Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung

Warum Cyber-Sicherheit immer wichtiger wird

Die zunehmende Digitalisierung und Vernetzung verändert Wirtschaft und Gesellschaft. Sie eröffnet einzigartige Möglichkeiten für Wachstum und Zukunftsfähigkeit durch neue Geschäftsmodelle. Die Geschwindigkeit und Komplexität des digitalen Wandels stellt Unternehmen aber auch vor eine Vielzahl von Herausforderungen.

Mit der exponentiellen Vernetzung von Daten, Objekten und Maschinen bei der Digitalisierung wächst die Angriffsfläche von Unternehmen und Kunden. Um die Chancen und Wachstumspotenziale der Digitalisierung zu realisieren, muss der IT- und Cyber-Sicherheit bei der Umsetzung digitaler Strategien hohe Priorität zukommen. Digitalisierung kann ohne IT-Sicherheit nicht erfolgreich sein.

DIGITALISIERUNG AKTIV GESTALTEN

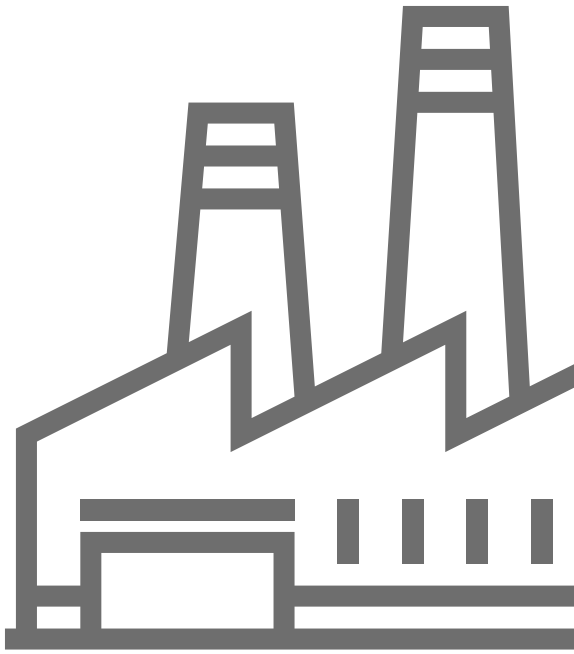
Digitale Geschäftsprozesse setzen großes Vertrauen voraus: Kunden verlassen sich darauf, dass ihre Daten bei den Unternehmen, mit denen sie interagieren, sicher sind. Wird dieses Vertrauen beschädigt, liegt die Verantwortung für die Konsequenzen in der Unternehmensführung. Und deshalb müssen Entscheider die Prozesse und Strukturen für die IT-Sicherheit unter Einbeziehung aller Abteilungen – von Management über Produktentwicklung bis hin zur IT-Organisation – aktiv vorantreiben.

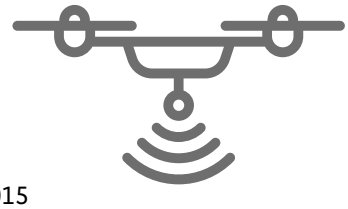
CYBER-SICHERHEIT STRATEGISCH BETREIBEN

Cyber-Sicherheit ist eine strategische Aufgabe und Teil des Risikomanagements in der Unternehmensführung. Sie ist weniger Option als vielmehr Pflicht, schon aus Gründen der Wettbewerbsfähigkeit. Unter Compliance-Aspekten und für Betreiber Kritischer Infrastrukturen im Rahmen des Cyber-Sicherheitsgesetzes sind hingegen auch gesetzliche Bestimmungen zu beachten.

Investitionen in die Cyber-Sicherheit sind Investitionen in die Zukunfts- und Wettbewerbsfähigkeit des Unternehmens. In einer vernetzten Welt sind Erfolg mit digitalen Geschäftsmodellen und Cyber-Sicherheit zwei Seiten der selben Medaille. Die Verantwortung für die Sicherheit liegt daher bei derselben Stelle wie die Verantwortung für den wirtschaftlichen Erfolg und die zukunftsweisende Strategie: bei der Unternehmensleitung.

