Charter
of Trust

Charter of Trust

zur Cybersicherheit

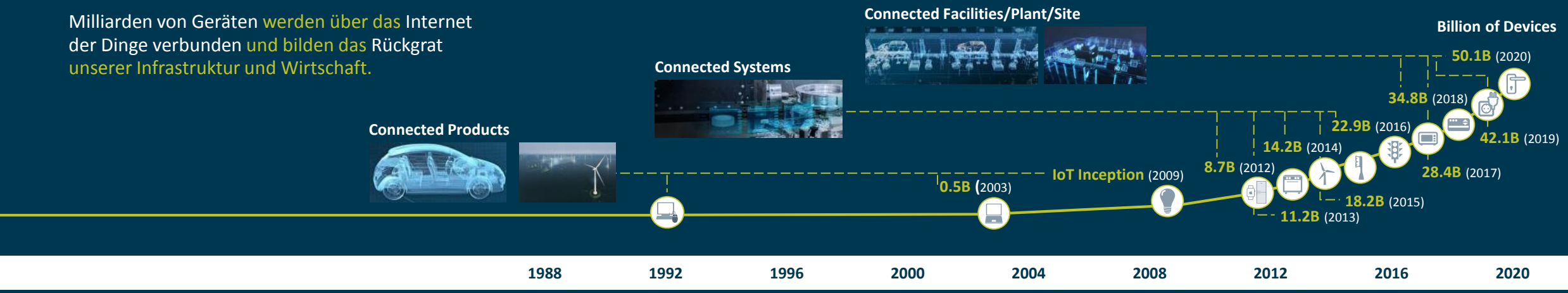
Die Digitalisierung schafft Möglichkeiten und Risiken

Charter of Trust

Die Digitalisierung schafft

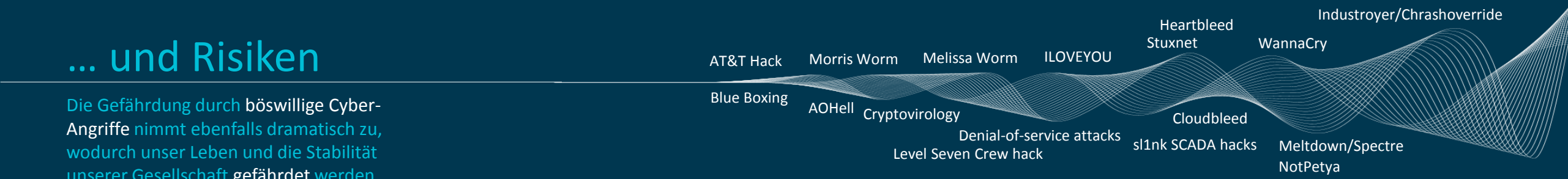
Möglichkeiten

Milliarden von Geräten werden über das Internet der Dinge verbunden und bilden das Rückgrat unserer Infrastruktur und Wirtschaft.



… und Risiken

Die Gefährdung durch böswillige Cyber-Angriffe nimmt ebenfalls dramatisch zu, wodurch unser Leben und die Stabilität unserer Gesellschaft gefährdet werden.



Charter of Trust

Und es stimmt:

Wir können nicht erwarten, dass Menschen die Digitalisierung aktiv unterstützen, wenn sie nicht auf die Sicherheit ihrer Daten und Systeme **VERTRAUEN** können.

Charter of Trust

Deshalb haben wir gemeinsam mit starken Partnern die Charta of Trust unterzeichnet – mit dem Ziel, drei wichtige Ziele zu erreichen:

1. **Die Daten von Einzelnen und Unternehmen** zu schützen

2. **Menschen, Unternehmen und Infrastrukturen** vor Schaden zu bewahren

3. **Ein zuverlässiges Fundament zu schaffen,** auf dem das Vertrauen in eine vernetzte digitale Welt verankert ist und wachsen kann

Charter of Trust

Und wir haben zehn Schlüsselprinzipien entwickelt und festgelegt:

01 **Verantwortung für Cyber- und IT-Sicherheit verankern**

02 **Verantwortung in der digitalen Lieferkette übernehmen**

03 **Cybersicherheit als Werks-einstellung konfigurieren**

04 **Bedürfnisse der Nutzer in den Mittelpunkt stellen**

05 **Innovation und Co-Creation vertiefen**

06 **Cybersicherheit zum festen Teil der Ausbildung machen**

07 **Kritische Infrastrukturen und IoT-Lösungen zertifizieren**

08 **Transparenz und Reaktionskraft steigern**

09 **Regulatorischen Rahmen schaffen**

10 **Gemeinsame Initiativen vorantreiben**

Charter of Trust

Für eine sichere digitale Welt

Charter of Trust

Und wir setzen sie um

Prinzip 1 — Verantwortung für Cyber- und IT-Sicherheit verankern

Unser Siemens-Ansatz für eine **neue Cybersicherheitsorganisation**

Unsere Vision

Für unsere Gesellschaft, unsere Kunden und unser Unternehmen sind wir
ein vertrauensvoller Partner in der digitalen Welt
durch die Bereitstellung von branchenführender Cybersicherheit
Zusammen machen wir Cybersicherheit real, weil es darauf ankommt

