Charter of Trust

Cyber-Sicherheit als Chance begreifen

Wie Sie Ihr Unternehmen effektiv schützen können – konkrete Maßnahmen für kleine und mittlere Unternehmen

Warum sind Sie besonders gefährdet?

In Zeiten globaler Vernetzung wird Cyber-Kriminalität zu einer immer größeren Herausforderung, die niemand übersehen kann. Die Daten und Fakten auf dieser Seite machen es deutlich sichtbar. Gerade kleine und mittlere Unternehmen sind besonders gefährdet. Doch das muss nicht sein: Mit einigen konkreten Maßnahmen können Sie entscheidende Schritte unternehmen, Ihr Unternehmen nicht nur sicherer zu machen, sondern auch neue Geschäftschancen zu erschließen. Diese Broschüre zeigt Ihnen wie. Lesen Sie weiter – auch immer aktuell unter:

www.charteroftrust.com/topics/education

43,4 Milliar

Gesamtschaden entstand deutschen Unternehmen durch Cyber-Kriminalität in den vergangenen zwei Jahren.[1]

68 %

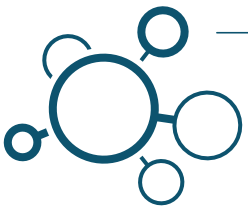
der Unternehmen mit 10 bis 99 Mitarbeitern waren in den vergangenen zwei Jahren Opfer von Spionage, Sabotage und Datendiebstahl.[2]

46 %

dieser Unternehmen wurden im gleichen Zeitraum durch digitale IT-Angriffe geschädigt.[3]

390.000

neue Schadprogrammvarianten, zum Beispiel Ransomware und Malware, werden täglich entdeckt.[4]

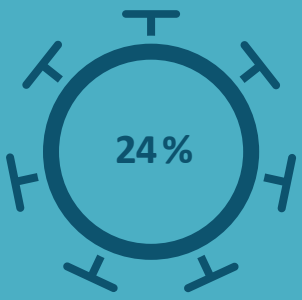


den Euro

Welche Rolle spielt der Mensch?

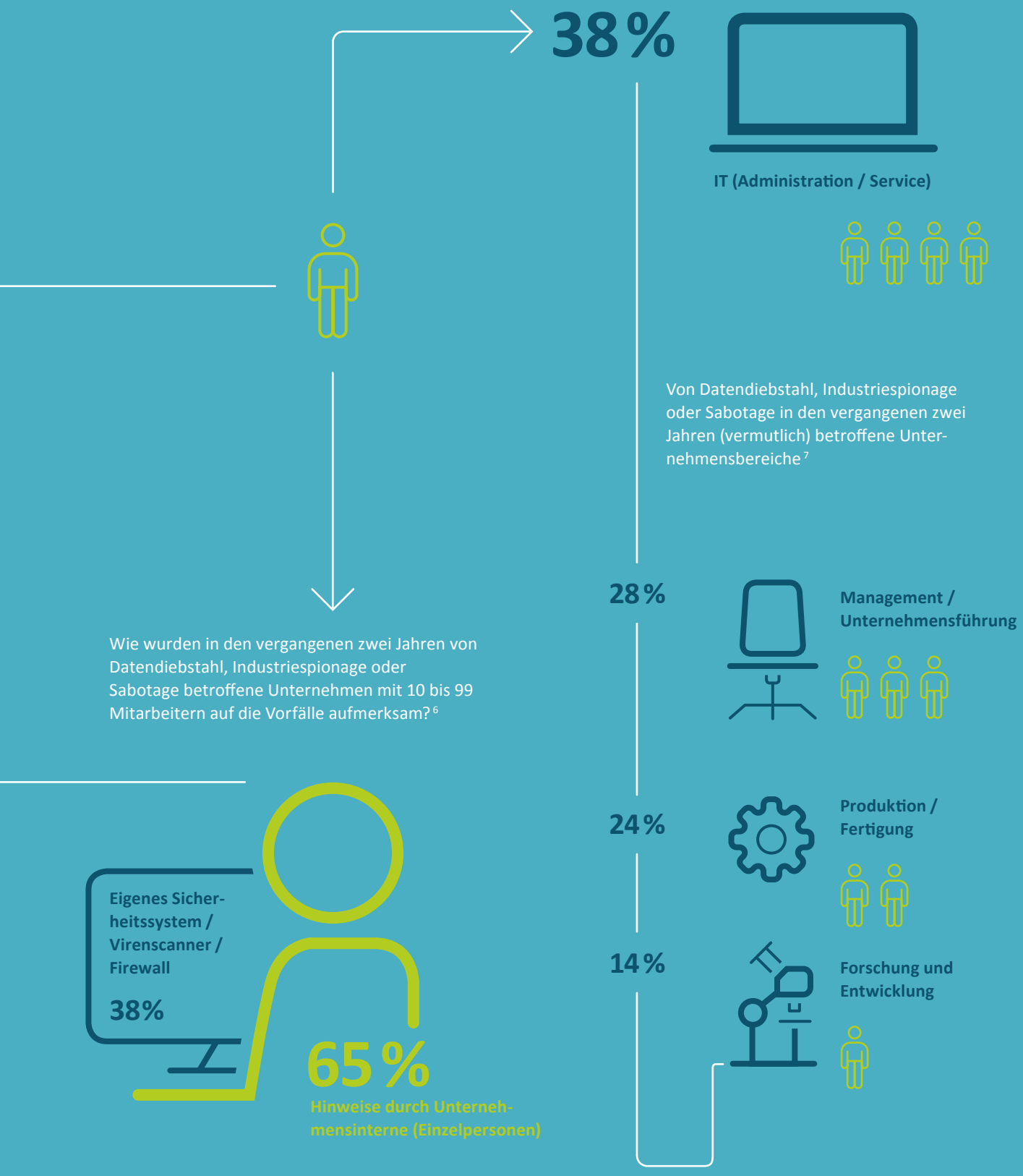
Cyber-Angriffe werden gerade in kleinen und mittleren Unternehmen zu einem Großteil von Mitarbeitern entdeckt. Der Faktor Mensch ist somit elementar. Wenn Sie Cyber-Sicherheit unternehmensweit in den Fokus rücken, Ihre Mitarbeiter entsprechend sensibilisieren und schulen, haben Sie eine wichtige Stellschraube zu mehr Cyber-Sicherheit in Ihrem Unternehmen gedreht. Denn ein bewusster und kritischer Umgang mit und in der digitalen Welt schafft Sicherheit und Vertrauen – und das zahlt sich aus. Das heißt im Gegenzug aber auch: Das größte Einfallstor für Cyber-Kriminelle ist nach wie vor der Mensch, der durch unachtsames Handeln Ihr Unternehmen in Gefahr bringen kann, wie die Zahlen dieser Seite unzweifelhaft dokumentieren. Also übernehmen Sie Verantwortung und schaffen Sie Bewusstsein, dann haben Sie den ersten wichtigen Schritt zu mehr Cyber-Sicherheit in Ihrem Unternehmen unternommen.

