Wirtschaftsschutztag Sachsen-Anhalt –

Effizienter Schutz für Unternehmen im In- und Ausland

IHK
Industrie- und Handelskammer Magdeburg
Regional. Unternehmerisch. Stark.

SACHSEN-ANHALT
Ministerium für Inneres und Sport

IHK
Industrie- und Handelskammer Halle-Dessau

Vorwort

Jochen Hollmann
Leiter der Abteilung Verfassungsschutz im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt

Am 16. September 2015 hat die Abteilung Verfassungsschutz des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt in Kooperation mit den Industrie- und Handelskammern Sachsen-Anhalts erstmals den Wirtschaftsschutztag des Landes Sachsen-Anhalt im IGZ Innovations- und Gründerzentrum Magdeburg GmbH in Barleben (Bördekreis) durchgeführt.

Unter dem Titel **„Effizienter Schutz für Unternehmen im In- und Ausland“** wandten sich Experten von Sicherheitsbehörden des Bundes sowie aus der Wirtschaftspraxis an das interessierte Fachpublikum mit ca. 100 Teilnehmern aus Wirtschaft und Verwaltung.

Der Wirtschaftsschutztag war darauf ausgerichtet, Beratungs- und Unterstützungsspektren des Wirtschaftsschutzes aufzuzeigen und Präventions- und Lösungsansätze vorzustellen.

Deshalb standen im Mittelpunkt der Veranstaltung u. a. folgende zentrale Fragen:

- Wie schütze ich mein Unternehmen vor fremder Ausspähung?
- Welche Hilfen werden meinem Unternehmen angeboten?
- Wie bewege ich mich sicherer auf ausländischen Märkten?
- Kann ich von den Erfahrungswerten anderer Unternehmen profitieren?

Herr Klaus Olbricht, Präsident der Industrie- und Handelskammer Magdeburg, begrüßte die Tagungsteilnehmenden. Die Tagesmoderation der Veranstaltung hatte der Herausgeber und Chefredakteur des Wirtschaftsmagazins „Aspekt“, Herr Rolf-Dietmar Schmidt, übernommen.

Die Veranstaltung eröffnete Herr Minister, der in seiner Ansprache die Bedeutung des Wirtschaftsschutzes deutlich machte, dem sich sowohl die Verfassungsschutzbehörde als auch die Unternehmensverantwortlichen des Landes Sachsen-Anhalt stellen müssen. Geeignete Maßnahmen des Wirtschaftsschutzes als präventiven Teil der Spionageabwehr seien geeignet, einen illegalen Know-how Transfer durch fremde Nachrichtendienste aus deutschen Unternehmen und Forschungseinrichtungen zu verhindern oder zumindest zu erschweren.

Herr Minister Stahlknecht betonte, der Verfassungsschutz werde auch in Zukunft die Kooperation mit den sachsen-anhaltischen Unternehmen und Unternehmensverbänden fortsetzen und als Kooperationspartner zur Verfügung stehen, sei es durch öffentliche Vorträge, Vorträge zur Sensibilisierung der Firmenbelegschaft oder durch vertrauliche Gespräche mit den Entscheidungsträgern.

Entsprechend reichten die Themenspektren von der Darstellung behördlicher Perspektiven und Angebote zum Wirtschaftsschutz über Beiträge zum Engagement der Konzerne bis zu Berichten und Erfahrungen aus der Wirtschaft.

Nicht nur im Ausland engagierte, sondern auch lokal agierende Unternehmen sind aufgrund ihrer Innovationsfähigkeit und Forschungsaktivitäten immer häufiger Zielobjekte von Wirtschaftsspionage und Sabotageangriffen.

Die Schärfung des Sicherheitsbewusstseins und der Schutz des geistigen Know-hows sowie der eigenen Informations- und Kommunikationssysteme rücken durch die globale Vernetzung und die zunehmende Digitalisierung immer mehr in den Fokus der deutschen Wirtschaft. Die Sicherheit von Unternehmen hat sich zu einem wesentlichen Standortfaktor entwickelt. Prävention und sicherheitsrelevantes Verhalten werden dabei für Entscheidungsträger in Unternehmen zu immer komplexeren Herausforderungen. Ausländische – insbesondere nichteuropäische Märkte mit anderen Rechtstraditionen – bedürfen einer erhöhten Wachsamkeit und besonderen Sorgfalt bei der Vorbereitung, Durchführung und Nachbereitung der Reisen dorthin.

Als Praxisschwerpunkt der Tagung vermittelte der Unternehmensberater Fred Maro anhand prägnanter Beispiele zentrale Hinweise zum Umgang mit „social engineering“, einer Methode des Vorspiegelns falscher Tatsachen und geschickten Fragenstellens zur unrechtmäßigen Erlangung von Geschäftsgeheimnissen.

Die Industrie- und Handelskammer Halle-Dessau gab Hinweise, die Auslandsaufenthalte von Mitarbeitern sicherer zu gestalten. Ein Magdeburger Unternehmer berichtete von der erfolgreichen Durchsetzung von geistigen Schutzrechten.

Ergänzend sei auf die Internetseite des Verfassungsschutzes Sachsen-Anhalt unter:
www. mi.sachsen-anhalt.de/verfassungsschutz
mit weiteren für die Firmensicherheit relevanten Informationen verwiesen.

Allen Mitwirkenden danke ich für Ihre Bereitschaft bei der Vorbereitung und Durchführung dieses Wirtschaftsschutztages.

Magdeburg, im Juni 2016

Inhalt

Hinweis:
Die Beiträge der Referenten bringen die Auffassungen der jeweiligen Verfasser zum Ausdruck.

Begrüßung

Klaus Olbricht
Präsident der Industrie- und Handelskammer Magdeburg

Es gilt das gesprochene Wort!

Sehr geehrter Herr Minister,
sehr geehrte Referenten der Veranstaltung,
meine sehr verehrten Damen,
sehr geehrte Herren,

im Namen der Industrie- und Handelskammern Halle-Dessau und Magdeburg und des Ministerium für Inneres und Sport des Landes Sachsen-Anhalt heiße ich Sie herzlich willkommen zu unserem Wirtschaftsschutztag.

Es ist mir eine große Freude, Sie, sehr geehrter Herr Minister Stahlknecht, als Schirmherr dieser Veranstaltung begrüßen zu dürfen und gemeinsam mit Ihnen den Wirtschaftsschutz einmal mehr in den Fokus der Öffentlichkeit zu rücken. Dessen Bedeutung, die ernstzunehmenden Gefahren, vor allem aber Lösungsansätze und -strategien aufzuzeigen. Sehr geehrter Herr Minister Stahlknecht, ich freue mich auf Ihr Grußwort.

Es freut mich ebenfalls sehr, dass wir diese Veranstaltung, deren Schwerpunkte sowohl für die großen, aber immer mehr auch für die klein- und mittelständischen Unternehmen an Bedeutung gewinnen, hier unter dem Dach des Innovations- und Gründerzentrums Barleben durchführen. Unser Tagungsort veranschaulicht, wie viel unternehmerisches Know-how und Potenzial in unserer Region ansässig ist und wie viele innovative Ideen und Produktentwicklungen hier Tag für Tag entstehen. Ich danke Ihnen, sehr geehrter Herr Dr. Ude, dass wir unsere Veranstaltung hier in Ihrem Hause durchführen dürfen.

Meine sehr geehrten Damen und Herren,

die so genannte IuK-Kriminalität – heute meist als „Cybercrime“ bezeichnet – nimmt dramatisch zu. Sie stellt eine ernsthafte Gefahr für die Sicherheit von Unternehmen dar. Insbesondere deren Forschungs- und Entwicklungsbereiche werden dabei zunehmend Opfer von Wirtschaftsspionage via Internet. Deutschland ist als Standort zahlreicher Firmen, die auf Schaffung von Innovationen und von Spitzentechnologie ausgerichtet sind, darauf angewiesen, seinen technologischen Vorsprung zu sichern. Dieser Vorsprung kann durch Cybercrime-Attacken zunichte gemacht werden. Der Aufwand für solche Angriffe und das Täterrisiko sind dabei häufig gering, der Schaden für die betroffenen Firmen dagegen meist immens.

Eine reale Gefahr besteht dabei nicht nur für große, sondern auch für klein- und mittelständische Unternehmen. Gerade letztere verfügen aber häufig nicht über das entsprechende Problem- oder Gefahrenbewusstsein und in Folge dessen auch in weit geringerem Maße als Großunternehmen über entsprechende Schutzmechanismen. Sie sind deshalb besonders häufig Opfer verschiedenster Delikte aus dem großen Bereich des „Cybercrime“.

Als mögliche „Täter“ kommen dabei kriminelle Strukturen, Einzeltäter, konkurrierende Unternehmen oder sogar fremde Nachrichtendienste in Betracht. Der Schaden für Unternehmen kann dabei von der Rufschädigung über den Informationsabfluss bzw. der Industriespionage

und dem Totalverlust von Informationen bis hin zum Lahmlegen oder zur Zerstörung von ganzen Rechnernetzwerken reichen. Entsprechend ist eine Gefährdung der Firmenexistenz zu befürchten.

Vor diesem Hintergrund möchten wir einen Beitrag zum Dialog zu einem äußerst aktuellen und hoch brisanten Thema leisten.

Information und Kommunikation in elektronischer Form und auf elektronischem Weg sind mittlerweile aus unserer Gesellschaft nicht mehr wegzudenken. Wie sicher sind unsere Daten, welcher Bedrohung vor Attacken sind wir wirklich ausgesetzt? Und welchen Schaden können diese anrichten? Unsere heutige Veranstaltung soll unter anderem auf diese Fragen Antworten geben und die Experten der Fachvorträge werden diese im Einzelnen genauer beleuchten.

Gerade vor dem Hintergrund der aktuellen Geschehnisse rund um das Thema Cybercrime und Cyberware werfen sich viele Fragen auf und führen zu Unsicherheiten. Nicht aus dem Blick zu verlieren ist neben dem Schutz der Informations- und Kommunikationssysteme auch der Schutz und die besondere Aufmerksamkeit und Bedeutung des Faktors Mensch. Wer Mitarbeiter im Rahmen der Ausweitung seiner Geschäftstätigkeit ins Ausland entsendet, muss rechtlich und kulturell gut vorbereitet und sich der zu erwartenden Risiken und rechtlichen Verpflichtungen bewusst sein. Der Schutz der Mitarbeiter und gleichsam der Schutz der wirtschaftlichen Unternehmensinteressen ist ebenfalls ein nicht außer Acht zu lassendes Thema des Wirtschaftsschutzes.

Wie bereits erwähnt, besitzen sachsen-anhaltinische Unternehmen und dabei gerade die klein- und mittelständischen Unternehmen ein sehr großes Potenzial und agieren zunehmend auch im europäischen und internationalen Umfeld. Wie schützen Unternehmen ihr Know-how über die Grenzen Deutschlands hinaus, welche Strategien und Maßnahmen haben sich bewährt? Gewerbliche Schutzrechte unterstützen Unternehmen und deren Unternehmenswerte, ihre Erfindungen und Marken und zeigen territorial Wirkung. Auch die Themen der Produkt- und Markenpiraterie und des Patentrechts zählen zu den wichtigen Aspekten des Wirtschaftsschutzes und finden in einigen Vorträgen der heutigen Veranstaltung Berücksichtigung.

