



Münchener Sicherheitskonferenz

Charter of Trust zur Cybersicherheit

Cybersicherheit – eines der wichtigsten Themen unserer Zeit

Die bedeutendsten Entscheidungsträger in der internationalen Sicherheitspolitik werden auch dieses Jahr zur Münchener Sicherheitskonferenz (Munich Security Conference, MSC) zusammenkommen, die vom 16. bis 18. Februar 2018 stattfindet. Etwa 500 VIPs aus aller Welt werden sich über aktuelle Krisen und künftige Herausforderungen der internationalen Sicherheitspolitik austauschen. Als strategischer Partner der MSC wird Siemens die Gelegenheit dazu nutzen, ein Thema anzusprechen, das nicht nur für Unternehmen von allergrößter Bedeutung ist, sondern für die gesamte Welt: Cybersicherheit.

Bedrohungen der Cybersicherheit haben Schätzungen zufolge allein im Jahr 2017 einen weltweiten Schaden von mehr als 500 Milliarden Euro angerichtet. Für einige europäische Länder beziffert sich der Schaden auf 1,6 Prozent des Bruttoinlandsprodukts. Und die Bedrohungen der Cybersicherheit nehmen zu: 2017 waren 8,4 Milliarden vernetzte Geräte in Gebrauch – das sind 31 Prozent mehr als 2016. Bis 2020 soll diese Zahl auf 20,4 Milliarden steigen.

Angemessene Cybersicherheit ist eine der Grundvoraussetzungen für den Schutz kritischer Infrastrukturen und sensibler Daten sowie für die Aufrechterhaltung eines störungsfreien Geschäftsbetriebs. Sie ist also mehr als nur ein metaphorischer Sicherheitsgurt: Sie ist ein wesentlicher Faktor für den Erfolg der digitalen Wirtschaft.

Menschen, Organisationen und sogar ganze Gesellschaften überall auf der Welt müssen sich auf vertrauenswürdige digitale Technologien verlassen können. Wir können allerdings nicht erwarten, dass Menschen die digitale Transformation aktiv unterstützen, wenn nicht gewährleistet ist, dass ihre Daten und vernetzten Systeme entsprechend dem aktuellen Stand der Technik angemessen geschützt werden. Aus diesem Grunde sind Digitalisierung und Cybersicherheit zwei Seiten einer Medaille, die sich parallel zueinander weiterentwickeln müssen. Wenn eines von beiden einwandfrei laufen soll, müssen beide funktionieren.

Das gilt vor allem in einer Zeit, in der die Digitalisierung in jeden Lebensbereich Einzug hält. Fehler oder sogar Ausfälle in den Systemen, die unsere Haushalte, unsere Krankenhäuser, unsere Fertigungsanlagen, unsere Stromnetze – ja unsere gesamte Infrastruktur – kontrollieren und vernetzen, könnten verheerende Folgen haben. Zeitgemäße Vorschriften, geschützte Umgebungen und klare Standards für Cybersicherheit sind wesentliche Voraussetzungen für das Vertrauen der Menschen in unsere digitalisierte Welt – und es ist wichtig, sich dieses Vertrauen zu verdienen, weil es der Dreh- und Angelpunkt für den künftigen Erfolg und unser aller Wohlstand ist.



Aus diesem Grund hat Siemens-CEO Joe Kaeser im November 2017 angekündigt, dass Siemens auf der Münchner Sicherheitskonferenz mit Partnern aus Industrie, Politik und Gesellschaft eine „Charter of Trust“ erarbeiten und unterzeichnen, diese veröffentlichen und für ihre allgemeine Verabschiedung eintreten wird. Die Charta enthält zehn Prinzipien, die unsere digitale Welt sicherer machen sollen, und gibt drei wichtige Ziele vor:

- Daten von Einzelpersonen und Unternehmen schützen,
- Schaden von Personen, Unternehmen und Infrastrukturen abwenden und
- ein zuverlässiges Fundament schaffen, in dem Vertrauen in eine vernetzte digitale Welt verankert wird und auf dem es wachsen kann.