Ursachen für Schäden durch IT-Angriffe in den vergangenen zwei Jahren[5]



Schadsoftware bzw. Malware

Softwareschwachstellen	**16 %**
Phishing-Angriffe	**16 %**
Angriffe auf Passwörter	**12 %**
Spoofing	**6 %**
DDOS-Attacken	**5 %**
Man-in-the-Middle- oder Mittelsmann-Angriffe	**4 %**


38 %
IT (Administration / Service)
Von Datendiebstahl, Industriespionage oder Sabotage in den vergangenen zwei Jahren (vermutlich) betroffene Unternehmensbereiche [7]
28 %
Management / Unternehmensführung
24 %
Produktion / Fertigung
14 %
Forschung und Entwicklung
Wie wurden in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffene Unternehmen mit 10 bis 99 Mitarbeitern auf die Vorfälle aufmerksam? [6]
Eigenes Sicherheitssystem / Virenscanner / Firewall
38%
65 %
Hinweise durch Unternehmensinterne (Einzelpersonen)

Wie können Sie als kleines oder mittleres Unternehmen besonders von Cyber-Sicherheit profitieren?

Machen Sie Cyber-Sicherheit zu Ihrem Erfolgsfaktor.

In Zeiten zunehmender Digitalisierung und wachsender Vernetzung wird Cyber-Sicherheit zu einem echten Erfolgsgaranten. Denn Cyber-Sicherheit ist nicht nur eine Bedrohung, sondern, wenn sie konsequent vorangetrieben wird, eine echte Chance, Ihre eigene **Wettbewerbsfähigkeit** weiter zu steigern.

Konkret schafft konsequent gelebte Cyber-Sicherheit viele positive Effekte – und zwar für jedes Unternehmen: Sie sichert eine höhere **Zuverlässigkeit** im Hinblick auf Ihre Lieferketten, sie schützt Ihren laufenden Betrieb und stärkt Ihre **Vertrauenswürdigkeit** bei Ihren Kunden durch den verantwortungsbewussten Umgang mit deren sensiblen Daten. Durch diese Sicherheit steigern Sie die Qualität der von Ihnen gelieferten Produkte oder Leistungen, erhöhen damit die Attraktivität Ihrer Angebotspalette und stärken so Ihre Wettbewerbs-position auf den Märkten.

Zuverlässigkeit

+

Vertrauenswürdigkeit

=

Wettbewerbsfähigkeit

Ihre Cyber-Sicherheit lässt sich in drei Schritten verbessern

Cyber-Sicherheit ist eine komplexe Herausforderung, die nach zielgerichteten organisatorischen, technischen und personellen Maßnahmen verlangt. Vergleicht man diese Aufgabe mit dem Laufsport, so geht es dabei nicht um einen kurzen Sprint, sondern um einen Marathon. Doch auch der längste Weg beginnt mit dem ersten Schritt.

Deshalb haben wir die Broschüre in drei einzelne Schritte – wir nennen sie Phasen – gegliedert. Machen Sie sich mit uns auf den Weg. Sie werden schnell sehen, dass jeder einzelne Schritt Sie dem Ziel näherbringt.