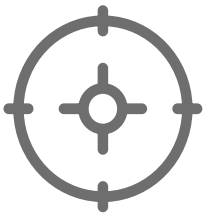
Investitionen in die Cyber-Sicherheit sind Investitionen in den Geschäftserfolg





69 %

Laut Bitkom waren 2014 und 2015 69 Prozent der Industrieunternehmen in Deutschland Opfer von Datendiebstahl, Spionage und Sabotage.



58 %

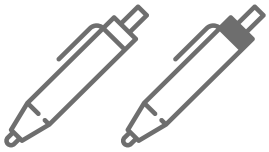
58 Prozent der Unternehmen und Behörden waren in den vergangenen zwei Jahren Ziel von Cyberangriffen (Umfrage des BSI Ende 2015).

243 Tage

Gezielte Cyber-Spionage (Advanced Persistent Threats) wird im Schnitt erst nach 243 Tagen entdeckt

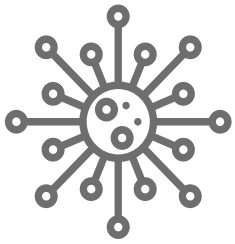
70 %

Laut VDMA sind 70 Prozent der Unternehmen von Produktpiraterie betroffen.



32 %

32 Prozent der deutschen Unternehmen waren nach einer Umfrage der Allianz für Cyber-Sicherheit Anfang 2016 in den vorangegangenen sechs Monaten von Ransomware betroffen.



390.000

Täglich werden rund 390.000 neue Schadprogramm-Varianten entdeckt.

41 %

In mehr als 41 Prozent aller Fälle von Industriespionage waren Computerhacker die Täter

(Corporate-Trust-Studie „Industriespionage 2014“).

€ 40

Die durchschnittlichen Kosten für eine DDoS-Attacke (Blockade durch Überlastung) liegen für die Angreifer bei rund 40 Euro pro Tag.

Wirtschaft im Fokus der Angriffe

Unternehmen in Deutschland sind und bleiben ein bevorzugtes Ziel von Cyber-Angriffen. Manche Firmen sind bei der IT-Sicherheit bereits gut aufgestellt, andere haben Nachholbedarf. Fast jedes Unternehmen ist ein mögliches Angriffsziel – viele merken nicht, dass sie angegriffen wurden.

Fast 70 Prozent aller Industrieunternehmen in Deutschland sind laut einer Umfrage des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) im Jahr 2015 Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden.

Betroffen sind Unternehmen aller Größen von Plagiaten, der Manipulation von Bieterverfahren, dem Diebstahl von Vertriebsinformationen sowie geistigem Eigentum. Das gilt insbesondere für den Mittelstand, der sich als Innovationsmotor in besonders hohem Maße durch Know-how, patentgeschützte Produkte und Lösungen auf höchstem Niveau auszeichnet. Dies zeigt einmal mehr, in welch engem Zusammenhang eine wirksame Sicherheitsstrategie mit Kerngeschäft, Prozessen und verschiedensten Abteilungen einer Organisation steht. Und es unterstreicht die Notwendigkeit von Cyber-Sicherheit als Chefsache.

„Wer der Cyber-Sicherheit in der Digitalisierung eine Nebenrolle zuweist, geht eine hochriskante Wette ein.“

Cyber-Erpressung durch Ransomware

Ransomware-Vorfälle machen deutlich, wie verwundbar viele Unternehmen sind. Neben Krankenhäusern und Stadtverwaltungen sind auch viele Unternehmen von dieser Erpressungsvariante betroffen. Eingeschleust wird der Schadcode meist durch einen E-Mail-Anhang, den ein Mitarbeiter öffnet. Die Folge: Daten und Festplatten werden verschlüsselt und damit unbrauchbar gemacht, Geschäftsprozesse sind beeinträchtigt.

