SCRYPTOS

Wirtschafts-**spionage**

Nicht nur Konzerne stehen im Fokus

Detlef Hastik
Henry Frenz

Was ist Wirtschafts - bzw. Industriespionage?

Das Bundesamt für Verfassungsschutz definiert Wirtschaftsspionage als „staatlich gelenkte oder gestützte, von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Wirtschaftsunternehmen und Forschungseinrichtungen.“[1]

Betreibt hingegen ein konkurrierendes Unternehmen eine Ausforschung, handelt es sich um Konkurrenzausspähung oder auch Industriespionage.[2] In den meisten Fällen handelt es sich dabei um die illegale Beschaffung von betriebsinternen Informationen.

Da es in diesem Whitepaper um den Schutz der Unternehmen geht, werden die beiden Begriffe von hieran synonym verwendet.

Wirtschaftsspionage früher und heute

Wirtschaftsspionage hat eine lange Historie und wurde damals wie heute dazu verwendet, Monopolstellungen von Staaten und Industriezweigen zu brechen. Gängige Beispiele für die beginnende Produktionsspionage findet man in der Seiden-, Stahl-, Papier-, Porzellan-, sowie der Kautschukindustrie.[3]

Auch heute gibt es noch zahlreiche Fälle von Industriespionage. Zu den aktuellen Beispielen zählt unter anderen der Fall der clearaudio electronic GmbH. Hier kam es zum Patentdiebstahl und das entsprechende Produkt wurde durch einen chinesischen Wettbewerber auf den Markt gebracht, bevor clearaudio es veröffentlichen konnte. Hacker waren von außen in das Unternehmensnetzwerk eingedrungen und hatten die sensiblen Daten entwendet.[4]

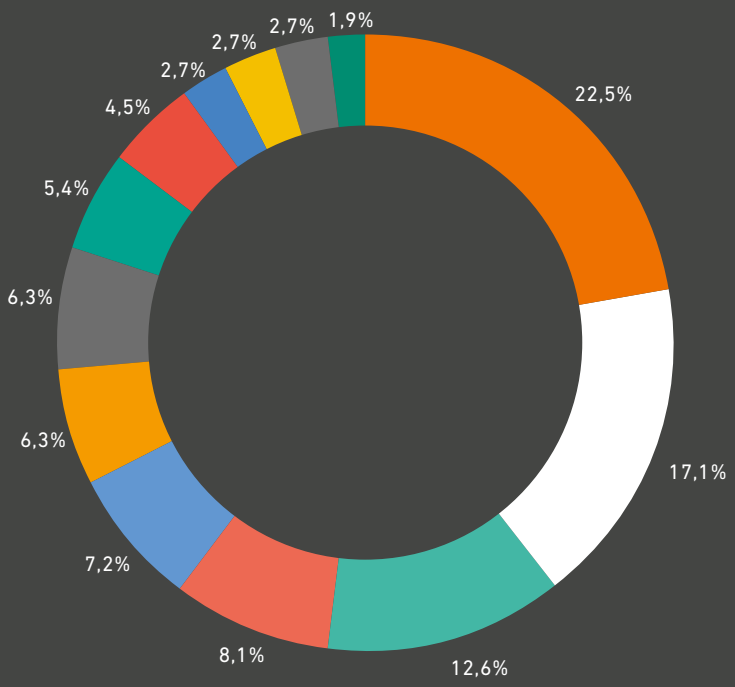
Im Jahr 2016 war die Deutsche Telekom Ziel von Wirtschaftsspionage. Hier war der Weg jedoch ein anderer. Ein Mitarbeiter der Deutschen Telekom nahm Bestechungsgelder des chinesischen Technologiekonzerns ZTE an und verriet im Gegenzug Betriebsgeheimnisse hinsichtlich des Einkaufsunternehmens Buyin.[5]

