

## **secure-it in Nordrhein-Westfalen**

Wirtschaftsspionage und Konkurrenzausspähung:  
So schützen Firmenchefs ihr Unternehmen

## Impressum

Agentur »secure-it.nrw«  
bei der IHK Bonn/Rhein-Sieg  
Bonner Talweg 17  
D-53113 Bonn  
Telefon: +49 (0) 228 / 2284-184  
Telefax: +49 (0) 228 / 2284-5184  
E-Mail: [info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)  
Internet: [www.secure-it.nrw.de](http://www.secure-it.nrw.de)  
[www.branchenbuch-it-sicherheit.de](http://www.branchenbuch-it-sicherheit.de)

Ministerium für  
Innovation, Wissenschaft,  
Forschung und Technologie  
des Landes Nordrhein-Westfalen  
[www.innovation.nrw.de](http://www.innovation.nrw.de)

Autor:  
Alfred Preuß

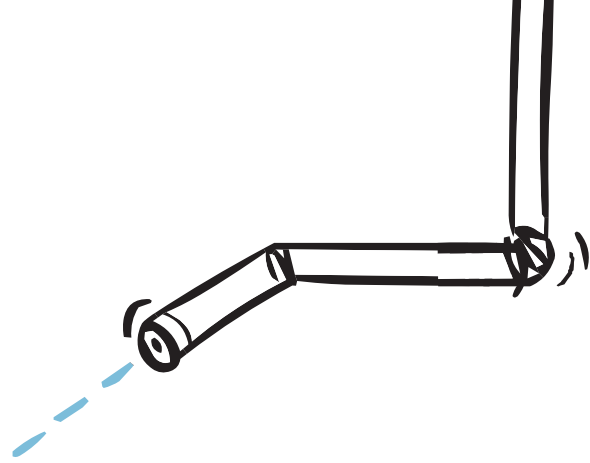
Illustrationen:  
Leowald

Realisation und Herstellung:  
Medienpool Köln GmbH

Haftungsausschluss: Alle Informationen  
sind nach bestem Wissen zusammenge-  
stellt. Wir übernehmen jedoch keine  
Gewähr für die Richtigkeit.

Alle im Text genannten Marken oder  
eingetragenen Marken sind Eigentum der  
jeweiligen Inhaber.

© 2008 »secure-it.nrw«



## Inhalt

- 2      Wirtschaftsspionage und Konkurrenzausspähung:  
Die neuen Risiken für Unternehmen.**  
Viele mittelständische Firmen sind im Visier von Wirtschaftsspionen.
- 4      Wie gefährdet ist Ihr Unternehmen?**  
Die Antwort gibt sofort der „Check für Firmenchefs“.
- 6      Anleitung für eine Sicherheitsstrategie.**  
Wie Firmen ihre Kernkompetenz ermitteln und schützen.
- 8      So sensibilisieren Firmen ihre Mitarbeiter.**  
Teamgeist und Kreativität steigern das Sicherheitsbewusstsein.
- 10     So machen Firmen ihre IT sicherer.**  
Praktische Sicherheitstipps für Internet und Informationstechnik.
- 12     So schützen Firmen ihre Telekommunikation.**  
Mehr Sicherheit für Festnetz, Mobiltelefon und Internet-Telefonie.
- 14     Wer Firmen im Notfall sicher hilft.**  
So gehen Polizei und Verfassungsschutz bei der Aufklärung vor.
- 16     Akteure im Kampf gegen Wirtschaftsspionage  
und Konkurrenzausspähung.**  
Firmen in Nordrhein-Westfalen können auf kompetente Partner zugreifen.

Wirtschaftsspionage?  
Konkurrenzausspähung?  
Produktpiraterie?  
Kaum ein Unternehmer  
fühlt sich davon betrof-  
fen. Aber Achtung! Viele  
Firmen sind unbemerkt  
schon im Visier der  
Wirtschaftsspione.



## Wirtschaftsspionage und Konkurrenzausspähung: Die neuen Risiken für Unternehmen

Das teure Notebook ließen die Einbrecher einfach liegen. Mehr Interesse zeigten die nächtlichen Besucher eines mittelständischen Unternehmens indes an einem älteren Laptop in der Schreibtischschublade des Entwicklungsingenieurs. Dort war die vom Unternehmen neu entwickelte Software für eine Maschinensteuerung gespeichert. Was dem Firmenchef im Nachhinein zu denken gibt: Wenige Wochen zuvor hatte sein Ingenieur einer ausländischen Delegation diese Innovation seines Unternehmens präsentiert – mit eben diesem Laptop.

### Das kann jedem Unternehmen passieren.

„Mittelständische Unternehmen sind verstärkt Ziel von Konkurrenzausspähung und Wirtschaftsspionage“, weiß Dr. Hartwig Möller, Leiter des Verfassungsschutzes im nordrhein-westfälischen Innenministerium. Firmen bemerken das meist erst, wenn es zu spät ist: Einem Unternehmen flattert eine Schutzrechtsklage ins Haus, weil eine von ihm entwickelte Technik von einem ausländischen Konkurrenten unvermittelt zum Patent angemeldet

wurde. Kunden springen überraschend ab, weil ein Wettbewerber auf einmal ein bislang nur von dem Unternehmen eingesetztes Spezialverfahren beherrscht und zu günstigeren Preisen anbietet. Auf Messen präsentieren ausländische Anbieter ohne Scheu im Design abgekupfer- te Produktplagiate.

Nach einer vom Sicherheitsdienstleister Corporate Trust gemeinsam mit dem Büro für angewandte Kriminologie und dem Handelsblatt durchgeführten Umfrage bei mehr als 700 deutschen Firmen nimmt die Zahl der Fälle von Industriespionage im Schnitt jährlich um zehn Prozent zu.

Der Datenklau geschieht auf unterschiedlichen Wegen: In annähernd 15 Prozent der Fälle haben sich Konkurrenten in die internen IT-Systeme gehackt, zudem wurden Firmen durch Geheimdienste abgehört. In fast jedem fünften Fall konnten die Spione Mitarbeiter dazu bringen, ihnen vertrauliche Firmeninformationen zu überlassen.

FINANCIAL TIMES  
DEUTSCHLAND

„Schätzungen zufolge entstehen der deutschen Wirtschaft durch Datenklau jährlich Schäden von 20 Milliarden Euro.“

Financial Times Deutschland, 7.1. 2008

Süddeutsche Zeitung

„Etwa jedes fünfte Unternehmen in Deutschland wurde bereits Opfer von Wirtschaftsspionage oder hat wichtige Firmendaten an Konkurrenten verloren.“

Süddeutsche Zeitung, 3.12. 2007



**Dr. Hartwig Möller,**  
Leiter des  
Verfassungsschutzes im  
nordrhein-westfälischen  
Innenministerium

## „Deutsche Firmen sind weiterhin Ziel aggressiver Wirtschaftsspionage.“

### Herr Dr. Möller, wie groß ist überhaupt das Risiko für eine Firma, ausspioniert zu werden?

Viele kleine Firmen schätzen die Gefahr leider zu gering ein. Sie halten sich für zu unwichtig, als dass sie jemand ausspionieren könnte. In Wahrheit aber kann jedes erfolgreiche Unternehmen Ziel einer Wirtschaftsspionage sein oder von Konkurrenten ausgespäht werden. Besonders gefährdet sind Marktführer, Hightech-Firmen oder innovative Maschinen- und Anlagenbauer.

### Wer steckt dahinter?

Nach dem Ende des Kalten Krieges haben sich viele Geheimdienste neue Aufgaben suchen müssen. Sie sind jetzt oftmals im Auftrag von Regierungsorganisationen und staatlichen Unternehmen in Deutschland als Wirtschaftsspione aktiv, vor allem, wenn sich in ihrem Heimatland privatwirtschaftliche und staatliche Interessen nicht voneinander trennen lassen.

### Wo können Firmen in Gefahr geraten?

Eigentlich überall: im eigenen Betrieb, auf Messen, auf Geschäftsreisen. Uns wurde zum Beispiel schon häufig der Diebstahl von Notebooks aus Hotelzimmern gemeldet. Aufpassen sollten Firmen auch nach einem Einbruch im Betriebsgebäude. Die Täter wollen über gestohlene Computer oftmals nur an wertvolles Firmen-Know-how kommen.

