Cyber Security

Suzhou, 2017

IT security plays a crucial role in critical infrastructures such as power and water supply systems, transportation systems and plant control systems operated with the aid of IT systems. The increasing openness of these infrastructures increases their attack surface. Industrial espionage and cyber-attacks also pose a growing threat. This translates into continuously increasing security requirements for Siemens' products and solutions, dictated by market demand from customers as well as by statutory regulations.

Experts at Siemens' Corporate Technology (CT) are specialists in methods for timely prevention and systematic defense. In particular, the integration of IT security at an early stage of development can create added value and prevent delays in product launches.

Attacks and industrial espionage

- According to conservative analyses by Germany's digital association Bitkom (in an April 2015 study), the damage incurred by the entire German economy through digital industrial espionage, sabotage and data theft amounts to some €51 billion every year.
- Countless hacker groups pursue industrial espionage, usually attacking through Internet browsers and e-mail systems.
- Attacks by means of social engineering are occurring ever more frequently, as are attacks directly enabled by the Internet of Things (IoT) and unprotected IoT devices.
- Siemens receives between 3.5 and 4 million e-mails daily, of which almost 50 percent are spam or even contain infectious links.
- Siemens operates several Cyber Defense Centers (CDC) worldwide – for its own protection and for customers. For example, one CDC registers some 1,000 alarms every month. Approximately 30 of these are particularly critical incidents that are then handled jointly by the Siemens' Cyber Emergency Response Team (CERT).

Responsibility for security

Since October of this year, the responsibilities for IT security at Siemens have been structured into two units:

- Corporate Technology is responsible company-wide for governance of information security as well as product and solution security.
- Global Services Information Technology is responsible for implementing information security.

Security by design

The experts at Corporate Technology systematically integrate security into processes and products through what is called "security by design." That means that security is woven into the product lifecycle, from development through to operation.

The technical aspects include:

- Secure communication (authentication and encryption, etc.)
- Access control
- Systematic hardening, integrated patch management and security testing, and
- User friendliness so that users are also capable of correctly operating the security precautions and arrangements in place.

Our own hackers and golden nuggets

- Our CT experts monitor Siemens' systems and usually discover attacks in time or prevent them outright using protective measures. One example is ransomware, in which a hacker disables a computer from an external location and won't reveal the code to re-enable the computer until a ransom is paid. Thanks to protective measures in place, Siemens has so far suffered hardly any damage from such attacks.
- So-called "golden nuggets," which refers to strategically important and critical data the loss of which would mean major damage to Siemens, are assigned special classifications and individually protected by a comprehensive approach.
- Due to the ongoing trend of shifting applications and systems to the Internet, cloud-enabled security schemes are needed as well. CT experts in this field are working for example on identity monitoring of users and access rights.

- To find security gaps before a real cyber-pirate attacks, CT has its own in-house hacking team whose job is to try to penetrate Siemens systems.

Handling identified vulnerable weak points in Siemens products

- When vulnerable weak points or deficiencies are identified in Siemens products or in third-party components built into Siemens products, well-practiced processes are in place to eliminate these vulnerabilities as quickly as possible and provide customers with what are termed advisories or patches.

Data analytics for cyber security

Data analytics play a key role in data security in all kinds of application cases, such as in detecting attacks and assessing damage. The expanding volume of security-relevant data and the complexity of cyber-attacks are making it increasingly important that IT security analysts have high-performance analysis methods at their disposal. At Corporate Technology, IT security experts and data analytics experts are joining forces to work on this topic. They're generating usable information and security intelligence from data, and thus enabling the Business Units to pursue new and improved services and solutions.