Für die meisten deutschen Unternehmen besitzt das Thema Industrie- oder Wirtschaftsspionage nur eine untergeordnete Relevanz, weil sie davon ausgehen, nicht im Fokus zu stehen.
Dies ist jedoch ein gefährlicher Trugschluss: **90% der Fälle von Wirtschaftsspionage betreffen mittelständische Unternehmen.**[6]

Im Vordergrund des Ausforschungsinteresses stehen innovative ebenso wie alteingesessene deutsche Unternehmen aus allen Branchenzweigen. Durch die zunehmende Globalisierung ist der Konkurrenzdruck zwischen den Mitbewerbern stetig gestiegen.
Dies hat in letzter Konsequenz einen Kampf um Marktanteile mit allen Mitteln zur Folge. Da kleinere und mittlere Unternehmen oftmals nicht über die personellen oder finanziellen Ressourcen verfügen, technologisch state oft the art zu sein, stehen diese Unternehmen meist im Fokus von Wirtschaftsspionage.[7]

1, 2 Vgl. BfV – Wirtschaftsspionage
3 Vgl. J. Meissinger.
4 Vgl. IHK Niederrhein.
5 Vgl. RP Online.
6 Vgl. IHK Niederrhein.
7 Vgl. BfV – Wirtschaftsspionage

Übersicht betroffener Branchen



- Automobil- / Luftfahrzeug- / Schiffs- / Maschinenbau
- Chemie / Pharma / Biotechnologie
- Elektro / Elektronik / Feinmechanik / Optik
- Eisen und Stahl / Metallverarbeitung / Grundstoffe
- Logistik / Verkehr
- Banken / Finanzdienstleistungen / Versicherungen
- Computer / Software
- Handel / E-Commerce
- Telekommunikation / Internet
- Versorgung / Energie
- Textil / Bekleidung / Leder / Holz / Glas
- Immobilien / Wohnungswirtschaft
- Unternehmens- / Personal- / Steuerberatung / Wirtschaftsprüfung

Abbildung 1.[8]

Keyfacts

- Mehr als jedes zweite deutsche Unternehmen wird ausspioniert.[9]
- 30% der Angriffe werden nur zufällig entdeckt.[10]
- 60% der Angriffe erfolgen aus dem Ausland.[11]
- Angriffe richten sich ebenso stark gegen KMUs wie gegen Konzerne.[12]
- 75% der angegriffenen Unternehmen erleiden einen finanziellen Schaden.[13]
- Der jährliche Schaden für die deutsche Wirtschaft beläuft sich auf bis zu 55 Mrd. €.[14]

---

8 Vgl. Corporate Trust.
9 Vgl. bitkom, Corporate Trust.
10, 11 Vgl. bitkom.
12 Vgl. bitkom, Corporate Trust.
13 Vgl. Corporate Trust.
14 Vgl. bitkom.

Datenklau, Spionage, Sabotage:
Jeder Zweite ist betroffen

War Ihr Unternehmen in den letzten zwei Jahren von Datenklau, Industriespionage oder Sabotage betroffen?