### Wie gehen die Täter vor?

Sie nutzen vor allem Sicherheitslücken in der EDV und Schwächen der Mitarbeiter. Auf Messen und bei Betriebsbesichtigungen schöpfen die Spione durch intensives Nachfragen offen Informationen ab, sie gehen Joint Ventures mit Mittelständlern ein oder kaufen sogar das Unternehmen auf.

## Aus den Akten der Spionageabwehr

### Daten per Einbruch geklaut.

Täter brachen in ein Firmengebäude ein und begaben sich – wie an den Spuren erkennbar war – direkt in den IT-Bereich. Dort hatten sie offensichtlich versucht, Firmendaten vom Server herunterzuladen.

### In der Verhandlungspause Laptops manipuliert.

Bei einer Geschäftsverhandlung in China wurden die deutschen Gäste in aufgeregter Form dringlich darum gebeten, sofort einen hochrangigen Politiker kurz zu begrüßen, der gerade am Ort weilte. In der Hektik sicherten die deutschen Firmenmitarbeiter ihre Notebooks nicht. Als sie

nach mehreren Stunden in den Besprechungsraum zurückkehrten, stellten sie fest, dass in der Zwischenzeit offensichtlich jemand an den Laptops war.

### Geheime Firmendokumente weitergegeben.

Eine Übersetzerin hatte die ihr von einem Unternehmen zwecks Übersetzung anvertrauten Firmenunterlagen Chinesen zum Kauf angeboten. Die Übergabe konnte im letzten Augenblick verhindert werden.

### Vor dem Firmengelände ein Funknetz installiert.

Beim Rundgang um das Firmengebäude eines mittelständischen Unternehmens entdeckte der Wachdienst eine Erhebung im Erdreich. Dort war in einer Plastikdose ein WLAN-Router vergraben. Ein daran befestigtes Kabel führte direkt zur EDV-Anlage im Gebäude. Der Täter konnte so von außen – etwa in einem geparkten Wagen – über einen Laptop direkt auf den Firmenrechner zugreifen.

## Handelsblatt

„Die Wanze kommt als Firmengeschenk: Wirtschaftsspionage wird zu einer immer größeren Bedrohung – oft sind arglose Mitarbeiter das Ziel der kriminellen Informationsbeschaffer.“

Handelsblatt, 16. 4. 2008



Wirtschaftsspione und Konkurrenten haben oftmals ein leichtes Spiel. Um an geheime Informationen zu kommen, nutzen sie das Vertrauen der Mitarbeiter aus, täuschen Geschäftsinteresse vor oder profitieren von Schwachstellen beim Computereinsatz und Telefonieren.

## Wie gefährdet ist Ihr Unternehmen?

Wirtschaftsspione sind Experten in ihrem Metier. Nach einer Untersuchung der Unternehmensberatung Price-WaterhouseCoopers kommen etwa zwei Drittel aller Wirtschaftsspionagefälle nämlich nur durch Zufall heraus. „Die Ausspäher profitieren besonders von dem mangelnden Bedrohungsbewusstsein in den Unternehmen“, sieht Thomas Faber, Leiter der vom nordrhein-westfälischen Innovationsministerium geförderten Landesinitiative »secure-it.nrw«, als einen der Hauptgründe dafür.

**Schwachstelle Informationstechnik und Telekommunikation.** Bei vielen kleinen Unternehmen besteht in Sachen IT-Sicherheit an unerwarteter Stelle noch deutlicher Handlungsbedarf. Das zeigt eine Auswertung der Landesinitiative »secure-it.nrw« von rund 200 in mittel-

ständischen Firmen durchgeführten „Basisprüfungen IT-Sicherheit“: Während die Unternehmen ihre IT bereits weitgehend mit Virenschutzsoftware und Firewalls vor Außenangriffen abschotten, besteht vielfach noch Handlungsbedarf bei der Entwicklung und Umsetzung einer umfassenden Sicherheitsstrategie. Dazu gehören IT-Sicherheitsmanagement, Notfallpläne und die Sensibilisierung der Mitarbeiter.

**Schwachstelle Außenwirtschaft.** Immer mehr mittelständische Unternehmen stoßen derzeit in ausländische Märkte vor oder machen bereits Geschäfte mit Partnern in aufstrebenden Wirtschaftsnationen wie China oder Russland. Sie müssen dabei feststellen, dass bei angestrebten Kooperationen zuweilen für sie ungewöhnliche Spielregeln gelten. Gängige Praxis ist das Auskundschaften vertraulicher Firmeninformationen. „Kaum ein Unternehmen kommt im globalen Wettbewerb am Thema Wirtschaftsspionage vorbei“, weiß Alexa Sipos, Geschäftsführerin des Verbands für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V. (VSW NW).

**Schwachstelle Mitarbeiter.** Firmenangehörige geben oftmals auf Messen oder in Gesprächen mit möglichen Geschäftspartnern leichtfertig vertrauliche Firmeninformationen preis. Ursachen: Sie wissen nicht, welche Details geheim bleiben müssen, wollen sich wichtig machen, werden durch Aussicht auf einen Geschäftserfolg unvorsichtig. Geheimdienste setzen weiterhin „altmodische Methoden“ ein und dokumentieren – beispielsweise über Kameras in Hotelzimmern – menschliche Schwächen wie Drogen- oder Spielsucht, Alkoholprobleme oder Prostituiertenkontakte.

### Social Engineering

Um durch „Aushorchen“ an Informationen zu gelangen, nutzen Wirtschaftsspione geschickt menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität aus. Dadurch manipulieren sie Mitarbeiter so, dass sie unzulässig handeln.

**Spionagetrick:** Eine angebliche Sekretärin ruft an und fragt im Auftrag eines Vorgesetzten, der noch dringend etwas erledigen muss, nach einer wichtigen Information. Der Mitarbeiter fühlt sich unter Druck gesetzt und gibt oftmals die gewünschte Auskunft.



**Thomas Faber,**  
Leiter der nordrhein-  
westfälischen  
Landesinitiative  
»secure-it.nrw«

## „Wirtschaftsspione profitieren von den Vorteilen der Informationstechnik“

### Herr Faber, welche neuen Risiken entstehen für Firmen durch die Informationstechnik?

Zwei Entwicklungen in der Informationstechnologie machen Unternehmen jetzt besonders anfällig für die Wirtschaftsspionage: erstens das Internet und zweitens die immer größere Informationsdichte in der IT.

### Welche Gefahren stecken im Internet?

Das Web ermöglicht jedem und von jedem Ort der Welt den immer schnelleren Zugriff auf Firmeninformationen. Dabei bleiben die Täter sogar weitgehend anonym. Ergiebige Quellen sind etwa die Websites der Unternehmen. Über Suchmaschinen stößt man leicht auf im Zusammenhang mit dem Unternehmen erstellte Diplomarbeiten, Forschungsprojekte, auf Presseberichte oder PowerPoint-Präsentationen. Gewiefte Täter gelangen über das Internet sogar direkt ins Unternehmensnetzwerk.

### Warum sind Speichermedien gefährlich?

Das gesamte Unternehmens-Know-how ist heute oftmals nur auf wenigen Quadratzentimetern Festplatte gespeichert. Damit haben Spione die besten Möglichkeiten, ohne viel Aufwand alle für sie relevanten Informationen beispielsweise schnell auf eine externe Harddisc zu kopieren. Kleinere Datenpakete können sie unbemerkt per USB-Stick abtransportieren.

### Wie kommen die Täter an die Informationen?

Den Zugriff auf Firmendaten und Firmendokumente verschaffen ihnen vielfach unwissentlich die Mitarbeiter des Unternehmens selber – zum Beispiel mit USB-Sticks, die sie auf Messen als Werbegeschenk bekommen haben und ohne vorhergehende Virenprüfung mit ihrem Firmen-PC verbinden. Spione nutzen die Leichtfertigkeit, indem sie USB-Sticks mit Trojanern infizieren. Diese nisten sich im Firmennetzwerk ein und liefern den Wirtschaftsspionen fortan unbemerkt vertrauliche Firmendokumente per Internet.

