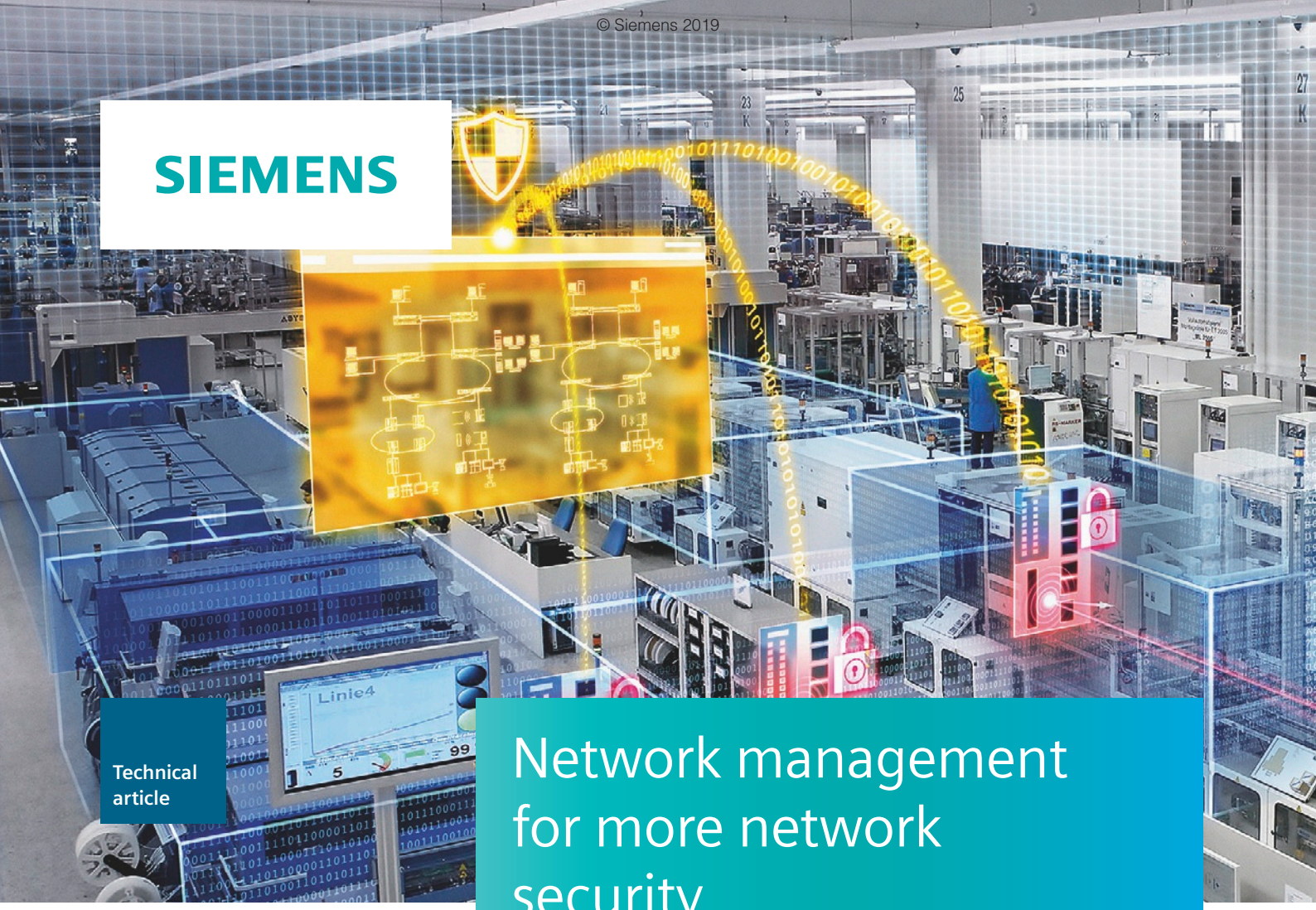
SIEMENS



Technical article

Network management for more network security

Experience new ways of Industrial Security

Each security update is followed by new software vulnerabilities. Each protective mechanism by new attack vectors. This race has existed since the first appearance of a malware, and often the question is raised how an effective protection against the "unknown" can even be established. The answer can be found in the seamless interaction of several measures.

"Oops, your files have been encrypted!" – just a few years ago, one of the most famous malicious software worldwide made headlines with these words. Although neither the nature of the threat nor the technology used was characterized by great innovation, this malware achieved notoriety within a few days. Other well-known worms and viruses, such as Blaster, Sasser, or MyDoom, have already caused billions in damage over 15 years ago. Even Stuxnet, which kept operators of industrial installations on their toes because of its primary infection target became widely known. If you ask for famous malware today, many will probably recall the ransomware WannaCry. And this despite the fact that other worms either infected significantly more devices, caused greater economic damage, or employed even more sophisticated attack vectors. So, what was different? What helped WannaCry reach such prominence?

The defense in depth concept from Siemens offers comprehensive and effective protection against cyberthreats through various measures and mechanisms on multiple levels.

The answer to this question is quite complex. Crucial aspects were probably the rapid spreading and the type of devices infected. Within just a few hours, the ransomware spread across many computer systems in over 150 countries and encrypted the data stored on them. As not only private users and industrial companies were affected, but also public facilities such as hospitals or display boards in long-distance traffic, this incident unforgivingly exposed the vulnerability of our networked infrastructure. And although its spreading could be stopped relatively quickly, the negative connotation of those easily attacked systems and fears of new, perhaps even more effective, threats remained. But how can one effectively protect oneself against new, still unknown attacks?

