Honeypots versus hackers

August 21 2015, by Katrin Nikolaus

As more and more machines throughout complex infrastructures communicate with one another, eliminating the possibility of hacking is becoming a top priority.

Production processes are becoming increasingly interconnected with digital communications technologies, opening new gateways for criminals operating on the Internet. The IT Security Technology Field at Siemens Corporate Technology is developing sophisticated solutions to protect against cyber crime and is subjecting them to rigorous testing, in part using its own team of hackers.

IT crime is on the rise. Once mainly limited to individual Internet users, it has become a major threat to industry and business, with damages caused by cyber attacks and industrial espionage already reaching many

billions of dollars per year. Many industrial companies are worried that as digital technologies spread and machines and installations become increasingly interconnected along the entire value chain, major additional security risks are being created. But to make their production faster and more flexible, and to keep it cost-effective, they have to convert their previously largely self-contained facilities into open production systems. It's a dilemma for which Dr. Rolf Reinema has a ready answer: "If industry uses an overarching and consistent security concept, the risks are manageable." Reinema, who is responsible for the IT Security Technology Field at Siemens Corporate Technology (CT), heads a group of IT experts focused on developing comprehensive security solutions for Siemens' businesses.

Ferreting out vulnerabilities

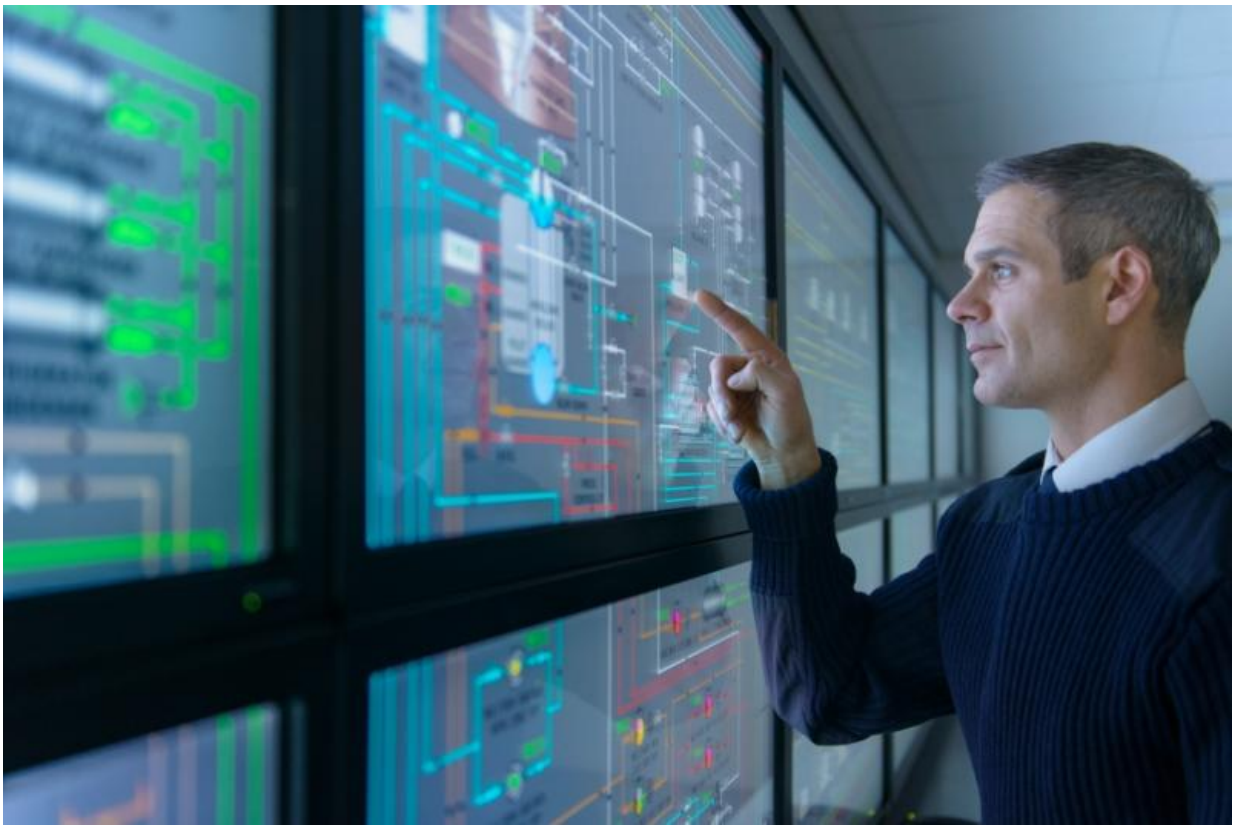
"In the past, gates and alarm systems protected factories. Today, on the other hand, the top priority for those responsible for security in industry is to be faster than hackers and uncover security gaps themselves," says IT security expert Dr. Heiko Patzlaff. To help them, his "Cyber Security Intelligence and Investigations" team, which is part of the IT Security Technology Field at Siemens, has developed a type of program that companies can use to quickly and easily check whether the security of their IT systems is up to date. It looks for obsolete software, missing updates, or poor management of access rights and passwords. A pilot project using the software has been successfully completed in one Siemens division. Now, Siemens is working to turn the easy-to-use software package into a service.