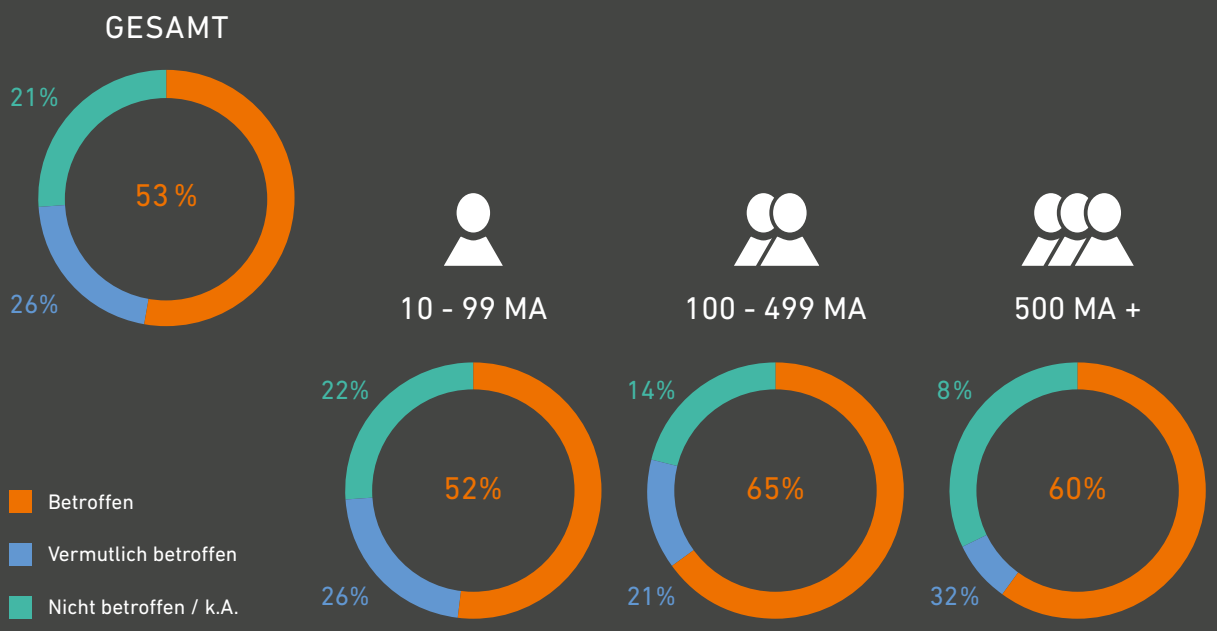


Abbildung 2: Wirtschaftsspionage und Unternehmensgröße | Quelle: bitkom – Wirtschaftsschutz in der digitalen Welt
Basis: Alle befragten Unternehmen (n=1.069) | bitkom research

Die Zahlen aus der aktuellen Studie der bitkom und des Verfassungsschutzes belegen in plakativer Art und Weise, dass Unternehmen jeder Größenordnung von Wirtschaftsspionage betroffen sind.

Die Kombination der Werte „Betroffen“ und „Vermutlich betroffen“ zeigen weiterführend das enorme Gefährdungspotential, welches durch Industriespionage für die heimische Wirtschaft entsteht (Vgl. Abbildung 2).[15]

Betrachtet man die Art der Handlungen genauer, wird deutlich wie breit gefächert die Angriffe sind und dass bis zu 38% der deutschen Unternehmen in den letzten beiden Jahren Opfer von digitalen Daten- bzw. Informationsdiebstahl geworden sind (Vgl. Abbildung 3).

15 Vgl. bitkom

Täter haben es **nicht immer nur auf Daten** abgesehen

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten zwei Jahre betroffen?