Unser ganzheitlicher Ansatz

Schutz unserer **IT- und OT-Infrastruktur**

Schutz unserer **Produkte, Lösungen und Dienstleistungen**

Cybersicherheits-lösungen für unsere Geschäfte anbieten

Konkrete Implementierungsschritte bei Siemens

Im Januar 2018 haben wir bei Siemens eine **neue Einheit für Cybersicherheit** unter der Leitung von Natalia Oropeza, **Chief Cybersecurity Officer** (CCSO), eingerichtet. Sie berichtet in dieser Funktion direkt an den Vorstand der Siemens AG. Mit dieser neuen Position erfüllen wir bereits eine der zentralen Forderungen aus der Charter of Trust.

»Cybersicherheit ist mehr als eine Herausforderung. Es ist eine große Chance. Indem wir mit einem engagierten und globalen Team Standards setzen, um die digitale Welt sicherer zu machen, investieren wir in die wertvollste Ressource der Welt: VERTRAUEN. Unsere konkreten Antworten auf die aktuellen Fragen der Cybersicherheit und unsere Vorschläge für weitergehende Cybersicherheitsregeln und -standards sind für unsere Partner, Stakeholder und Gesellschaften auf der ganzen Welt von unschätzbarem Wert. Das nennen wir »Ingenuity at work«.

Natalia Oropeza,
Chief Cybersecurity Officer, Siemens AG

Charter of Trust

Und wir setzen sie um

Prinzip 2 — Verantwortung in der digitalen Lieferkette übernehmen

Das Siemens-Security-Konzept
Defense in Depth

Konkrete Implementierungsschritte bei Siemens

Siemens stellt ein **mehrschichtiges Sicherheitskonzept** bereit, das Industrieanlagen **umfassend** und **weitreichend** schützt.

- Know-how und Kopierschutz
- Authentifizierung und Benutzer-management
- Firewall und VPN (Virtuelles Privates Netzwerk)
- Systemschutz und kontinuierliche Überwachung

Konkrete Implementierungsschritte mit CoT-Partnern

Gemeinsam mit unseren Partnern definieren wir eine Liste von **Mindestanforderungen für alle Akteure in der Lieferkette** und wirksame **Mechanismen**, die deren **Umsetzung unterstützen** können.

Charter of Trust

Nichtsdestotrotz

»Wir können es nicht allein schaffen.
Es ist höchste Zeit zu handeln –
gemeinsam mit starken Partnern,
die an ihren Märkten führend sind.«

Joe Kaeser
Initiator der Charter of Trust

Charter of Trust

Charter of Trust

charter-of-trust.de

Gemeinsam glauben wir fest daran:

— Effektive Cybersicherheit ist die Grundvoraussetzung für eine offene, faire und erfolgreiche digitale Zukunft.

— Durch die Einhaltung und Förderung unserer Grundsätze schaffen wir dafür eine neue Vertrauensbasis.

Denn als glaubwürdige und zuverlässige Stimme arbeiten wir mit wichtigen Stakeholdern weltweit zusammen, damit die Menschen in die Sicherheit ihrer Produkte und Lösungen vertrauen.

Charter of Trust

Werden Sie Teil eines **Netzwerks**, das nicht nur unterzeichnet, sondern **aktiv gemeinsam daran arbeitet**, mehr **Cybersicherheit zu schaffen**!

Lassen Sie uns Ihr **vertrauensvoller Partner** für mehr **Cybersicherheit** und **Digitalisierung** sein.

Gemeinsam werden wir unsere **Technologien** und **Prozesse** verbessern und **Menschen** hierfür gewinnen.

Schließen Sie sich uns an, indem Sie unsere **Prinzipien befolgen** und die **digitale Welt sicherer machen**.