Und sie beschreibt, worauf es ankommt, um diese Ziele zu erreichen: Zunächst einmal bedarf es einer intensiven multilateralen Zusammenarbeit von Politik und Wirtschaft, um sich für die weitreichenden Auswirkungen von Cyberkriminalität zu wappnen und eine gemeinsame Vertrauensbasis an den globalisierten Märkten zu schaffen. Die Verantwortung dafür muss auf höchster Ebene von Regierungen und Unternehmen übernommen werden und ihren Niederschlag in klaren Zielen und Maßnahmen in den jeweiligen Organisationen finden. Darüber hinaus muss die Verantwortung für Cybersicherheit in der gesamten digitalen Wertschöpfungskette verankert werden. Dies beinhaltet eine fortlaufende Fortbildung und professionelle Schulung im Bereich Cybersicherheit. Firmen und politische Entscheidungsträger sollten – so beschreibt es die Charta – ihr gemeinsames Verständnis für die Sicherheitsanforderungen vertiefen und dafür sorgen, dass zeitgemäße Regeln und Standards aufgestellt und eingehalten werden, die für eine kontinuierliche Entwicklung und Anpassung der Technologien im Bereich Cybersicherheit notwendig sind. Datenströme machen nicht an Landesgrenzen halt; deshalb profitiert jeder von international geltenden Regeln.

All diese erforderlichen Maßnahmen umzusetzen kann nicht Aufgabe einer einzigen Organisation sein – das gilt auch für einen Weltkonzern wie Siemens. Mit unserer „Charter of Trust“ versuchen wir, den Anstoß für eine enge Zusammenarbeit auf allen Ebenen zu geben. Die Sicherheit von Informationen, Produkten und Lösungen muss ein fester Bestandteil unserer digitalen Welt sein. Wir sind überzeugt: Unternehmen und Länder, die in den globalen digitalen Märkten eine entscheidende Rolle spielen wollen, müssen sich gemeinsam für Cybersicherheit einsetzen, um das Vertrauen der Öffentlichkeit, der Kunden und der Geschäftspartner zu stärken.

Cybersicherheit – eine wichtige Säule der Digitalisierungsstrategie von Siemens

Cybersicherheit genießt bei Siemens oberste Priorität. Die Fähigkeit, Kunden mit Produkten und Systemen beliefern zu können, die in puncto Cybersicherheit State-of-the-Art-Funktionalitäten beinhalten, ist ein Wettbewerbsvorteil in der zunehmend digitalisierten Geschäftswelt. Eine McKinsey-Studie, basierend auf 250 Interviews mit Branchengrößen, stellt Folgendes fest: „Große Technologietrends wie Analytik, Cloud Computing und Big Data könnten einen Wert von 9,6 bis 21,6 Billionen US-Dollar für die Weltwirtschaft schaffen. Wenn die raffinierten Angriffsmethoden schneller zunehmen als die Abwehrmöglichkeiten – was zu noch destruktiveren Angriffen führen würde –, könnte

Weitere Informationen

charter-of-trust.de
siemens.com/cybersecurity
siemens.de/pof-cybersecurity



dies die Innovationsfähigkeit bremsen. Das hätte in der Summe wirtschaftliche Auswirkungen in Höhe von rund drei Billionen US-Dollar.“

Das Geschäft mit Cybersicherheit wächst rasant, sowohl für Produkte als auch bei Dienstleistungen. Analysten gehen davon aus, dass der Sicherheitsmarkt für Industrie-Controller mit einer Rate von sieben Prozent von neun Milliarden US-Dollar im Jahr 2016 auf 12,6 Milliarden US-Dollar im Jahr 2021 wachsen wird. Gleichzeitig besteht auf Kundenseite ein zunehmender Bedarf an Cybersicherheitsdienstleistungen, beispielsweise zum Schutz ganzer Infrastrukturen wie Fabriken und Energienetze vor Cyberangriffen.