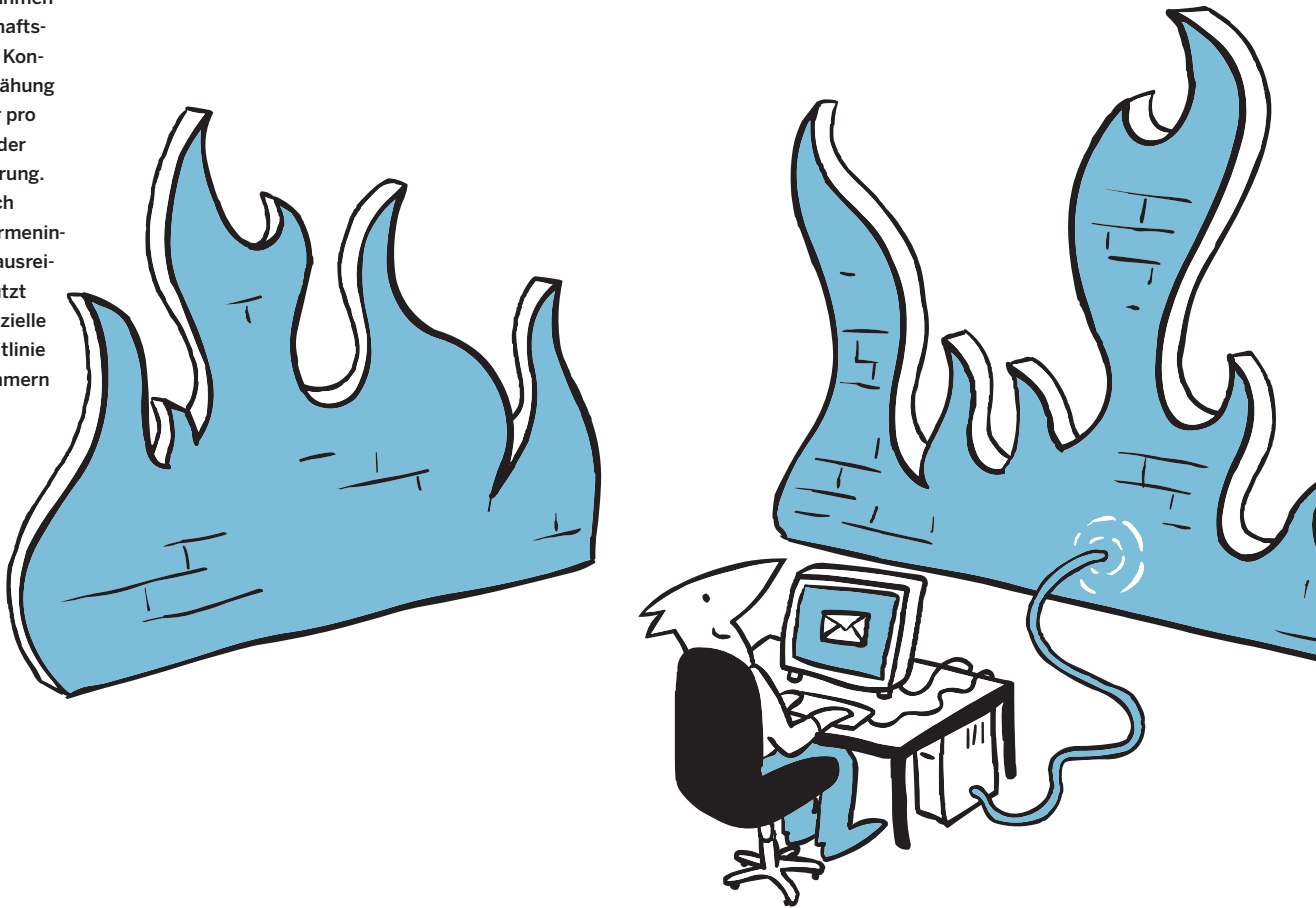


## Check für Firmenchefs

Wenn Sie eine dieser Fragen mit „Ja“ beantworten, sollten Sie ab jetzt besonders wachsam sein. Ihre Firma gerät rasch ins Visier von Wirtschaftsspionen und kriminellen Konkurrenten – oder wird bereits ausgespioniert. Einen Check, den jedes Unternehmen anonym durchführen kann, bietet der Verfassungsschutz in Nordrhein-Westfalen auf seiner Website an.

1. Besitzt Ihr Unternehmen Wettbewerbsvorteile gegenüber Konkurrenten (z. B. Kostenführerschaft, besondere Produktqualität, Spezialprodukte)?
  2. Bieten Sie Produkte oder Dienstleistungen an, die sowohl für militärische als auch für zivile Zwecke genutzt werden können?
  3. Liegen bereits Anhaltspunkte für eine Ausforschung Ihres Unternehmens vor?
- Zum Beispiel:
- Häufiger Verlust von sicher geglaubten Aufträgen
  - Ungewöhnliche Anfragen von unbekanntem Unternehmen, die beispielsweise nicht den Geschäftsgewohnheiten der Branche entsprechen
  - Rätselhaftes Bekanntwerden von Firmeninterna in der Öffentlichkeit
  - Plagiate Ihrer Produkte sind auf dem Markt erhältlich

Schutzmaßnahmen gegen Wirtschaftsspionage und Konkurrenzausspähung sind nicht nur pro forma Sache der Geschäftsführung. Sie haftet auch dafür, dass Firmeninformationen ausreichend geschützt sind. Eine spezielle Sicherheitsleitlinie hilft Unternehmern dabei.



## Anleitung für eine Sicherheitsstrategie

Für viele Notfälle sind Unternehmen bereits bestens gerüstet: In klaren Anweisungen legen sie fest, was bei einem Brand, einem Mitarbeiterunfall oder einem Produktionsschaden zu passieren hat. Eine solche Leitlinie sollten Firmen auch für den Schutz gegen Wirtschaftsspionage und Konkurrenzausspähung zur Hand haben. Damit entdecken sie rechtzeitig Lücken, sind für die Gefahren sensibilisiert und können im Bedarfsfall schnell handeln.

Größere Firmen müssen nach dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sogar ein Risikofrüherkennungs- und Überwachungssystem in ihrem Unternehmen implementieren. Die Unternehmensleitung macht sich strafbar, wenn sie billigend in Kauf nimmt, dass geheime Informationen an Dritte gelangen könnten. Firmenchefs haften für fehlende Schutz-

maßnahmen auch dann, wenn sie die Aufgabe einem Mitarbeiter übertragen.

Das Erstellen einer Sicherheitsleitlinie ist kein großer Aufwand: Fünf Textseiten sind das Maximum.

**1. Schutzbedarf ermitteln.** Ein guter Anhaltspunkt ist dabei, welchen Sicherheitsbedarf das Unternehmen im Bereich der Informationstechnik hat. In der EDV läuft nämlich von der Konstruktion über die Archivierung bis hin zur Kommunikation alles zusammen. Der Schnell-Test „Wie viel Sicherheit braucht Ihr Unternehmen?“ hilft dabei. Er basiert auf einer vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellten Anleitung.

**2. Kernkompetenz herausfinden.** Nur fünf Prozent aller Firmeninformationen sind das elementar wichtige Firmen-Know-how, fand die Uni Lüneburg heraus. Unternehmen sollten diese Werte ausmachen und gezielt schützen (siehe: „Kernkompetenz ermitteln“). Damit sparen sie auch Kosten für unnötige Sicherheitsmaßnahmen.

**3. Handlungsschritte festlegen.** Detailliert beschreiben, wie das Unternehmen diese Kernkompetenz vor Wirtschaftsspionage schützt. Der Aktionsrahmen sollte drei Bereiche umfassen: Mitarbeiter sensibilisieren, EDV absichern und die Telekommunikation schützen. Organisatorische Maßnahmen bringen oftmals den größten Nutzen.



### Umsetzungswege

Auf den folgenden Ratgeberseiten finden Sie konkrete Vorschläge zur Umsetzung Ihrer Sicherheitsstrategie.

**Mitarbeiter sensibilisieren.** Mehr dazu ab Seite 8

**IT schützen.** Mehr dazu ab Seite 10

**Telekommunikation sichern.** Mehr dazu ab Seite 12

**Expertenhilfe nutzen.** Mehr dazu ab Seite 14



## Schnell-Test: Wie viel IT-Sicherheit braucht Ihr Unternehmen?

Zentraler Informationsknoten ist in den meisten Unternehmen die IT. Dort setzen Wirtschaftsspione gern an. Mit der Checkliste finden Firmen heraus, wie groß ihr Schutzbedarf ist. Kreuzen Sie bitte an.

