Leitfaden

Wirtschaftsschutz

75 %
der angegriffenen Unternehmen erleiden finanziellen Schaden [1]

50.000.000.000 €
Schadenspotenzial jährlich [1]

Jedes 4.
deutsche Unternehmen wird ausspioniert [1]

Jeder 5. Angriff wird nur
durch Zufall
entdeckt [4]

50 %
der Angriffe laufen über Mitarbeiter [2]

300.000
neue IT-Schadsoftware-varianten pro Tag [3]

KMU
im Fokus [1]

Und was tun Sie dagegen?

Nur 20 %
holen sich Hilfe durch Spezialisten [1]

60 %
der Angriffe erfolgen aus dem Ausland [2]

Unternehmenswerte richtig schützen

Mitarbeiter, Maschinen, Gebäude, Produkte, Dokumente (z. B. Kunden- und Preislisten), Entwicklungs-Know-how, Innovationen und vieles mehr sind Unternehmenswerte (Assets), die Sie vor Ausspähung schützen sollten. Sie gefährden sonst Ihre Wettbewerbsfähigkeit.

Finden Sie die wichtigsten Assets

Als Unternehmer wissen Sie am besten, welche Assets besonders schützenswert sind. Wie wichtig ist es für Ihren Betrieb, dass ein bestimmtes Asset funktioniert und geheim bleibt? Eine Analyse hilft Ihnen, dies festzulegen, zu priorisieren und adäquaten Schutz sicherzustellen.

Schutzwürdige Dokumente kennzeichnen

Handeln Sie beim Zugang zu Informationen nach dem Need-to-know-Prinzip. Teilen Sie nicht-öffentliche Dokumente in Schutzklassen ein und weisen Sie diese auf den Dokumenten aus. Dafür ist jeder Autor selbst verantwortlich.

Intern: Weitergabe nur im Betrieb
Vertraulich: Weitergabe nur an Berechtigte

Assets ordnen

Wenn Sie Ihre Unternehmenswerte ordnen, ist es leichter, die jeweils kritischen Assets herauszufinden.

Was ist für Ihren Betrieb unverzichtbar von Ihren...

- **Funktionen**
- **Abteilungen**
- **Informationen**
- **(IT-)Infrastrukturen**
- **Standorten und Gebäuden**

Mitarbeiter

Der wichtigste Wissensträger

Ihre Mitarbeiter sind Ihr wichtigster Unternehmenswert. Aufgrund ihres Wissens sind sie für Spione ein vielversprechendes Angriffsziel.

Tipps

- Informieren und sensibilisieren Sie sich und Ihre Mitarbeiter.
- Achten Sie auf die Motivation, Zufriedenheit und private Notlagen Ihrer Kollegen.
- Stellen Sie unternehmensinterne Regeln im Umgang mit Daten und Dritten auf und leben Sie diese vor!
- Fördern Sie eine Unternehmenskultur des guten Miteinanders.

Social Engineering...

ist eine Methode, die Ihre Mitarbeiter meist über zwischenmenschliche Beziehungen manipuliert und sie zur Preisgabe von Know-how bewegen kann. Sie wird z. B. auf Messen, Veranstaltungen, in sozialen Medien oder über fingierte E-Mails, inszenierte Forschungsangebote oder Headhunter-Kontakte eingesetzt.

Frustration am Arbeitsplatz

Ein schlechtes Arbeitsklima oder persönliche Notlagen machen Mitarbeiter zu einem leichten Angriffsziel. Sie können dadurch zum Innentäter werden.

50%
Innentäter [2]

"Zufriedene Mitarbeiter sind loyal und damit die wichtigste Sicherheitsmaßnahme."

50%
Außentäter

Mitarbeiter

Vorsicht auf Reisen

Besonders auf Auslandsreisen sind Mitarbeiter gefährdet, Opfer von Ausspähung zu werden. In einigen Ländern erlaubt die Rechtslage den gezielten Zugriff auf Ihre Daten, z. B. bei Einreisekontrollen, Kommunikation, Internetnutzung und durch Verschlüsselungsverbote.

Denken Sie daran, dass Ihre Mitarbeiter neben Ausspähung auch Opfer von Kidnapping, Erpressung, Diebstahl, oder anderen kriminellen Handlungen in Ländern mit fragiler Sicherheitslage werden können.