Meine sehr geehrten Damen und Herren,

wie ich Ihnen in meiner kurzen Ausführung bereits aufzeigen wollte, bietet Ihnen der heutige Wirtschaftsschutztag ein vielfältiges und facettenreiches Programm. Ich wünsche uns allen eine spannende, erkenntnisreiche Veranstaltung und danke Ihnen für die Aufmerksamkeit.

Sehr geehrter Herr Minister Stahlknecht, Sie haben das Wort.

Grußwort

Holger Stahlknecht
Minister für Inneres und Sport
des Landes Sachsen-Anhalt

Es gilt das gesprochene Wort!

Sehr geehrter Herr Olbricht,
sehr geehrte Damen und Herren,

zunächst möchte ich mich bei den Industrie- und Handelskammern Magdeburg und Halle-Dessau für die gute Zusammenarbeit in Vorbereitung der Veranstaltung herzlich bedanken.

Im Zeitalter einer globalisierten Wirtschaft, das die sachsen-anhaltischen Unternehmen dazu zwingt, sich der internationalen Konkurrenz zu stellen, rückt das Thema Sicherheitsprävention besonders in den Fokus der exportorientierten Wirtschaft, die sich ihrer üblichen Geschäftsrisiken bewusst ist. Bei diesem Prozess kann das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt die Unternehmen unterstützen. Die Mitarbeiter des Wirtschaftsschutzes gehen gern in die Unternehmen, um sie dabei zu beraten und zu unterstützen, Sicherheitsvorfälle zu verhindern oder Schaden zu begrenzen. Dabei gilt: Alle vertraulichen und sensiblen Daten und Fakten sind in der Verfassungsschutzbehörde gut aufgehoben, denn der Verfassungsschutz kann und darf schweigen. Gerade in Fällen tatsächlicher Angriffe ist es wichtig, miteinander die Methodik des Angriffs herauszuarbeiten und zu analysieren, denn sie kann in anonymisierter Form dazu dienen, die deutsche Wirtschaft mit Ihnen zusammen sicherer zu machen.

Sachsen-Anhalt liegt an der Achse des transeuropäischen Ost-West-Transitverkehrs, mittels nahegelegener Flughäfen sind viele globale Ziele unmittelbar erreichbar. Unsere wirtschaftliche Basis liegt beim verarbeitenden Gewerbe, beim Baugewerbe und beim Handel. Automotive und der Chemiesektor spielen eine nicht zu unterschätzende Rolle.

Kleine und Mittlere Unternehmen (KMU) mit weniger als 50 Beschäftigten stellen 97,7 Prozent aller Betriebe Sachsen-Anhalts dar. Sie verfügen in der Regel über keine Compliance-Abteilungen; auch die Unternehmenssicherheit, einschließlich der IT-Sicherheit, stellt eine Aufgabe meist weniger Mitarbeiter dar.

Über Perspektiven für die Informationssicherheit in den KMU wird Sie gleich Herr Schober vom Bundesamt für Sicherheit in der Informationstechnik informieren.

Sehr geehrte Damen und Herren,

Fakten belegen, dass das Internet einen Angriffsvektor gegen Unternehmen mit zunehmender Bedeutung ausmacht. Die Bedrohung auf diesem Sektor der Unternehmenssicherheit nimmt besonders rasant zu. Der Branchenverband BITKOM meldete im Februar 2015 auf der Basis einer Umfrage

unter seinen Mitgliedern, dass jedes dritte Unternehmen bei einer Größe zwischen 20 und 500 Beschäftigten in Deutschland in den letzten zwei Jahren IT-Sicherheitsvorfälle zu verzeichnen hatte.

Die Nationale Wirtschaftsschutzstrategie, die das Bundesministerium des Innern und das Bundesamt für Verfassungsschutz zusammen mit den anderen Sicherheitsbehörden des Bundes und den führenden Wirtschaftsverbänden auflegen wird, begrüßen wir daher sehr. Sie wird neue Impulse für den Wirtschaftsschutz auf nationaler Ebene und auf der Landesebene geben, die wir gern mit Ihnen gemeinsam umsetzen wollen. Herr Becker vom Bundesamt für Verfassungsschutz wird auch hierzu nähere Ausführungen machen.

Spionageangriffe auf Firmennetzwerke werden in aller Regel so geführt, dass der Angegriffene sie gar nicht oder erst zu spät bemerkt. Dank der guten Zusammenarbeit mit dem Bundesamt für Verfassungsschutz ist mein Haus in der Lage, Hinweise und Daten an potenziell gefährdete Unternehmen und außeruniversitäre Forschungsinstitute zu geben, um zu sensibilisieren und den Eigenschutz zu verbessern.

Die „NSA-Affäre“ hat meines Erachtens auch eine positive Seite. Sie hat den Blick geschärft für Gefahrenlagen, die von fremden Nachrichtendiensten zum Nachteil Deutschlands hervorgerufen werden. Die Mehrzahl der Nachrichtendienste, die Unternehmen im Visier haben, sind auf dem asiatischen Kontinent beheimatet, z. B. in der Russischen Föderation, der Volksrepublik China, in Syrien, Pakistan oder Iran. Der sachsen-anhaltischen Wirtschaft drohen auch diese Gefahren, insbesondere den Branchenführern und den „hidden champions“, den verborgenen Weltmarktführern. Geschäftsführung, Vertrieb, Wartungs- und Servicepersonal unterliegen einer besonderen Gefährdung in den genannten Ländern, denn dort agiert der jeweilige Nachrichtendienst auf eigenem Territorium. Ich freue mich insofern ganz besonders, dass der Bundesnachrichtendienst uns dazu über die Bedrohungen und strategischen Herausforderungen in Asien informieren will.

Das Exportgeschäft ist nicht nur mit einem höheren unternehmerischen Risiko, sondern auch mit einer höheren Gefährdung durch Nachrichtendienste verbunden.

Frau Stodtko von der IHK Halle-Dessau wird Ihnen zur Entsendung der Mitarbeiter in fremde Staaten weiterführende Hinweise geben.

Sehr geehrte Damen und Herren,

Sicherheitsvorfälle in Sachsen-Anhalt, die dem Wirtschaftsschutz meines Hauses bekannt geworden sind, waren bislang keine Fälle von nachrichtendienstlich gesteuerter Wirtschaftsspionage. Nicht-staatliche Akteure sind aber auch in der Lage, ähnlich zu agieren. Dies kann u. U. illegal sein, aber den gewünschte Erfolg hervorbringen. Nicht zu unterschätzen ist insoweit der Faktor Mensch.

Der „Engagement Index“ der Fa. Gallup zeigt, dass 15 Prozent aller Beschäftigten – Wirtschaft und Verwaltung – über eine hohe emotionale Bindung zu ihrem Arbeitsplatz verfügen, 70 Prozent haben eine geringe Bindung und 15 Prozent gar keine Bindung. Aus dem letztgenannten Personenpotenzial rekrutieren sich die Innentäter. Ihnen genügt zur Rechtfertigung, dass es vermeintlich alle tun. Sowie die Gelegenheit besteht, erfolgt der Verrat.

Wie Innentäter erkannt werden können, wird uns Herr Maro zeigen, wenn er uns die unterschätzten Gefahren der Industriespionage durch „Social Engineering“ plastisch vor Augen führen wird.

Was für den Schutz innovativer Ideen der Unternehmen getan werden kann, darüber berichtet der Unternehmer Herr von Limburg und Herr Dr. Heesemann von der Firma B. T. innovation GmbH.

Meine Damen und Herren,

für die Unternehmenssicherheit kann demnach nicht nur der Staat verantwortlich sein. Die unternehmerische Eigenverantwortung ist in diesem Zusammenhang sicherlich von noch größerer

Bedeutung.

Sie tragen die Verantwortung. Nutzen Sie die Ihnen zur Verfügung gestellten Informationen zur Unternehmenssicherheit. Nehmen sie die Beratungsleistungen des Wirtschaftsschutzes in Anspruch.

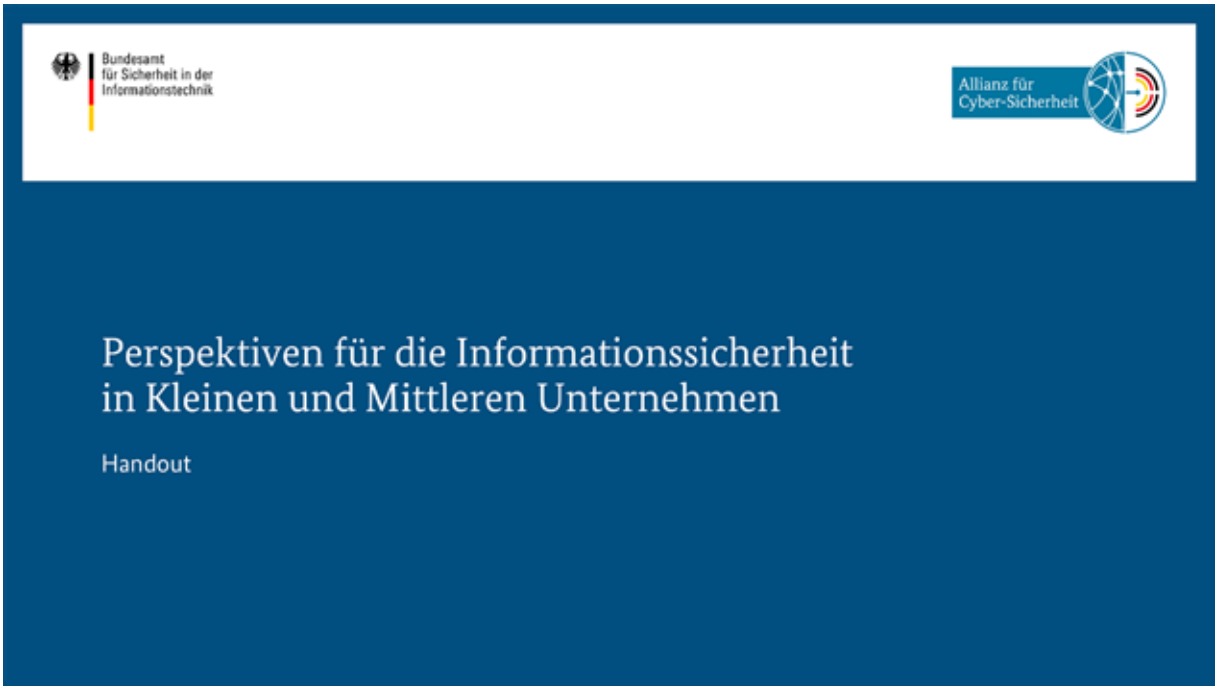
Werden Sie präventiv tätig! Es lohnt sich, Management und die besonders gefährdeten Mitarbeitergruppen zu sensibilisieren und in ihre Sicherheitsvorkehrungen einzubeziehen. Die Mitarbeiter des Wirtschaftsschutzes (Verfassungsschutz) meines Hauses stehen Ihnen als Ansprechpartner gern zur Verfügung.

Ich danke Ihnen für Ihre Aufmerksamkeit.

„Perspektiven für Informationssicherheit in Kleinen und Mittleren Unternehmen“

Marc Schober
Bundesamt für Sicherheit
in der Informationstechnik (BSI)

Es gilt das gesprochene Wort!



