Partner With The SUPPLY CHAIN

Stefan Woronka, Director
Industrial Security Services
Siemens AG, siemens.com

IN EARLY 2018, Siemens founded the Charter of Trust to establish cybersecurity as a major factor in the transformation of manufacturing and process industries to digital enterprises. The Charter follows three goals:

- protect the data of individuals and companies
- prevent damage to people, companies, and infrastructures
- establish a reliable foundation on which confidence in a networked, digital world can take root and grow.

Based on these goals, Siemens and 15 signing partners have agreed upon 10 key principles, with the following four directly related to industrial environments.

CYBER, IT, SECURITY OWNERSHIP

"To anchor responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs (chief information security officers) and establishing clear measures, targets, and the right mindset throughout organizations, *i.e.,* it is everyone's task."

What does that mean?

People, organizations, and entire societies must rely on digital technologies and will support this transformation only if data and networks are secure and can be trusted.

This requires clear responsibilities at the highest levels of companies and governments. For those in manufacturing or process industries, it means establishment of clear responsibilities and targets for cybersecurity is of importance for office-related business IT and, foremost, industrial OT that controls manufacturing processes and technology. Bringing together what has been kept separated for years and sharing goals, ideas, and measures will help increase overall company security.

SECURITY BY DEFAULT

"To adopt the highest appropriate level of security and data protection and ensure it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures, and business models."

What does that mean?

Only if security requirements are already taken into account in the early phase of product development, especially the design phase, can the highest appropriate level of security be offered proactively. The same applies to all other steps in the value chain—from functionalities and default security-configuration settings to manufacturing processes, technologies used, and operational processes, as well as underlying architectures and business models.

Siemens has implemented a holistic cybersecurity concept for its industrial divisions to raise the level of security within the whole supply chain. From the start of R&D for new or existing products and on through production, supplier integration, implementation with end customers, and after-sale support, cybersecurity is considered in every step of the process.

USER CENTRICITY

"To serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services, as well as guidance, based on the customer's cybersecurity needs, impacts, and risks."

What does that mean?

Companies are exposed to the same risks as any other user of IT and the internet. In addition, companies

are the targets of attacks that do not occur in the private environment. That's why companies need products, systems, and services that meet their security needs over an appropriate lifecycle.

The holistic approach of the industry-specific concept is based on state-of-the-art technologies, as well as the applicable security rules and standards. Siemens proactively offers security solutions throughout the industrial lifecycle. Threats and malware are detected at an early stage, vulnerabilities analyzed in detail, and appropriate comprehensive security measures initiated.

Continuous monitoring provides plant operators with the greatest possible transparency regarding the security of their industrial facility and optimal investment protection at all times.

TRANSPARENCY, RESPONSE

"To participate in an industrial cybersecurity network to share new insights, information on incidents, *et. al.,* report incidents beyond today's practice, which focuses on critical infrastructure."

What does that mean?

The digital world is all about one thing: speed. When cyberattacks occur, you need an immediate, coordinated, and goal-oriented response. That's why it's critical for companies to work together and create an industrial cybersecurity network to instantly share new insights and information about attacks and incidents.

Siemens is a member of FIRST (Forum of Incident Response and Security Teams, Morrisville, NC, first.org), the umbrella organization for all CERTS (cyber emergency response teams), and has established direct relationships with several national CERT organizations worldwide. As a FIRST member, we wage a determined battle against approximately 1,000 cyber-attacks every month, gathering cyber-threat intelligence and sharing it with FIRST members and other partners.

+

DETECT INDUSTRIAL ANOMALIES

Siemens has released a new portfolio element for its industrial customers: Industrial Anomaly Detection. This solution complements the existing Industrial Security Services portfolio with new capabilities to gain transparency and visibility into an Industrial Automation and Control System.

Industrial Anomaly Detection consists of at least one sensor installed on a Siemens IPC 427e to sniff and dissect network traffic, and a center installed on a second Siemens IPC 427e to perform analysis and visualization using a graphical user interface (GUI). Switches connect the systems in the plant network topology. These switches often make it possible to mirror the entire data traffic through a SPAN port. The anomaly sensors, when connected to the SPAN ports, make it possible to perform data evaluation. With this approach, the monitored automation-and-control system is not affected and can continue to operate.

How does Industrial Anomaly Detection work? Based on the monitored data, the center creates an inventory of all existing assets in the system. A communication overview of the shop floor environment is then created, based on the telegrams. This results in a security baseline.

The asset inventory contains information such as vendor, device type, hardware and firmware version, software version, and serial number. The communication matrix shows which devices talk to each other and what kind of traffic is sent. Included is direction of communication and the protocol used.

The baseline is used to detect any deviations and subsequently raise an alarm. As a result, changes in communication (new devices, new communication paths, changes in traffic) are identified and raised. In addition, anything that affects system components is detected. These factors include a PLC start or stop, configuration change, and/or download of a new configuration or firmware.

Designed for Siemens and multivendor environments, Industrial Anomaly Detection is bundled into three packages (small, medium, large), making it easy to match package size with plant size.

Siemens has formed partnerships for developing industrial IT, standards, and collaborations with universities, business partners, customers, startups, and respected research institutes to further advance cybersecurity innovations. This includes contributing to ISA 99/IEC 62443, the leading standard of cybersecurity for industrial-automation-and-control systems. We also support customers, partners, and researchers whenever there are vulnerabilities within our products.

To protect plants, systems, machines, and networks from cyberthreats, it is necessary to implement and continuously maintain a holistic, state-of-the-art industrial-security concept. 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 internet if, and to the extent, those connections are necessary and only when appropriate security measures are in place. **EP**