Charter of Trust

Ihre Ansprechpartner für unsere gemeinsame Initiative

Chief Cybersecurity Officer (CCSO)
Natalia Gutierrez Oropeza
natalia.oropeza@siemens.com

»Charter of Trust«-Initiative
Eva Schulz-Kamm
eva.schulz-kamm@siemens.com

Globaler Koordinator für die
»Charter of Trust«-Initiative
Kai Hermsen
kai.hermsen@siemens.com

Ansprechpartner für die CoT-Kommunikation
Johannes von Karczewski
johannes.karczewski@siemens.com

Charter of Trust

Ein wesentlicher Faktor für den Erfolg der digitalen Wirtschaft

Grundprinzipien

Charter of Trust für eine sicherere digitale Welt

charter-of-trust.de

01 Verantwortung für Cyber- und IT-Sicherheit verankern

Die Verantwortung für Cybersicherheit ist auf höchster Regierungs- und Unternehmensebene zu verankern, indem eigene Ministerien und Chief Information Security Officer (CISO) benannt werden. Es gilt eindeutige Maßnahmen und Ziele zu definieren. Und wir wollen die richtige Mentalität etablieren – und zwar auf allen Ebenen. »Cybersicherheit ist jedermanns Aufgabe«.

02 Verantwortung in der digitalen Lieferkette übernehmen

Unternehmen und – falls erforderlich – Regierungen müssen risikobasierte Regeln etablieren, die einen adäquaten Schutz quer durch alle Ebenen des Internets der Dinge sicherstellen, mit eindeutig definierten und verbindlichen Anforderungen. Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit müssen sichergestellt werden, indem grundlegende Standards festgesetzt werden:

- **Identitäts- und Zugangsmanagement:** Vernetzte Geräte müssen sichere Identitäten haben und über Schutzmechanismen verfügen, die nur autorisierten Nutzern und Geräten erlauben, auf sie zuzugreifen
- **Verschlüsselung:** Vernetzte Geräte müssen – wo immer erforderlich – Vertraulichkeit bei der Datenspeicherung und Datenübertragung sicherstellen.
- **Kontinuierlicher Schutz:** Unternehmen müssen in einem angemessenen Rahmen für ihre Produkte, Systeme und Dienstleistungen Updates, Upgrades und Patches bereitstellen – und das über einen sicheren Update-Mechanismus.

03 Cybersicherheit als Werkseinstellung

Das höchstmögliche angemessene Maß an Sicherheit und Datenschutz ist anzuwenden, und dies muss beim Design von Produkten, Funktionalitäten, Prozessen, Technologien, betrieblichen Abläufen, Architekturen und Geschäftsmodellen vorkonfiguriert werden.

04 Die Bedürfnisse der Nutzer in den Mittelpunkt stellen

Unternehmen stellen Produkte, Systeme und Services sowie Beratungsleistungen auf Basis der Sicherheitsanforderungen ihrer Kunden bereit und stehen ihnen während eines angemessenen Lebenszyklus als vertrauenswürdiger Partner zur Verfügung.

05 Innovation und Co-Creation vertiefen

Das gemeinsame Verständnis zwischen Unternehmen und politischen Entscheidungsträgern über Cybersicherheits-Anforderungen und Regeln ist zu vertiefen, um Cybersicherheits-Maßnahmen kontinuierlich voranzutreiben und an neue Bedrohungen anzupassen. Vertraglich vereinbarte Partnerschaften von Staat und Privatwirtschaft sind zu fördern und zu unterstützen. Branchenspezifisches Wissen muss zusammengeführt werden.

06 Cybersicherheit zum festen Teil der Ausbildung machen

In Lehrpläne – als Studienfächer an Universitäten, in der beruflichen Ausbildung sowie bei Trainings – sind spezielle Kurse zur Cybersicherheit zu integrieren, um die Transformation künftiger benötigter Fähigkeiten und Berufsprofilen voranzutreiben.

07 Kritische Infrastrukturen und IoT-Lösungen zertifizieren

Unternehmen und – falls erforderlich – Regierungen müssen verpflichtende und unabhängige Third-Party-Zertifizierungen (auf Basis von zukunftssicheren Definitionen und insbesondere dort, wo Leib und Leben in Gefahr sind) für kritische Infrastrukturen und IoT-Lösungen etablieren.

08 Transparenz und Reaktionskraft steigern

Unternehmen müssen sich an einem Netzwerk für industrielle Cybersicherheit beteiligen, um neue Erkenntnisse und Informationen zu Angriffen und Vorfällen zu teilen. Dieses Engagement sollte über die derzeitige Praxis hinausgehen, die auf kritische Infrastrukturen fokussiert ist.

09 Regulatorischen Rahmen schaffen

Multilaterale Zusammenarbeit bei Regulierung und Standardisierung muss gefördert werden, um gleiche Ausgangsbedingungen für alle Beteiligten zu schaffen – vergleichbar mit der globalen Reichweite der Welthandelsorganisation (WTO). Regeln zur Cybersicherheit sollten auch Bestandteil von Freihandelsabkommen sein.

10 Gemeinsame Initiativen vorantreiben

Gemeinsame Initiativen mit allen relevanten Akteuren müssen vorangetrieben werden, um die genannten Prinzipien in den versch. Bereichen der digitalen Welt unverzüglich umzusetzen.

Charter of Trust