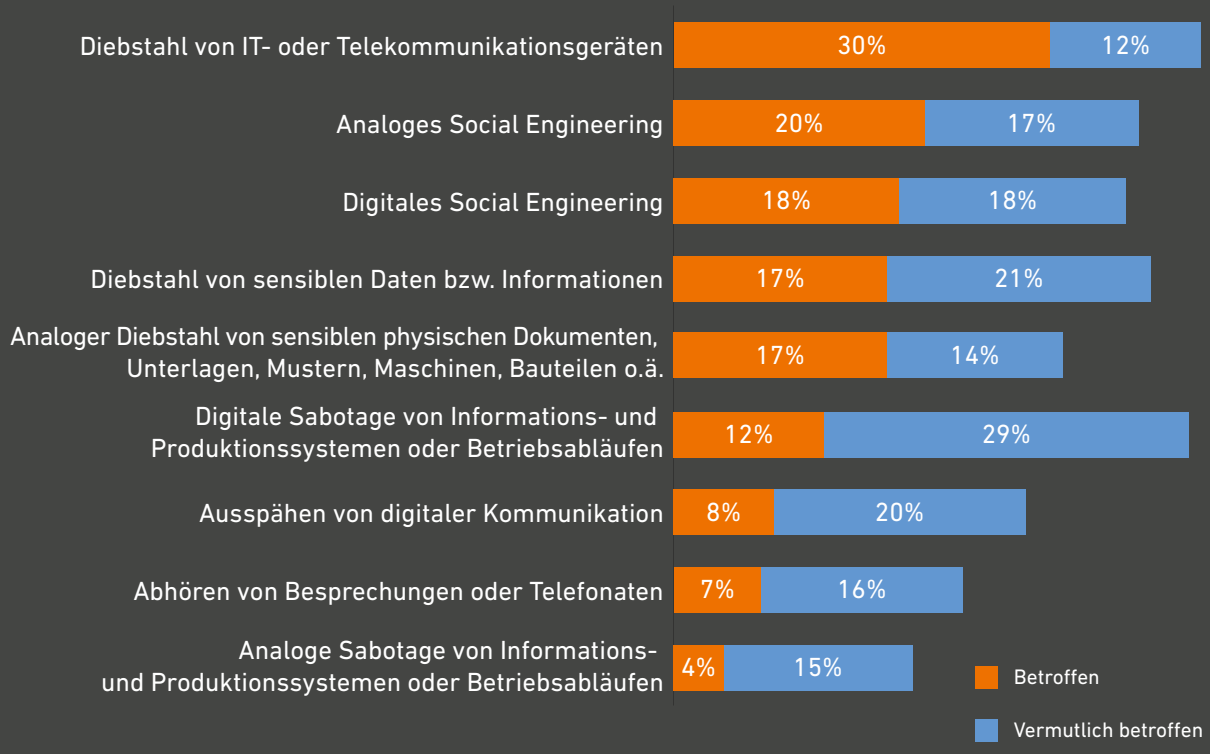


Abbildung 3: Schadenskategorien der Wirtschaftsspionage und -sabotage | Quelle: bitkom – Wirtschaftsschutz in der digitalen Welt
Basis: Alle befragten Unternehmen (n=1.069) | bitkom research

Methoden der Wirtschaftsspionage[16]

Im Rahmen der Wirtschaftsspionage werden verschiedene Ansätze der Informationsbeschaffung unterschieden.

Human Source Intelligence (HUMINT) beschreibt die Informationsgewinnung mit Hilfe des Menschen.[17] Dem gegenüber steht die Informationsbeschaffung mit technischen Mitteln (TECHINT: Technical Intelligence), die wiederum in Unterkategorien hinsichtlich der genutzten Techniken unterschieden wird.[18]

16 Vgl. BfV – Witschaftsspionage
17 Vgl. BND
18 Vgl. Carl von Ossietzky Universität Oldenburg

Wirtschaftsspionage via HUMINT

Eines der größten Risiken für Unternehmen hinsichtlich Wirtschaftsspionage ist der Mensch selbst. Alle technischen Sicherheitsvorkehrungen verlieren an Wirkung, wenn der potenzielle Täter sich im Inneren des Unternehmens befindet.

Hierbei lassen sich drei Risikogruppen unterscheiden: Externes Personal, Besucher und die eigenen Mitarbeiter.[19]

In Unternehmen wird oft externes Personal eingesetzt. Zu den häufigsten Bereichen zählen Projektmanagement, Facility Management oder der Sicherheitsdienst. Eine Kontrolle dieser Gruppen hinsichtlich der Bewegung im Unternehmen ist kaum möglich. Umso wichtiger ist es, sensible Informationen zu sichern, besonders sensible Bereiche mit Zugangskontrollen zu versehen und den Zugriff auf technische Systeme zu reglementieren.

Durch die Nutzung von SCRYPTOS kann der Zugriff des externen Personals auf die Daten genau auf die notwendigen Bedürfnisse eingeschränkt werden, ohne dass diese Zugang zum Unternehmensnetzwerk benötigen.

