Charter of Trust erzielt deutlichen Fortschritt bei Cyber-Sicherheit

Neue Partner: Bundesamt für Sicherheit in der Informationstechnik, National Cryptologic Center und Technische Universität Graz treten Charter bei/ Zulieferer im Fokus: Partner wollen Cyber-Sicherheit in ihren globalen Lieferketten etablieren/ Ziele für 2019: künftig nur noch Produkte mit vorab implementierter Cyber-Sicherheit, mehr Aus- und Weiterbildung bei IT-Sicherheit

München, Deutschland - 15 Feb 2019: 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. Ein Jahr nach Unterzeichnung ist die Charter of Trust auf 16 Mitglieder angewachsen. Zum Dokument verpflichten sich neben Siemens und der Münchner Sicherheitskonferenz die Unternehmen Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, Enel, IBM, MSC, NXP, SGS und TÜV SÜD. Erstmals treten nun mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem National Cryptologic Center (CCN) aus Spanien zwei Regierungsbehörden der Charter bei. Zudem wird die Technische Universität Graz Mitglied der Initiative.

Die TU Graz ist seit Langem in der Cybersicherheits-Forschung engagiert und hat im Jahr 2018 die IT-Sicherheits-Lücken „Meltdown“ und „Spektre“ mitentdeckt. Die neuen Mitglieder werden dabei als assoziierte Partner aufgenommen – das ist ein neues Format, mit dem sich die Charter nun auch für Regierungsstellen, Universitäten und Forschungseinrichtungen öffnet. Ein Vorteil für solche Organisationen ist, dass sie mit den Partnern der Charter of Trust an konkreten Projekten zusammenarbeiten können, ohne Vollmitglied mit allen Rechten und Pflichten werden zu müssen.

„Im Zeitalter des Internet ist Cyber-Sicherheit eine grundlegende Aufgabe. Die Charter of Trust ist ein erster sehr wichtiger Schritt“, sagt Joe Kaeser, Vorstandsvorsitzender von Siemens. „Wir sind offen für weitere Partner. Cyber-Sicherheit ist das Schlüsselelement für eine erfolgreiche Digitalwirtschaft und für den Schutz kritischer Infrastrukturen. Wir hoffen, dass die Charter zu einer lebhaften öffentlichen Diskussion zum Thema Cyber-Sicherheit führt – und künftig zu verbindlichen Standards und Regeln.“

Im Oktober 2018 haben die Partner zudem grundsätzliche Anforderungen für die Cyber-Sicherheit digitaler Lieferketten erarbeitet. Diese Anforderungen betreffen technische Merkmale und organisatorische Maßnahmen, die für Produkte und Dienstleistungen und ebenso für die entsprechende IT-Infrastruktur relevant sind. Zu den Anforderungen gehören etwa der Schutz von Daten über ihren gesamten Lebenszyklus hinweg oder Mindestanforderungen für die Ausbildung von Mitarbeitern im Bereich IT-Sicherheit. Die Mitglieder der Charter planen, diese Aufgaben in ihren eigenen globalen Lieferketten einzuführen und dabei die Lieferanten einzubinden. Die Lieferkette gilt als der schwächste Punkt im Cybersecurity-Ökosystem von Unternehmen: 60 Prozent der Cyber-Attacken lassen sich im Ursprung auf Teile der Lieferketten zurückverfolgen und kleine Unternehmen sind laut Accenture Strategy für 92 Prozent der Cyber-Vorfälle verantwortlich.

Im Jahr 2018 haben weltweite Diskussionsrunden der Charter of Trust einen intensiven Austausch zwischen den Charta-Partnern und der Politik ermöglicht. Global ist das Thema Cyber-Sicherheit nun ein fester Bestandteil der politischen Agenda: Der im November vom französischen Staatspräsidenten Emmanuel Macron vorgestellte „Pariser Aufruf zu Vertrauen und Sicherheit im Cyberspace“ lehnt sich an die Prinzipien der Charter of Trust an und bekräftigt die Bereitschaft, gemeinsam an internationalen Standards zur Cyber-

Sicherheit zu arbeiten. Für das Jahr 2019 hat sich die Charter of Trust ehrgeizige Ziele gesetzt. Zusätzlich zur weiteren Vertiefung und zum Ausbau des politischen Dialogs sollen die Themen „Cybersecurity by Default“ und „Education“ vorangetrieben werden – also die vorausschauenden Cyber-Sicherheitseinstellungen beispielsweise eines Produkts und globale Weiterbildungsmaßnahmen in- und außerhalb der Unternehmen.

Laut dem Center for Strategic and International Studies richteten Cyber-Angriffe im Jahr 2018 einen weltweiten Schaden von mehr 500 Milliarden Euro an. Und die Bedrohungen nehmen in einer digitalisierten Welt ständig zu: Laut Gartner waren im Jahr 2017 rund 8,4 Milliarden vernetzte Geräte in Gebrauch – das sind 31 Prozent mehr als 2016. Bis 2020 sollen es bereits 20,4 Milliarden sein.

Die Charter of Trust im Wortlaut finden Sie hier.

Über die Siemens AG
Die Siemens AG 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 Elektrifizierung, Automatisierung und Digitalisierung. Siemens ist einer der größten Hersteller energieeffizienter ressourcenschonender Technologien. Das Unternehmen ist außerdem einer der führenden Anbieter effizienter Stromerzeugungs- und Stromübertragungslösungen, Pionier bei Infrastrukturlösungen sowie bei Automatisierungs-, Antriebs- und Softwarelösungen für die Industrie. Darüber hinaus ist das Unternehmen mit seiner börsennotierten Tochtergesellschaft Siemens Healthineers AG ein führender Anbieter bildgebender medizinischer Geräte wie Computertomographen und Magnetresonanztomographen sowie in der Labordiagnostik und klinischer IT. Im Geschäftsjahr 2018, das am 30. September 2018 endete, erzielte Siemens einen Umsatz von 83,0 Milliarden Euro und einen Gewinn nach Steuern von 6,1 Milliarden Euro. Ende September 2018 hatte das Unternehmen weltweit rund 379.000 Beschäftigte. Weitere Informationen finden Sie im Internet unter www.siemens.com.

Über IBM
IBM betreibt eine der weltweit größten Forschungs-, Entwicklungs- und Bereitstellungsorganisationen für Sicherheit. Sie überwacht weltweit rund 60 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hat weltweit mehr als 8.000 Sicherheitspatente erhalten. Mehr als 8000 Mitarbeiter weltweit im Bereich Security und neun X-Force Command Center, aus denen Managed Security Services erbracht werden, ermöglichen es, auch auf individuelle Compliance-Anforderungen, zum Beispiel Service-Erbringung aus dem Europäischen Wirtschaftsraum, einzugehen.

Mehr Informationen finden Sie unter http://www.ibm.com/de
sowie auf dem IBM Unternehmensblog IBM THINKBlogDACH.

Kontaktinformation

Annette Fassnacht

Unternehmenskommunikation IBM Deutschland 0160 90105052 annettefassnacht@de.ibm.com

https://de.newsroom.ibm.com/2019-02-15-Charter-of-Trust-erzielt-deutlichen-Fortschritt-bei-Cyber-Sicherheit