Scanning Data for Anomalies

Another IT security component from Patzlaff's team is a new monitoring system that identifies cyber attacks in close to real time. "In general,

attacks aren't detected fast enough. Once malware has penetrated a system, it can take its time looking through data and accomplishing its objective, whether that be pilfering data or manipulating it," says Patzlaff. The monitoring system is intended to improve matters. "We're developing algorithms that scan data streams for abnormalities," he adds. For example, movements of large quantities of data at unusual times of the day or night might indicate an attack. The same goes for commands that are executed countless times in succession for no apparent reason. Or, if users who only work during the day suddenly log in at night, this could be a sign of a cyber attack. "Since every IT system has its own typical routines and patterns of behavior, the search for clues has to be adapted to that," says Patzlaff. If the monitoring system detects anomalies, it automatically notifies the appropriate security center. "There, IT security specialists analyze the attempted breach and take countermeasures," he says.

ID check for machines



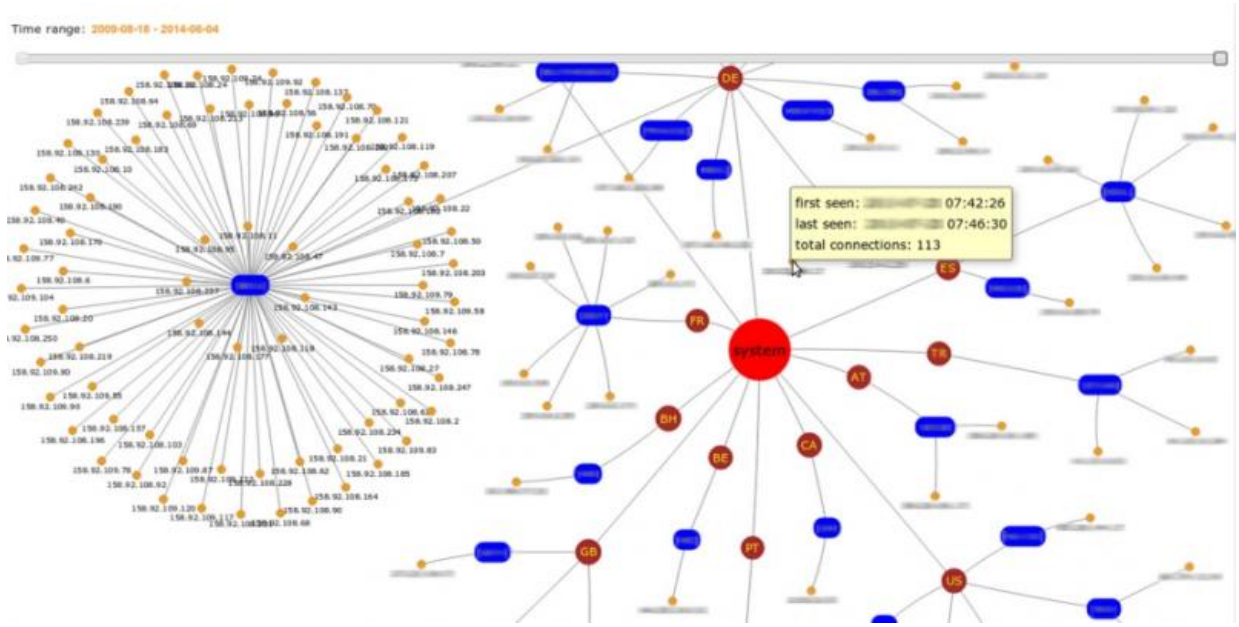
IT managers must discover vulnerabilities quickly and then take countermeasures.

