Joint press release

Press

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total and TÜV SÜD

Munich, February 14, 2020

Charter of Trust partners decide on further measures for more cybersecurity

- **Cybersecurity by default: Next-generation products are to be equipped with preconfigured security**
- **New partners: NTT, Infineon and Hasso Plattner Institute for Digital Engineering join Charter of Trust**
- **Cybersecurity extended along the supply chain: Numerous suppliers meet baseline requirements of the Charter of Trust companies**
- **Education campaign for Small and Medium enterprises and schools: Charter of Trust partners provide cybersecurity materials**

The Charter-of-Trust (CoT) partners have agreed to deliver next-generation products with preset cybersecurity, following a clear “Security by Default” philosophy. At present, there are no uniform regulations governing this issue – many products leave the factory solely dependent on safety systems that do not provide comprehensive protection. Users often have to adjust security settings afterward. As a first step, the Charter partner companies have now defined which security features should be present and activated by default in next-generation products – ranging from strong authentication features to a unique product identity and the requirement that passwords must be changed upon first use.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany

The CoT partners also believe that no undocumented functionalities or possibilities for remote connection should be part of initial device setup – another aspect that is not yet a general rule today. All these requirements are now being rolled out step by step within the relevant portfolios of the Charter of Trust member companies.

“Cybersecurity is a key ingredient for trust of our customers in all our businesses offering digitally connected products. It is also the basis for sustainable success and the foundation of a strong ecosystem “, says Roland Busch, deputy CEO, CTO, CHRO and Managing Board Member of Siemens AG.

At the Munich Security Conference in February 2018, Siemens and eight partners from the industrial sector launched a joint charter for more cybersecurity for the first time. Two years after signing, the Charter of Trust has grown to 17 members. In addition to Siemens and the Munich Security Conference, the companies AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, Mitsubishi Heavy Industries, NXP Semiconductors, SGS, Total and TÜV SÜD have committed themselves to the document. Furthermore, the Federal Office for Information Security (BSI), the National Cryptologic Center (CCN) and Graz University of Technology are accompanying the Charter’s work as Associated Partners. Today, the Charter of Trust is gaining two new members in NTT, a Japan-origin IT consulting and managed service provider, and the German semiconductor manufacturer Infineon Technologies AG. With the Hasso Plattner Institute for Digital Engineering GmbH (HPI), one of Germany’s leading IT institutes is now also contributing to the cybersecurity initiative as an Associated Partner.

Last year, the partners already agreed on 17 concrete baseline requirements with which they can increase the security of their supply chains. Since then, numerous suppliers of CoT companies have already committed to meeting these requirements.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany

Siemens, AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, MHI, MSC, NXP, SGS, Total and TÜV SÜD

Siemens has been introducing them step-by-step since February 15, 2019, and they have been internationally anchored and made binding as part of the general ordering conditions. This primarily affects suppliers of safety-critical components – such as software, processors or electronic components. Existing suppliers are expected to implement the requirements gradually if they are not already being fulfilled. The aim is to better protect the digital supply chain from hacks. The baseline requirements include, for example, that suppliers incorporate safety standards, processes and methods into their products or services. This concerns both technical features and organizational measures relevant to products, services and the corresponding IT infrastructure. The goal here is to reduce risks caused by weaknesses in the software and malware. Suppliers bear the responsibility to carry out regular safety checks, tests and corrections. The CoT partners have agreed to these requirements for themselves as well. The supply chain is the weakest point in a company's cybersecurity ecosystem: The origin of 60 percent of cyberattacks can be traced back to parts of the supply chain, and in 60% of those cyber incidents, it is smaller companies who are affected, according to a Verizon study.

The CoT partners have also decided to promote education and training on cybersecurity issues, including for small and medium-sized enterprises (SMEs), which are increasingly targeted by cyberattacks. For example, in Germany, the Charter of Trust partnered with the "Alliance for Cybersecurity," and developed a set of materials with an emergency card that explains quickly and easily what to do in the event of a cyberattack. In addition, the partners have developed further training material that are made available to SMEs free of charge. In doing so, they aim to prevent cybercrime, but above all to highlight the opportunities for effective cybersecurity measures. The partners have developed a special cybersecurity simulation for schools to give students and teachers a clear and easily digestible overview of the challenges.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany

According to the Center for Strategic and International Studies, cyberattacks will cause more than €500 billion in global damage in 2018. And the threats are constantly increasing in a digitalized world: According to Cisco, there are around 50 billion networked devices in use in 2020 – double the amount than in 2015, and the figure is expected to rise to 500 billion by 2030.

The text of the Charter of Trust can be found at: www.charteroftrust.com
You can find this press release at sie.ag/2w9OXOs

Follow us on Twitter: www.twitter.com/siemens_press

Contact person for journalists

Siemens
Florian Martini; Phone: +49 89 636 33446;
E-mail: florian.martini@siemens.com

AES
Gail Chalef; Phone.: +1 703 682 6428 ; E-Mail: gail.chalef@aes.com

Airbus
Florian Taitsch; Phone: +49 89 3179 4644; E-mail: florian.taitsch@airbus.com
Ambra Canale; Phone: +49 89 31 79 99 29; E-mail: ambra.canale@airbus.com

Allianz
Daniel Aschoff; Phone: +49893800-18900;
E-mail: Daniel.Aschoff@allianz.com

Atos

Lucie Duchateau; Phone: +33 7 62 85 35 10;

E-mail: lucie.duchateau@atos.net

Cisco

Jessica Tompkinson; Phone: +44 20 8824 3701;

E-mail: jetompki@cisco.com

Dell Technologies:

Media.Relations@Dell.com

Deutsche Telekom

Christian Fischer; Phone: +49 151 121 85073;

E-mail: christian.fischer03@telekom.de

IBM

Jonathan Sage; Phone: +44 7738310713;

E-mail: jonathan.sage@uk.ibm.com

MHI

Daniela Stawinoga-Carrington, Phone: +44 20 3480 7521,

E-mail: daniela_stawinoga-carrington@mhie.com

MSC

Johannes Schmid; Phone: +49 89 379794920;

E-mail: j.schmid@securityconference.de

NXP

Svend Buhl; Phone: +49 40 5613 2289;

E-mail: svend.buhl@nxp.com

SGS

Daniel Rüfenacht; Phone: +41 22 739 94 01;

E-mail: Daniel.Rufenacht@sgs.com

TÜV SÜD

Sabine Krömer; Phone: +49 151 5587 3235;

E-mail: Sabine.Kroemer@tuev-sued.de

Siemens AG (Berlin and Munich) is a global technology powerhouse that has stood for engineering excellence, innovation, quality, reliability and internationality for more than 170 years. The company is active around the globe, focusing on the areas of power generation and distribution, intelligent infrastructure for buildings and distributed energy systems, and automation and digitalization in the process and manufacturing industries. Through the separately managed company Siemens Mobility, a leading supplier of smart mobility solutions for rail and road transport, Siemens is shaping the world market for passenger and freight services. Due to its majority stakes in the publicly listed companies Siemens Healthineers AG and Siemens Gamesa Renewable Energy, Siemens is also a world-leading supplier of medical technology and digital healthcare services as well as environmentally friendly solutions for onshore and offshore wind power generation. In fiscal 2019, which ended on September 30, 2019, Siemens generated revenue of €86.8 billion and net income of €5.6 billion. At the end of September 2019, the company had around 385,000 employees worldwide. Further information is available on the Internet at www.siemens.com.

Siemens AG
Werner-von-Siemens-Str.
180333 Munich
Germany