### Kriterien für Sicherheitsstufe 1

- Eine Vertraulichkeit von Informationen ist in unserem Unternehmen nicht erforderlich.
- Fehler in der EDV sind tolerierbar, solange sie unsere Arbeit nicht völlig unmöglich machen.
- Ein dauernder Ausfall der IT ist zu vermeiden, längere Ausfallzeiten sind jedoch hinnehmbar.

**Niedriger Schutzbedarf:** Schäden in der IT beeinträchtigen die Arbeit Ihrer Firma nur unwesentlich.

### Kriterien für Sicherheitsstufe 2

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss in unserem Unternehmen gewährleistet sein.
- Kleinere Fehler können wir zwar tolerieren. Sie müssen aber erkennbar oder vermeidbar sein, wenn sie die Aufgabenerfüllung erheblich beeinträchtigen.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, können wir uns nicht leisten.

**Mittlerer Schutzbedarf:** Schäden in der IT beeinträchtigen die Geschäftstätigkeit Ihrer Firma.

### Kriterien für Sicherheitsstufe 3

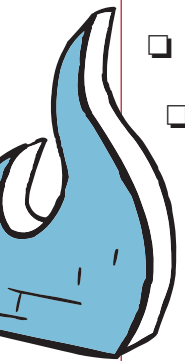
- Der Schutz vertraulicher Informationen muss hohen gesetzlichen Anforderungen genügen und in sicherheitskritischen Bereichen stärker sein.
- Verarbeitete Informationen müssen korrekt sein, auftretende Fehler erkennbar und vermeidbar.
- In zentralen Bereichen laufen zeitkritische Vorgänge ab, oder es werden dort Massenaufgaben wahrgenommen, die ohne IT-Einsatz nicht zu erledigen sind. Kurze Ausfallzeiten sind tolerierbar.

**Hoher Schutzbedarf:** Im Schadensfall sind zentrale Bereiche der Firma handlungsunfähig.

### Kriterien für Sicherheitsstufe 4

- Der Schutz vertraulicher Informationen muss gewährleistet sein. Strenge Vertraulichkeitsanforderungen in sicherheitskritischen Bereichen.
- Die von uns herausgegebenen Informationen müssen in höchstem Maße korrekt sein.
- Zentrale Aufgaben sind ohne IT-Einsatz nicht durchführbar. Für wichtige und schnell zu treffende Entscheidungen brauchen wir stets aktuelle Informationen, Ausfallzeiten sind nicht akzeptabel.

**Maximaler Schutzbedarf:** Der Ausfall der IT führt zum Zusammenbruch der Firma.



## Kernkompetenz ermitteln

Die Ermittlung von Kernkompetenzen eines Unternehmens – als Grundlage für Schutzmaßnahmen – wird am geeignetsten in Workshops durchgeführt. Daran sollten Mitarbeiter aus verschiedenen Bereichen teilnehmen.

**1. Bestandsaufnahme machen.** Gemeinsam mit ihren leitenden Mitarbeitern sollten Firmenchefs Antworten auf diese vier Fragen finden:

- Warum sind wir am Markt?
- Worin liegt der Unterschied zur Konkurrenz?
- Welche sind unsere innovativsten Produkte?
- Was garantiert, dass wir auch im nächsten Jahr noch am Markt sind?

**2. Bekanntes aussieben.** Viele der gesammelten Informationen stehen bereits im Internet oder in Firmenbrochüren. Sie sind also schon öffentlich bekannt und müssen deshalb nicht mehr aufwendig geschützt werden.

**3. Kompetenz-Dokument erstellen.** Firmen sollten ihre Kernkompetenzen ausformuliert zu Papier bringen und zum Bestandteil ihrer Sicherheitsleitlinie machen. Das schafft unter allen Beteiligten Klarheit und Verbindlich-

keit. Zudem unterliegen auch Kernkompetenzen einem Lebenszyklus. Deshalb in regelmäßigen Zeitabständen anhand der Aufstellung überprüfen, inwiefern bestimmte Kompetenzen obsolet und neue zu schützen sind.

**4. Mitarbeiter informieren.** Alle Mitarbeiter sollten wissen, welche Firmeninformationen unbedingt geheim bleiben müssen. Das macht sie auch misstrauisch, wenn ein Gesprächspartner genau an diese Informationen kommen will – beispielsweise auf Messen oder bei einem Telefonat.

**5. IT besonders schützen.** Zunächst erkunden, welche Informationen mit Kernkompetenzbezug im IT-Bereich abgelegt sind – zum Beispiel Konstruktionspläne, Geschäftskonzepte, Zukunftsvisionen, Innovationen, Kundenlisten. Diese Dokumente sollten Unternehmen aus dem offen zugänglichen IT-Sektor herausnehmen und in einem abgeschirmten Verzeichnis ablegen.

**6. Den Zugriff einschränken.** Neben der Geschäftsleitung darf nur eine begrenzte Anzahl von Mitarbeitern Zugriff auf Dokumente und Daten mit Kernkompetenz-Qualität haben.



Eine der größten Schwachstellen bei der IT-Sicherheit sind die eigenen Mitarbeiter. Mit Informationen und Aktionen schaffen Unternehmen schnell mehr Sicherheitsbewusstsein. Damit werden Firmenmitglieder auch wachsamer gegenüber Spionageversuchen.

## So sensibilisieren Firmen ihre Mitarbeiter

Aus welchen Gründen machen Mitarbeiter Fehler, die IT-Sicherheitssysteme in Unternehmen aushebeln? Die Antwort klingt paradox: „Die meisten Mitarbeiter wissen sehr wohl, was richtig und falsch ist“, sagt Dietmar Pokoyski, Geschäftsführer der Kölner Agentur known\_sense, „aber je dichter das Sicherheitsnetz einer Firma ist, umso mehr versuchen die Mitarbeiter unbewusst, dieses System zu durchbrechen.“

Das ist das Ergebnis einer von known\_sense mit Partnern durchgeführten Studie. Sie hat auch gezeigt, dass Mitarbeiter Unternehmenssicherheit als gemeinsame Sache erleben wollen, für die man im spielerischen Sinne kämpft. „Sicherheit braucht eine Geschichte, eine verbindende Story“, beschreibt Dietmar Pokoyski die Herausforderung an erfolgreiche Maßnahmen, „das fördert den Teamgeist und spricht die Kreativität an.“

### Wissen spielerisch vermitteln

Um bei ihren Mitarbeitern das Sicherheitsbewusstsein („Security Awareness“) zu erhöhen, sollten Firmen die Informationen auf eingängige Weise vermitteln. Dies kann beispielsweise durch einprägsame Vorträge, Schulungen per PC oder Plakate erfolgen.

Wie Firmen dabei vorgehen können – auch zum Schutz vor Wirtschaftsspionage –, zeigt das innerbetriebliche IT-

Sicherheitstraining der Schwelmer Spedition Schmidt-Gevelsberg GmbH. Das Unternehmen wurde dafür mit dem Sonderpreis „Vorbildliche Bewusstseinsbildung“ beim „IT-Sicherheitspreis NRW 2006“ ausgezeichnet.

„Das trockene Vermitteln von Kenntnissen ist bei der IT-Sicherheit nicht geeignet“, befand Geschäftsführer Rolf Lorenz. Er ließ deshalb auf den PCs seiner Mitarbeiter ein interaktives Lernprogramm installieren. Dieses schärft mit Comics und knackigen Sprüchen das Bewusstsein für die Sicherheitsrisiken beim Umgang mit E-Mail und Internet. „Diese spielerische Art, für IT-Sicherheit zu sensibilisieren, ist effektiver, weil es Spaß macht und jeder Einzelne sich aktiv mit dem Programm beschäftigt“, hat Rolf Lorenz inzwischen erfahren.