This field is therefore in need of special security solutions. One idea, for example, is for machines to "identify" themselves before they can exchange data with one another or transmit it to databases. "This would make IT infrastructures more resistant to attacks," says Hendrik Brockhaus. His team in Siemens' IT Security Technology Field is currently demonstrating how an ID system of this kind for machines might work in a pilot system that was put together for the Siemens Mobility division. For the first time, Brockhaus is applying a public-key infrastructure (PKI) to industrial installations and using digital certificates to verify the authenticity of machines, sensors, or components.

For example, in the context of the pilot system, if a control system issues a switching command to the control unit of a field device, both the control system and control unit make certain, based on the PKI certificate, that the counterpart really is what it purports to be and that no hacking attempt is involved. The PKI certificates are issued by a "Trust Center" that operates according to very high standards of security and thereby establishes trust in the PKI certificates.

An immune system for industrial data analytics

Many industrial components have been retrofitted with defensive features against the new threats from cyberspace. At Siemens, however, new data platforms and services are equipped with robust and comprehensive security mechanisms during the development process. One example is the Industrial Data Analytics platform IDA, the security concept for which was developed by Dr. Fabienne Waidelich, Senior Key Expert for Smart Data Security, and her colleagues.



Corporate Technology has developed a monitoring service that helps to identify dangerous attacks.

IDA is a platform that collects data from the sensors and electronic maintenance logs of machines such as gas turbines, and evaluates them using advanced analytical tools. The reason this is useful for operators, and thus Siemens customers, is that they get an early indication of whether a component has to be replaced to prevent an operational failure, or how the temperature setting of a gas combustion chamber can be adjusted to optimize performance, for example. "If unauthorized persons get access to customer data, they could manipulate it and do things like simulate a maintenance issue that doesn't exist," says Waidelich. When designing the data platform, Siemens therefore put great emphasis on security. "The whole platform is accessible only from the intranet, and it's protected by additional firewalls," says Waidelich. Furthermore, all users have to prove their identity using a public key infrastructure ID in addition to a card equipped with an authentication chip.

The data source, which in this case might be a storage memory at the turbine, also has to go through an authentication process when it logs in at the server. That means it has to have an appropriate cryptographic key before it is even able to deliver any data. As soon as the data become available to the IDA—the landing zone, as it were—valuable knowledge can be extracted from it. This information is visualized as dashboards in reporting tools such as TIBCO Spotfire and Tableau. "Each of these applications must log in at the data storage systems, with its own login credentials in order to access the data," says Waidelich.

Hackers in the service of research

A gas turbine's operating data must be constantly analyzed. Before being transmitted, it must be encoded.

Another team in the IT Security Technology Field is also involved in defending against cyber attacks. "Our in-house hackers deliberately look for vulnerabilities in standard software for their attacks," says Reinema. In order to understand the methods hackers use, his department sets up what are called "honeypots." These are vulnerabilities that are specifically sought out by hackers. Of course, the honeypot isn't located in the real IT system. Instead, it simulates a piece of software, a network, or a server and merely leads the hacker to believe that he is attacking the

actual system. "By carefully analyzing hacker methods in this way, we can improve our threat intelligence and our ability to defend against attacks on our solutions," says Reinema.

At the same time, in addition to IT infrastructure and Siemens products, Reinema's IT security specialists also thoroughly examine the department's own solutions. Only then does it becomes apparent whether the walls erected by people like Fabienne Waidelich and her team are high enough, and whether the security checkpoints are rigorous enough.

Provided by Siemens