Tipps auf Reisen

- Informieren Sie sich schon vorab über die Sicherheits- und Rechtslage vor Ort.
- Hinterlassen Sie Ihre Kontaktdaten und Reisepläne bei Kollegen.
- Verwenden Sie nach Möglichkeit ein spezielles Reiseequipment, z.B. Prepaid Handys, Reise-Laptop.
- Nehmen Sie kritische Daten nur ausreichend verschlüsselt oder gar nicht mit.
- Seien Sie sich bewusst: im öffentlichen Raum kann jeder mithören und mitlesen.
- Schützen Sie Ihren Laptop mit Sichtschutzfolie.
- Nutzen Sie kein öffentliches WLAN ohne zusätzlichen Schutz.

171.000.000

Geschäftsreisen von Mitarbeitern deutscher Unternehmen (2013). (5)

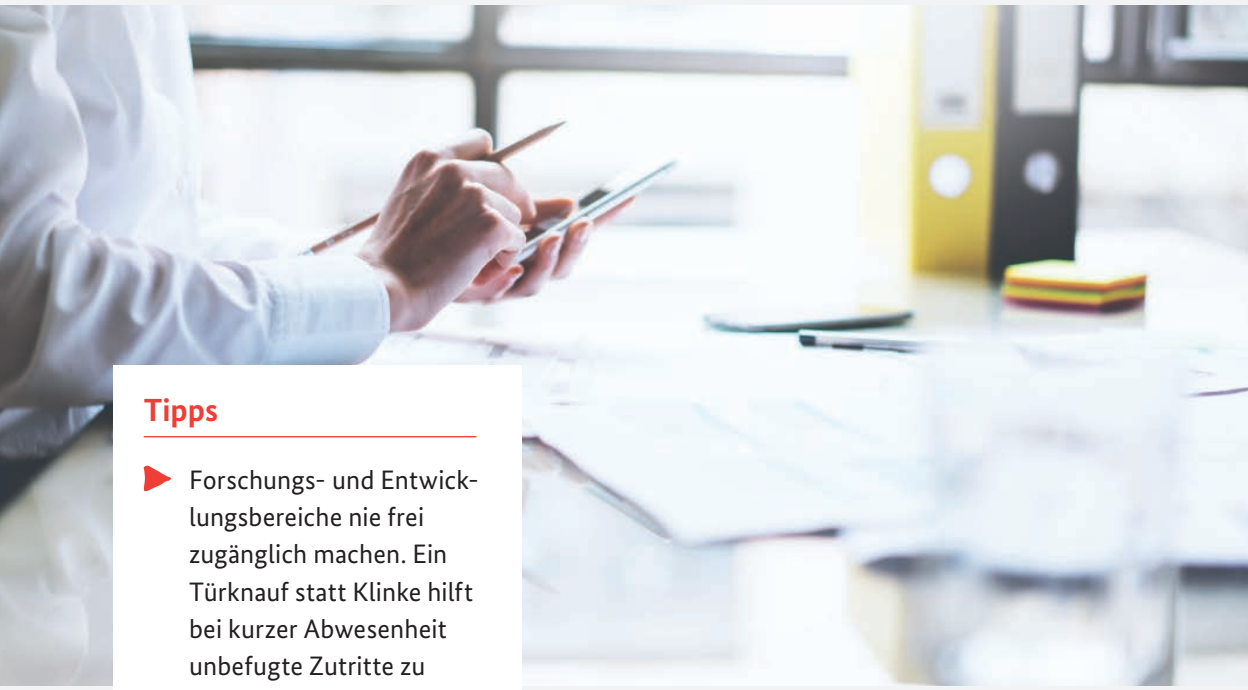
190.000

Handys bleiben jährlich in Londoner Taxis liegen. (6)

Forschung und Entwicklung

Innovationen geheim halten

Innovationen sichern Markterfolg und Wettbewerbsvorsprung Ihres Unternehmens. Dies kann sich schnell ändern, wenn es Ihnen nicht gelingt, Ihre Entwicklungsstandorte und Ihr Know-how ausreichend zu schützen.



Tipps

- Forschungs- und Entwicklungsbereiche nie frei zugänglich machen. Ein Türknauf statt Klinke hilft bei kurzer Abwesenheit unbefugte Zutritte zu vermeiden.
- Lassen Sie Besuchergruppen, Handwerker und Reinigungskräfte nicht unbeaufsichtigt in Chef-Büros, Sekretariate oder Konferenzräume.
- Schließen Sie Geheimhaltungsverträge mit Dienstleistern ab.
- Entfernen Sie sensitives Material nach Besprechungen auch aus dem Papierkorb.
- Nutzen Sie Aktenvernichter für vertrauliche Dokumente.
- Seien Sie sorgfältig bei der Auswahl von Praktikanten.