Das gesamte Trainingsprogramm dauert drei Stunden. Um es zu absolvieren, steht den Mitarbeitern ein Zeitrahmen von drei Monaten zur Verfügung. „In ruhigen Zeiten dreimal in der Woche eine Viertelstunde am Programm zu arbeiten, ist gut zu schaffen“, ermuntert Rolf Lorenz seine Mitarbeiter. Lohn der Leistung: Nach erfolgreichem Lernen – bestätigt durch einen Wissenstest – erhalten die Mitarbeiter ein Zertifikat. Erfolg für das Unternehmen: „Nachlässigkeit oder Unwissenheit im Umgang mit Daten können Sicherheitslücken verursachen“, so Rolf Lorenz, „und das lässt sich mit einem regelmäßigen Training verhindern.“

## Klare Anweisungen für den betrieblichen Alltag

Organisatorische Maßnahmen kosten nicht viel Geld – und bringen den größten Nutzen.

**Voraussetzungen schaffen.** Festlegen, welche Daten und Akten als besonders vertraulich einzustufen sind, und die Mitarbeiter mit diesen Vorgaben vertraut machen.

**Geschäftspartner bewerten.** Mitarbeiter informieren, welche Informationen sie welchem Externen geben dürfen und wer die Ansprechpartner in anderen Unternehmen und Organisationen sind, welche Kompetenzen diese haben und wie sie sich ordnungsgemäß zu erkennen geben.

**Kommunikationswege festlegen.** In welcher Form ist eine Kommunikation mit dem jeweiligen Geschäftspartner erlaubt (Brief, E-Mail, Telefon, Fax)? Welche Daten dürfen über E-Mail ausgetauscht werden? Wie lauten die korrekten Telefonnummern oder Web-Adressen der Geschäftspartner?

**Verhaltensregeln aufstellen.** Vertrauliche Akten sind bei Verlassen des Arbeitsplatzes im Schrank oder Safe zu verschließen. Magnetbänder, Disketten und CD-ROMs mit vertraulichen Informationen dürfen nie offen herumliegen.

**Zugangsberechtigung geheim halten.** Rigosos verbieten, dass Medien, die beim Zutritt in Firmengebäude oder beim Zugriff auf Dokumente zur Authentisierung des Mitarbeiters dienen, an Dritte weitergegeben werden.

**Entsorgung organisieren.** Vertrauliche Ausdrucke niemals in den Papierkorb werfen, sondern per Aktenvernichter zerkleinern. Datenträger wie Festplatten, Speicherkarten oder USB-Sticks beim Aussortieren durch mehrfaches Überschreiben sicher löschen. CD-ROM und DVD mit Shredder (gibt es als Zusatz zu Aktenvernichtern) zerstören.

**Private Geräte verbieten.** Der Anschluss privater Hardware wie USB-Sticks oder Fotokameras an den Firmen-PC birgt große Gefahren für Firmennetzwerke. Sie können auf diesem Weg mit Computerschädlingen infiziert werden.

**Firmen-Laptops vor Fremden schützen.** Mitarbeiter dürfen die ihnen von der Firma zur Verfügung gestellten elektronischen Geräte weder Freunden noch Familienangehörigen vorübergehend überlassen.



Mehr Informationen enthält die Broschüre „**Mitarbeiter sensibilisieren für IT-Sicherheit und Datenschutz**“

Kostenlos als PDF  
 ⓘ Link auf Seite 17

### Locker lernen:

Das Team der Kommunikationsagentur known\_sense setzt auf Teamgeist und Kreativität.



## Awareness mit System

Ein neues dreistufiges Management-Tool hilft Firmen, ihre Mitarbeiter für mehr IT-Sicherheit zu begeistern.

1. Eine Analyse, die auch intensive Einzel- und Gruppengespräche beinhaltet, spürt verdeckte Motive auf, die das Verhalten der Mitarbeiter im Umgang mit IT und sensiblen Informationen beeinflussen. 2. In der Beratung werden strukturelle Verbesserungen der Sicherheitskultur im Unternehmen entwickelt und 3. in der Kreativphase anhand zielgerichteter Awareness-Maßnahmen umgesetzt.

Das „askit – awareness security kit“ der Kölner Beratungsgesellschaft known\_sense wurde vom nordrhein-westfälischen Innovationsministerium und der Landesinitiative »secure-it.nrw« mit dem „IT-Sicherheitspreis NRW 2007“ ausgezeichnet.

Über die EDV kommen Wirtschaftsspione und Konkurrenten schnell an die für sie wichtigen Informationen. IT-Sicherheit heißt deshalb: Daten und Dokumente nicht für jeden zugänglich machen sowie Manipulationen erkennen und vermeiden.



## So machen Firmen ihre IT sicherer

Wenn Firmen die gängigen Standards zur IT-Sicherheit umsetzen, ist ihre Informationstechnologie auch weitgehend vor Wirtschaftsspionage geschützt. Vor zwei Risiken warnen Verfassungsschützer dennoch besonders: Spionageprogramme und Gerätediebstahl.

**Risiko 1: Spionageprogramme nisten sich in Computernetze ein.** Zu den Spionageprogrammen gehören beispielsweise Trojaner. Sie gelangen per E-Mail-Anhang oder Download aus einer Website auf den Firmenrechner und leiten dort gespeicherte Daten per Internet unbemerkt weiter, oft direkt an die Konkurrenz.

Nach Angaben des Bundeskriminalamtes sind etwa 750.000 Rechner in Deutschland mit Trojanern infiziert. Tückisch sind z. B. sogenannte Keylogger; das sind Programme, die alle Eingaben – also auch Passwörter – mitschneiden.

**Risiko 2: Täter kommen oftmals per Diebstahl leichter ans Ziel.** Firmen sollten sich beim Schutz ihrer elektronischen Geräte nicht nur auf Soft- und Hardwaremaßnahmen verlassen, sondern sie auch vor Diebstahl schützen. Dafür gibt es kostengünstige Lösungen.

**Wie sich Firmen gegen Risiken wappnen, zeigen die nebenstehenden Sicherheitstipps für das Internet sowie für die stationäre und mobile IT:**



### Sicherheitsideen für das Internet

Firmen müssen ihre Sicherheitsmaßnahmen in zwei Richtungen auslegen: Ausgehende Informationen sind vor Mitlesen und Manipulationen zu schützen, das Firmennetz ist vor unbefugtem Zugriff abzuschotten.

**Virtual Private Network einrichten.** Über eine VPN-Software lassen sich externe Computer sicher in das Firmennetz einbinden. Die Daten werden – wie in einem geheimen Tunnel – verborgen im Internet übertragen.

**E-Mails verschlüsselt versenden.** Schützt geschäftliche E-Mails vor unerwünschten Mitlesern. Zentrale Server („virtuelle Poststelle“) und Unternehmensschlüssel erleichtern die organisatorische Einbettung.

**Internet-PC aufstellen.** Für das Surfen im Internet gesonderten PC ohne Verbindung zum internen Netz aufstellen. Hier auch heruntergeladene Dateien auf Inhalt und Viren prüfen. Nur „saubere“ Dokumente per Datenträger oder E-Mail ins interne Netz weiterleiten.

**Mehrstufige Firewall einrichten.** Der Firewall zusätzliche Filterelemente (beispielsweise Router) vor- und nachschalten. Erschwert den Zugriff auf das Firmennetz.



## Wächter für die stationäre EDV

Mitarbeiter bringen Betriebsfremden oftmals zu viel Vertrauen entgegen. Sie lassen Besucher und Handwerker ungehindert durchs Haus gehen oder in Büros arbeiten. Wirtschaftsspione profitieren davon.

**Vor unbefugtem Zugriff schützen.** Computer mit Zugang zu vertraulichen Daten so aufstellen, dass Fremde nicht unbemerkt daran gehen können.

**Manipulation verhindern.** Bei Abwesenheit Computer sperren oder Bildschirmschoner mit Kennworteingabe aktivieren. Entsperrung erst nach Eingabe eines korrekten Passwortes ermöglichen.

**Festplatten sicher löschen.** Wenn bei Reparaturen oder bei der Ausmusterung alter PCs Datenträger das Haus verlassen, Daten vorher sorgfältig mit Spezialprogrammen löschen. Auch defekte Festplatten lassen sich oftmals noch auslesen.

