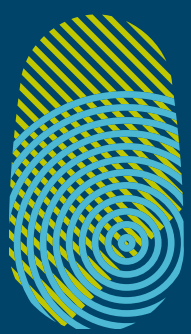
Cybersicherheit

Sicherheit schaffen in einer vernetzten Welt



Charter of Trust

Cybersicherheit

Charta für eine sichere digitale Welt

Die digitale Welt verändert alles. Künstliche Intelligenz und Big-Data-Analysen revolutionieren unsere Entscheidungsfindung; Milliarden von Maschinen werden über das Internet der Dinge (IoT) miteinander verbunden und interagieren auf einer völlig neuen Ebene und in nie da gewesenem Umfang.

Doch so sehr diese Fortschritte unser Leben und unsere Wirtschaft auch bereichern: **Das Risiko, aggressiven Cyberangriffen ausgesetzt zu sein, steigt gleichzeitig dramatisch.** Wenn die Systeme, die unser Zuhause steuern, unsere Krankenhäuser und Fabriken, unsere Stromnetze – also unsere gesamte Infrastruktur – gefährdet sind, drohen katastrophale Folgen für alle Lebensbereiche. **Deshalb müssen wir unsere wirtschaftlichen, gesellschaftlichen und demokratischen Werte vor Cyber- und Hybridbedrohungen schützen.**

Um einen anschaulichen Vergleich zu wählen: Cybersicherheit ist mehr als der Sicherheitsgurt oder Airbag, der uns schützt; sie ist entscheidend für den Erfolg der digitalen Wirtschaft. Menschen und Unternehmen müssen sich auf die Sicherheit ihrer digitalen Technologien verlassen können; andernfalls werden sie den Wandel hin zu einer digitalen Welt nicht mittragen. **Digitalisierung und Cybersicherheit müssen sich gemeinsam weiterentwickeln.**

Um mit der rasanten technologischen Entwicklung und den Bedrohungen durch kriminelle Elemente Schritt zu halten, **müssen Unternehmen und Regierungen an einem Strang ziehen und gezielt handeln. Sie müssen alles dafür tun, Daten und Vermögenswerte von Einzelnen und Unternehmen zu schützen, Menschen, Unternehmen und Infrastrukturen vor Schaden zu bewahren und eine zuverlässige Basis für das Vertrauen in eine vernetzte und digitale Welt zu schaffen.**

Es geht also darum, Vertrauen in die Cybersicherheit aufzubauen, sie in all ihren verschiedenen Gestaltungsebenen voranzutreiben und so der Digitalisierung den Weg zu bereiten. Dies kann aber nicht Aufgabe einzelner Unternehmen sein, sondern **muss in enger Zusammenarbeit aller relevanten Akteure angegangen werden. In dem vorliegenden Dokument skizzieren die Unterzeichner Schlüsselprinzipien für eine sichere digitale Welt – Prinzipien, die sie gemeinsam mit Gesellschaft, Politik, Geschäftspartnern und Kunden aktiv vorantreiben.**

AES · cisco · IBM · SIEMENS
AIRBUS · DAIMLER · msc · T
Allianz · DELL Technologies · NXP · TOTAL
Atos · enel · SGS · TÜV SÜD

Unsere Prinzipien

1 Verantwortung für Cyber- und IT-Sicherheit | 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".

2 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 es 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.

3 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.

4 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.

5 Innovation und Co-Creation | 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.

6 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 von künftig benötigten Fähigkeiten und Berufsprofilen voranzutreiben.

7 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.

8 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.

9 Regulatorischer Rahmen | 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 verschiedenen Bereichen der digitalen Welt unverzüglich umzusetzen.

charter-of-trust.com

Cybersicherheit geht uns alle an

5 Tipps für mehr Sicherheit

1 Halten Sie Hardware und Antivirensoftware auf dem neuesten Stand. Seien Sie vorsichtig bei unbekannten Apps.

· Internetfähige Geräte sollten immer auf dem aktuellen Stand sein.
· Installieren Sie Updates, sobald diese verfügbar sind.
· Installieren Sie möglichst keine unbekannten Apps.

2 Verwenden Sie für Ihre Konten unterschiedliche Passwörter und eine Zwei-Faktor-Authentifizierung.

· Lange, kryptische Passwörter mit Zahlen, Zeichen, Groß- und Kleinschreibung sind sicherer.
· Verzichten Sie auf einfache Zahlen- oder Zeichenfolgen, Klarnamen und komplette Wörter.
· Machen Sie Ihre Passwörter nicht anderen zugänglich, zum Beispiel durch Notizzettel.
· Setzen Sie auf eine Zwei-Faktor-Authentifizierung mit zusätzlicher Identifizierung, etwa durch einen SMS-Code.

3 Erkennen Sie betrügerische Mails und seien Sie vorsichtig bei Anhängen und Links.

· Misstrauen Sie E-Mails mit unangeforderten Informationen oder Anlagen sowie Nachrichten mit bekanntem Namen, aber unbekannter E-Mail-Adresse.
· Klicken Sie nicht auf Links, die in unbekannte E-Mails eingebettet sind. Mit dem Mauszeiger können Sie ohne Klicken den Pop-up-Text mit dem Link vergleichen.
· Öffnen Sie keine ausführbaren Dateien (.exe, .scr, .cpl, Zip-Dateien) oder Office-Dokumente, die Makros enthalten.
· Löschen Sie E-Mails von Diensten, die Sie nicht verwenden oder in der Regel nicht per E-Mail empfangen, etwa von Lieferdiensten, Banken, Telefonanbietern oder Hotels.
· Ignorieren Sie Aufforderungen, Software aus einer unbekannten Quelle zu installieren.

4 Akzeptieren Sie nicht jede Freundschaftsanfrage auf Social Media.

· Überprüfen Sie, ob Ihnen die Person bekannt ist und ob es sich tatsächlich um ebendiese handelt.
· Im Zweifel ignorieren Sie die Anfrage.

5 Machen Sie nur bestimmte Daten und Informationen zugänglich.

· Geben Sie nicht leichtfertig personenbezogene Daten preis.