Gemeinsame Presseinformation

Presse

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

München, 14. Februar 2020

Charter-of-Trust-Partner beschließen weitere Maßnahmen für mehr Cyber-Sicherheit

- **Cyber-Sicherheit ab Werk: Produkte der nächsten Generation sollen mit bereits vorkonfigurierter Sicherheit ausgestattet werden**
- **Neue Partner: NTT, Infineon Technologies und Hasso-Plattner-Institut für Digital Engineering treten Charter of Trust bei**
- **Cyber-Sicherheit entlang der Lieferkette ausgebaut: Zahlreiche Lieferanten erfüllen Mindestanforderungen der Charter-of-Trust-Unternehmen**
- **Bildungskampagne für KMUs und Schulen: Charter-of-Trust-Partner stellen Cyber-Sicherheits-Materialien zur Verfügung**

Die Charter-of-Trust (CoT)-Partner haben sich darauf geeinigt, Produkte der nächsten Generation mit voreingestellter Cyber-Sicherheit auszuliefern und dabei einer eindeutigen „Security by Default“-Philosophie zu folgen. Derzeit gibt es hierzu noch keine einheitlichen Regelungen – viele Produkte aus den Werkshallen sind in ihrer Anwendung auf Sicherheitssysteme angewiesen, die keinen ganzheitlichen Schutz aufbauen. Oft müssen die Nutzer Sicherheitseinstellungen daher nachträglich vornehmen. In einem ersten Schritt haben die Charter-Unternehmen nun festgelegt, welche Sicherheitsmerkmale in Produkten der nächsten Generation standardmäßig aktiviert sein sollen – das reicht von starken Authentifizierungsverfahren über die eindeutige Identität eines Produktes bis hin zur Anforderung, dass Passwörter bei der ersten Verwendung geändert werden müssen. Auch definieren die CoT-Partner,

Siemens AG
Werner-von-Siemens-Str.1
80333 München
Deutschland

keine undokumentierten Funktionalitäten oder Möglichkeiten zur Fernverbindung mit einem Gerät einzurichten – auch das ist heute noch nicht durchgängig die Regel. All diese Anforderungen werden nun sukzessive in den Mitgliedsunternehmen der Charter of Trust für das relevante Portfolio der nächsten Generation ausgerollt.

„Cybersecurity ist in jedem unserer Geschäfte mit digital vernetzten Produkten der Schlüssel für das Vertrauen der Kunden und die Grundlage für nachhaltigen Erfolg sowie die Basis eines starken Ökosystems“, sagt Roland Busch, stellvertretender Vorstandsvorsitzender der Siemens AG.

Im Februar 2018 haben Siemens und acht Partner aus der Industrie auf der Münchner Sicherheitskonferenz erstmals eine gemeinsame Charta für mehr Cyber-Sicherheit ins Leben gerufen. Zwei Jahre nach Unterzeichnung ist die Charter of Trust (CoT) auf 17 Mitglieder angewachsen. Zum Dokument verpflichten sich neben Siemens und der Münchner Sicherheitskonferenz die Unternehmen AES, Airbus, Allianz, Atos, Cisco, Dell Technologies, Deutsche Telekom, IBM, Mitsubishi Heavy Industries, NXP Semiconductors, SGS, Total und TÜV SÜD. Ferner begleiten das Bundesamt für Sicherheit in der Informationstechnik (BSI), das National Cryptologic Center (CCN) und die TU Graz die Arbeiten der Charter als Associated Partner. Ab Mitte Februar 2020 werden NTT, der japanische IT-Dienstleister für Consulting und Managed Services, sowie der deutsche Halbleiterhersteller Infineon Technologies AG der Charter of Trust beitreten. Mit dem Hasso-Plattner-Institut für Digital Engineering GmbH (HPI) trägt ab sofort auch eines der führenden deutschen IT-Institute als Associated Partner zur Cyber-Sicherheits-Initiative bei.

Bereits im Vorjahr hatten sich die Partner auf 17 konkrete Mindestanforderungen verständigt, mit denen sie die Sicherheit ihrer Lieferketten erhöhen können. Seitdem haben sich bereits zahlreiche Lieferanten der CoT-Unternehmen verpflichtet, diese

Siemens AG
Werner-von-Siemens-Str.1
80333 München
Deutschland

Anforderungen zu erfüllen. Bei Siemens wurden sie ab 15. Februar 2019 schrittweise eingeführt und als Teil der allgemeinen Bestellbedingungen international verankert und verbindlich gemacht. Dies betrifft vorrangig Lieferanten von sicherheitskritischen Komponenten – dazu zählen etwa Software, Prozessoren oder elektronische Bauteile. Bestehende Lieferanten sollen die Anforderungen nach und nach umsetzen, wenn diese nicht bereits erfüllt sind. Ziel ist es, die digitale Lieferkette besser vor Hacker-Angriffen zu schützen. Zu den Mindestanforderungen gehört es etwa, dass Lieferanten Sicherheitsnormen, -prozesse und -methoden in ihre Produkte oder Dienstleistungen einbauen. Dies betrifft sowohl technische Merkmale als auch organisatorische Maßnahmen, die für Produkte, Dienstleistungen und die entsprechende IT-Infrastruktur relevant sind. Das Ziel: Risiken durch Schwachstellen in der Software und Malware-Funktionen zu reduzieren. Es ist Aufgabe der Lieferanten, regelmäßige Sicherheitsüberprüfungen, Tests und Korrekturen vorzunehmen. Diese Anforderungen machen die CoT-Partner auch für sich selbst verpflichtend. Die Lieferkette ist der schwächste Punkt im Cybersecurity-Ökosystem von Unternehmen: 60 Prozent der Cyber-Attacken lassen sich im Ursprung auf Teile der Lieferketten zurückverfolgen, und bei 60 Prozent dieser Cyber-Vorfälle sind laut einer Verizon-Studie kleinere Unternehmen betroffen.