Weitere Informationen und Links zum Vortrag

Allianz für Cyber-Sicherheit : www.allianz-fuer-cybersicherheit.de

- Über 100 Best-Practice-Empfehlungen öffentlich im Informationspool | Cyber-Sicherheits-Warnungen und monatliche BSI IT-Sicherheitslageberichte nur für registrierte Teilnehmer www.allianz-fuer-cybersicherheit.de/ACS/registrierung
- Cyber-Sicherheits-Umfrage und Ergebnisse aus dem Vorjahr www.cybersicherheitsumfrage.de

Bundesamt für Sicherheit in der Informationstechnik : www.bsi.bund.de

- Lagebericht 2014 www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf
- BSI IT-Grundschutz www.bsi.bund.de/grundschutz
- BSI Schwachstellen-Kurzinformationen im WID-Portal www.cert-bund.de/wid
- BSI Bürger-CERT www.buerger-cert.de

Bundesamt für Sicherheit in der Informationstechnik

Fallbeispiel: Servicetechniker

- BSI wurde durch Infrastrukturbetreiber um Unterstützung gebeten
- Auf USB-Stick eines Servicetechnikers wurde Malware gefunden
- USB-Stick wurde zuvor in verschiedenen Leitstellen eingesetzt
- Infektion des USB-Stick über privaten PC wahrscheinlich
- Aufgrund von RT-Anforderungen und regulatorischen Vorgaben keine AV-Software auf Leitstellensystemen möglich
  → Wie kann jetzt geprüft werden? Was tun?
- Prüfung ergab: Einige Systeme waren tatsächlich infiziert worden aber keine schlimmeren Auswirkungen da vom Internet getrennt
- **Kein gezielter Angriff**, dennoch hohes Schadenspotential

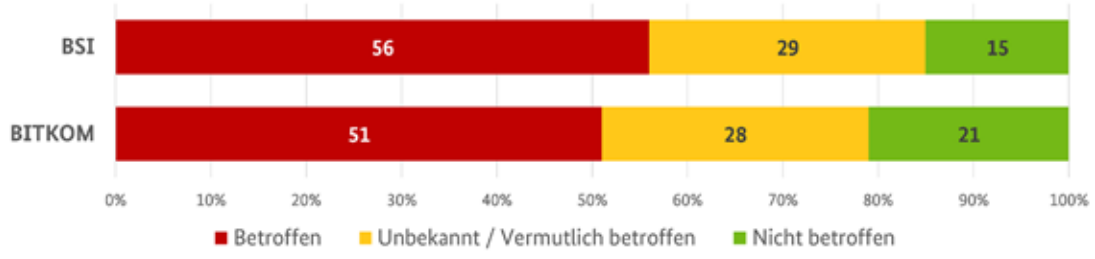
Bundesamt für Sicherheit in der Informationstechnik

Cyber-Sicherheitslage

„Die Gefährdungslage im Cyber-Raum darf nicht auf nachrichtendienstliche Aktivitäten reduziert werden“

Betroffenheit durch Cyber-/Digitale-Angriffe

- BSI: Cyber-Sicherheits-Umfrage 2014
- BITKOM: Studie Digitale Wirtschaftsspionage, Sabotage und Datendiebstahl (2015)



Datengrundlage BSI: n=257, Frage nach Betroffenheit in den letzten 2.5 Jahren
Datengrundlage BITKOM: n=1.074, Frage nach Betroffenheit in den letzten 2 Jahren

Betroffenheit durch Cyber-/Digitale-Angriffe

- BITKOM-Studie: **„51 Milliarden Euro Schaden pro Jahr“**
- **Mittelstand und Großunternehmen** in beiden Umfragen tendenziell etwas höhere Betroffenheit als Kleinunternehmen
- Hochtechnologiebranchen (Automobilbau, Rüstungsindustrie, Schiffsbau, Chemie, ...), Forschungseinrichtungen und öffentliche Verwaltung im Fokus **gezielter Angriffe**
- **Standard-Sicherheitsmaßnahmen** häufig schon umgesetzt (75% - 95%), Defizite u.a. bei **Mitarbeitersensibilisierung** (60%) und **strukturiertem Sicherheitsmanagement** (47%)

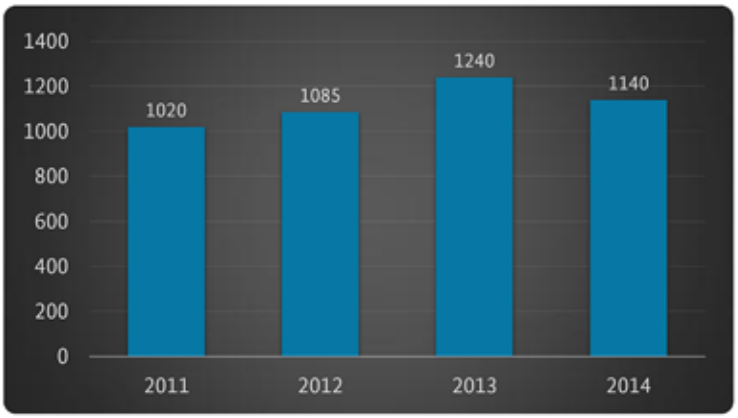
! Technische Maßnahmen immer nur im **Gesamtpaket** mit organisatorischen Maßnahmen (voll) wirksam

Bundesamt für Sicherheit in der Informationstechnik

Schwachstellen in Standard-Software

Hier berücksichtigte Produkte

- Adobe Reader
- Adobe Flash
- Mozilla Firefox
- Mozilla Thunderbird
- Microsoft Internet Explorer
- Microsoft Windows
- Microsoft Office
- Linux Kernel
- Apple OS X
- Apple Safari
- Google Chrome
- Oracle Java/JRE



Zahl bekannt gewordener Schwachstellen in Standardsoftware

Bundesamt für Sicherheit in der Informationstechnik

„Die Bedrohungslage im Cyber-Raum ist heute gekennzeichnet durch ein **breites Spektrum diverser Angriffsformen**, die von **Tätergruppen mit unterschiedlichen Motiven** ausgehen."

Bundesamt für Sicherheit in der Informationstechnik

Fallbeispiel: Gezielter Angriff auf ein Stahlwerk in Deutschland (2014)

- Office-Netzwerk mittels **Spear-Phising** und ausgefeiltem **Social Engineering** kompromittiert
- Aus dem Office-Netzwerk Übernahme von Komponenten im Produktionsnetz
- Störungen und Ausfälle im Produktionsnetz, Beeinträchtigung einer Hochofensteuerung
  → nicht mehr geregelt herunterfahrbar
  → massive Beschädigungen der Anlage
- Angreifer mit detailliertem Fachwissen zu eingesetzten Komponenten und Produktionsprozessen

Bild: © industrieblick - Fotolia.com

Bundesamt für Sicherheit in der Informationstechnik

Fallbeispiel: APT Angriff auf RSA Security (2011)

- RSA Security: Hersteller der marktgängigen 2-Faktor-Authentisierungslösung SecurID
- Angriff wurde im März 2011 bekannt
  - **Spear-Phishing** Angriff: „2011 Recruitment plan.xls“
  - Dokument enthielt **0-day Exploit** für Adobe Flash Schwachstelle
  - Angreifer installierten gängiges Remote Administration Tool
  - Angreifer „bewegten“ sich durch das Unternehmensnetz
  - Daten wurden verschlüsselt nach extern transferiert
- Zumindest Teile der Daten zu SecurID kompromittiert, Kunden verloren das Vertrauen, RSA tauschte auf Wunsch die Token aus
- RSA Security vermutet staatliche Angreifer
- Gerüchte über Zshg. mit Angriff auf Lockheed Martin im Mai 2011

Bundesamt für Sicherheit in der Informationstechnik

Hinweis: Dieses Fallbeispiel enthält nicht durch das BSI verifizierte Informationen aus grundsätzlich vertrauenswürdigen öffentlichen Quellen

Was tun?

Individuelle Risikobewertung

- Allgemeine Zahlen können **nicht ausschlaggebend** für das eigene Handeln sein
- In jedem Fall **individuelle Bewertung** des eigenen Risikos notwendig
- Valide **Informationen zur Lage** sind eine Grundlage für die Bewertung
- Verschiedene Ansätze zur Risikobewertung möglich, z.B. **Cyber-Sicherheits-Check**

BSI IT-Lagezentrum – Die Lage Beobachten | Bewerten | Bewältigen

Bundesamt für Sicherheit in der Informationstechnik

Maßnahmen

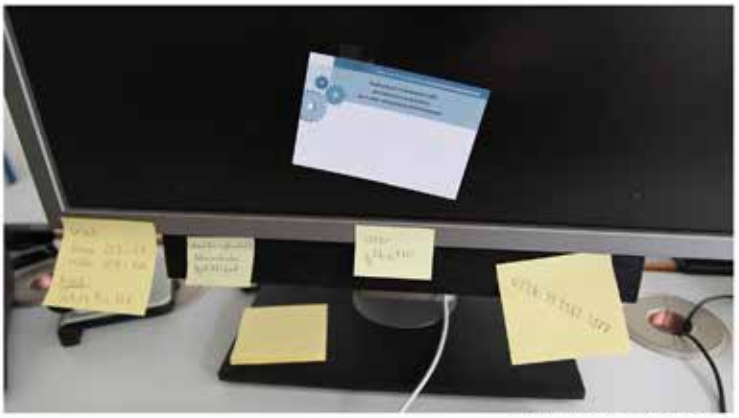
- **Strukturiertes Vorgehen → ISMS nach etablierten Standards als Rahmen**
- Technische Maßnahmen
  - Firewall, Anti-Virus, Spam-Filter, ...
  - Datenträger-/Mobile-Verschlüsselung, E-Mail-Verschlüsselung, ...
  - ...
- Übergreifende Organisatorische Maßnahmen
  - Management-Entscheidung zur Nutzung von Cloud-Diensten
  - Management-Entscheidung zu Bezugsquellen und Anforderungen an eingesetzte Produkte
  - ...
- Organisatorische Maßnahmen : Personal

Bundesamt für Sicherheit in der Informationstechnik

Nicht nur Technik! Organisatorische Maßnahmen

- Mitarbeiter / Awareness sind ein wesentlicher Faktor
- Social Engineering vorbeugen

- Clean-Desk Policy?
- Social Media Richtlinie?
- Private Nutzung von Internet und Firmen-IT?
- Private IT im Unternehmen?



