SIEMENS
Ingenuity for life

Cybersecure digitalization of power distribution in infrastructures and buildings

Secure communication – with the SENTRON product portfolio

siemens.com/powermonitoring

The challenge

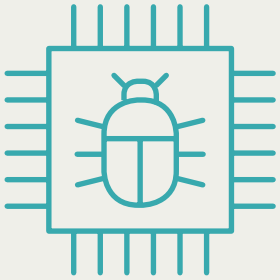
Security is a crucial factor for the way in which power distribution in infrastructures and buildings is handled in a digitalized world.

Cybersecurity – the security of communication and IT systems, power grids and other digital infrastructures – is playing an increasingly important role. It is a highly sensitive area that requires dependable partners as well as secure and reliable hardware and software. Although the Internet of Things (IoT) and new, digital business models offer many advantages, they also involve risks. The greater the number of devices in your infrastructure that are networked and connected to the cloud, the more opportunities there are for attacks.

In recent years, cybersecurity experts at Siemens have noticed a steady increase in malware and exploits that attack a variety of applications and devices.

Malware, for example, changes device or software configurations or downloads manipulated firmware to IoT devices, thus causing these devices to cease functioning or allowing them to be misused for other purposes. Siemens' holistic approach to the protection and secure operation of these IoT environments makes it a pioneer in the field of cybersecurity.

Malware:
A malicious computer code that interferes with the actual functioning of an application or product.



Exploits:
Taking advantage of vulnerabilities to attack software and download malware.

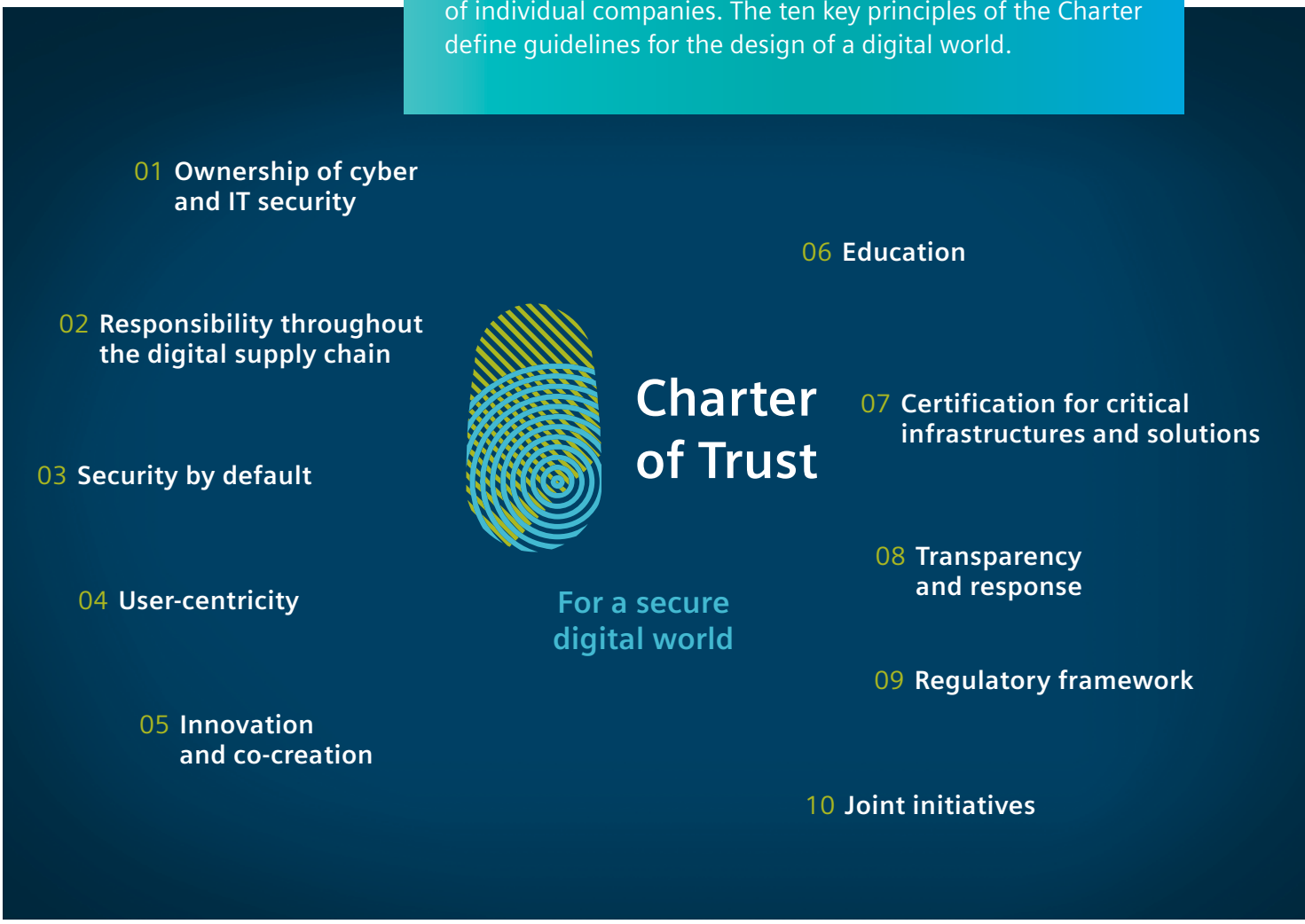
Strategically planned cybersecurity

Because this topic isn't limited to Siemens' own sphere of influence but is also an important issue for the business partners and suppliers in its immediate environment, Siemens began at an early stage to make this extended environment as cybersecure as possible.