**Funknetz in Grenzen halten.** Sendeleistung des WLAN einschränken, Voreinstellungen (Netzname, Passwort) abändern, sichere Verschlüsselung (WPA statt WEP) nehmen. Verhindert unbefugtes Eindringen ins Funknetz und unerwünschtes Mitlesen.



## Security-Tipps für die mobile IT

In Notebooks stecken oftmals zwei Sicherheitsrisiken: umfangreiche Firmeninformationen und die Möglichkeit, auf Dokumente in der Firmen-EDV zuzugreifen.

**Laptops vor Diebstahl schützen.** Notebooks nie unbeaufsichtigt im Auto zurücklassen. Im Büro nachts oder bei längerer Abwesenheit einschließen. Bei Veranstaltungen mit einem Sicherungskabel befestigen.

**Zugriff auf Daten erschweren.** Biometrische Authentisierung einsetzen – zum Beispiel per Fingerabdruck. Spezialsoftware verschlüsselt vertrauliche Dokumente.

**Hotspots sicher nutzen.** Vor Nutzung eines öffentlichen Funknetzes (Hotspot) sich darüber informieren, welche Sicherheitsvorkehrungen der Betreiber getroffen hat. Sensible Daten nur verschlüsselt übertragen. Hotspots nur mit geschützten Geräten benutzen (aktueller Virenschutz, lokale Firewall).

**Bluetooth-Lücken schließen.** Standard-PIN durch eigene, mindestens achtstellige PIN ersetzen; Benutzererkennung verstecken; Verschlüsselung und Authentisierung aktivieren. Automatische Bluetooth-Verbindungen nur mit bekannten Geräten zulassen.



## Mobile Datenträger sichern

Diese Sicherheitsmaßnahmen sind besonders wichtig: USB-Sticks vor Datenklau absichern (\*) und die eigene EDV vor Schad-Sticks schützen.

**Verschlüsselungssoftware installieren.\*** Sticks ins Verschlüsselungskonzept des Unternehmens integrieren.

**Biometrische Erkennung nutzen.\*** Sticks mit Fingerprintsensor geben Daten erst nach Überprüfung des Abdrucks frei.

**Kopierschutz einrichten.** Programme verschlüsseln Dokumente beim Übertragen vom PC auf einen USB-Stick.

**Autostart abschalten.** Für fremde Sticks nicht auf Firmenrechnern die Autostart-Funktion freigeben.

**U3-Sticks im Firmennetz einschränken.** Unbefugte können damit auf Firmen-PCs eigene Programme ausführen und Sicherheitsmaßnahmen unterlaufen.

**Werbe-Sticks per Virenschutz überprüfen.** Auf geschenkten Sticks kann ein Schadprogramm sein.

## Handlungshelfer

**IT-Grundschutz.** Detaillierte Handlungsanweisungen zum Schutz von IT und Telekommunikation enthält die Website des Bundesamtes für Sicherheit in der Informationstechnik. [www.bsi.bund.de](http://www.bsi.bund.de)



**Basisprüfung IT-Sicherheit:** Kostenlose Vor-Ort-Beratung hilft bei der Einschätzung des eigenen IT-Sicherheitsniveaus weiter. Infos unter [www.secure-it.nrw.de](http://www.secure-it.nrw.de)

**Branchenbuch IT-Sicherheit:** Kostenfreies Online-Portal für die Suche nach geeigneten IT-Sicherheitslösungen und IT-Dienstleistern. [www.branchenbuch-it-sicherheit.de](http://www.branchenbuch-it-sicherheit.de)



Telefongespräche sind für Wirtschaftsspione eine lohnende Informationsquelle. Mit wenigen Maßnahmen sorgen Firmen dafür, dass keine Interna nach außen dringen.

## So schützen Firmen ihre Telekommunikation

In der Vergangenheit waren Telefonwanzen eine bei Spionen besonders beliebte Spezies: Sie klemmten die Minisender an die Telefonleitung und hörten jedes Telefonat mit. „Heute kommen Spione schneller und einfacher an vertrauliche Firmeninformationen“, berichtet Dr. Hartwig Möller, Leiter des Verfassungsschutzes im nordrhein-westfälischen Innenministerium, „denn Mitarbeiter gehen oft mit der Abhörgefahr im Telekommunikationsbereich leichtfertig um.“

**Diese Verhaltensregeln müssen sich Mitarbeiter besonders gut merken:**

**„Bei Telefonanfragen immer die Identität des Kommunikationspartners hinterfragen, bevor detaillierte Auskünfte gegeben werden.“**

Anrufer erschleichen sich oftmals das Vertrauen durch die Nennung eines bekannten Firmennamens, mit dem Hinweis auf einen Kontakt zur Geschäftsleitung oder verweisen auf ein gemeinsames Treffen auf einer Veranstaltung,

an der auch der Angerufene teilgenommen hat. Mitarbeiter beantworten dann oftmals bereitwillig auch besonders firmenspezifische Fragen. Sie empfinden es meist als unhöflich, die Identität zu hinterfragen. Tipp: Im Zweifelsfall sollen Mitarbeiter die Telefonnummer des Anrufers notieren und nach Klärung der Identität gegebenenfalls zurückrufen.

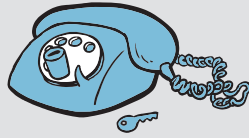
**„Bei der Benutzung eines Mobiltelefons dürfen betriebliche Angelegenheiten nicht in der Öffentlichkeit besprochen werden.“**

Viele Mitarbeiter kommunizieren per Mobiltelefon an öffentlichen Plätzen detailliert über Firmeninterna – sei es im Zugabteil, im Wartebereich des Flughafens oder im Café. Fremde kommen damit aus erster Hand an firmenbezogene Informationen. Wenn sie anschließend im unverbindlichen Gespräch mehr über das Unternehmen und die Funktion des Anrufers erfahren, haben sie schnell das beste Basismaterial für weitere Aktivitäten zusammen.

## Sicher kommunizieren per Telefon

### Sicherheit im Festnetz

**Telefon mit Verschlüsselungstechnik.** Wer mit wichtigen Mitarbeitern oder Geschäftspartnern vertraulich per Festnetz kommunizieren will, kann dafür ein spezielles Zusatzgerät einsetzen. Es wird zwischen dem vorhandenen Endgerät (Telefon, Fax oder PC) und der ISDN-Steckdose installiert und verschlüsselt automatisch die Botschaft. Der Empfänger braucht zum Entschlüsseln ein gleiches Zusatzgerät. Für den Einsatz der Technik in Vermittlungszentralen lassen sich individuelle Sonderlösungen entwickeln.



**Schnurlose DECT-Telefone.** Externe Angreifer können mittels sogenannter Protokollanalytoren passiv den Funkverkehr zwischen Handgerät und Basisstation empfangen und aufzeichnen. Mehr Sicherheit bieten Geräte, die Gespräche zwischen beiden Stationen verschlüsselt übertragen (DECT Standard Cipher). Aufpassen: Durch unbefugtes und unbemerktes Aktivieren der sogenannten Babyphon-Funktion können Angreifer DECT-Geräte auch zum Abhören von Raumgesprächen verwenden.

**Räume bei Bedarf abschirmen.** Unternehmen, die einen wirklich abhörgeschützten Raum brauchen, erreichen das jetzt schnell und kostengünstig mit einer neuen elektromagnetischen Schirmung: Ein mit Kupfer metallisierter Nylonvliesstoff an der Decke, am Boden und an den Wänden ersetzt die bislang übliche Blechabschirmung. Das Material (Emscreen) lässt sich wie eine Tapete verlegen.

### Mobil sicher telefonieren

**Verschlüsselung überprüfen.** In Deutschland erfolgt die Übertragung der Sprachinformationen zwischen Mobiltelefon und Basisstation stets verschlüsselt. Im Ausland ist die Verschlüsselung nicht immer gewährleistet. Abhören ist damit einfach. Tipp: Manche Mobiltelefone zeigen auf dem Display an, wenn die Übertragung zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird. Wenn diese Anzeige an Firmen-Handys vorgesehen ist, die Benutzer darüber informieren.



**Sicherheits-Handy nutzen.** Für vertrauliche Gespräche können Firmen spezielle Mobiltelefone einsetzen. Sie verschlüsseln die Kommunikation automatisch. Beide Gesprächspartner brauchen kompatible Geräte.

