructure that provides the basic services supporting civil society, such as the power grid and Bulk Electric System (BES), Oil & Gas (O&G) and Intelligent Transportation Systems (ITS).

Due to the physical realm in which ICSs and OT-based networks operate, a cybersecurity breach in this domain also produces the very real possibility of life-threatening physical damage. Put simply, the breach of ICS and OT networks, especially those involved in critical infrastructure, produce a fundamental, real-world risk to human safety and operational continuity as well as our economic and national security.

Imagine a hacking breach that deliberately blacks out a city or leads to a transmission substation transformer explosion. Protecting society and national interests against such scenarios has become a legal, business and moral imperative. Cybersecurity breaches may be caused by hactivists, insiders, nation/states or criminal organizations, non-targeted malware, or may even stem from the unintended consequences of an employee who makes a simple mistake. Therefore, a sound defensive strategy that employs multiple measures, including an Intrusion Detection System (IDS), is required.

Recent headlines reflect trend

Unfortunately, the actual breaches of ICSs and OT-based networks has been well established by events abroad as well as in the United States, as reflected by recent headlines.

"Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid"
Wired, 3 March 2016

"Cyberattack Targets Safety System at Saudi Aramco"
Foreign Policy, 21 December 2017

"Advanced Persistent Threat Activity Targeting [U.S.] Energy and Other Critical Infrastructure Sectors" United States Computer Emergency Readiness Team (US-CERT), 15 March 2018

"Industrial Control Systems: The holy grail of cyberwar"
The Christian Science Monitor, 24 March 2017

Headlines, of course, serve to inform the public, policy makers and stakeholders of significant events and threats that require counter-measures. In this case, policy makers have already determined that electric power utilities and other critical infrastructure sectors and their cybersecurity managers have distinct legal and ethical responsibilities to protect their operations from cyber attacks.

Mandated reliability standards

The organization known as the North American Electric Reliability Corporation (NERC) has long pursued standards for electric grid reliability. In 2006, NERC acted under authority granted it by the Federal Energy Regulatory Commission (FERC) to address Critical Infrastructure Protection (CIP) to protect the assets of the bulk power grid. Over the past dozen years, NERC CIP has required the power industry to achieve effective cybersecurity and pass audits on compliance with specific cybersecurity standards and measures.

Two sections of NERC CIP are pertinent to the protection of ICSs: CIP-005-5 Cyber Security – electronic security perimeters, and CIP-007-6 Cyber Security – System Security Management.

The first measure requires power utilities "to manage electronic access to Bulk Electric System (BES) Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES."

The second measure mandates that power utilities "manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."

Both measures are aimed, in general, at the protection of ICSs, in which "misoperation or instability" could interrupt transmission grid operations and lead to real-world physical damage, with consequences for human safety. Both measures specifically require that power utilities implement an IDS to sense and report when their electronic perimeters have been breached. The implementation of an effective IDS adds another layer to the Defense in Depth strategy for cybersecurity. However, all IDSs are not equally effective. Traditional, so-called "signature-based" IDSs have significant drawbacks that make them less effective than "anomaly-based" IDSs.

Compliance vs. overall security

As important as compliance with NERC CIP's cybersecurity mandates is, however, the electric power industry and other critical infrastructure sectors actively debate whether compliance per se – with its emphasis on checklist mandates – equates to effective, overall security. This practical issue, often referred to as "security versus compliance," often focuses on the wisdom of adopting cybersecurity measures that achieve optimal cybersecurity and reach beyond minimum mandated measures. This perspective recognizes that operational continuity is critical to public, shareholder and stakeholder trust in an investor-owned utility's ability to protect critical infrastructure. An effective overall security strategy is called Defense in Depth and we will discuss it below.

Constant ubiquitous threats

Though power utilities interpret cyber threats and their resulting responsibilities differently, the history of cyber attacks underscores one inescapable truth: modern cyber attacks on IT and OT networks are constant and ubiquitous. Penetration of a power utility's IT and OT networks is no longer a question of "if," but "when." British journalist Misha Glenny, renowned for his cybersecurity work, has commented: "There are two types of companies in the world: those that know they've been hacked, and those that don't know."