Symbolbild, keine echten Daten

Unser Angebot zur Unterstützung

BSI IT-Grundschutz und Basismaßnahmen der Cyber-Sicherheit

- Anerkannter Standard zum IT-Sicherheitsmanagement
- Strukturierte Umsetzung von Maßnahmen
- Umfangreiche Kataloge mit Maßnahmenbeschreibungen

! optionale Zertifizierung

→ Umfangreiches Nachschlagewerk für alle

- „Basismaßnahmen der Cyber-Sicherheit" als Einstieg
- Keine Zertifizierung aber „Cyber-Sicherheits-Check"

Allianz für Cyber-Sicherheit

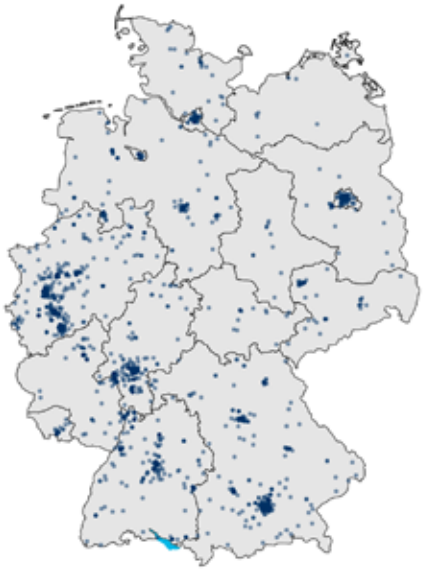
Allianz für Cyber-Sicherheit

1357 teilnehmende Institutionen

2229 registrierte Personen

83 Partner

41 Multiplikatoren



Bundesamt für Sicherheit in der Informationstechnik

Allianz für Cyber-Sicherheit

Allianz für Cyber-Sicherheit

Networking und Arbeitsgruppen
- Cyber-Sicherheits-Tage, 4x pro Jahr
- Expertenkreise des BSI
- Erfahrungskreise, Workshops, Fachkonferenzen, ...

Informations- und Schulungsangebote
- Rund 200 Veröffentlichungen des BSI
- Zahlreiche Best-Practice-Paper der Partner
- Kostenfreie Schulungsangebote der Partner und des BSI

Cyber-Sicherheitslage und anonyme Meldestelle
- Aktuelle Informationen zur Cyber-Sicherheitslage
- Monatlicher Lagebericht, Themenlagebilder, ...
- Möglichkeit zur anonymen Meldung von Vorfällen

Bundesamt für Sicherheit in der Informationstechnik

Vielen Dank für Ihre Aufmerksamkeit

Allianz für Cyber-Sicherheit

Kontakt

Geschäftsstelle der Allianz für Cyber-Sicherheit
c/o Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 – 189
53175 Bonn

info@cyber-allianz.de

Tel. +49 (0) 228 99 9582 5977
Fax +49 (0) 228 99 109582 6050
www.allianz-fuer-cybersicherheit.de

Bundesamt für Sicherheit in der Informationstechnik

„Wirtschaftsschutz in Deutschland: Ein Angebot des Verfassungsschutzes“

Bodo Becker
Bundesamt für Verfassungsschutz (BfV)

Es gilt das gesprochene Wort!

Bundesamt für Verfassungsschutz

Begriffserklärungen - Angriffsrichtungen

Wirtschaftsspionage

Staatlich gelenkte oder gestützte Ausforschung von Wirtschaftsunternehmen und Betrieben. →StGB

Wirtschaftsschutz

Beinhaltet alle relevanten Maßnahmen, die geeignet sind, einen illegalen Know-how-Transfer durch fremde Nachrichtendienste aus deutschen Unternehmen und Forschungseinrichtungen zu verhindern oder zu erschweren.

Konkurrenzausspähung

Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt. →UWG

17.09.2015 Seite 2

Bundesamt für Verfassungsschutz

Methoden der Spionage

HUMINT ⇨ Human Intelligence
Spionage mit menschlichen Quellen

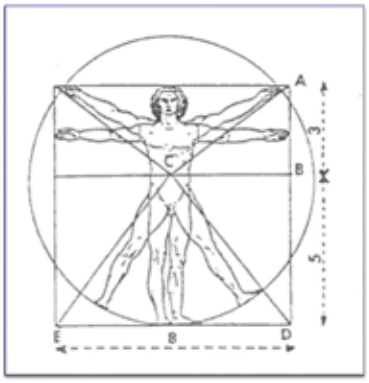
SIGINT ⇨ Signal Intelligence
Fernmeldeaufklärung, Elektronische Angriffe

17.09.2015 Folie 3

Bundesamt für Verfassungsschutz

Achtung, Innentäter!

- **„Der Mensch bleibt die größte Sicherheitslücke!“**



17.09.2015 Folie 4

Bundesamt für Verfassungsschutz

10 Punkte zum Know-how-Schutz

Effizientes Informationsschutzmanagement:

- Identifizierung der berühmten 5% Kronjuwelen
- Risiko- und Schwachstellenanalyse
- Zugriffsschutz
- BYOD-Regelungen
- „Need to Know“
- „clean-desk-policy“
- IT-Sicherheit
- Notfallpläne u. a. für IT
- Ausland: Datensparsamkeit
- Ausland: Kommunikation begrenzen

17.09.2015 Seite 5

Bundesamt für Verfassungsschutz

Nationale Wirtschaftsschutzstrategie 2015

- **4 Expertengruppen, über 100 Experten:**

Bundesministerium des Innern

- **Expertengruppe1:**
  - Informationsaustausch
  - Operative Sicherungsprozesse
- **Expertengruppe 2:**
  - Sensibilisierung und Öffentlichkeitsarbeit
- **Expertengruppe 3:**
  - Ausbildung und Qualifizierung
- **Expertengruppe 4:**
  - Best practices international

DIHK

BDI

Made in Germany

17.09.2015 Seite 6

Bundesamt für Verfassungsschutz

Internetplattform Wirtschaftsschutz

- **Ein Angebot von BfV, BKA, BND und BSI gemeinsam mit BDI, DIHK, ASW und BDSW**

wirtschaftsschutz.info
Informationsportal Wirtschaftsschutz

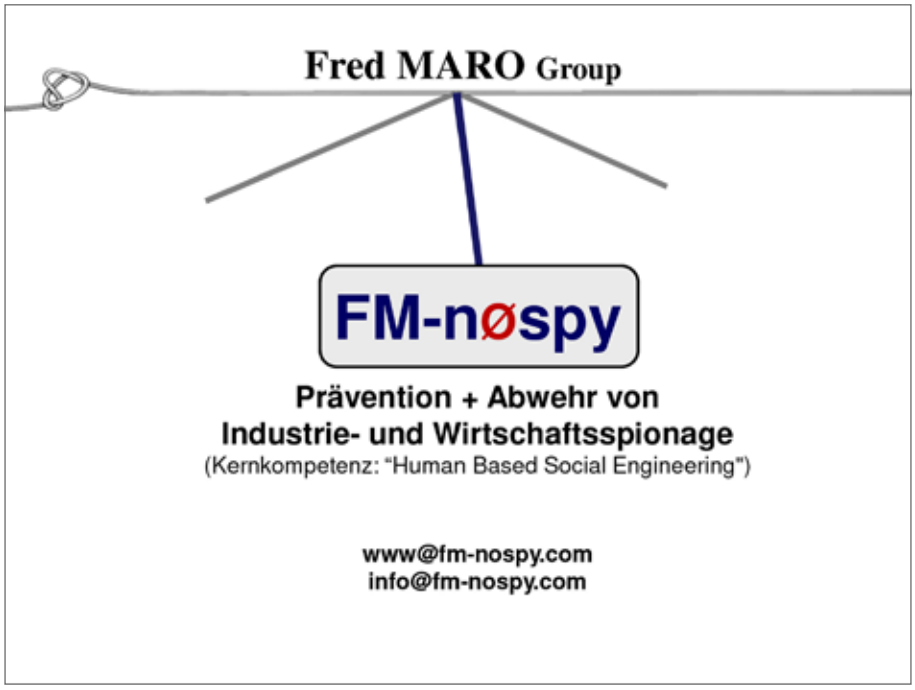
17.09.2015 Folie 7


Bundesamt für Verfassungsschutz
Sprechen Sie uns an
Bodo W. Becker M.A.
Referatsleiter Wirtschaftsschutz
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
Tel.: 0221 / 792-3322
E-Mail: wirtschaftsschutz@bfv.bund.de
Bundesamt für Verfassungsschutz
Das Wirtschaftsschutzteam im Referat 44
Ministerium für Inneres und Sport des
Landes Sachsen Anhalt – Verfassungsschutz
Nachtweide 82, 39124 Magdeburg
Tel.: 0391 / 567-3965
E-Mail: abwehr@mi.sachsen-anhalt.de
SACHSEN-ANHALT
Ministerium für Inneres und Sport
Passen Sie gut auf sich und Ihr Know-how auf!
17.09.2015
Folie 8

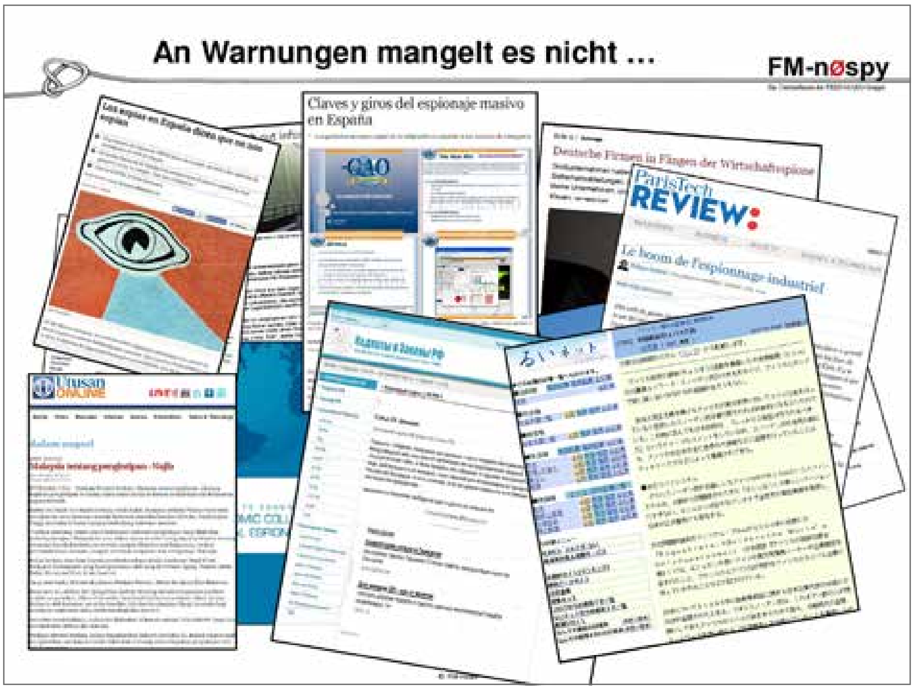
„Von netten und anderen Menschen – Die unterschätzte Gefahr der Informationsspionage durch Social Engineering“

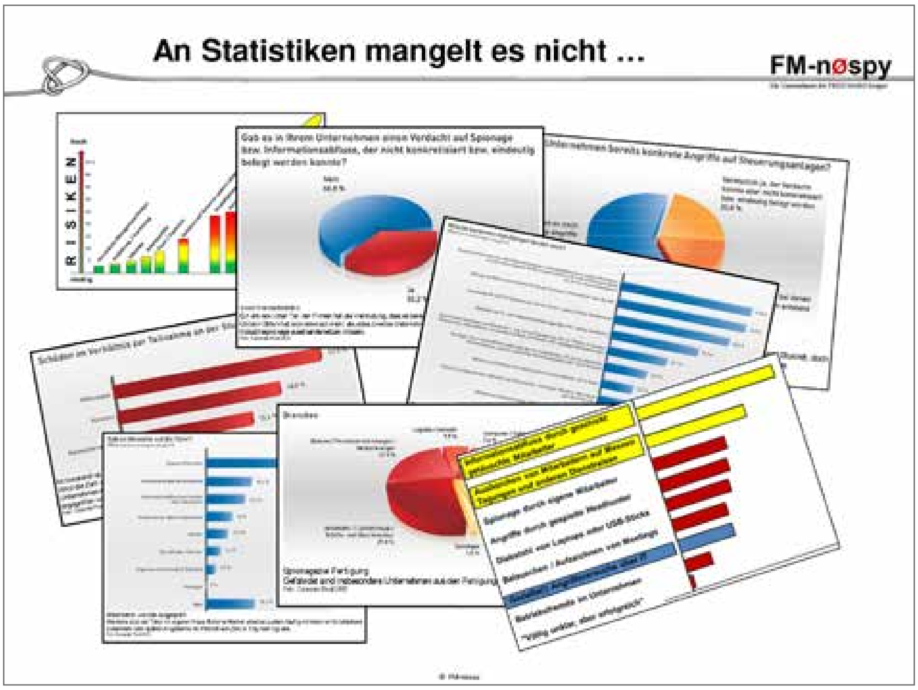
Fred Maro
Geschäftsführer, FM-nospy, Hürth bei Köln

Es gilt das gesprochene Wort!