Weitere wichtige Informationsquellen:

www.bsi.bund.de
www.allianz-fuer-cybersicherheit.de
www.bdi.eu/themenfelder/digitalisierung/cybersicherheit
www.enisa.europa.eu
www.weforum.org/centre-for-cybersecurity

Phase 1 Gefahren erkennen und Verantwortung übernehmen

- **A** Verantwortung leben
- **B** Bewusstsein für Sicherheitsrisiken schärfen
- **C** Cyber-Sicherheits-Kultur im Unternehmen prägen

Phase 2 Maßnahmen ergreifen und Sicherheit verankern

- **A** Cyber-Sicherheit in der Organisation verankern
- **B** Cyber-Sicherheit in Produkte und Leistungen einbetten

Phase 3 Aufstellung zu Cyber-Sicherheit transparent machen und Vorbild für andere sein

- A Eigene Cyber-Sicherheits-Aufstellung publik machen
- B Aktiv werden – auch außerhalb des eigenen Unternehmens

Phase 1 — A Verantwortung leben

Schaffen Sie klare Verantwortlichkeiten für Cyber-Sicherheit in Ihrem Unternehmen.

Das Thema Cyber-Sicherheit muss auf allen Ebenen wahrgenommen und gelebt werden – von der Produkt- und Leistungsebene über die Netzwerkebene bis hin zur Unternehmensebene, in der Lieferkette und beim Kunden. Ein ganzheitliches Sicherheitskonzept muss deshalb alle Ebenen des Unternehmens sowie die gesamte Lieferkette adressieren.

Dabei ist strategisch vorzugehen, denn die Risiken, die aus Cyber-Angriffen entstehen, können so massiv sein, dass sie im schlimmsten Fall sogar den Fortbestand Ihres eigenen Betriebs oder den Ihrer Kunden gefährden.

Um die einzelnen Maßnahmen richtig zu koordinieren, sind bereichs- und abteilungsübergreifende Verantwortlichkeiten festzulegen. **Machen Sie Cyber-Sicherheit zur Chefsache und schaffen Sie die Funktion eines Cyber-Security-Koordinators (beispielsweise eines Chief Information Security Officers),** der die Fäden unternehmensweit in der Hand hält. Zusätzlich müssen Sie Ihren Mitarbeitern, insbesondere aber Ihren Führungskräften klarmachen, dass sie die Hauptverantwortung für Cyber-Sicherheit in Ihrem Unternehmen tragen. **Cyber-Sicherheit muss zu den festgelegten Arbeitsinhalten und Stellenbeschreibungen des gesamten Managements gehören.**

Verantwortlichkeiten regeln und steuern

Jedes Unternehmen hat mehrere Ebenen, für die das Thema Cyber-Sicherheit relevant ist.

Ein ganzheitliches Sicherheitskonzept berücksichtigt nicht nur alle Ebenen des Unternehmens, sondern auch die gesamte Lieferkette.

Kundenunternehmen

Lieferkette

Lieferantenunternehmen

1 Die Unternehmensebene — Büronetzwerk (IT)
Kommunikation über Internet und Intranet, Management von Daten in lokalen und dezentralen (Cloud-) Systemen

2 Die produktive Ebene — Produktion, IT- / OT-Netzwerk
Datenverkehr und Kommunikation in den Produktionssystemen im IT- / OT-Netzwerk und teilweise in vernetzten Geräten (IoT, SCADA, …)

3 Die Produktebene — Produkte, Systeme, Komponenten
Bei der Herstellung von Software und Hardware, Produkten und Systemen werden Komponenten und Teilsysteme von Lieferanten hergestellt und an Kunden geliefert (Anforderungen an die Cyber-Sicherheit in der gesamten Lieferkette).

Phase 1 — B Bewusstsein für Sicherheitsrisiken schärfen

Rücken Sie die Risiken von Cyber-Attacken ins Zentrum Ihrer Aufmerksamkeit.

Die aus Cyber-Attacken resultierenden Gefahren gehören zu den betrieblichen Risiken. Deshalb müssen sie in das Risikomanagement Ihres Unternehmens Eingang finden. Verantwortlich dafür ist die Unternehmensleitung, gegebenenfalls mandatiert an den Koordinator für Cyber-Sicherheit oder Chief Information Security Officer. Führen Sie folgende Schritte durch:

Schritt 1:
Führen Sie eine vorausschauende, unternehmensweite Risikobewertung durch – insbesondere im Hinblick auf die Identifizierung kritischer Geschäftsprozesse und kritischer Daten.

Schritt 2:
Bewerten Sie die aktuelle Bedrohungslandschaft und das Risikobild Ihres Unternehmens. Dann legen Sie verbindlich die eigene Risikobereitschaft fest.