One important step is the Charter of Trust initiated by Siemens – a steadily growing group currently comprising 16 large corporations from various markets (e.g., IBM, Daimler, and Total).

In October 2018 under the patronage of Joe Kaeser, CEO of Siemens AG, the partners developed basic requirements for the cybersecurity of digital supply chains as one of the first measures of the Charter of Trust. They will integrate these requirements into their own global supply chains with the inclusion of their suppliers.

The Charter of Trust organizes the trust-based collaboration between leading companies from around the world on a global scale to promote cybersecurity beyond the boundaries of individual companies. The ten key principles of the Charter define guidelines for the design of a digital world.



The ten key principles of the Charter of Trust

Siemens' holistic approach

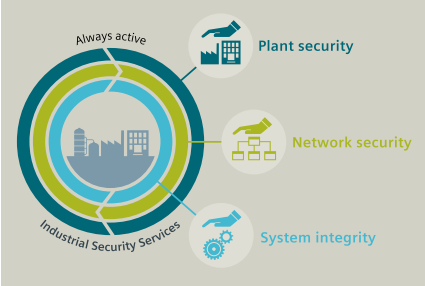
To deal with the diverse threats to data security in the IoT, a strategic approach on many levels is recommended.

Siemens takes a comprehensive approach to protection. Based on the defense-in-depth concept, a multilayer information security concept is established on all levels simultaneously – from the operational to the field level and from access control to copy protection.

Siemens' ProductCERT is largely responsible for all these processes, applications, and solutions. CERT stands for "Computer Emergency Response Team." A team of cybersecurity experts informs and advises customers and searches for indications of vulnerabilities in Siemens products worldwide in order to immediately develop appropriate countermeasures.

Siemens also emphasizes the proactive communication of attacks as they become known as well as suitable countermeasures like patches and updates. Siemens also disburses information – for example, via the openly accessible website Siemens Security Advisories (SSA), the free Twitter account @ProductCERT, and free advisory e-mails for registered recipients.

Defense in Depth:
A strategy of layered, staggered defense mechanisms that serve to protect valuable information and data. If one defense mechanism fails, the next one immediately takes effect.



Know the problems. Know the counter-measures

Subscribe to Siemens Security Advisories

Educated employees

Social Engineering:
Uncovering personal data through a variety of channels.

At Siemens, a comprehensive cybersecurity solution also includes employee education.

Every year, Siemens conducts a mandatory, in-house cybersecurity awareness training course for all employees. Among the topics covered are attack scenarios like social engineering.

Siemens also has a cybersecurity organization that is rolled out via all the company's operational and strategic units. With PSS (Product and Solution Security), any employee or internal project team can ask for advice and further training in the area of cybersecurity. This enables them to deliver solutions and products to their customers that pose no cybersecurity risks when customers configure, install, or operate them.

In-depth vulnerability analyses

Based on the PSS strategy, a threat and risk analysis is also conducted that already subjects devices and applications to various cybersecurity tests before and during development.

One of these tests is the vulnerability scan, by means of which known cybersecurity vulnerabilities can be immediately detected and corrected. At the same time, an automated test checks the robustness of the communication interface. The stability of the device when specific IP communication parameters are changed is also tested.

Protective mechanisms for the SENTRON product portfolio

The following cybersecurity measures provide the basis for secure operation of communication-capable products:

- Only firmware signed by Siemens is used in these products. This means that only authentic software produced by Siemens can be installed and operated on the particular IoT device. This prevents the firmware from being manipulated by third parties.
- For many Siemens devices, password protection can be set up that protects the device configuration against unauthorized write accesses.
- An IP address filter can be configured that only allows specific IP addresses approved by the customer to communicate with the device.
- A hardware write-protect switch can be used to lock the configuration against remote manipulations.

With these measures, Siemens has laid the groundwork for a cybersecure SENTRON product range. Because the threats are constantly changing and evolving, Siemens also adapts its SENTRON products to heightened security requirements and develops new security technologies that continually reduce risks. With SENTRON products, customers are investing in the state of the art, and thus in a secure future.

Published by
Siemens AG

Smart Infrastructure
Low Voltage Products
Siemensstrasse 10
93055 Regensburg
Germany

For more information, please contact
our Customer Support Center.
Tel.: +49 180 524 70 00
Fax: +49 180 524 24 71
(Charges depending on provider)
E-mail: support.energy@siemens.com

Article no. SILP-I10063-00-7600
Dispo 30407 TH 477-191191 BR 0420
© Siemens 2020

Subject to changes and errors.
The information provided in this document contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies, or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.