Fred MARO Group
FM-nøspy
Prävention + Abwehr von
Industrie- und Wirtschaftsspionage
(Kernkompetenz: "Human Based Social Engineering")
www@fm-nospy.com
info@fm-nospy.com


Ausspähung
Social Engineering
Informationsschutz
Industriespionage !!!
RADIOAKTIV
CYBERWAR


An Warnungen mangelt es nicht …
FM-nøspy
Claves y giros del espionaje masivo en España
Deutsche Firmen in Fängen der Wirtschaftsspione
ParisTech REVIEW
Le boom de l'espionnage industriel


An Statistiken mangelt es nicht …
FM-nøspy
RISIKEN
Gab es in Ihrem Unternehmen einen Verdacht auf Spionage bzw. Informationsabfluss, der nicht konkretisiert bzw. eindeutig belegt werden konnte?
Branchen

Gleiche Schätzung in allen EU-Ländern

FM-nøspy

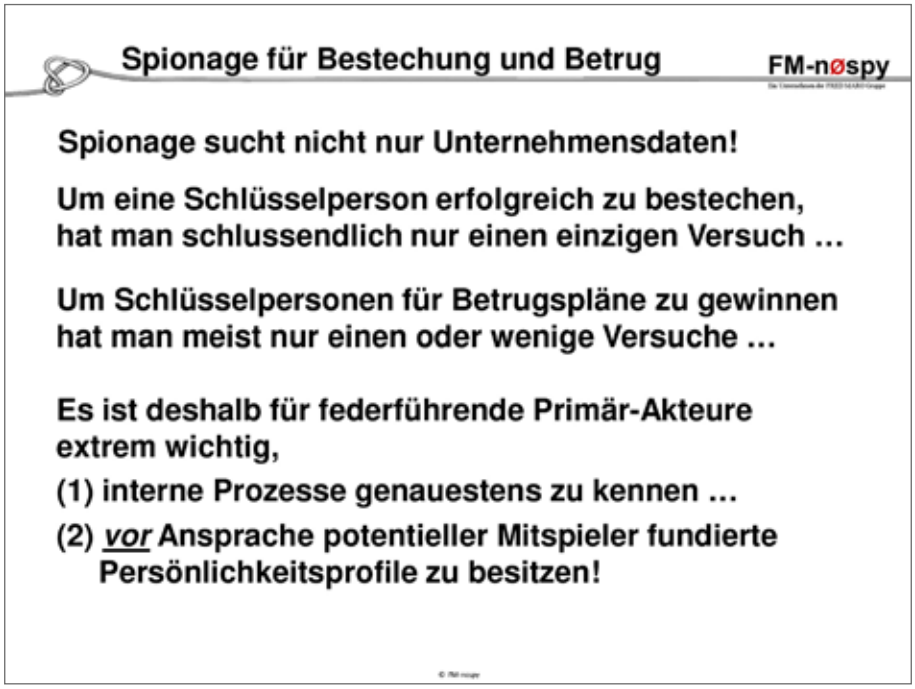
- **Etwa jedes 3. bis 5. (!) Unternehmen in Europa**
  (gleich welcher Größe und Art)
  wird jedes Jahr ein / mehrmals angegriffen!
- **Nur ein Bruchteil der Angriffe wird sofort bemerkt!**
- **Etwa 80% der Angriffe laufen über - nichts ahnende - Dienstleiser und Zulieferer!**
- **Etwa 10% der Angriffe sind erfolgreich → geschätzte Schäden in zweistelliger Milliardenhöhe!**
- **Das Problem dieser Zahlen: Es sind Einschätzungen**

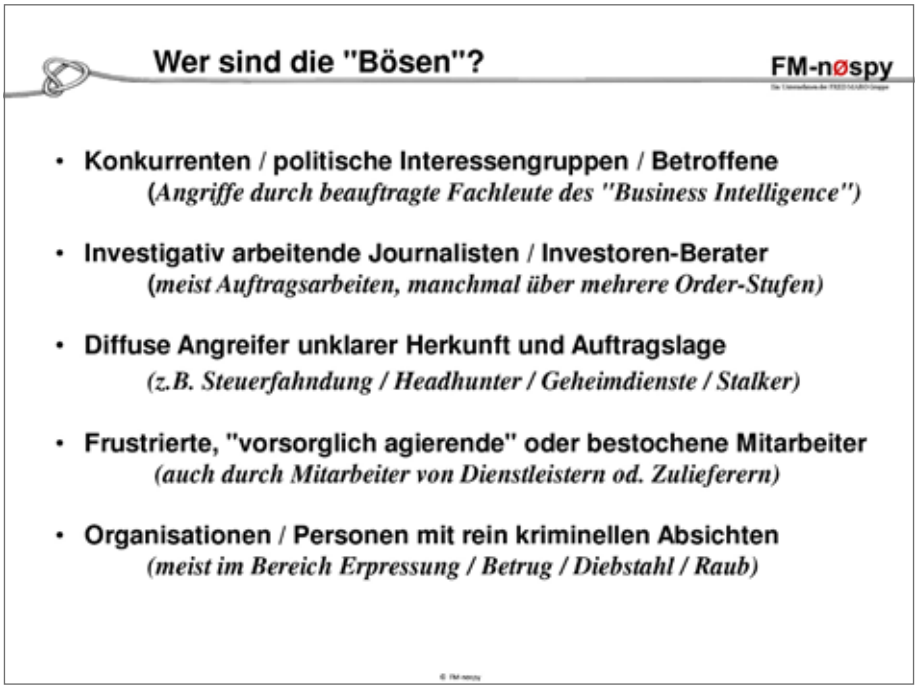
Nicht repräsentativ – trotzdem aufschlussreich!

FM-nøspy

Ref: FM-nospy 2013 /
122 befragte angegriffene Unternehmen


Begehrte Spionageobjekte
FM-nøspy
• Ausweise und Identifikationsmittel
• Aufsichtsrats-u. Vorstandsprotokolle
• Ausschreibungen
• Baupläne + Bebauungspläne
• Boni + Gehälter für Mitarbeiter
• Designvorlagen
• Einkaufspreise
• Erfindungen + innovative Ideen
• Fertigungsdetails
• Gewinn-u. Umsatzkalkulationen
• Krankenakten und Gutachten
• Kostenkalkulationen
• Kontodaten + Zahlungsprozedere
• Kundendaten
• Lagepläne + LageR-Pläne
• Lieferantennamen
• Lieferanten-u. Serviceverträge (SLA)
• Logistikdetails
• Maschinenbauteile
• Materialproben
• Passwörter
• Patentvorhaben
• Personenbezogene Daten
• Pilotprojekte / Experimentals
• Produktbestandteile
• Reisepläne
• Roadmaps
• Sicherheitssysteme
• Studienergebnisse
• Technisches KnowHow
• Telefon- und Kurzwahlnummern
• Testanordnungen + Ergebnisse
• Transportwege + Zeiten
• Unfallanalysen + Berichte
• Unternehmenskennzahlen
• Verkaufsabsichten
• Vertragsdetails
• Vertriebsstrategien
• Warenproben
• Zugangsmöglichkeiten


Spionage für Bestechung und Betrug
FM-nøspy
Spionage sucht nicht nur Unternehmensdaten!
Um eine Schlüsselperson erfolgreich zu bestechen, hat man schlussendlich nur einen einzigen Versuch …
Um Schlüsselpersonen für Betrugspläne zu gewinnen hat man meist nur einen oder wenige Versuche …
Es ist deshalb für federführende Primär-Akteure extrem wichtig,
(1) interne Prozesse genauestens zu kennen …
(2) vor Ansprache potentieller Mitspieler fundierte Persönlichkeitsprofile zu besitzen!


Wer sind die "Bösen"?
FM-nøspy
• Konkurrenten / politische Interessengruppen / Betroffene
(Angriffe durch beauftragte Fachleute des "Business Intelligence")
• Investigativ arbeitende Journalisten / Investoren-Berater
(meist Auftragsarbeiten, manchmal über mehrere Order-Stufen)
• Diffuse Angreifer unklarer Herkunft und Auftragslage
(z.B. Steuerfahndung / Headhunter / Geheimdienste / Stalker)
• Frustrierte, "vorsorglich agierende" oder bestochene Mitarbeiter
(auch durch Mitarbeiter von Dienstleistern od. Zulieferern)
• Organisationen / Personen mit rein kriminellen Absichten
(meist im Bereich Erpressung / Betrug / Diebstahl / Raub)


Industriespionage→"Social Engineering"
FM-nøspy
"Social" = "Soziales" / "Engineering" = "etwas zusammenbauen"
WICHTIG: Ungeschulte Menschen bemerken die Angriffe auf sie meist NICHT !
Weshalb Compliance Regeln hierbei versagen !
SE
Wirtschafts + Industriespionage
Diffuses Spionieren (z.B. für Bestechung)
Militärische Spionageformen aller Art
Erpressung / Rufmord
Angriffe auf Personen / Sachen

Angriffstechniken

FM-nøspy

Wichtig:
"Cyber-War" spielt in der gezielten Spionage nur eine geringe Rolle!
(dient eher dem "Profiling" / der Sabotage / dem Massenabgreifen)

Data-Based Social Engineering — ca. 30%
(gezieltes Stehlen von Passwörtern / Token / Ausweisen / Dokumenten)
(Angriffe auf Datenträger, meist mit Hilfe von Schadsoftware)