Schritt 3:
Entwickeln Sie einen unternehmensweiten Plan für Cyber-Sicherheits-Maßnahmen und -Resilienz sowie eine interne Kommunikationsstrategie und führen Sie diese für alle Abteilungen und Geschäftseinheiten ein. Orientieren Sie sich dazu an den weiteren Empfehlungen in dieser Broschüre (beispielsweise zur Cyber-Sicherheits-Kultur) sowie an den genannten Quellen und nehmen Sie bei Bedarf externe Dienstleister zu Hilfe.

Schritt 4:
Überwachen Sie die Effektivität der Cyber-Sicherheits-Maßnahmen und der Cyber-Resilienz des Unternehmens und berichten Sie die Erkenntnisse an die Geschäftsführung.

Wiederholen Sie den Risikomanagementzyklus regelmäßig.

Phase 1 — C Cyber-Sicherheits-Kultur im Unternehmen prägen

Schulen Sie Ihre Mitarbeiter und Führungskräfte regelmäßig zu Fragen der Cyber-Sicherheit.

Nach einer Untersuchung von Accenture gehen 60 Prozent der Cyber-Angriffe auf Unternehmen von fehlerhaftem Verhalten der eigenen Mitarbeiter aus. Allein diese hohe Zahl zeigt, wie wichtig es ist, die Belegschaft in Sachen Cyber-Sicherheit zu schulen. Mitarbeiter, die den Umgang mit Sicherheitsangriffen nicht gelernt haben, können und dürfen nicht im digitalen Raum Verantwortung für Ihr Unternehmen tragen.

Wenn Sie hier an entsprechenden Schulungen sparen, laufen Sie Gefahr, bei einer Attacke Ihr gesamtes Unternehmen zu gefährden. Aufmerksamkeit muss auch im Kollegenkreis sichergestellt werden, so wie im Privatbereich bei der sogenannten guten Nachbarschaft: Wachsame Nachbarn schützen gegen Einbrüche, wachsame Kollegen gegen Angriffe aus dem Cyberspace. Deshalb: Trainieren Sie mit Ihren **Mitarbeitern regelmäßig den richtigen Umgang mit Cyber-Sicherheit.** Schon mit einfachen Regeln können Sie das sichere Verhalten Ihrer Belegschaft im digitalen Raum erreichen.

Darüber hinaus ist es elementar wichtig, stets die unternehmensspezifischen Ansätze zu Cyber-Sicherheit weiterzuentwickeln. **Bilden Sie daher ausgewählte Mitarbeiter zu Cyber-Sicherheits-Experten fort.** Dazu bieten verschiedene Organisationen Trainings an, die Sie nutzen sollten.

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.

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.

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

- Internetfähige Geräte sollten immer auf dem aktuellen Stand sein.
- Spielen Sie Updates auf, sobald diese verfügbar sind.
- Laden Sie möglichst keine unbekannten Apps auf Ihre Hardware.

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.

Machen Sie nur bestimmte Daten und Informationen zugänglich.

- Geben Sie nicht leichtfertig personenbezogene Daten preis.
- Achten Sie darauf, welche Daten Sie innerhalb und außerhalb Ihres Unternehmens teilen.

Die ersten Schritte sind gemacht: Sie haben in Ihrem Unternehmen klare Verantwortlichkeiten für Cyber-Sicherheit geschaffen, in Ihrer Belegschaft das Bewusstsein für die Risiken aus Cyber-Angriffen geweckt und gestärkt sowie die Entwicklung einer Cyber-Sicherheits-Kultur gestartet.

Nun ist es Zeit für Phase 2:

Phase 2
Maßnahmen ergreifen und Sicherheit verankern

A **Cyber-Sicherheit in der Organisation verankern**

B **Cyber-Sicherheit in Produkte und Leistungen einbetten**

Phase 2 — A Cyber-Sicherheit in der Organisation verankern

Um die Cyber-Sicherheit in Ihrem eigenen Unternehmen zu stärken, gilt es, konkrete organisatorische Maßnahmen zu ergreifen. Diese sollten Sie zunehmend auch von Geschäftspartnern einfordern. Sie können sich dabei verstärkt auf die in der Charter of Trust definierten Mindestanforderungen beziehen.

Die intern zu ergreifenden Maßnahmen und die externen Mindestanforderungen ergeben zusammen einen guten Orientierungsrahmen, wie Sie Ihr Unternehmen optimal aufstellen können. Schwerpunkte sind Themen wie Datenschutz, Sicherheitsrichtlinien, Reaktion auf akute Cyber-Sicherheits-Vorfälle, physische Sicherheit, Datenintegrität, Zugangsverwaltung, Kundenservice und Schulungsmaßnahmen.

Erfahren Sie mehr:

Auf der Website der Charter of Trust finden Sie weitere Informationen zu den 17 Mindestanforderungen für Lieferanten unter:

www.charteroftrust.com


Integrität und Verfügbarkeit
Datenschutzbestimmungen
Sicherheitsrichtlinien
Standortsicherheit
Mindestanforderungen
Unterstützungsleistung
Zugang, Intervention, Transfer & Trennung
Training
Störfallreaktion

Phase 2 — B
Cyber-Sicherheit in Produkte und Leistungen einbetten

Gerade Unternehmen, die „smarte“ und netzfähige Produkte und Leistungen anbieten, sind durch Cyber-Attacken besonders stark gefährdet und müssen strengste Anforderungen an die eigene Cyber-Sicherheit erfüllen – und das von Anfang an. Schließlich finden Ihre Produkte und Leistungen unmittelbar Eingang in die Infrastruktur Ihrer Kunden.