Ein zusätzliches Gefährdungspotential entsteht durch externe Lieferanten und erhöhten Kunden bzw. Publikumsverkehr. Hier müssen noch strengere Sicherheitsvorkehrungen greifen als bei externem Personal. Besucher sollten sich nur in besonders dafür ausgelegten Bereichen bewegen können und ansonsten immer in Begleitung eines Unternehmensangehörigen sein.

Deutlich schwieriger ist die Absicherung gegenüber eigenen Mitarbeitern. Oftmals haben Mitarbeiter heute noch weitreichenden Zugriff auf Informationen und genießen ein hohes Vertrauen. Somit ist es ihnen oftmals möglich, sich auch in sensiblen Unternehmensbereichen frei zu bewegen. Sind PCs nicht entsprechend gesichert, ist somit bspw. das Einschleusen eines Keyloggers ohne großen Aufwand möglich.

Ein weiteres Risiko stellen aber ebenso offen abgelegte Unterlagen an den Arbeitsplätzen von Kollegen und Vorgesetzten dar. Unachtsamkeit dieser Art wird auch in der Öffentlichkeit zu einem Problem, wenn sensible Informationen bspw. durch lautstarke Telefonate im Zug oder am Flughafen, offen einsehbar auf dem Laptop-Bildschirm oder bei der Nutzung öffentlicher WLAN-Netzwerke ungeschützt sind.[20]

Mindestens ebenso riskant ist aber schlichtweg der Verlust oder Diebstahl mobiler Geräte, wenn diese nicht ausreichend geschützt sind. Wie verbreitet dieses Problem ist, zeigen aktuelle Zahlen:

- 175.000 Laptops verschwinden jährlich an den 8 größten Flughäfen Europas.
- 12.000 Laptops verschwinden wöchentlich an den Flughäfen in den USA, d.h. 648.000 Geräte pro Jahr. 57% der in Fundbüros abgegebenen Geräte werden nicht abgeholt.
- In Deutschland werden jährlich 4.000.000 Handys verloren oder gestohlen.[21]

Mit SCRYPTOS sind ihre Daten auch im Verlustfall des Endgerätes sicher, da die Daten nicht auf diesem gespeichert, sondern ausschließlich sicher in Rechenzentren in Deutschland abgelegt sind.

Informationsverluste drohen auch beim Ausscheiden von Mitarbeitern aus dem Unternehmen, insbesondere, wenn diese im Streit gehen. Diese Mitarbeiter sammeln oftmals Aufzeichnungen, Beschreibungen von Produkten bis hin zu ganzen Datenbanken.[22] Auch hier schützt SCRYPTOS, da alle Aktionen in einem revisionssicheren Auditlog aufgezeichnet werden.

---

19 Vgl. BfV – Wirtschaftsspionage
20 Vgl. Carl von Ossietzky Universität Oldenburg
21 Vgl. Zentrales Fundbüro
22 Vgl. Carl von Ossietzky Universität Oldenburg

Social Engineering

Eine Sonderform der menschlichen Informationsbeschaffung stellt Social Engineering dar. Das BSI beschreibt definiert Social Engineering wie folgt:

„Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten."[23]

Die Methode des Social Engineerings verspricht insbesondere in Unternehmen mit überdurchschnittlichen IT-Sicherheitsvorkehrungen gute Chancen für den Angreifer. Aber auch immer mehr kleine und mittelständische Unternehmen sind davon betroffen. Dazu nutzen die Kriminellen die größte Schwachstelle eines Unternehmens: seine Mitarbeiter.

Social Engineering Angriffe beschränken sich nicht auf den persönlichen Kontakt, sondern betreffen bspw. auch Telefonanrufe, E-Mails und soziale Netzwerke.

Mehr als 60 Prozent der Angriffe[24] auf die unternehmensweite IT erfolgen heutzutage nicht mehr von außen, sondern von den eigenen Mitarbeitern. Nicht weil sie generell böswillig sind, sondern weil sie manipuliert werden und aus Unwissenheit oder Bequemlichkeit betriebliche Sicherheitsvorgaben missachten.