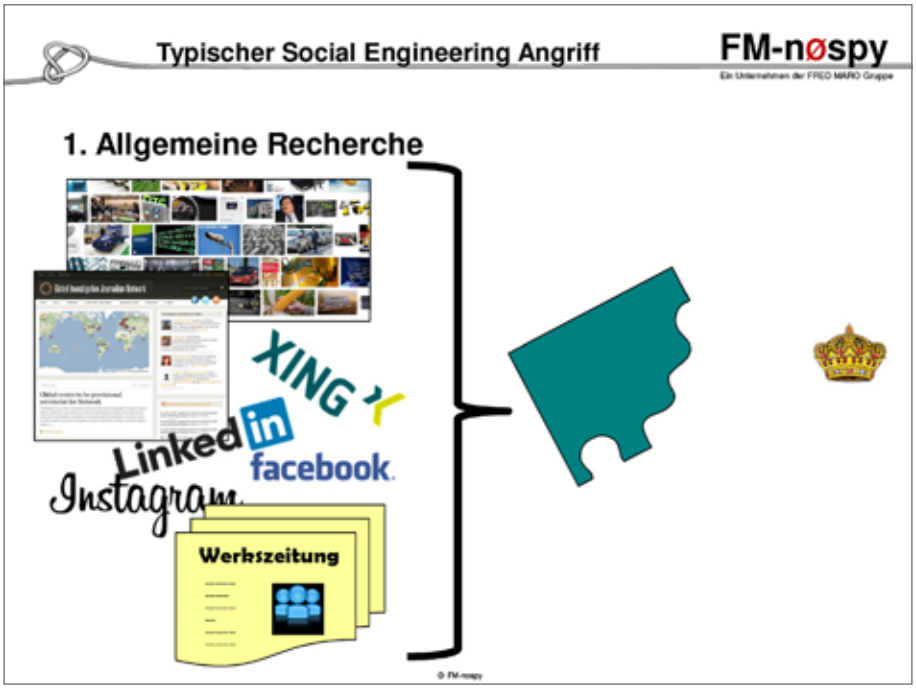
Reverse Social Engineering — ca. 20%
(Verursachen von Schaden + Angriff in der Tarnung von Helfern)
(Ziele: Elektronische Daten, aber auch Material und Papier)

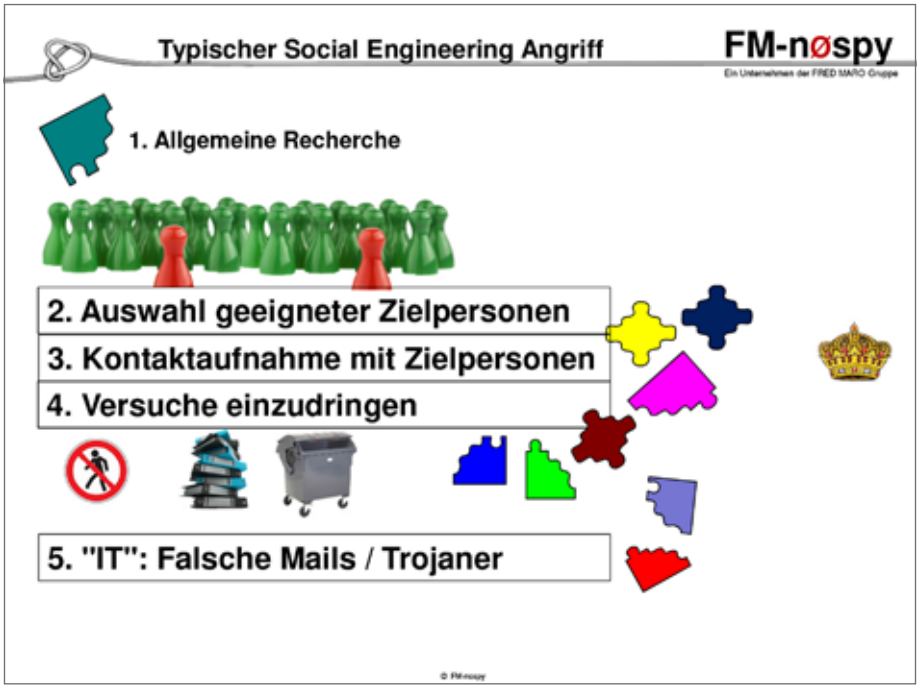
Human Based Social Engineering — ca. 50%
Subtil und psychologisch gestalteter Angriff
durch geschicktes Ausfragen / Austricksen von Mitarbeitern

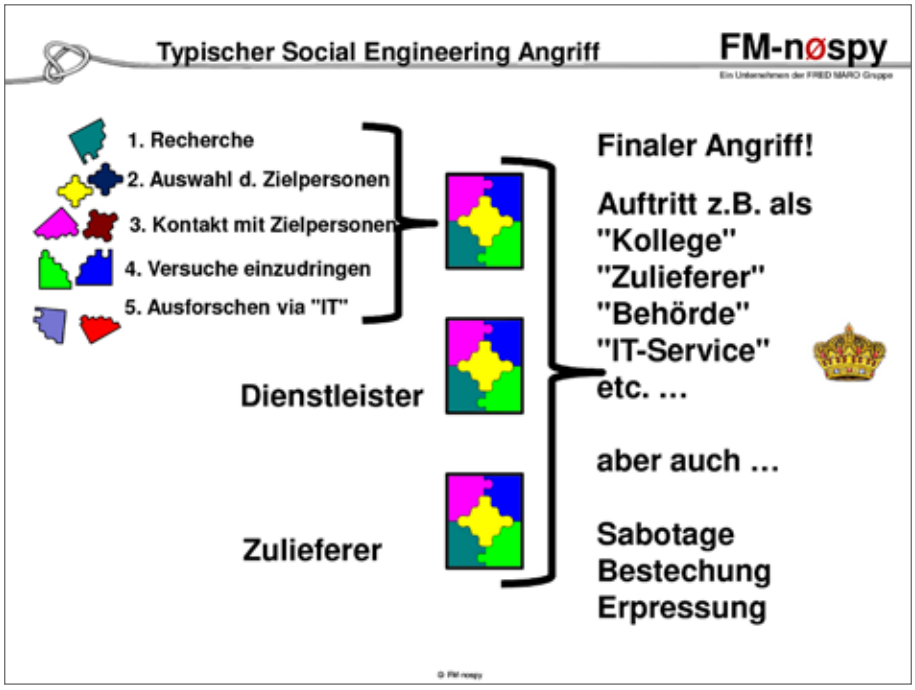
Typischer Social Engineering Angriff

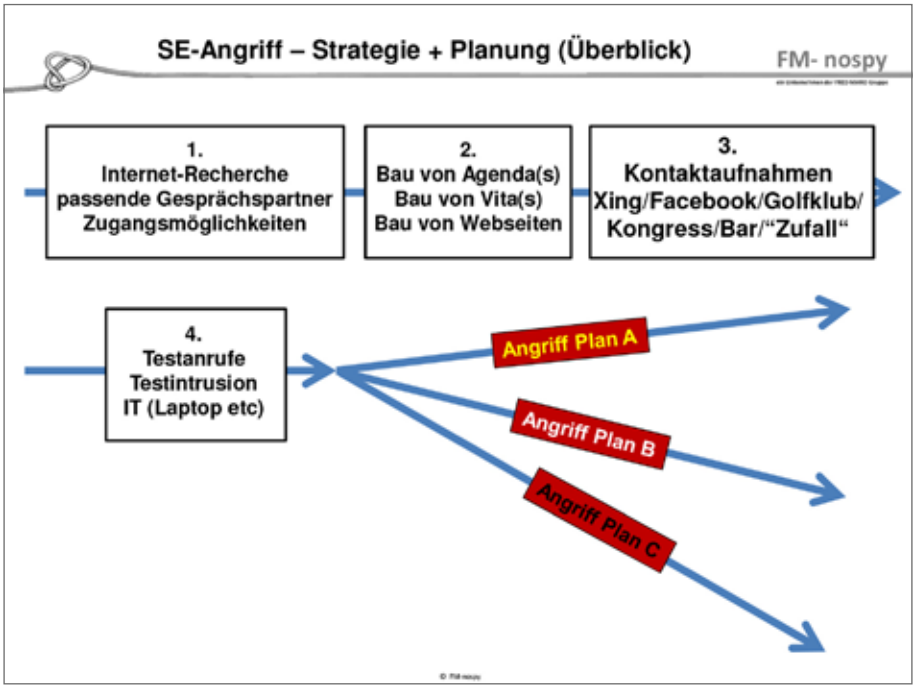
FM-nøspy
Ein Unternehmen der FRED MARO Gruppe

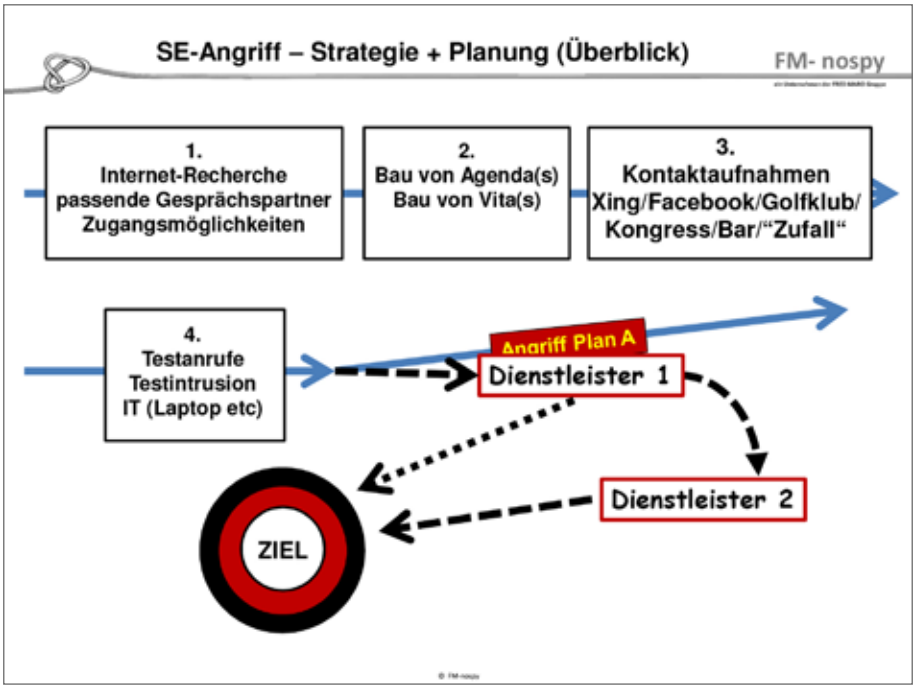
Das "ZIEL"
... digital aufbewahrte Daten
... in Papier vorliegende Daten
... haptisches Material
... virtuelle Informationen
... Sabotage / Attentat


Typischer Social Engineering Angriff
FM-nøspy
1. Allgemeine Recherche
XING
Linked in
facebook
Instagram
Werkszeitung

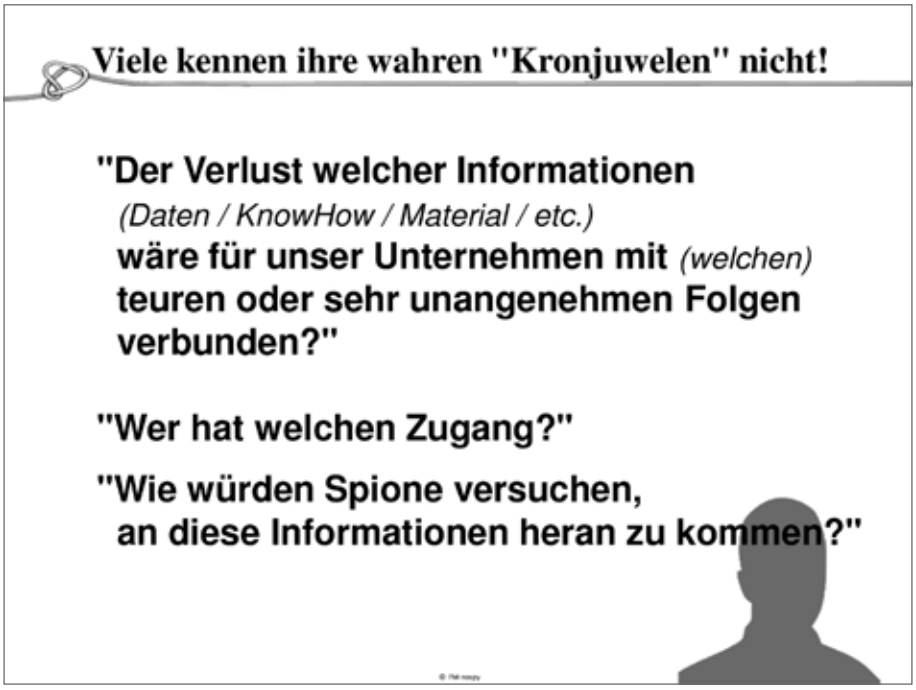

Typischer Social Engineering Angriff
FM-nøspy
1. Allgemeine Recherche
2. Auswahl geeigneter Zielpersonen
3. Kontaktaufnahme mit Zielpersonen
4. Versuche einzudringen
5. "IT": Falsche Mails / Trojaner