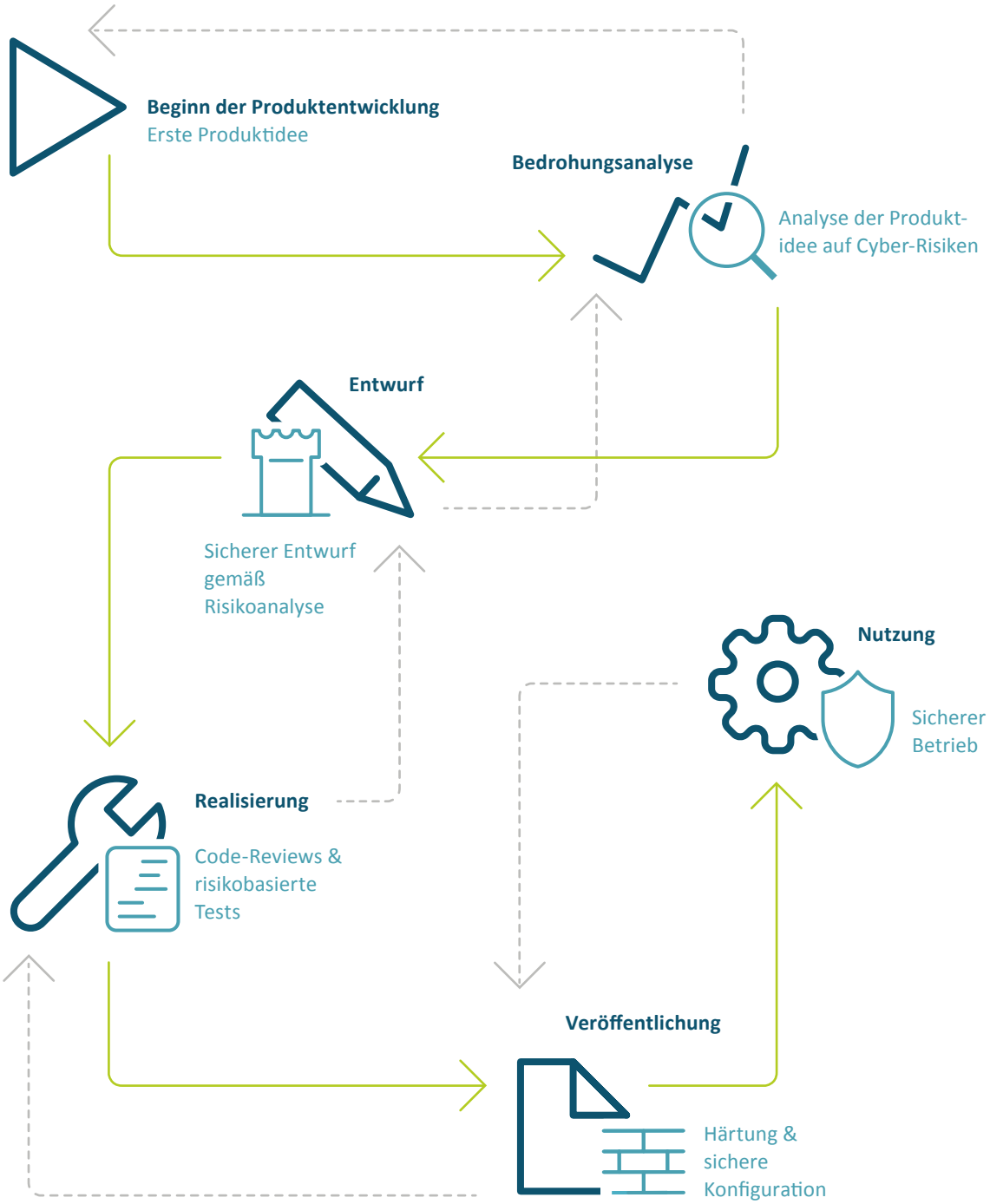
Ihr Ziel muss es daher sein, über den gesamten Produkt- und Leistungslebenszyklus wirkungsvolle Maßnahmen für Cyber-Sicherheit zu treffen – das Schlagwort lautet: „Security by Design“. Die Maßnahmen sind in Ihre bereits bestehenden Prozesse wie Produktmanagement, Forschung und Entwicklung, Projektmanagement, Kommissionierung, Betrieb und Service einzubauen. Dabei gilt es, die Bedürfnisse Ihrer Kunden in den Mittelpunkt zu stellen. Nur so schaffen Sie Vertrauen in Ihr Unternehmen.