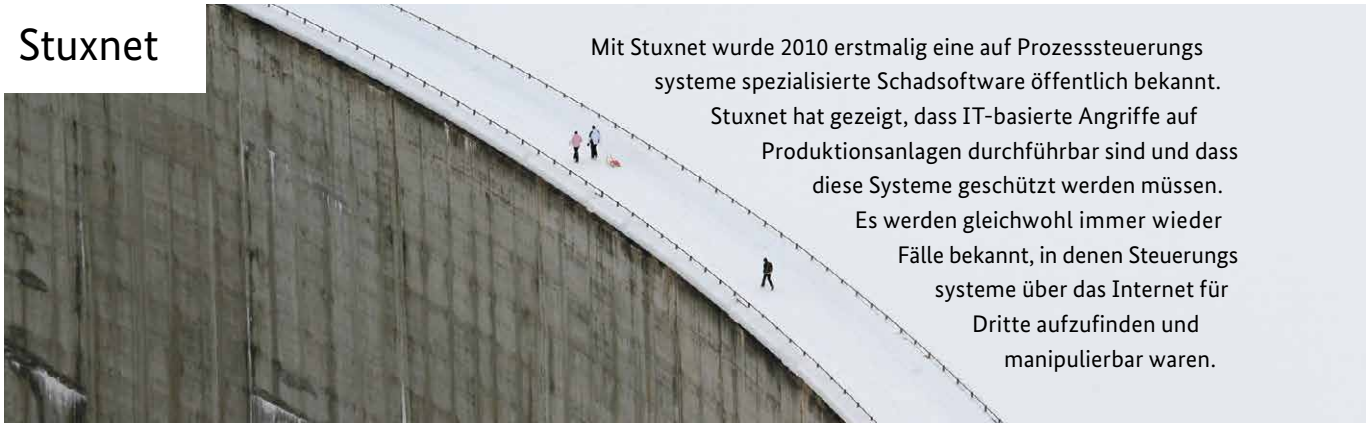
CEO-Betrug

Wie wichtig es ist, neben technischen Maßnahmen auch die Schwachstelle Mensch in das IT-Sicherheitskonzept einzubeziehen, zeigen Cyber-Angriffe, die man als „CEO-Betrug“ bezeichnet: Dabei gibt sich ein Angreifer in täuschend echten E-Mails als Mitglied der Unternehmensleitung aus und veranlasst einen Mitarbeiter, für ein vermeintliches Geheimprojekt einen hohen Geldbetrag auf ein fremdes Konto zu überweisen. Dafür spionieren die Betrüger ihre Opfer vorab aus und können dadurch unter anderem den Stil der Kommunikation im Unternehmen authentisch nachstellen. Die Kriminellen erbeuten dabei Euro-Beträge zum Teil in Millionenhöhe.

Cyber-Angriff auf den Bundestag

Anfang Mai 2015 wurde bekannt, dass zentrale Systeme des internen Bundestagsnetzes kompromittiert wurden. Gemeinsam mit einem externen Dienstleister untersuchte das hinzugerufene BSI den Vorfall. Die Täter waren anhand der klassischen APT-Methode vorgegangen, die von nahezu allen bekannten Cyber-Spionagegruppen angewandt wird. Dabei wurden zunächst einzelne Arbeitsplatzrechner mit einer Schadsoftware infiziert, über die die Angreifer jederzeit auf das System zugreifen konnten. Aufgrund der Analyse ist davon auszugehen, dass es die Täter unter anderem auf E-Mail-Postfächer abgesehen hatten.