Managers with cybersecurity responsibilities must acknowledge that every system has vulnerabilities and every system can be penetrated. An IDS solution plays an important part of the overall Defense in Depth strategy in helping to detect, identify and notify personnel of potential risks and intrusion throughout the network. Having this detailed awareness of assets, resources, and traffic patterns on the operators OT network allows them to help mitigate any potential harm as part of the overall Defense in Depth strategy.

To understand how an anomaly-based IDS represents an effective role in the Defense in Depth strategy from the OT and ICS perimeter, it is useful to understand the key differences between IT and OT networks.

Crucial differences between IT and OT networks

IT networks are designed, built and operated by IT professionals with computer science backgrounds, whereas OT professionals typically possess backgrounds in process and industrial engineering. IT's risk management responsibilities focus on data confidentiality and integrity, whereas OT risk focus is on human safety and process continuity. Too often in the past, these two domains were mutually exclusive. Today, both the IT and OT professional must integrate their expertise to defeat threats to both domains.

Developing a mutual understanding of the IT and OT concerns will help these professionals to work together to identify and address cyber vulnerabilities. Such cooperation is critical to business continuity as both IT and OT have regulatory mandates for cyber security.

The use of the Ethernet protocol to connect ICS and Supervisory Control and Data Acquisition (SCADA) networks to enterprise IT networks for monitoring and control of physical assets via Human-Machine Interfaces (HMI) such as laptops and tablets has led to the exposure of the vulnerabilities discussed in this paper. Legacy OT systems, often proprietary in nature, may rely on devices and software built without cybersecurity controls. The

Figure 1. Defense in Depth for ICS networks and the OT systems those networks support.

integration of OT systems with IT systems, involving OT, IT and OEM teams, may well result in ambiguity over cybersecurity governance. And the advent of open-source operating systems and software, as well as an Industrial Internet of Things (IIoT) and the proliferation of peripheral devices, only exacerbates existing vulnerabilities.

IT networks rely on standard communication protocols, whereas OT networks often use a variety of legacy and proprietary protocols that are vulnerable to hackers.

IT system security typically is an integral part of the development process. In contrast, OT-related devices and systems often are retrofitted with security solutions, if at all.

Another major difference between IT and OT networks is that OT often runs 24/7 with 99.9% uptime, versus IT networks that operate on a "best effort" basis that can endure downtime outside of standard business hours.

Therefore, solutions to secure operational networks must require minimal maintenance (zero downtime), a minimal footprint (simple operation) and be non-intrusive (no degrading of ongoing operations).

Defense in Depth

The most effective strategy to achieve cybersecurity is an approach commonly referred to as Defense in Depth. (See Figure 1) This layered approach is designed to implement measures at the electronic perimeter, as well as at the network, device and software application levels. Defense in Depth requires an electric utility to identify its assets, protect its assets, detect intrusions, remediate problems, and recover normal operations.

Enacting and supporting this strategy, in turn, requires embracing the three pillars of security: people, processes and technology. No technology provides complete security. Proper training of employees and establishment of well-considered processes are required to support technological solutions.

Indeed, guidance on NERC CIP compliance relies on the layered Defense in Depth concept because it avoids incomplete point solutions that carry the risk of a single point of failure. Yet the success of a Defense in Depth strategy relies on the rigorous application of best practices at every level – including people, processes and technology – to achieve the most effective security stance.

Shortcomings of signature-based IDSs

As discussed, Defense in Depth measures are only as effective as the rigor applied to the people, processes and technologies that support them. That is why an effective IDS, policing the ICS's electronic perimeter, can play a critical role in alerting IT and OT personnel to a cyber attack.

One of the most insidious cyber threats to ICSs is a so-called "low-and-slow" attack, also referred to as an Advanced Persistent Threat (APT). A sophisticated APT can execute a series of events without disrupting ICS operations and operate under the radar of conventional IT cyber security tools, yet the APT can serve as the eyes and ears of a hacker who wants to understand system vulnerabilities before attacking them.

APTs underscore the vulnerabilities left unmonitored by signature-based IDSs, firewalls and other conventional IT tools. Signature-based IDSs rely on a database of malware "signatures" or characteristics that are sought by the IDS. Sophisticated attackers simply use alternative methods to evade signature-based IDSs.