Nachdem Sie „Security by Design“ in Ihre Prozesse integriert haben, geht es im nächsten Schritt darum, die gewählten Schutzmaßnahmen „per Werkseinstellung“ standardmäßig vorzukonfigurieren – Stichwort „Security by Default“. Mehr zu „Security by Design“ erfahren Sie im Folgenden.

Erfahren Sie mehr:

Auf der Website des Bundesamts für Sicherheit in der Informationstechnik (BSI) finden Sie zum Thema „Security by Design“ weiterführende Informationen:

https://bit.ly/2s6AssK


Beginn der Produktentwicklung
Erste Produktidee
Bedrohungsanalyse
Analyse der Produkt-idee auf Cyber-Risiken
Entwurf
Sicherer Entwurf gemäß Risikoanalyse
Nutzung
Sicherer Betrieb
Realisierung
Code-Reviews & risikobasierte Tests
Veröffentlichung
Härtung & sichere Konfiguration

Phase 2 der strategischen Verankerung von Cyber-Sicherheit im Unternehmen war schon recht umfangreich, Ihr Unternehmen sollte nun bereits ein höheres Maß an Cyber-Sicherheit erreicht haben.

Jetzt sollten Sie auch an die Außenwirkung Ihrer Maßnahmen denken. Um im Wettbewerb bestehen zu können und Ihren Kunden Ihre gute Aufstellung auf dem Gebiet der Cyber-Sicherheit sichtbar zu machen, sollten Sie nun – in Phase 3 – eine Zertifizierung anstreben und sich proaktiv für mehr Cyber-Sicherheit einsetzen.

Phase 3
Aufstellung zu Cyber-Sicherheit transparent machen und Vorbild für andere sein

A **Eigene Cyber-Sicherheits-Aufstellung publik machen**

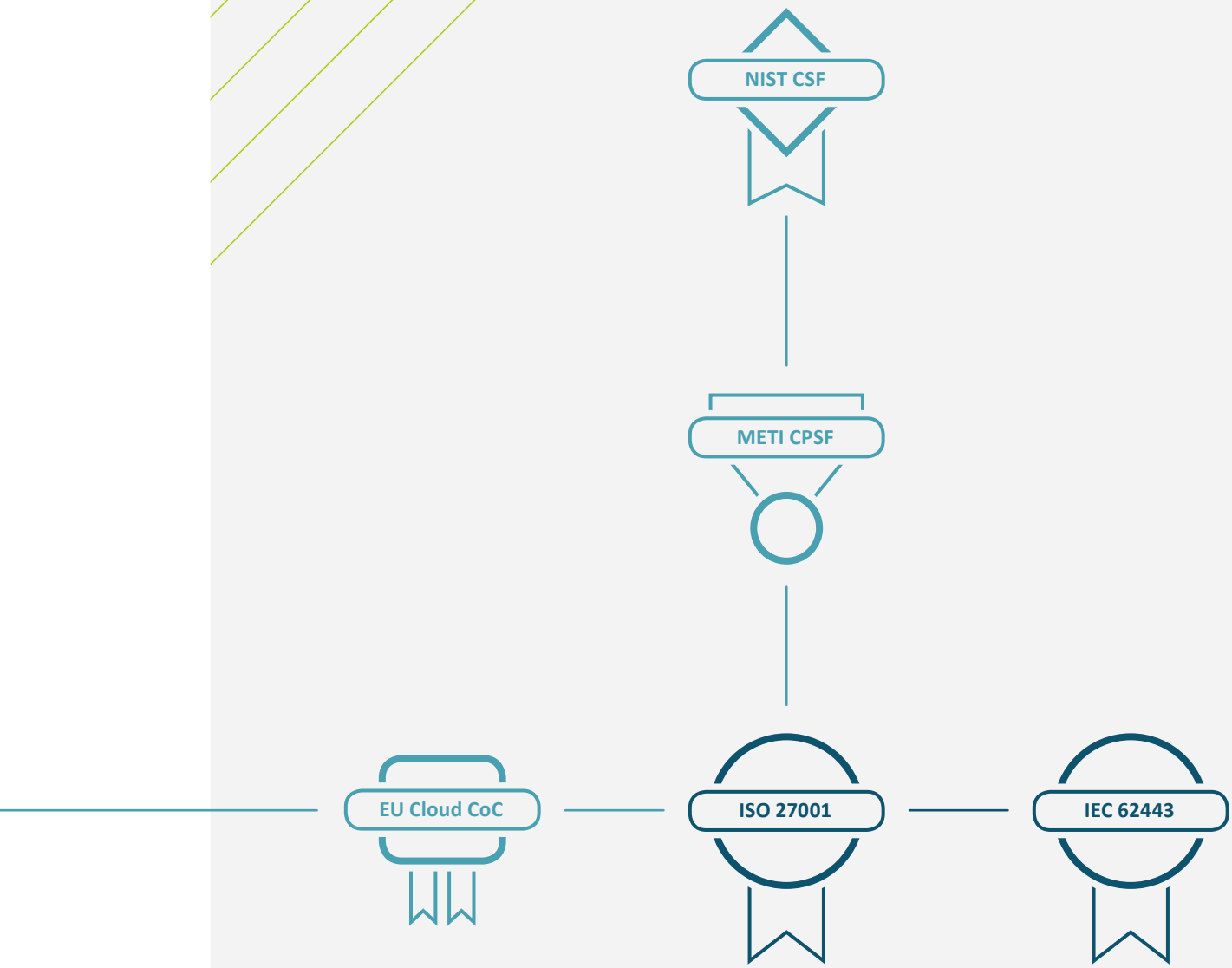
B **Aktiv werden – auch außerhalb des eigenen Unternehmens**

Phase 3 — A
Eigene Cyber-Sicherheits-Aufstellung publik machen

Ziehen Sie die Zertifizierung Ihrer Produkte und Geschäftsprozesse in Betracht.