Bei mehr als 80 % deutscher Unternehmen werden Unterlagen abends nicht eingeschlossen. (1)

26 % aller deutschen Unternehmen sind von Know-how-Abflüssen betroffen. (1)

Geschäftsleitung

Sicherheit ist Chefsache

Die Geschäftsleitung ist ein lohnendes Angriffsziel. Sie steht in der Öffentlichkeit und ist z. B. im Internet für Angreifer leicht identifizierbar.

Als Chef sind Sie auch maßgeblich dafür verantwortlich, dass Sicherheit im Betrieb großgeschrieben wird.

Handy & Co. als Einfallstor

Die Handy- und E-Mailkommunikation von Geschäftsführern wird bevorzugt abgehört. Durch die gewonnenen Informationen erhalten Angreifer z.B. Einblick in Angebote, Preisgestaltung, Strategie sowie die interne Organisation und können Finanzdaten missbrauchen.

In 14 %

der Fälle wird die Geschäftsleitung ausspioniert. (2)

Tipps

- Entwickeln Sie ein Sicherheitskonzept für Ihr Unternehmen. Nutzen Sie dabei staatliche Fördermöglichkeiten.
- Seien Sie Vorbild bei der Einhaltung der Sicherheitsregeln.
- Auch wenn Sie stolz darauf sind, was Ihr Unternehmen leistet, achten Sie in Gesprächen mit Partnern, Dritten und in sozialen Netzwerken dennoch darauf, was Sie preisgeben.
- Führen Sie Ihr Handy nicht in vertraulichen Besprechungen mit. Es kann als Abhörgerät missbraucht werden.

In 66 % **der deutschen Firmen ist Know-how-Schutz nicht Chefsache.** (1)

Einkauf, Zulieferer und Dienstleister

Gemeinsam gut geschützt

Dienstleister und Zulieferer sind in der Regel eng in Ihre IT- und Arbeitsprozesse eingebunden. Dadurch haben sie Zugang zu sensiblen Daten und zu Ihren Geschäftsräumen. Dieses Vertrauensverhältnis kann ausgenutzt werden.

Partner als Täter

Nicht jeder Geschäftspartner ist vertrauenswürdig. Er kann Ihr Know-how entwenden, um sich oder Wettbewerbern einen Vorteil zu verschaffen, z. B. durch die Weitergabe von technischen Unterlagen.

Partner als Angriffsziel

Selbst wenn Sie sich vorbildlich schützen, können Zulieferer und Dienstleister eine Sicherheitslücke für Ihr Unternehmen darstellen.

33 %

aller Angriffe gehen von Vertragspartnern aus. (7)

Tipps

- Binden Sie Dienstleister und Zulieferer in Ihr Schutzkonzept ein.
- Regeln Sie den Umgang mit vertraulichen Daten in Verträgen und kontrollieren Sie deren Einhaltung.
- Daten über Dienstleister sind sensible Informationen, die genauso schützenswert sind, wie Ihr eigenes Know-how.
- Stellen Sie sicher, dass Ihre Unternehmensdaten bei Outsourcing nicht missbraucht werden können.

Vertrieb und Kunde

Verdächtiges Interesse

Nicht jeder, der sich für Ihre Produkte interessiert, hat Kaufabsichten. Durch die systematische Auswertung frei zugänglicher Informationen können Täter wertvolle Rückschlüsse auf Ihr aktuelles Know-how und Produktportfolio ziehen.