**Daten vor Missbrauch schützen.** Täglich gehen zuhauf Handys verloren oder werden gestohlen. Firmendokumente und Kontaktadressen geraten damit schnell in falsche

Hände. Deshalb: Zugriff auf gespeicherte Dateien durch sicheres Passwort (PIN-Nummer) verhindern und Dokumente durch spezielle Softwareprogramme stets verschlüsseln.

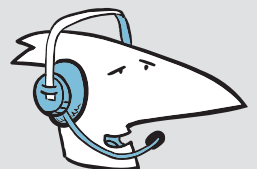
**Abhören vermeiden.** Angreifer können handelsübliche Mobiltelefone auch zum Abhören von Konferenzen einsetzen. Deshalb bei Meetings mit vertraulichem Inhalt das Mitbringen von Handys in den Konferenzraum untersagen. Passive Warngeräte (GSM-Mobiltelefon-Detektoren) melden, wenn sich dennoch Mobiltelefone im Sendebetrieb befinden oder ihn aufnehmen. Tipp: Bei der Übertragung hochsensibler Informationen Mobiltelefone oder SIM-Karten wechseln. Dann ist es enorm aufwendig, gezielt Telefonate abzuhören.

**Manipulierte Mobiltelefone ausschließen.** Mobiltelefone sollten Mitarbeiter nur bei vertrauenswürdigen Händlern kaufen, damit nicht schon beim Erwerb mit einer Manipulation gerechnet werden muss. So werden im Internet spezielle Spionagehandys zum Kauf angeboten, in denen sich das Mikrofon per Anruf aktivieren lässt.

**Vor Spionagesoftware schützen.** Leicht lässt sich auch ein frei verkäufliches Programm (FlexiSPY) auf einem Handy installieren. Es überwacht unbemerkt für den Nutzer alle Aktivitäten des Handybesitzers und gibt automatisch von jeder empfangenen und abgeschickten SMS eine Kopie an eine vorher eingegebene Rufnummer weiter. Bei einem Manipulationsverdacht das Gerät sofort aus dem Verkehr ziehen.

### Geschützt per Internet telefonieren

**Voice over IP.** Vor der Umstellung auf Internet-Telefonie sollten Firmen die Auswirkungen auf die IT-Sicherheit überprüfen. Denn die meisten VoIP-Lösungen übertragen die Sprachpakete in Netzen unverschlüsselt. Mittels im Internet frei erhältlicher Tools lassen sich so Gespräche mitschneiden und anschließend in ein Audio-Format umwandeln. Unverschlüsselt sind auch die Verbindungsdaten.



**Telefonieren per Skype.** Viele Firmen haben das Gratis-Programm Skype auf ihren Rechnern installiert. Sie können so weltweit kostenlos per Internet miteinander telefonieren oder Videokonferenzen abhalten. Skype verschlüsselt Sprache und Daten automatisch mit einem 256-Bit-Schlüssel. Vertrauliche Informationen sind damit umfassender geschützt als bei einem Festnetztelefonat.

## Wer Firmen im Notfall sicher hilft

Gerade einmal acht Prozent aller Unternehmen, deren Betriebsgeheimnisse durch Spione oder Konkurrenten ausgekundschaftet wurden, lassen sich nach einer aktuellen Untersuchung des Branchenverbands BITKOM von Experten helfen. Grund: Die meisten Firmen wissen gar nicht, an wen sie sich wenden sollen. Das Informationsmanko ist schnell behoben: Bei Konkurrenzausspähung sollten Unternehmen die Polizei einschalten, bei Verdacht einer Wirtschaftsspionage den Verfassungsschutz.



**Viele Firmen haben schon vom Einsatz des Verfassungsschutzes profitiert.**

**Beispiel 1:** Als der Verdacht aufkam, dass eine Praktikantin Firmeninformationen weitergeleitet haben könnte, schaltete das Unternehmen den Verfassungsschutz ein. Die Experten überprüften die E-Mail-Korrespondenz der Studentin, fanden heraus, dass darüber wichtige Firmeninformationen nach außen gelangt sind, und erkundeten, wer hinter der E-Mail-Empfängeradresse steckte.

Den Verfassungsschutz können Unternehmen auch dann ansprechen, wenn sie verdächtige Aktivitäten nicht eindeutig dem Spionageumfeld oder Konkurrenten zuordnen können. Er prüft dann, ob der Fall in seinen Zuständigkeitsbereich fällt oder die Polizei dafür zuständig ist. „Firmen brauchen keine Sorge zu haben, dass wir ihnen unangenehme Fragen stellen“, sagt Dr. Hartwig Möller, Leiter des Verfassungsschutzes im nordrhein-westfälischen Innenministerium, „alle Informationen behandeln wir absolut vertraulich.“

**Beispiel 2:** Nach einem Einbruch im Büro eines Geschäftsführers stellten die Verfassungsschützer fest, dass jemand eine Stunde lang an dessen Laptop aktiv war. In dieser Zeit wurden Dateien heruntergeladen und eine Verbindung zum Internet aufgebaut. Vom Verfassungsschutz eingesetzte IT-Experten fanden durch eine Analyse der Protokoll-Dateien schnell heraus, an welchen Dokumenten der Täter interessiert war. Das Unternehmen konnte so rechtzeitig Vorsorge treffen und weiteren Datenklau stoppen.

## Bei Konkurrenzausspähung oder Produktpiraterie hilft die Polizei

Bei Verdacht, dass Konkurrenten heimlich Firmendaten kopiert oder Gespräche abgehört haben, sollten sich Unternehmen an die Polizei wenden.

Die Polizei kann eine Straftat jedoch z. T. nur dann verfolgen, wenn der Geschädigte ausdrücklich einen Strafantrag stellt. Tipp: Bei der Anzeigenerstattung grundsätzlich folgende Formulierung verwenden: „Ich stelle Strafantrag aus allen rechtlichen Gründen.“ Damit ist gewährleistet, dass die Strafverfolgung nicht wegen des fehlenden Antrags eingestellt wird.

**Die örtliche Polizeidienststelle nimmt die Anzeige auf.** Der Polizeibeamte dokumentiert alle tatrelevanten Daten und leitet sie an die kriminalpolizeilichen Spezialisten für Computerkriminalität weiter. Diese übernehmen die weiteren Ermittlungen und wenden sich oftmals mit vertiefenden Fragen noch einmal an den Geschädigten.

**Die Experten beginnen mit der Untersuchung.** Bei Bedarf untersuchen Spezialisten der Polizei den PC oder machen eine Kopie von der Festplatte. Sie werten beispielsweise die vom PC automatisch mitgeschriebenen Protokolle aus – die sogenannten Log Files – und stoßen so oftmals auf die Spuren der Täter.

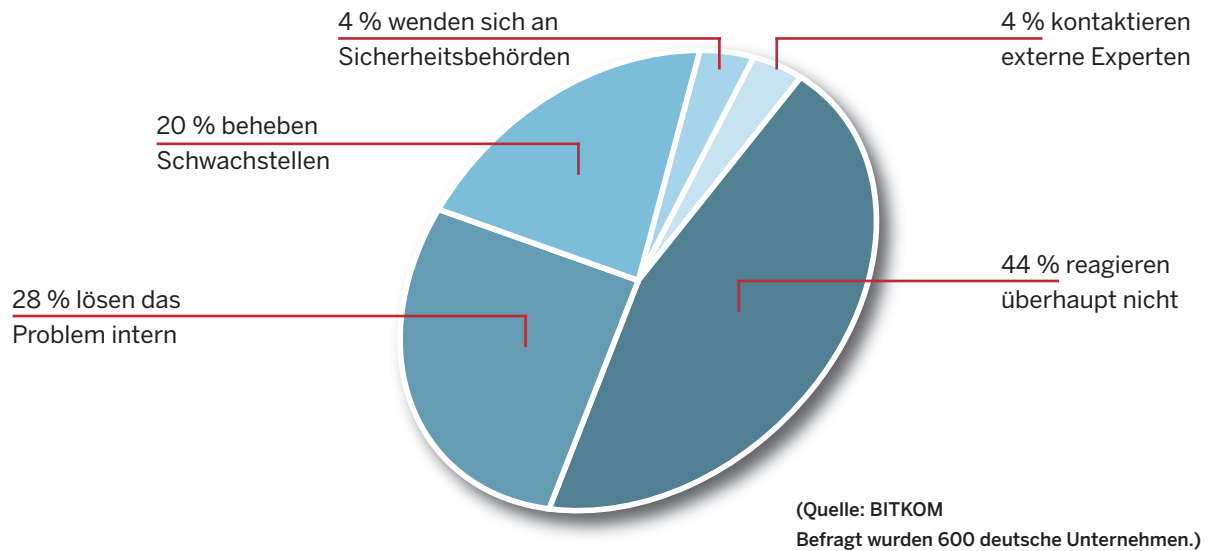
**Die Fahnder spüren den Täter auf.** Bei der Fahndung kann die Polizei vom Netzbetreiber die sogenannte Systemdokumentation anfordern. Daraus lässt sich ablesen, wer wann und mit welcher Computerkennung im Netz unterwegs war. Anhand dieser IP-Adresse lässt sich der Täter oftmals identifizieren und lokalisieren.