Angreifer nutzen dazu menschliche Eigenschaften wie Gutgläubigkeit, Hilfsbereitschaft, Stolz, Konfliktvermeidung oder Respekt vor Autoritäten aus, um mit psychologischen Tricks an die gewünschten Informationen zu gelangen.

Ein Social Engineering-Angriff beginnt in der Regel mit der Beschaffung von allgemeinen Informationen über das Unternehmen, das angegriffen oder ausspioniert werden soll. Schon ein Organigramm und eine Telefonliste können einem versierten Angreifer genügen. Dieser ruft nun in dem Wissen um die vorherrschenden hierarchischen Strukturen beim Unternehmen an. Der Angreifer täuscht eine falsche Identität vor, um sich durch eine geschickte Fragestellung und mit psychologischen Mitteln langsam an die Zielinformation heranzutasten. Häufig schlüpft der Täter in die Rolle einer Autoritäts- oder Vertrauensperson. Dabei sammelt er Informationspuzzlesteine, die ihn an anderer Stelle als vertrauenswürdig erscheinen lassen.

Das Hauptaugenmerk des Social Engineers liegt dabei meist auf Passwörtern. Der Angreifer täuscht ein Problem vor, das einer sofortigen Lösung bedarf, z.B. ein Hackerangriff, der sofortigen Zugriff auf den Account des Mitarbeiters erfordert. Weil er bestimmt und autoritär auftritt, sein Opfer zuvor unter psychologischen Gesichtspunkten ausgewählt hat und es zusätzlich mit Stress konfrontiert, gibt ihm dieses oftmals bereitwillig die Zugangsdaten heraus.

Mit diesen Informationen ist der Angreifer in der Lage erheblichen Schaden anzurichten. Dabei sind nicht immer nur Geschäftsgeheimnisse, Patente oder Entwicklungsblaupausen von Interesse, sondern oft auch schlichtweg die Finanzen des Unternehmens.

2016 wurde der Autozulieferer Leoni unter Zuhilfenahme gefälschter Dokumente und Identitäten sowie mittels elektronischer Kommunikation dazu veranlasst, Gelder des Unternehmens auf Zielkonten ins Ausland zu transferieren. Es entstand ein Schaden in Höhe von 40 Millionen Euro.[25]

---

23 Vgl. BSI
24 Vgl. bitkom
25 Vgl. heise

Technical Intelligence (TECHINT)

Informationsgewinnung mit Hilfe von Technik

TECHINT bezeichnet die Informationsgewinnung mit rein technischen Mitteln. Hierbei geht es um die Ausnutzung technischer Schwachstellen, um Informationen zu sammeln oder Schaden zu verursachen. Das Eindringen in Systeme durch Computerviren, Trojaner, Skimming aber auch Bruteforce-Attacken etc. gehört zum klassischen Handwerkszeug der Wirtschaftsspionage.

Aufgrund der Informationsverbreitung im Internet bzw. Darknet sind ausreichend Skripte vorhanden, die selbst Standard-Nutzer in die Lage versetzen, ohne tiefgreifendes Wissen Schäden zu verursachen.

Zusätzliche Informationen finden Sie in unserem Whitepaper „Trügerische Sicherheit durch SSL-Zertifikate“

SCRYPTOS speichert Ihre Daten ausschließlich in hochsicheren Rechenzentren in Deutschland. Hierdurch sind diese Daten unabhängig von der Sicherheit des Unternehmensnetzwerks geschützt und genießen höchsten Schutz vor technischer Spionage.

Prävention

Durch einige wenige Maßnahmen können sie das Gefährdungspotential ihres Unternehmens verringern.