Stuxnet



Mit Stuxnet wurde 2010 erstmalig eine auf Prozesssteuerungssysteme spezialisierte Schadsoftware öffentlich bekannt. Stuxnet hat gezeigt, dass IT-basierte Angriffe auf Produktionsanlagen durchführbar sind und dass diese Systeme geschützt werden müssen. Es werden gleichwohl immer wieder Fälle bekannt, in denen Steuerungssysteme über das Internet für Dritte aufzufinden und manipulierbar waren.

DAS BSI UND DIE WIRTSCHAFT

Gemeinsam Risiken minimieren

Damit die für den digitalen Wandel erfolgskritische Cyber-Sicherheit gewährleistet werden kann, müssen Wirtschaft und Staat vertrauensvoll zusammenarbeiten. Dafür baut das BSI die Zusammenarbeit sowohl mit den IT-Herstellern, als auch insbesondere mit den Anwendern von IT kontinuierlich aus.

Als nationale Cyber-Sicherheitsbehörde gestaltet das BSI die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft. Dies kann nur gelingen, wenn Staat und Wirtschaft zusammenarbeiten.

Durch eine vertrauensvolle Kooperation kann gemeinsam größtmögliche Cyber-Sicherheit erreicht werden. Der kooperative Ansatz wird vom BSI auf verschiedenste Weise umgesetzt, beispielsweise mit konkreten Angeboten wie das Einbinden der Wirtschaft in den Informationskreislauf zur Cyber-Gefährdungslage mit Lagebildern und Warnungen oder einen durch das BSI moderierten Austausch betroffener Unternehmen – und dies nicht nur im Bereich KRITIS.

Durch die starke Einbindung der IT-Anwender der Wirtschaft kann sich jedes Unternehmen engagieren und so von einer gestiegenen IT-Sicherheit profitieren.

„Ohne Cyber-Sicherheit wird Digitalisierung nicht erfolgreich sein.“

Angebote für die Wirtschaft

Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des BSI in Zusammenarbeit mit dem Bitkom. Der Allianz gehören bereits mehr als 1.800 Institutionen an, davon rund 100 Partner-Unternehmen und über 40 Multiplikatoren. Ziel der Allianz ist es, aktuelle und valide Informationen zu Gefährdungen im Cyber-Raum bereitzustellen und vor allem den Informations- und Erfahrungsaustausch zwischen den Teilnehmern zu fördern. Hierzu werden verschiedene Arbeitskreise wie zum Beispiel im Bereich Automotive eingerichtet. Damit soll die Cyber-Sicherheit in Deutschland erhöht und die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen gestärkt werden.

Seit Gründung steigt die Zahl der Partner, Multiplikatoren und Teilnehmer stetig an, sodass mit den Angeboten immer mehr Institutionen regelmäßig und dauerhaft erreicht werden. Dazu gehören neben dem Aufbau einer umfangreichen Wissensbasis und von Erfahrungs- und Expertenkreisen zur Cyber-Sicherheit auch Beiträge der Partner in Form von Schulungen, zusätzlichen Informationsveranstaltungen oder die kostenfreie Bereitstellung von Sicherheitsprodukten. Die Teilnahme an der Allianz für Cyber-Sicherheit ist kostenfrei und kann grundsätzlich durch jede deutsche Institution beantragt werden.