Typischer Social Engineering Angriff
FM-nøspy
1. Recherche
2. Auswahl d. Zielpersonen
3. Kontakt mit Zielpersonen
4. Versuche einzudringen
5. Ausforschen via "IT"
Dienstleister
Zulieferer
Finaler Angriff!
Auftritt z.B. als
"Kollege"
"Zulieferer"
"Behörde"
"IT-Service"
etc. …
aber auch …
Sabotage
Bestechung
Erpressung


SE-Angriff – Strategie + Planung (Überblick)
FM- nospy
1.
Internet-Recherche
passende Gesprächspartner
Zugangsmöglichkeiten
2.
Bau von Agenda(s)
Bau von Vita(s)
Bau von Webseiten
3.
Kontaktaufnahmen
Xing/Facebook/Golfklub/
Kongress/Bar/"Zufall"
4.
Testanrufe
Testintrusion
IT (Laptop etc)
Angriff Plan A
Angriff Plan B
Angriff Plan C


SE-Angriff – Strategie + Planung (Überblick)
FM- nospy
1.
Internet-Recherche
passende Gesprächspartner
Zugangsmöglichkeiten
2.
Bau von Agenda(s)
Bau von Vita(s)
3.
Kontaktaufnahmen
Xing/Facebook/Golfklub/
Kongress/Bar/"Zufall"
4.
Testanrufe
Testintrusion
IT (Laptop etc)
Angriff Plan A
Dienstleister 1
Dienstleister 2
ZIEL


Warum funktioniert
Social Engineering so gut?


Viele kennen ihre wahren "Kronjuwelen" nicht!
"Der Verlust welcher Informationen
(Daten / KnowHow / Material / etc.)
wäre für unser Unternehmen mit (welchen)
teuren oder sehr unangenehmen Folgen
verbunden?"
"Wer hat welchen Zugang?"
"Wie würden Spione versuchen,
an diese Informationen heran zu kommen?"


Wir kennen das Vertrauliche nicht!
Social Engineering gestaltet den Weg zu den
Kronjuwelen ...

Wir kennen das Vertrauliche nicht!

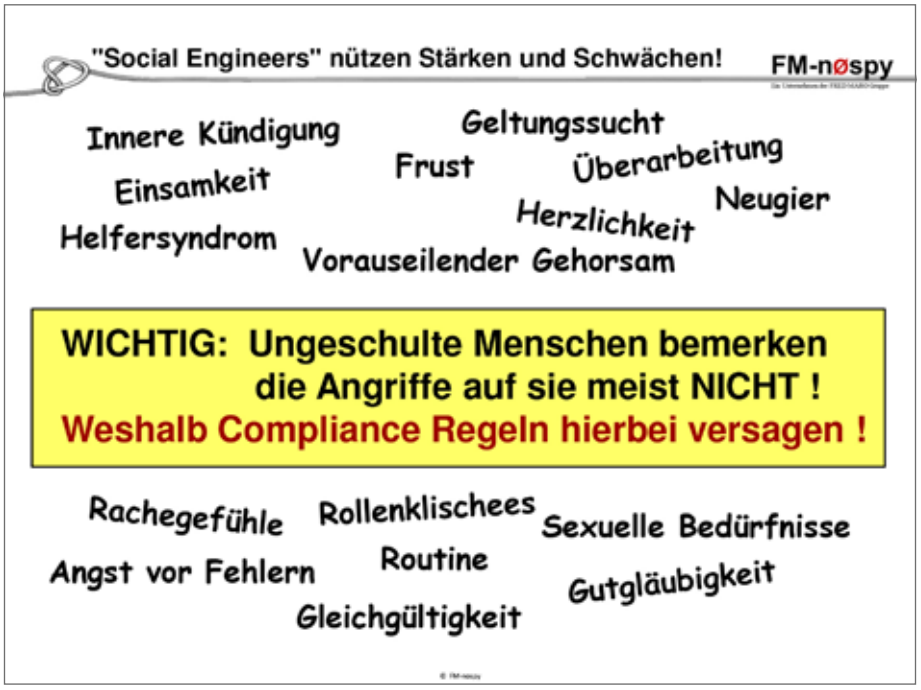
**Vertraulich ist alles,
was nicht einfach im Internet zu finden ist!**

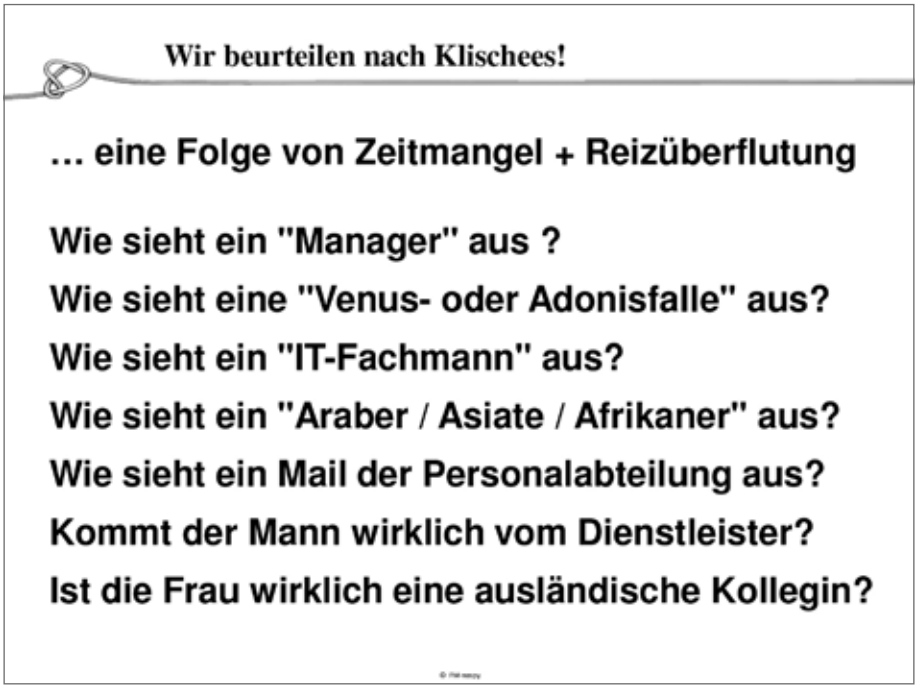
Urlaubszeiten / Urlaubsorte / Abteilungsnamen / Projektmanager
Telefonnummern / Roadmaps / Kongressteilnahmen / Reisepläne
Zahlungsprozedere / Spitznamen / Service Level Agreements
Vorstandsprotokolle / Hobbys / Lagerorte / Dienstleister-Namen
Tagungsorte / Tagung-Agenda / Formulare / Strategien / Hauspost
Abfallmanagement / Zugangswege / Zwischenfälle / Ausweise
Urlaubsvertretungen / Autokennzeichen / Passwörter
Namen von Schlüsselpersonen / Namen von Beratern
und vieles ähnliches mehr …

Wir haben keine Zeit, aufmerksam zu sein !

**Viele Mitarbeiter sind völlig "übertaktet" !
Sie reagieren nur noch, anstatt zu "agieren"!**

**Die Systeme, die Aufmerksamkeit verlangen,
gestatten keine Zeit für Hinschauen und
Nachfragen …**


"Social Engineers" nützen Stärken und Schwächen!
FM-nøspy
Innere Kündigung
Geltungssucht
Frust
Überarbeitung
Einsamkeit
Neugier
Herzlichkeit
Helfersyndrom
Vorauseilender Gehorsam
WICHTIG: Ungeschulte Menschen bemerken die Angriffe auf sie meist NICHT !
Weshalb Compliance Regeln hierbei versagen !
Rachegefühle
Rollenklischees
Sexuelle Bedürfnisse
Angst vor Fehlern
Routine
Gutgläubigkeit
Gleichgültigkeit


Wir beurteilen nach Klischees!
... eine Folge von Zeitmangel + Reizüberflutung
Wie sieht ein "Manager" aus ?
Wie sieht eine "Venus- oder Adonisfalle" aus?
Wie sieht ein "IT-Fachmann" aus?
Wie sieht ein "Araber / Asiate / Afrikaner" aus?
Wie sieht ein Mail der Personalabteilung aus?
Kommt der Mann wirklich vom Dienstleister?
Ist die Frau wirklich eine ausländische Kollegin?

Wir sind – untrainiert – Profis nicht gewachsen!

Wir geben viel Geld für Vertriebstraining aus!

**Wir geben kaum Geld aus,
um die Wächter unserer Kronjuwelen fit zu machen,
gegen Profis (Psychologen/Schauspieler) zu bestehen.**

**Wir geben kein Geld aus, um Dienstleister
und Zulieferer zu überprüfen und zu schulen.**

**… wir kaufen teures E-Learning,
reduzieren unsere Awareness auf "Normen"
und drucken kaum gelesene Broschüren,
damit wir Zeit sparen …**

Awareness ist nicht gleich Awareness

FM-nøspy
Ein Unternehmen der FRED MARO Gruppe

- **Mitarbeiter müssen "Spaß" am Thema haben!
Standard-Awareness-Schulungen verfehlen ihr Ziel!**
- **Im Idealfall gehen Mitarbeiter selbständig auf die
Suche nach Schwachstellen im eigenen Bereich**
- **Zielgruppen müssen unterschiedlich geschult werden
Nur wer weiß, wie angegriffen wird, kann sich dagegen
wappnen.**
- **Geschult werden NIE "alle" Mitarbeiter, sondern
immer nur die "innersten 1-2 Zwiebelringe" rund um
eine definierte "Kronjuwelen" …**

Warum viele "Awareness-Schulungen" kaum helfen … FM-nøspy

Hoch belastete Mitarbeiter sind leichte Ziele!

"Awareness-Schulungen" sind für sie "Zeitfresser" …

致以

Viele verstehen Unternehmenssprachen (z.B. Englisch) nur bedingt – ohne dies zuzugeben …
Sec. Awareness MUSS in Landessprache geschult werden!

Bestimmte Zielgruppen im Unternehmen werden -*wenn* - dann auf unterschiedliche Art und Weise angegriffen!

Standardisierte "Awareness-Schulungen" bieten selten konkrete – praxisgerechte - Hilfestellungen.