Defense in depth – the foundation of an effective protection concept

Certainly, the most important step is to also address cybersecurity in industrial environments and to lose the fear of the "unknown." Thus, with professional support, an effective approach to more security can be established via so-called defense in depth. The principle behind it states that a wide range of different, independently working protective measures should be utilized to fend off a possible attack. With these, the attack is either to be stopped immediately or enough time should be gained collaboratively for appropriate countermeasures to be taken.

If also the automation components already sufficiently account for security aspects during their development phase, the concept can be anchored to a solid foundation. For this reason, the secure product life cycle in accordance with IEC 62443 is a fixed and certified component of the development process at Siemens Digital Industries. Since these process requirements and the concept of defense in depth – including prevalent mechanisms such as firewalls or further applications for attack detection – are already extensively described in the IEC 62443 standard or relevant literature, a detailed listing of these possibilities will be omitted at this point. The focus is instead placed on a scenario that shows which additional means can be used to protect production systems from new, previously unknown attack waves.

Although it can be speculated about all possible attack vectors and exploitable vulnerabilities today, some aspects of the chronological sequence of most attack waves continue to follow a familiar pattern. After the first infections have surprisingly struck, security experts worldwide become active. They begin to analyze the behavior and functioning of the malware as quickly as possible and initiate effective countermeasures. These range from, for example, initial recommendations for containing infected systems to new signatures for virus scanners or deep packet inspection firewalls to security updates for affected user programs.

Transparency and detailed information about the participants of a network are key factors in order to deploy security measures effectively and targeted.

However, as those specific countermeasures can only be rolled out after the malware has been detected and analyzed, the existing defense in depth measures continue to be relied on to ward off the initial infection. Before the attack pattern changes, as is common with so-called polymorphic attacks, or if, despite preventive protective mechanisms, an infection of individual systems has occurred, local propagation paths must be suppressed, and vulnerabilities exploited be permanently closed. In both instances, the use of a centralized Network Management System (NMS) exhibits clear advantages and helps to achieve the required transparency in the network.

Identify vulnerabilities – control the communication

After the first analyses by the security experts, well-known product manufacturers such as Siemens publish corresponding security alerts that inform whether products are affected by a vulnerability. As the first step, with the aid of the network management system, the assets – the components and participants of the network – can be listed with little effort and compared with the information of the security alerts. In the case of possible matches, further containment measures can now be taken in the production network until security updates by the product suppliers for the affected components become ultimately available.

The identified, vulnerable components must be especially protected from the threat by limiting the spreading of the malicious software over open ports of various protocols and network services in the local network. Consequently, the next step would be to block those protocols and network services via firewalls. While this procedure can be implemented relatively effortlessly at the zone transition from the office to the production environment, the cell firewalls already present a certain complexity. The additional rules must be applied to many firewalls and may only be activated temporarily or not at all for some cells so as not to influence the production process. If, as a further measure within an emergency policy, secondary systems such as archiving servers are to be temporarily disconnected completely from the plant network by deactivating entire interfaces in addition to the ports at the switch or router, the extent of the complexity quickly becomes apparent. Combining firewall and network management into a single system then offers the user simple and flexible options for limiting the communication relationships between the network cells and for keeping the production running, e.g., with limited diagnostic or access options.

With a cell protection concept and SCALANCE S Industrial Security Appliances, individual production areas can be effectively separated from the plant network and protected.

Security updates – a must for long-term protection

For a sustainable protection, the vulnerable components must ultimately be permanently protected from this specific threat. To do so, the software and firmware updates provided by the manufacturers must be installed in a timely manner. Depending on the network and system architecture, this can already be done during operation or a maintenance cycle of the production. In both cases, this can be associated with enormous effort. For computer systems in closed domains, therefore, a central variant via so-called update servers has established itself. To take advantage of these qualities with industrial infrastructure components such as switches, routers or firewalls, a central network management is required once again, with which firmware updates can be centrally deployed.

Once the vulnerability has been remedied on all components, the previously activated restrictive firewall rules as well as the decoupled systems can be restored to normal operation. The entire production network can then be used to the full extent again as usual with data archiving or further diagnoses. Reflecting the knowledge gained on the spreading of WannaCry, one very clearly recognizes the potential of a network management system. While the initial infection would not have been prevented, the spreading in the local network could have been sufficiently contained until the existing security update would have been deployed on the vulnerable systems.

A modern network management system is therefore not just for purely administrative or diagnostic purposes. Rather, it also helps to maintain plant availability in threat situations as part of defense in depth in conjunction with firewalls and other security components. Especially against the background of continuously increasing cyberattacks and constantly varying attack scenarios, a network management system can deliver the decisive advantage. As a competent partner for industrial communication and Industrial Security, Siemens provides comprehensive consulting services, integrated solutions, and end-to-end concepts to prepare production networks against future threats.

For further information about Industrial Security, see:
www.siemens.com/industrial-security

For further information about Network Management, see:
www.siemens.com/sinec-nms

Security information

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

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
Technical article
DI-PA-18/19-16
PDF 1219 4 En
Produced in Germany