Mehr Informationen enthält die Broschüre „**Computerkriminalität: So hilft die Polizei**“

Kostenlos als PDF  
 ⓘ Link auf Seite 17

## Wie reagieren Unternehmen auf das Auskundschaften von Betriebsgeheimnissen?



## Ansprechpartner bei Wirtschaftsspionage ist der Verfassungsschutz

Wenn Firmen den Verdacht haben, dass ausländische Geheimdienste in ihrem Unternehmen aktiv sind, sollten sie den Verfassungsschutz ansprechen. In Nordrhein-Westfalen ist er beim Innenministerium angesiedelt. Ihm gehören 280 Mitarbeiter an – darunter Spezialisten für Schutz und Aufklärung bei Wirtschaftsspionage. Sie bieten Firmen ein großes Spektrum an Hilfeleistungen an.



Detaillierte Auskunft gibt die Broschüre „**Wirtschaftsspionage – Information und Prävention**“

Kostenlos als PDF  
 ⓘ Link auf Seite 17

**Kostenlose Informationen.** Firmen können sich zum Thema Wirtschaftsspionage auch ohne konkreten Anlass an den Verfassungsschutz wenden. Die Experten informieren per Telefon oder im persönlichen Gespräch kostenlos über aktuelle Bedrohungen und Schutzmaßnahmen.

**Beratung in der Firma.** Die Verfassungsschützer kommen zur Beratung auch direkt ins Unternehmen. Dabei wollen sie keine Interna wissen und sich auch nicht im Unternehmen umsehen. Sie berichten vielmehr im Gespräch mit der Geschäftsleitung oder den Mitarbeitern über ihre Erfahrungen zu Aktivitäten von Wirtschaftsspielen. Alle Informationen, die das Unternehmen den Verfassungsschutz-Experten freiwillig gibt, werden vertraulich behandelt.

**Experteneinsatz im konkreten Fall.** Sofern ein Unternehmen einen konkreten Verdacht auf Wirtschaftsspionage hat, kann der Verfassungsschutz mit eigenen Fachleuten oder speziellen Experten aktiv werden. Für technische Untersuchungen greift der Verfassungsschutz auf IT-Spezialisten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zurück.

# Akteure im Kampf gegen Wirtschaftsspionage und Konkurrenzausspähung

Zum Schutz vor Wirtschaftsspionen und kriminellen Konkurrenten können Firmen in Nordrhein-Westfalen auf kompetente Partner zugreifen. Sie helfen mit fundierten Informationen und tatkräftigem Handeln.



**Landesinitiative »secure-it.nrw«** unterstützt Unternehmen mit Informationen für mehr Sicherheit bei elektronischen Geschäftsprozessen. Materialien zur Sensibilisierung finden Sie unter:  
[www.secure-it.nrw.de](http://www.secure-it.nrw.de)



**Polizei Nordrhein-Westfalen** ermittelt bei Straftaten.  
[www.polizei-nrw.de](http://www.polizei-nrw.de)



**Verband für Sicherheit in der Wirtschaft Nordrhein-Westfalen e. V.** bietet Information, Beratung und Schulung zu sicherheitsrelevanten Themen.  
[www.vsw-nw.de](http://www.vsw-nw.de)



**Verfassungsschutz in Nordrhein-Westfalen** informiert Firmen über Gefahren und Schutzmaßnahmen gegen Wirtschaftsspionage. Übernimmt die nachrichtendienstliche Fallbearbeitung.  
[www.im.nrw.de/verfassungsschutz](http://www.im.nrw.de/verfassungsschutz)



**Sicherheitsberater** helfen Unternehmen bei Aufbau und Realisierung einer Sicherheitsstrategie. Experten finden Firmen über:  
[www.branchenbuch-it-sicherheit.de](http://www.branchenbuch-it-sicherheit.de)

## Wer leistet was?

Präventionsarbeit	... zur Verhütung von Spionage mithilfe klassischer Methoden	... zur Verhütung von Spionage mithilfe von IT-Technik
Sensibilisierung, Information		
Beratung		
Qualifizierung		
Lösungshilfe für Schutzmaßnahmen		
<b>Strafverfolgung</b>		
bei Wirtschaftsspionage		
bei Konkurrenzausspähung		

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Nordrhein-Westfalen herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden.

Dies gilt für Landtags-, Bundestags- und Kommunalwahlen sowie auch für die Wahl der Mitglieder des Europäischen Parlaments.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Eine Verwendung dieser Druckschrift durch Parteien oder sie unterstützende Organisationen ausschließlich zur Unterrichtung ihrer eigenen Mitglieder bleibt hiervon unberührt. Unabhängig davon, wann, auf welchem Wege und in welcher Anzahl diese Schrift dem Empfänger zugegangen ist, darf sie auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zu Gunsten einzelner politischer Gruppen verstanden werden könnte.



## Link-Liste Broschüren

Unter diesen Internetadressen können Sie die Broschüren als PDF herunterladen:

### **Mitarbeiter sensibilisieren für IT-Sicherheit und Datenschutz**

[www.secure-it.nrw.de/\\_media/pdf/sec\\_1250.pdf](http://www.secure-it.nrw.de/_media/pdf/sec_1250.pdf)



### **Computerkriminalität: So hilft die Polizei**

[www.secure-it.nrw.de/\\_media/pdf/initiative/compkrim\\_neu\\_2008.pdf](http://www.secure-it.nrw.de/_media/pdf/initiative/compkrim_neu_2008.pdf)



### **Wirtschaftsspionage – Information und Prävention**

[www.im.nrw.de/sch/doks/vs/wirtsch.pdf](http://www.im.nrw.de/sch/doks/vs/wirtsch.pdf)



## Kontakt

Agentur »secure-it.nrw«  
 bei der IHK Bonn/Rhein-Sieg  
 Bonner Talweg 17, 53113 Bonn  
 Telefon: +49 (0) 228 / 2284-184  
 Telefax: +49 (0) 228 / 2284-5184  
 E-Mail: [info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)  
 Internet: [www.secure-it.nrw.de](http://www.secure-it.nrw.de)  
[www.branchenbuch-it-sicherheit.de](http://www.branchenbuch-it-sicherheit.de)

Bei Verdachtsfällen von Wirtschaftsspionage:  
 Innenministerium  
 des Landes Nordrhein-Westfalen  
 Abteilung Verfassungsschutz  
 Haroldstraße 5, 40213 Düsseldorf  
 Tel. +49 (0) 211 / 871-2821  
 Fax: +49 (0) 211 / 871-2980  
 E-Mail: [kontakt.verfassungsschutz@im.nrw.de](mailto:kontakt.verfassungsschutz@im.nrw.de)  
 Internet: [www.im.nrw.de/verfassungsschutz](http://www.im.nrw.de/verfassungsschutz)

Verband für Sicherheit in der Wirtschaft  
 Nordrhein-Westfalen e. V. (VSW NW)  
 Uerdinger Straße 56, 40474 Düsseldorf  
 Tel.: +49 (0) 211 / 157757-0  
 Fax: +49 (0) 211 / 157757-15  
 E-Mail: [info@vsw-nw.de](mailto:info@vsw-nw.de)  
 Internet: [www.vsw-nw.de](http://www.vsw-nw.de)