Tipps

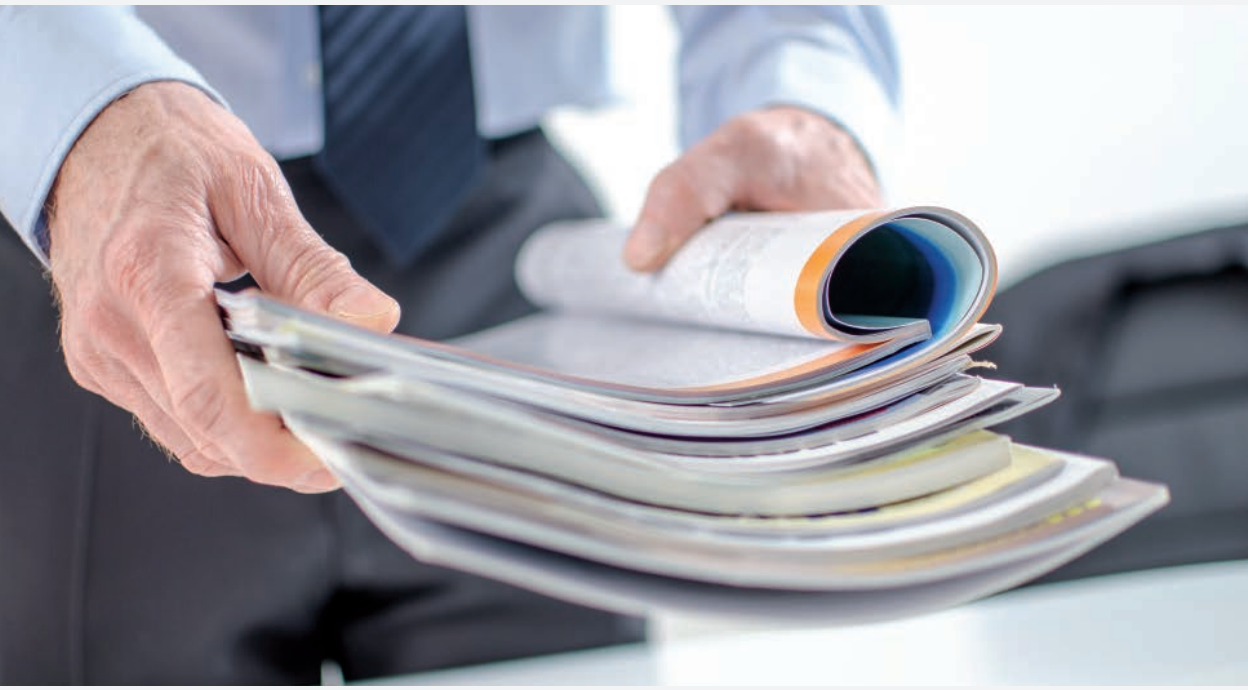
- Trotz kundenfreundlicher Transparenz: Achten Sie darauf, nicht zu viele Informationen über Ihr Produkt preiszugeben.
- Kundendaten, Angebots- und Preisgestaltung sind sensible Informationen, die genauso schützenswert sind wie Ihr unternehmensrelevantes Wissen.
- Lassen Sie Besuchergruppen durch eigene Mitarbeiter begleiten.

Offene Quellen

- Werkszeitungen
- Firmenpräsentation
- Produktbeschreibungen
- Handbücher und Dokumentationen
- Patent- und Lizenzunterlagen
- Forschungsberichte

Delegationen und Werksführungen

Besuchergruppen und Handelsdelegationen stehen im Ruf, zielgerichtet Informationen zu beschaffen, z. B. durch heimliches Fotografieren auf Werksführungen mit versteckten Kameras und Mitnahme von Produktproben.



Produktion

Schwachstelle Maschine

Die Produktion ist ein zentraler Bestandteil Ihres Unternehmens. Besonders schützenswert sind die technischen Einstellungen Ihrer Maschinen und die Produktionsprozesse. Täter verschaffen sich digital oder physisch Zugriff, z. B. bei Wartungsarbeiten. Im Ausland sind die Bedingungen für Angreifer oft günstiger.

Tipps

- Erstellen Sie ein Sicherheitskonzept schon vor Produktionsaufbau. Dies senkt Kosten und steigert die Qualität.
- Schützen Sie Kernbereiche der Produktion vor unbefugtem Zugang.
- Kontrollieren Sie den Zugriff auf produktionsrelevante Informationen, z. B. Maschineneinstellungen und Rezepturen.
- Unterteilen Sie nach Möglichkeit die Produktionsprozesse in abtrennbare Abschnitte.
- Führen Sie ausreichend Qualitätskontrollen ein, um Folgeschäden zu vermeiden.
- Schotten Sie IT-Systeme in Produktionsanlagen vom allgemeinen Netzwerk ab.

Sabotage

Ihr Unternehmen kann durch die mutwillige Beschädigung Ihrer Produktionsprozesse, Betriebsabläufe oder Produkte große Schäden erleiden und seine Konkurrenzfähigkeit verlieren.

Industrie 4.0

Durch die Digitalisierung werden Produktionsanlagen und moderne Informations- und Kommunikationstechnik vernetzt. Dadurch entstehen wechselseitig neue Gefährdungen.

Know-how

Täter versuchen, Know-how über Produktionsprozesse zu gewinnen, um sich dadurch einen Wettbewerbsvorteil zu verschaffen.

