SIEMENS

Ingenuity for life

Cybersecurity

Company Core Technology

Background

In the digital age Cybersecurity is the key prerequisite for organizations to safeguard critical infrastructure, protect sensitive information and assure business continuity. There is no digitalization of industry (Industrie4.0) without a high level of trust and a functioning Cybersecurity regime.

- For 2016, the global economic damage caused by Cybersecurity incidents is estimated to be from 330b to 560b EUR. For certain European countries, this damage amounts to 1.6% of GDP (ENISA Threat Landscape Report 2016).
- The scope for Cybersecurity threats is growing: 8.4 billion connected “things" will be in use in 2017, up 31% from 2016; this number will reach 20.4 billion by 2020.

  (Gartner, January 2017, http://www.gartner.com/newsroom/id/3598917)
- Operators of critical infrastructure such as telecommunication networks or power grids are already subject to high legal security requirements and depend on their suppliers to meet these. In the future hyper-connected world, higher requirements will have to apply to most devices as the definition of what is ‘critical’ is shifting (e.g. automated driving, human-robot collaboration).

Cybersecurity is about more than just technology, it has to become part of the DNA of every company (and every citizen). Anyone that wishes not only to supply secure products and systems to the market, but also to maintain Cybersecurity along their entire life cycle, needs a holistic Cybersecurity strategy that is clearly formulated and consistently implemented across the entire organization.

Importance for Siemens

Cybersecurity is a top priority for Siemens. We hold ourselves accountable to the highest Cybersecurity standards and want to lead by example. This is why we have developed a Charter of Trust that outlines our core commitments.

Siemens offers products and solutions with highest security standards by maintaining information security and protection against industrial espionage, denial of service, and attacks via malicious software, while we also ensures the availability of (critical) infrastructures.

The ability to supply customers with secure products and systems is a competitive advantage within a growing business field. The unique combination of technical know-how in Cybersecurity and the very deep domain know-how puts Siemens in an ideal position to be both a market and a thought leader.

Success stories and research focus

Siemens has about 570 Cybersecurity experts worldwide. This includes about 25 whitehead hackers who continuously challenge the security of both internal IT Systems and products to be shipped to customers.

Cybersecurity is not a new topic for Siemens. The first IT Security team at Siemens was set up in 1986 – about 30 years ago – at the central research department Corporate Technology.

Siemens operates 3 global Cyber Defense Centers in Lisbon, Portugal, in Milford (Ohio), USA, and in Suzhou, China. Here the company monitors its own infrastructure, production plants and facilities around the world for cyber threats, warning them in the event of a security incident and coordinate proactive countermeasures.

Specifically, Siemens offers Plant Security Services, which include the assessment of security risks in factories and production plants as well as the implementation of security measures for our customers. These may include the implementation anti-virus software, security trainings, firewall management, anti-virus management, or incident handling.

In a similar manner, Siemens offers Cybersecurity services for utilities and power grid operators, including the evaluation of the current system as well as the implementation, testing and maintenance of security upgrades.

Siemens Healthineers is offering virus protection for tomographs and other imaging products, which are typically connected to the internet for the purpose of remote maintenance.

Some examples of the research focus: Siemens works on providing tested and hardened components to all its businesses, on the development of automated intrusion detection and response in an industrial context and on automated “security for life cycle” concepts for industrial equipment.

Further information

siemens.com/innovationday
siemens.com/press/inno2017