- Sensibilisierung und Schulung der Mitarbeiter.
- Stetige Begleitung von Gästen, Lieferanten und Dienstleistern durch eigene Mitarbeiter.
- Clean Desk Policy.
- Beschränkung des Zugangs zu sensiblen Daten und Informationen durch die Nutzung von SCRYPTOS.
- Sicherung mobiler Devices bzw. Beschränkung für lokale Speicherung. Durch die Nutzung von SCRYPTOS liegen die Daten nicht auf den lokalen Endgeräten, sondern nur in hochsicheren Rechenzentren in Deutschland.
- Portverschlüsselung.
- Ausreichende Ressourcen für IT Security und Datenschutz.
- Festlegung von Prozessen hinsichtlich Datenaustausch und Kommunikation unter Berücksichtigung der IT Security und des Datenschutzes.

Warum SCRYPTOS?

Wirtschaftsspionage betrifft Unternehmen aller Größenklassen und Branchen in Deutschland. Der Anteil betroffener Unternehmen alleine aus den letzten 2 Jahren zeigt, dass das bisherige Schutzniveau nicht ausreichend ist und Unternehmen ihre sensiblen Daten deutlich besser gegen Spionage und Sabotage sichern müssen.

SCRYPTOS schützt Ihre Daten zuverlässig vor Wirtschafts- und Industriespionage.

Durch die detaillierten Rechtestrukturen ist sichergestellt, dass nur die wirklich relevanten Mitarbeiter Zugriff auf kritische Informationen besitzen.

Darüber hinaus lässt sich feingliedrig festlegen, welche Rollen welche Funktionen innerhalb des Systems nutzen dürfen.

Durch das Vermeiden der lokalen Speicherung von Daten werden Endgeräte als häufigste Quelle für Wirtschaftsspionage weitgehend ausgeschlossen. Da die Daten nur in Rechenzentren und nicht im Unternehmensnetzwerk gespeichert sind, sind sie ebenso vor den Augen nicht authentifizierter Mitarbeiter sicher.

Überzeugen Sie sich selbst und melden Sie sich noch heute für einen Testzugang auf **www.scryptos.com** an.

Quellen:
[1], [2], [7], [16], [19] Bundesamt für Verfassungsschutz – Wirtschaftsspionage: Risiko für Unternehmen, Wissenschaft und Forschung;
www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/Spionage/Wirtschaftsspionage_Risiken.pdf?__blob=publicationFile&v=4
[3] J. Meissinger (2006) - Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland, Hamburg.
[4], [6] IHK Niederrhein – tw 03/2016: Tatort Internet: Im Visier von Industriespionen.
[5] RP Online – Spionageangriff gegen Telekom;
www.rp-online.de/wirtschaft/unternehmen/zte-unter-verdacht-spionageangriff-gegen-telekom-aid-1.6151657.
[8], [9], [12], [13] Corporate Trust – Studie: Industriespionage 2014.
[9], [10], [11], [12], [14], [15] bitkom – Wirtschaftsschutz in der digitalen Welt, 2017.
[17] BND – Informationsgewinnung;
www.bnd.bund.de/DE/Auftrag/Informationsgewinnung/HUMINT/humint_node.html.
[18], [20], [22] Carl von Ossietzky Universität Oldenburg - Industriespionage und Angriffe auf Firmen;
www.informatik.uni-oldenburg.de/~iug14/is/.
[21] Zentrales Fundbüro – Faktencheck;
www.zentralesfundbuero.com/de/faktencheck.
[23] BSI – Glossar;
www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817308.
[24] bitkom – IT-Sicherheit in der Industrie, 2016.
[25] heise – „Chef-Masche": Kriminelle klauen wohl per Social Engineering 40 Millionen Euro;
www.heise.de/newsticker/meldung/Chef-Masche-Kriminelle-klauen-wohl-per-Social-Engineering-40-Millionen-Euro-3296847.html.

SCRYPTOS

Kontakt:
SYGNOMI GmbH
Am Kreuzstein 80 | 63477 Maintal
06109-24 54 0 | mail@sygnomi.de

Vertrieb:
SMC Consult GmbH
040-8888 299 69 | vertrieb@sygnomi.de

Autor:
Detlef Hastik

Version: 1.0
Veröffentlichungsdatum: 20.10.2017

EINFACH VIERFACH SICHER.