IT

Digitaler Einbruch

Digitalisierung ergreift das komplette Unternehmen von der Verwaltung bis zur Produktion und über Ländergrenzen hinweg. Die digitale Vernetzung ermöglicht Angreifern unzählige neue Zugangswege. Die Folgen bleiben oft unbemerkt, Wettbewerbsnachteile zeigen sich erst später und kommen Unternehmen teuer zu stehen.

Tipps

- Aktualisieren Sie Ihre Software regelmäßig. Dies ist ein guter Anfang.
- Verwenden Sie Schutzprogramme.
- Vermeiden Sie unverschlüsselte Kommunikation im WLAN.
- Nutzen Sie keine fremden Datenträger, z. B. geschenkte USB-Sticks.
- Seien Sie vorsichtig bei E-Mails von unbekannten Absendern und generell bei Anhängen.
- Erstellen Sie Nutzungsrichtlinien für Internet und Hardware.
- Nutzen Sie E-Mail-, Festplatten- und Geräteverschlüsselungen.

Digitaler Datendiebstahl

Angreifer hacken sich in Ihre Systeme ein und kopieren wichtige Daten, oft sogar ohne Spuren zu hinterlassen. Zugang verschaffen sie sich z. B. durch Social Engineering und Schadsoftware, die per E-Mail, USB-Sticks oder über Internetseiten eingeschleust wird.

In 30 % der Angriffsfälle werden IT-/Kommunikationsgeräte gestohlen. (2)

40 % der Angriffe erfolgen durch Hacker. (1)

Keine Angst vor...

... negativen Konsequenzen (z. B. Beschlagnahmung, Haftung)

Der Verfassungsschutz kann vertraulich helfen und ist grundsätzlich nicht zur Strafverfolgung verpflichtet.

... Imageschäden

Die Polizei hat Expertise und Erfahrung im vertraulichen Umgang mit Unternehmen.

BKA – "Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime"

... hohem Folgeaufwand

Ermittlungen werden möglichst geschäftsverträglich durchgeführt.

... ausbleibendem Erfolg der Strafverfolgungsbehörden

Melden hilft, künftige Angriffe zu verhindern und das Schutzniveau insgesamt zu erhöhen.

... fehlender Expertise staatlicher Stellen

Sicherheitsbehörden haben umfassende Expertise und Ressourcen.

Holen Sie sich Unterstützung!

1 Informieren Sie sich auf den Internetseiten des *Bundesamts für Sicherheit in der Informationstechnik* (BSI) und des *Bundesamtes für Verfassungsschutz* (BfV).

2 Nutzen Sie das Know-how vertrauenswürdiger Dienstleister und lassen Sie sich bei der Erstellung von Sicherheitskonzepten und bei der Auswahl von Sicherheitsmaßnahmen und -produkten beraten.

3 Fragen Sie die Sicherheitsabteilung anderer Unternehmen und Ihre Fach-, Branchen- und Sicherheitsverbände vertraulich um Rat.

Herausgeber

initiative wirtschaftsschutz

Gemeinsam. Werte. Schützen.

www.wirtschaftsschutz.info

Autoren

Felix Esser (BDI)
Peter Eickelbaum (DIHK)
Prof. Timo Kob (HiSolutions AG)
Axel Petri (Deutsche Telekom AG)
Andrea Rohmeder (Siemens AG) – Projektleitung
Thorsten Sprenger (Kenthor GmbH)
Dr. Berthold Stoppelkamp (BDSW)
Jan Wolter (ASW Bundesverband)

Partner

BDI Bundesverband der Deutschen Industrie e.V. — www.bdi.eu

DIHK Deutscher Industrie- und Handelskammertag — www.dihk.de

BDSW Bundesverband der Sicherheitswirtschaft — www.bdsw.de

ASW Bundesverband — www.asw-bundesverband.de

Referenzen

1) „Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co.?“; Corporate Trust - Business Risk & Crisis Management GmbH

2) Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter; BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

3) BSI – Die Lage der IT-Sicherheit in Deutschland 2014, S. 16

4) Datenklau: neue Herausforderungen für deutsche Unternehmen 23-Jul-2015 Germany. Ernst & Young GmbH: Ergebnisse einer Befragung von 450 deutschen Unternehmen

5) Geschäftsreiseanalyse 2014. Fakten und Zahlen 2014, DRV Deutscher ReiseVerband e.V.

6) ESET Deutschland GmbH

7) The Global State of Information Security® Survey 2016; PricewaterhouseCoopers AG

Bildnachweise

initiative wirtschaftsschutz

Gemeinsam. Werte. Schützen.