Die CoT-Partner haben zudem beschlossen, die Aus- und Weiterbildung in Fragen der Cyber-Sicherheit zu fördern – unter anderem für kleine und mittelständische Unternehmen (KMU), die zunehmend in den Fokus von Cyber-Angriffen geraten. In Deutschland hat die Charter of Trust beispielsweise mit der „Allianz für Cyber-Sicherheit“ eine Reihe von Lehrmaterialien entwickelt – wie eine Notfallkarte, die schnell und einfach erklärt, was im Fall einer Cyber-Attacke zu tun ist. Darüber hinaus haben die Partner weitere Bildungsmaterialien entwickelt, die KMUs kostenfrei zur Verfügung gestellt werden. Das Ziel: der Cyber-Kriminalität vorbeugen, vor allem aber die Chancen effektiver Cyber-Sicherheits-Maßnahmen verdeutlichen. Im nächsten

Siemens AG
Werner-von-Siemens-Str.1
80333 München
Deutschland

Schritt sollen die Materialien auch international verfügbar sein. Speziell für Schulen haben die Partner unter anderem eine Cyber-Sicherheits-Simulation entwickelt, um Schülern und Lehrern die Herausforderungen anschaulich und leicht nachvollziehbar näherzubringen.

Laut dem Center for Strategic and International Studies richteten Cyber-Angriffe im Jahr 2018 einen weltweiten Schaden von mehr als 500 Milliarden Euro an. Und die Bedrohungen nehmen in einer digitalisierten Welt ständig zu: Cisco zufolge sind im Jahr 2020 bereits rund 50 Milliarden vernetzte Geräte im Gebrauch – das sind doppelt so viele wie noch im Jahr 2015. Bis 2030 soll diese Zahl sogar auf 500 Milliarden steigen.

Die Charter of Trust im Wortlaut finden Sie unter: www.charteroftrust.com
Diese Presseinformation finden Sie unter: sie.ag/38q1602

Folgen Sie uns auf Twitter: www.twitter.com/siemens_press

Ansprechpartner für Journalisten

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

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

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

Allianz

Daniel Aschoff; Tel.: +49893800-18900; E-Mail: Daniel.Aschoff@allianz.com

Atos

Lucie Duchateau; Tel.: +33 7 62 85 35 10; E-Mail: lucie.duchateau@atos.net

Cisco

Jessica Tompkinson; Tel.: +44 20 8824 3701; E-Mail: jetompki@cisco.com

Dell Technologies:

Media.Relations@Dell.com

Deutsche Telekom

Christian Fischer; Tel.: +49 151 121 85073;

E-Mail: christian.fischer03@telekom.de

IBM

Jonathan Sage; Tel.: +44 7738310713;

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

MHI

Daniela Stawinoga-Carrington, Tel.: +44 20 3480 7521,

E-Mail: daniela_stawinoga-carrington@mhie.com

MSC

Johannes Schmid; Tel.: +49 89 379794920; E-Mail: j.schmid@securityconference.de

NXP Semiconductors

Svend Buhl; Tel.: +49 40 5613 2289; E-Mail: svend.buhl@nxp.com

SGS

Daniel Rüfenacht; Tel.: +41 22 739 94 01; E-Mail: Daniel.Rufenacht@sgs.com

TÜV SÜD

Sabine Krömer; Tel.: +49 151 5587 3235; E-Mail: Sabine.Kroemer@tuev-sued.de

Die **Siemens AG** (Berlin und München) ist ein führender internationaler Technologiekonzern, der seit mehr als 170 Jahren für technische Leistungsfähigkeit, Innovation, Qualität, Zuverlässigkeit und Internationalität steht. Das Unternehmen ist weltweit aktiv, und zwar schwerpunktmäßig auf den Gebieten Stromerzeugung und -verteilung, intelligente Infrastruktur bei Gebäuden und dezentralen Energiesystemen sowie Automatisierung und Digitalisierung in der Prozess- und Fertigungsindustrie. Durch das eigenständig geführte Unternehmen Siemens Mobility, einer der führenden Anbieter intelligenter Mobilitätslösungen für den Schienen- und Straßenverkehr, gestaltet Siemens außerdem den Weltmarkt für Personen- und Güterverkehr. Über die Mehrheitsbeteiligungen an den börsennotierten Unternehmen Siemens Healthineers und Siemens Gamesa Renewable Energy gehört Siemens zudem zu den weltweit führenden Anbietern von Medizintechnik und digitalen Gesundheitsservices sowie umweltfreundlichen Lösungen für die On- und Offshore-Windkrafterzeugung. Im Geschäftsjahr 2019, das am 30. September 2019 endete, erzielte Siemens einen Umsatz von 86,8 Milliarden Euro und einen Gewinn nach Steuern von 5,6 Milliarden Euro. Ende September 2019 hatte das Unternehmen weltweit rund 385.000 Beschäftigte. Weitere Informationen finden Sie im Internet unter www.siemens.com.

Siemens AG
Werner-von-Siemens-Str.1
80333 München
Deutschland