Mit seiner einzigartigen Kombination aus technischem Know-how im Bereich Cybersicherheit und profundem Branchenwissen ist Siemens ideal aufgestellt, um sowohl eine führende Marktposition einzunehmen als auch Thought Leader auf diesem Gebiet zu sein. Unser Unternehmen beschäftigt aktuell rund 1275 Experten für Cybersicherheit weltweit. Dazu gehören circa 25 Whitehead Hacker, die kontinuierlich die Sicherheit der internen IT-Systeme sowie der Produkte, die an Kunden ausgeliefert werden, auf die Probe stellen. Und Cybersicherheit ist bei Siemens kein neues Thema: Das erste IT-Sicherheitsteam bei Siemens wurde schon 1986 – also vor gut 30 Jahren – in der zentralen Forschungsabteilung des Unternehmens, Corporate Technology, eingerichtet.

Mit über einer Million Geräten, die bereits mit MindSphere verbunden sind, haben wir im Zeitalter des industriellen Internets der Dinge Erfahrungen in Fragen der Cybersicherheit aus erster Hand.

Siemens ist das erste Unternehmen, das – in seiner Division Digital Factory– Sicherheit in allen Phasen seines industriellen Produktentwicklungszyklus integriert hat und dafür vom TÜV Süd zertifiziert ist. Siemens bietet insbesondere Plant Security Services an. Hierzu gehören die Bewertung von Sicherheitsrisiken in Fabriken und Produktionsanlagen sowie die Umsetzung von Sicherheitsmaßnahmen für unsere Kunden basierend auf IEC 62443 und dem ganzheitlichen Sicherheitskonzept. Letzteres kann den Einsatz von Antivirensoftware, Sicherheitstrainings, Firewall-Management, Antivirenmanagement und Incident-Bearbeitung beinhalten.

Siemens bietet darüber hinaus Cybersicherheitsdienstleistungen für Industriekunden, Versorger und Stromnetzbetreiber sowie Gesundheitsdienstleister an, einschließlich der Bewertung und kontinuierlichen Überwachung des aktuellen Systems, der Implementierung, dem Testen und Warten von Sicherheits-Upgrades sowie der Reaktion auf Cyber-Vorfälle.

Einige Beispiele unserer Forschung spiegeln auch die Führungsposition des Unternehmens auf diesem Gebiet wider. Siemens stellt getestete und gehärtete Komponenten bereit, entwickelt automatisierte Prozesse zur Erkennung unbefugter Zugriffe und eine entsprechende Reaktion darauf im industriellen Kontext und automatisiert „Security along the Lifecycle“-Konzepte für Industrieanlagen. Cybersicherheit ist eines unserer wichtigsten Kerntechnologie- und Forschungsgebiete.

Siemens ist ein Mitglied von FIRST, dem Dachverband für alle CERTS (Cyber Emergency Response Teams). Wir unterhalten zudem enge Beziehungen zu nationalen CERTS (wie US-CERT, EU-CERT und ICS-CERT) und Strafverfolgungsbehörden (wie dem FBI, BKA, Europol und DHS), und wir sammeln Bedrohungsinformationen und verbreiten sie über diese Allianzen. Wir haben uns mit Partnern zusammengeschlossen,



**Charter
of Trust**

SIEMENS

Ingenuity for life

um industrielle IT und Standards zu entwickeln und kooperieren mit Universitäten, Geschäftspartnern, Kunden, Start-ups und angesehenen Forschungsinstituten, um gemeinsam an Innovationen im Bereich Cybersicherheit zu arbeiten.

Kurzum: Mit diesem einzigartigen und vielfältigen Know-how sowie den umfassenden Technologielösungen für Cybersicherheit ist Siemens ein zuverlässiger und bevorzugter Partner für Kunden, die ein Höchstmaß an Cybersicherheit für ihre Systeme anstreben – von Fabriken über Stromnetze bis hin zur Gesundheitsversorgung.

Ansprechpartner für Journalisten

Florian Martini

Tel.: +49 89 636 33446;

E-Mail: florian.martini@siemens.com

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