Cybersicherheit

Company Core Technology

Hintergrund

Im digitalen Zeitalter ist Cybersicherheit die Grundvoraussetzung für Unternehmen, um kritische Infrastrukturen und sensible Daten zu schützen und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Es gibt keine Digitalisierung der Industrie (Industrie 4.0) ohne ein hohes Maß an Vertrauen und einem funktionierenden Regelwerk für Cybersecurity.

- Im Jahr 2016 wurde der durch Cybersicherheitsvorfälle verursachte weltweite wirtschaftliche Schaden auf 330 bis 560 Milliarden Euro geschätzt. In bestimmten europäischen Ländern beläuft sich dieser Schaden auf 1,6 Prozent des Bruttoinlandsprodukts (ENISA Threat Landscape Report 2016 (Report zur Bedrohungslandschaft)).
- Das Risiko für Bedrohungen durch Hacker wächst: 2017 werden 8,4 Milliarden vernetzte „Dinge“ in Gebrauch sein - das sind 31 Prozent mehr als 2016. Bis 2020 wird diese Zahl auf 20,4 Milliarden steigen.

  (Gartner, Januar 2017, http://www.gartner.com/newsroom/id/3598917)
- Die Betreiber kritischer Infrastrukturen wie Telekommunikations- oder Stromnetzen unterliegen hohen rechtlichen Sicherheitsanforderungen. Um diese Anforderungen erfüllen zu können, sind sie von ihren Lieferanten abhängig. In einer künftigen hyper-vernetzten Welt unterliegen die meisten Geräte und Systeme höheren Anforderungen, weil immer mehr von ihnen als kritisch eingestuft werden – etwa bei den Themen autonomes Fahren und Mensch-Roboter-Zusammenarbeit.

Cybersicherheit ist mehr als Technologie: Es muss in die DNS eines jeden Unternehmen und jedes Einzelnen. Jeder, der sichere Produkte und Systeme an den Markt bringen möchte und Cybersicherheit über deren gesamten Lebenszyklus aufrechterhalten will, benötigt eine umfassende Cybersicherheitsstrategie, die klar ausgearbeitet und in der gesamten Organisation konsequent umgesetzt wird.

Bedeutung für Siemens

Cybersicherheit hat bei Siemens oberste Priorität. Wir schützen unsere Daten mit dem höchstmöglichen Grad an Sicherheit. Wir möchten hier mit gutem Beispiel vorangehen und haben deswegen eine Charta of Trust erarbeitet, die unser Commitment zu Cybersecurity festhält.

Siemens sorgt für maximale Sicherheit seiner Assets und bietet Produkte und Lösungen mit diesen Sicherheitsstandards an. Siemens tut dies, indem es die Informationssicherheit und den Schutz vor Industriespionage, Denial-of-Service

und Angriffen durch bösartige Software gewährleistet. Darüber hinaus stellt das Unternehmen die Verfügbarkeit von (kritischen) Infrastrukturen sicher.

Die Fähigkeit, Kunden mit sicheren Produkten und Systemen beliefern zu können, ist ein Wettbewerbsvorteil in einem wachsenden Markt. Siemens mit seiner einmaligen Kombination von technischem Know-how im Bereich Cybersicherheit und umfassendem Domänenwissen ist ideal aufgestellt, um diese Chance zu nutzen – führend am Markt und als Vordenker.

Weiterführende Informationen

siemens.com/innovationday
siemens.com/presse/inno2017

Erfolgsgeschichten und Forschungsschwerpunkt

Siemens hat weltweit etwa 570 Cybersicherheitsexperten. Dazu gehören etwa 25 „weiße" Hacker, die kontinuierlich die Sicherheit der internen IT-Systeme sowie der Produkte, die an Kunden ausgeliefert werden sollen, überprüfen.

Cybersicherheit ist für Siemens kein neues Thema. Das erste IT-Sicherheitsteam bei Siemens wurde bereits 1986 – vor gut 30 Jahren – in der zentralen Forschungsabteilung Corporate Technology eingerichtet.

Siemens betreibt drei globale Cyber Defense Centers in Lissabon, Portugal, in Milford (Ohio), USA und in Suzhou, China. Von hier aus überwacht das Unternehmen seine eigenen Infrastrukturen und Fertigungseinrichtungen sowie Produktionsstätten und Einrichtungen in aller Welt hinsichtlich Cyberbedrohungen, warnt sie bei Sicherheitsvorfällen und koordiniert proaktive Gegenmaßnahmen.

Insbesondere bietet Siemens Plant Security Services an. Dazu gehören die Bewertung von Sicherheitsrisiken in Fabriken und Produktionsanlagen sowie die Umsetzung von Sicherheitsmaßnahmen für unsere Kunden, z.B. der Einsatz von Antiviren-Software, Sicherheitstrainings, Firewall-Management, Antivirus-Management und Incident-Bearbeitung.

In ähnlicher Weise bietet Siemens Cybersicherheitsdienste für Versorger und Stromnetzbetreiber an, und zwar einschließlich Bewertung des aktuellen Systems, Implementierung, Testen und Wartung von Sicherheitsupgrades.

Siemens Healthineers bietet Virenschutz für Tomographen und andere bildgebende Produkte, die für die Fernwartung mit dem Internet verbunden sind.

Forschungsschwerpunkte sind unter anderem: getestete und „gehärtete" Komponenten für alle Geschäftsbereiche zur Verfügung zu stellen, automatisierte Prozesse für die Erkennung von Angriffen zu entwickeln und darauf im industriellen Kontext reagieren zu können sowie automatisierte "Security for Lifecycle"-Konzepten für Industrieanlagen zu entwickeln.