Advantages of an anomaly-based IDS

To increase the efficacy of intrusion detection for ICS and OT networks, Siemens RUGGEDCOM and Secure-NOKs non-intrusive, anomaly-based IDS – the SNOK™ – which is hosted on the Siemens RUGGEDCOM RX1500 Multi-Service Platforms, designed and built for reliability in harsh industrial environments.

SNOK™ software monitors network traffic and detects anomalies to that traffic's baseline characteristics. SNOK™ assesses the risk of intrusive anomalies and responds accordingly, providing early, actionable alerts to inform an incident response by personnel with cybersecurity governance responsibilities.

Anomaly detection is based on the deployment of SNOK™ software agents deep in an ICS network as well as at end points to collect data for a baseline of normal network behavior.

SNOK™ analyzers, hosted by Siemens RUGGEDCOM Multi-Service Platforms, can then identify anomalous behavior such as APT or other cyber threats within an ICS network or at its end points. SNOK™ then alerts network operators to the attack and provides sufficient data to inform decisions on an effective response.

Installation of SNOK™ is plug-and-play. The IDS solution runs on the RX1500's Application Processing Engine (APE), an x86-based computer designed for a single-line module slot in the RX1500 appliance. Hardening unnecessary ports will also help to reduce potential attack vectors.

Deployment of SNOK™ adds a critical element in a Defense in Depth strategy aimed not only at compliance with NERC CIP mandates but also at more rigorous efforts to provide comprehensive cybersecurity to ICSs and OT networks in the BES.

SNOK™ in-depth

The SNOK™ IDS is effective because it monitors internal and external communications of an industrial controls system. It detects viruses, malware and sophisticated attacks – the APTs or Advanced Persistent Threats – including those that are undetectable by conventional security tools. It provides transparency that adapts to emerging cyber threats as it monitors network traffic behavior for anomalies. It uses statistical and behavior-based algorithms rather than a predetermined set of threat signatures. Therefore, it detects Zero Day vulnerabilities – i.e., attacks that have never been seen before. And, perhaps most importantly, SNOK™ is specifically designed to protect ICSs and runs on RUGGEDCOM Multi-Service Platforms designed by Siemens, whose heritage is based on a focus on industrial processes and systems.

SNOK™ establishes the characteristics of network baseline behavior over a short, set learning period. Once the SNOK™ IDS is activated, it reports to system operators when it detects deviations from baseline network behavior, including new devices on the network, new ports and new or changed communication patterns. SNOK™'s Monitoring and Detection modules collect and analyze cybersecurity data, while its Risk Assessment module determines the criticality of detected intrusions and events, and the Response module assists in responding to a cyber attack. A valuable bonus of using real time anomaly detection is identification of hardware and software malfunction and reconfiguration unrelated to cyber attacks.

By combining statistical and behaviour analysis SNOK™ minimizes false positives. Its light footprint does not slow network traffic or use excessive central processing unit (CPU) resources. SNOK™ does not stop network traffic nor isolate files, thereby eliminating the risk of unintended consequences. Its graphical user interface (GUI) is easy to navigate to find relevant information about detected threats. By aggregating the data from the various SNOK agents deployed in the network into a single user interface, the Secure-NOK detection server provides a single interface of any anomalies detected on the networks for an easy to read and maintain solution.

Let's talk

Power utilities have legal and ethical responsibility for human safety, operational continuity, and safeguarding critical infrastructure. Your power utility's approach to ICS and OT network security may require review and upgrading, in light of the rapid rise in threats to operational networks. Perhaps your utility already relies on RUGGEDCOM multi-service platforms and SNOK™ can be easily deployed to provide a more effective IDS in your current Defense in Depth strategy.

Contact us for a conversation on how to protect your brand, your operational continuity, and the safety of your employees and the public by adding an effective, anomaly-based IDS to your operational networks.

Jeff Foley
Business Development Manager – RUGGEDSOLUTIONS
Siemens Industry
Mobile: (954) 296-5648
Email: jeff.foley@siemens.com

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact
our Customer Support Center.
Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/ruggedcom

Order No: RCWP-SNKNC-0818
Printed in U.S.A.