Zeigen Sie Ihren Kunden, Lieferanten und Partnern, dass Ihr Unternehmen bestens gegen Cyber-Angriffe gewappnet ist, und lassen Sie dazu gegebenenfalls Ihre Produkte und Lösungen mithilfe etablierter Standards wie zum Beispiel IEC 62443 oder ISO 27001 zertifizieren.

Überprüfen Sie ungeachtet dessen regelmäßig die Sicherheit Ihrer Produkte, Dienstleistungen und Lösungen – auch zum Schutz Ihrer Partner und Kunden.



Erfahren Sie mehr:

IEC 62443:
www.isasecure.org/en-US

ISO 27001:
www.iso.org/isoiec-27001-information-security.html

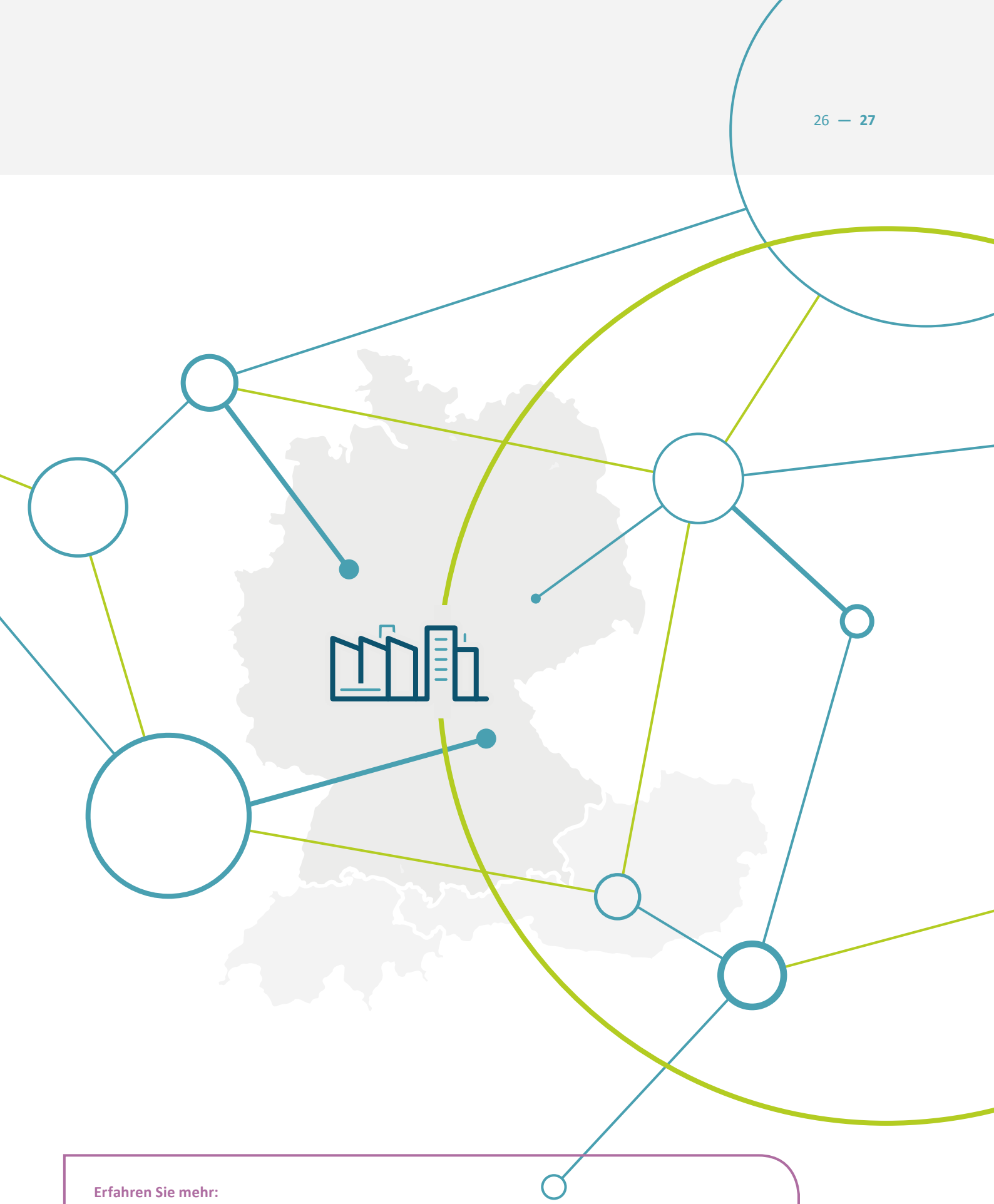
Phase 3 — B
Aktiv werden – auch außerhalb des eigenen Unternehmens

Ergreifen Sie die Initiative und stärken Sie die Zusammenarbeit in Cyber-Sicherheits-Fragen.