Allianz für Cyber-Sicherheit

https://www.allianz-fuer-cybersicherheit.de/

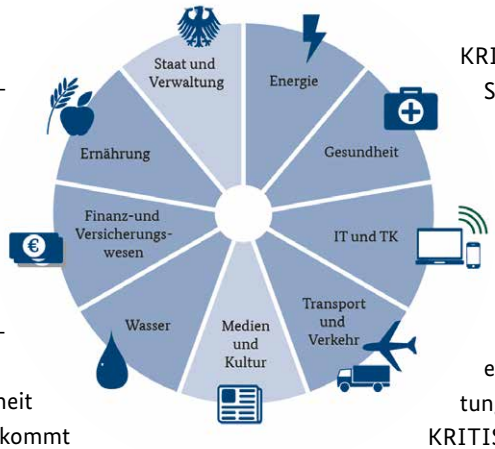
IT-Grundschutz

Der IT-Grundschutz des BSI ist der meist genutzte Standard für Informationssicherheit in Deutschland. Das etablierte Managementsystem für Informationssicherheit (ISMS) wird derzeit grundlegend überarbeitet. Ziele der Modernisierung sind unter anderem die bessere Strukturierung und Verschlankung der IT-Grundschutz-Kataloge, die Beschleunigung der Umsetzung von Sicherheitsmaßnahmen, die Flexibilisierung der Vorgehensweise sowie die stärkere Berücksichtigung von anwenderspezifischen Anforderungen. Im Zusammenhang mit dem IT-Sicherheitsgesetz und wegen der rasanten Zunahme von Vorfällen wie Ransomware verzeichnet das BSI ein stark steigendes Interesse der Wirtschaft am Thema IT-Grundschutz.

https://www.bsi.bund.de/IT-Grundschutz

UP KRITIS

Der UP KRITIS ist eine Kooperation zwischen den Betreibern kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Oberstes Ziel ist, durch die Zusammenarbeit, die Versorgung mit Dienstleistungen von kritischen Infrastrukturen wie beispielsweise Energie, Wasser oder Lebensmitteln sicherzustellen. Der Einschätzung der Cyber-Sicherheitslage und der Förderung der Robustheit kritischer Informationstechnik-Systeme kommt dabei überragende Bedeutung zu.



Durch das IT-Sicherheitsgesetz sind zahlreiche Betreiber kritischer Infrastrukturen gefordert, ihr IT-Sicherheitsniveau weiter zu erhöhen. Die Unternehmen, die die in der KRITIS-Verordnung festgelegten Schwellwerte erreichen, müssen einen Mindeststandard an IT-Sicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das BSI melden. Diese Meldungen werden vom BSI bewertet und schnellstmöglich allen Betreibern mit einer entsprechenden Aufbereitung zur Verfügung gestellt. Auch KRITIS-Betreiber, die nicht unter die Regelungen des IT-Sicherheitsgesetzes fallen, können im Rahmen des UP KRITIS freiwillige Meldungen abgeben und so von einer umfassenden Kooperation profitieren. Über 350 Unternehmen sind bereits Partner im UP KRITIS.

https://www.bsi.bund.de/kritis

Zertifizierung

Das BSI ist Weltmarktführer im Bereich der Zertifizierung für IT-Sicherheit. Bundesweit führen neun durch das BSI anerkannte Prüfstellen Zertifizierungen nach Common Criteria und entsprechend der Technischen Richtlinien durch. Dabei beziehen sich die Common Criteria ausschließlich auf die Sicherheitseigenschaften von Produkten, während bei den Technischen Richtlinien die Funktionalität und Interoperabilität im Fokus stehen. Im Auftrag der öffentlichen Hand werden unter anderem Dokumente wie der elektronische Personalausweis oder die Gesundheitskarte geprüft. In der freien Wirtschaft gilt eine BSI-Zertifizierung weltweit als Differenzierungs- und Qualitätsmerkmal für die Sicherheit von Produkten wie Lesegeräten, Firewalls oder Sicherheitselementen wie den Trusted-Platform-Modulen.

https://www.bsi.bund.de/zertifizierung

Mit dem BSI verbinden

Telefon: +49 228 999582-5977
E-Mail: info@cyber-allianz.de

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185 - 189
53175 Bonn
Tel.: +49 228 99 9582-0
E-Mail: bsi@bsi.bund.de

Layout und Gestaltung
Fink & Fuchs AG, Wiesbaden

Druck
Druck- und Verlagshaus Zarbock, Frankfurt am Main

Bildnachweis
Fotolia LLC, San Jose, CA 95110, USA

Stand
10/2016

Artikelnummer
BSI-MIBro16/802

www.bsi.bund.de