Cyber-Angriffe machen in der Regel weder an Unternehmensgrenzen noch an Landesgrenzen halt – im Gegenteil: Schnell können sie zu einer sich rasch ausbreitenden Bedrohung werden. Deshalb darf auch das Finden und Umsetzen von Lösungen nicht an den Unternehmens- oder Landesgrenzen zu Ende sein.

Nutzen Sie bestehende oder neue Foren, um sich zum Thema Cyber-Sicherheit auszutauschen. Mit seiner gestärkten Aufstellung im Bereich Cyber-Sicherheit kann Ihr Unternehmen zum Vorbild für andere werden und sich selbst im intensiven Austausch mit der öffentlichen Hand, Wissenschaft und Verbänden weiter stärken.

Nutzen Sie für diesen Austausch beispielsweise Ihre lokale Industrie- und Handelskammer.



Erfahren Sie mehr:

Gute Ansprechpartner sind die Industrie- und Handelskammern vor Ort:

www.ihk.de/datensicherheit

oder die zentralen Ansprechstellen für Cyber-Kriminalität der Polizeibehörden der Länder und des Bundes:

www.allianz-fuer-cybersicherheit.de

Charta für eine sichere digitale Welt

Im Februar 2018 haben auf der Münchner Sicherheitskonferenz Siemens und andere global tätige Industrieunternehmen eine gemeinsame Charta für mehr Cyber-Sicherheit ins Leben gerufen.

Die Charter of Trust hat zehn Prinzipien für mehr Cyber-Sicherheit vorgelegt (siehe Folgeseite), in denen Politik und Unternehmen gleichermaßen aktiv werden müssen. Denn so sehr die Digitalisierung unser Leben und unsere Wirtschaft auch bereichert: Das Risiko, aggressiven Cyber-Angriffen ausgesetzt zu sein, steigt gleichzeitig dramatisch. Deshalb müssen wir unsere wirtschaftlichen, gesellschaftlichen und demokratischen Werte vor Cyber-Bedrohungen schützen.

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 Organisationen 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.

www.charteroftrust.com


AES
AIRBUS
Allianz
Atos
CISCO
DELL
Technologies
IBM
infineon
msc
MITSUBISHI
HEAVY INDUSTRIES
NTT
NXP
SGS
SIEMENS
TOTAL
TÜV
SÜD

Zehn Prinzipien für eine sicherere digitale Welt

01

Verantwortung für Cyber- und IT-Sicherheit

Die Verantwortung für Cyber-Sicherheit 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. Cyber-Sicherheit 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 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 Automatismus.

03

Cyber-Sicherheit 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**
Das gemeinsame Verständnis zwischen Unternehmen und politischen Entscheidungsträgern über Cyber-Sicherheits-Anforderungen und -Regeln ist zu vertiefen, um Cyber-Sicherheits-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 **Cyber-Sicherheit zum festen Teil der Ausbildung machen**
In Lehrpläne – als Studienfächer an Universitäten, in der beruflichen Ausbildung sowie bei Trainings – sind spezielle Kurse zur Cyber-Sicherheit zu integrieren, um die Transformation von künftig benötigten 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 Cyber-Sicherheit 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 **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 Cyber-Sicherheit 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.

Impressum

Anschrift Siemens AG
Werner-von-Siemens-Str. 1, D-80333 München
Internet www.charteroftrust.com
Kontakt Telefon: + 49 (0) 89 636 - 33443
Telefax: + 49 (0) 89 636 - 30085
E-Mail: press@siemens.com

Redaktion & Text Dr. Johannes von Karczewski, Kai Hermsen
Konzept & Design hw.design GmbH
Lektorat Dr. Renate Öttinger, Ingrid Tzschaschel
Druck Gotteswinter und Aumaier GmbH

Quellen

[1-3] Bitcom e. V.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018. https://bit.ly/2rFcGUW
[4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung. https://bit.ly/2YHpRRf
[5-7] Bitcom e. V.: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018. https://bit.ly/2rFcGUW

Verhalten bei IT-Notfällen

Etablieren Sie für den Fall des Auftretens von Datendiebstahl, Industriespionage oder Sabotage ein Notfallmanagement – also schriftlich geregelte Abläufe und Ad-hoc-Maßnahmen.

Ruhe bewahren und IT-Notfall melden

IT-Notfallrufnummer:

Wer meldet?

Wie haben Sie mit dem System gearbeitet?
Was haben Sie beobachtet?

Welches System ist betroffen?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen

Beobachtungen dokumentieren

Maßnahmen nur nach Anweisung einleiten