Ein Beispiel:
Der Anrufer einer Assistentin könnte auch echt sein …
Kennt und beherrscht sie die Wege, dies schnell herauszufinden und gegebenenfalls "nein" zu sagen, ohne den Anrufer zu verärgern? *(… der Anrufer ist gegebenenfalls Psychologe …)*

Rezeptionen, Redakteure, Techniker werden möglicherweise völlig anders angegriffen …

Nachdenkenswertes

FM-nøspy

- Unterschätzen wir vielleicht die Angriffshäufigkeit, weil wir Angriffe oft gar nicht bemerken?
- Konzentrieren wir uns leichtsinnigerweise fast nur auf die IT-Seite der Industriespionage?
- Ignorieren wir, dass ein großer Teil der SE-Angriffe über – nichts Böses ahnende – Dienstleister oder Zulieferer läuft?
- Investieren wir mehr in irgendwelche Tagungen als in den wichtigen Schutz unserer Kronjuwelen?
- Ein mittelständisches Unternehmen gegen Spionage zu sichern, kostet nur etwa 20% der Aufwände für eine sichere IT !


ευχαριστώ
terima kasih
merkzi
takk
kiitos
감사합니다
taiku
köszönöm
matondo
murakoze
sobodi
matondi
謝謝
tak
hvala
zikomo
terima kasih
salamat
gha-ana
mauruuru
dankie
thank you
misaotra
grazie
danki
бузныг
danke
vinaka
faleminderit
sukriya
takk fyri
gràcies
na som
akpé
gracias
nanni
мерси
ke ya leboha
merci
wado
tänan
mèsi
хвала
najis tuke
maruuru
tualumba
спасибо
akiba
Дзякую
tashakor
arigatô
aguyjé
dankewol
murakoze
gracie
grazie
miigwetch
diolch
tenki
barka
matondo
wopila
Рахмат
marahaba
dank u wel
მადლობა
mulţumesc
paldies
manana
sulpáy
marci
faafetai lava
tanmirt
ДЯКУЮ
dhanyavadalu
enkosi
dziękuję
شكرا
obrigado
gratzias
rahmat
yekeniele
a dank
stuutiyi

„Sicherheit bei der Entsendung von Mitarbeitern“

Birgit Stodtko
Geschäftsführerin International, IHK Halle-Dessau

Es gilt das gesprochene Wort!

IHK Industrie- und Handelskammer Halle – Dessau

International

Begriffsbestimmung

„Sicherheit“ umfasst vielfältige Aspekte:

1. Soziale Sicherheit
2. Gesundheitsschutz („Health & Safety“)
3. Schutz vor Kriminalität und Spionage

Aussagen zu 3. gelten nicht nur für Entsendung, sondern auch für Überlassung, Dienstreisen, Abordnung & Delegation

16. September 2015 Wirtschaftsschutztag Sachsen-Anhalt 2015 2

IHK Industrie- und Handelskammer Halle – Dessau

International

EU-Binnenmarkt

- keine Arbeitsgenehmigung für EU-Bürger!
  aber (zumeist) Anzeige der Entsendung
- Anzeige (noch) nicht harmonisiert → unterschiedliche Formalitäten und Möglichkeiten der Onlineregistrierung

16. September 2015 Wirtschaftsschutztag Sachsen-Anhalt 2015 3

IHK Industrie- und Handelskammer Halle – Dessau

International

Sozialversicherung

Nachweis: Bescheinigung A1 (früher: E101)

- 24 Monate gültig
- Ausstellung durch: 1) gesetzliche Krankenkasse
  2) Träger der gesetzlichen Rentenversicherung
  3) Arbeitsgemeinschaft Berufsständischer Versorgungseinrichtungen e. V.

Formular unter www.dvka.de

16. September 2015 Wirtschaftsschutztag Sachsen-Anhalt 2015 4

IHK Industrie- und Handelskammer Halle – Dessau

International

Tipp

→IHK, GTAI und AHKn bieten Merkblätter „Zur Erbringung von Dienstleistungen im Ausland“

16. September 2015 Wirtschaftsschutztag Sachsen-Anhalt 2015 5

IHK Industrie- und Handelskammer Halle – Dessau

International

Erste Informationsquellen

- Reise- und Sicherheitshinweise des Auswärtigen Amts
  www.auswaertiges-amt.de
- Auslandshandelskammern
  www.ahk.de
- Germany Trade & Invest
  www.gtai.de
- Transparency International
  www.transparency.de


Kenia: Reise- und Sicherheitshinweise

Kontaktanfragen aus Westafrika mit Vorsicht bearbeiten

16. September 2015 Wirtschaftsschutztag Sachsen-Anhalt 2015 6

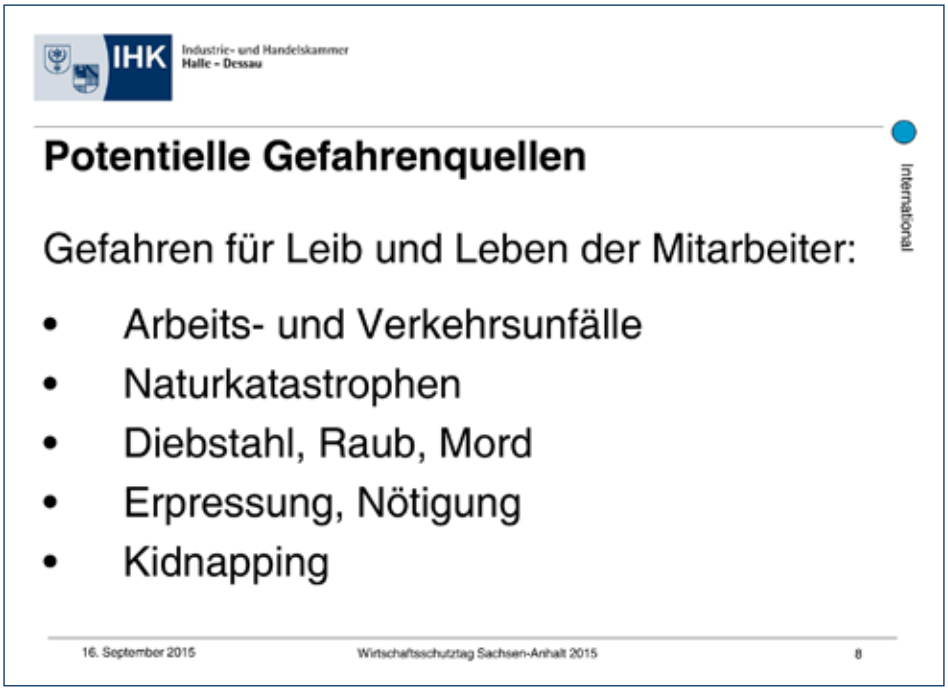
IHK Industrie- und Handelskammer Halle – Dessau

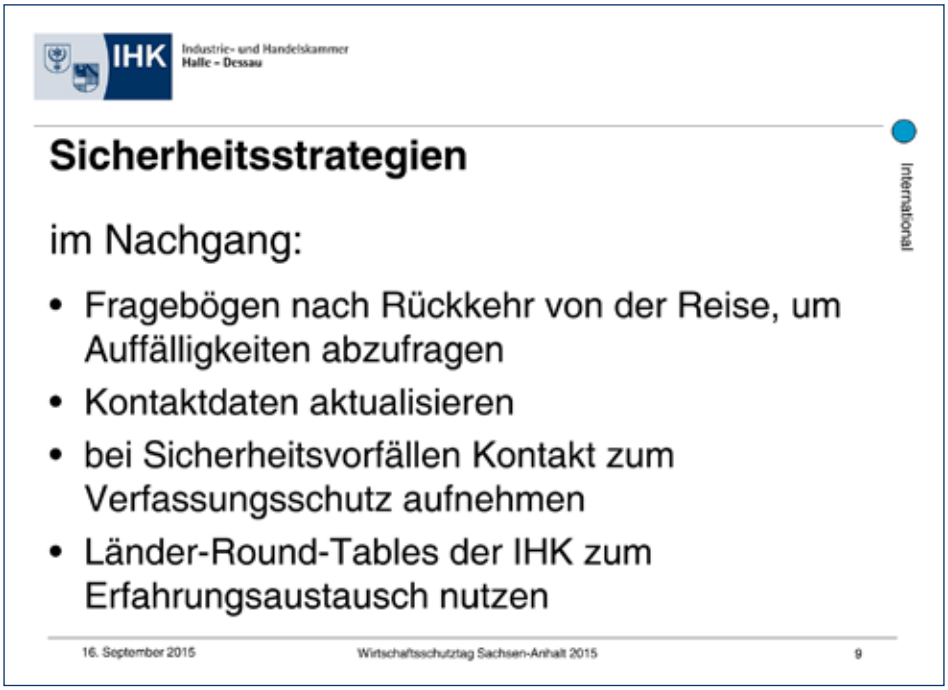
International

Sicherheit im Vorfeld:

- arbeitsmedizinische Vorsorgeuntersuchungen
- Prüfung Visabeantragung und Sicherstellung der Sozialversicherung
- ggfs. Arbeitsverträge ergänzen oder anpassen
- je nach Gefährdungseinschätzung Risiken versichern
- schon im Vorfeld geeignete Dolmetscher, Transport- und Sicherheitsunternehmen finden

16. September 2015 Wirtschaftsschutztag Sachsen-Anhalt 2015 7


IHK
Industrie- und Handelskammer
Halle - Dessau
Potentielle Gefahrenquellen
International
Gefahren für Leib und Leben der Mitarbeiter:
• Arbeits- und Verkehrsunfälle
• Naturkatastrophen
• Diebstahl, Raub, Mord
• Erpressung, Nötigung
• Kidnapping
16. September 2015
Wirtschaftsschutztag Sachsen-Anhalt 2015
8


IHK
Industrie- und Handelskammer
Halle - Dessau
Sicherheitsstrategien
International
im Nachgang:
• Fragebögen nach Rückkehr von der Reise, um Auffälligkeiten abzufragen
• Kontaktdaten aktualisieren
• bei Sicherheitsvorfällen Kontakt zum Verfassungsschutz aufnehmen
• Länder-Round-Tables der IHK zum Erfahrungsaustausch nutzen
16. September 2015
Wirtschaftsschutztag Sachsen-Anhalt 2015
9


IHK
Industrie- und Handelskammer
Halle - Dessau
Wir machen uns stark für Ihren Erfolg!
International
Danke für Ihre Aufmerksamkeit!
Birgit Stodtko
Tel: 0345 2126-274
E-Mail: bstodtko@halle.ihk.de
Homepage: www.halle.ihk.de
16. September 2015
Wirtschaftsschutztag Sachsen-Anhalt 2015
10

„Know-how-Klau – Wie schütze ich innovative Unternehmen? Erfahrungsbericht eines Unternehmers“

Felix von Limburg
Geschäftsführer, B. T. innovation GmbH;

Dr. Ingo Heesemann
B. T. innovation GmbH

Felix von Limburg betätigt sich seit Anfang der 1990er Jahre unternehmerisch in Sachsen-Anhalt. Sein Augenmerk galt zunächst der Zulieferung von Baustellen und Betonfertigteilwerken mit Bauspezialartikeln. Wie so oft ergaben sich aus der jahrelangen Erfahrung im Umgang mit Kunden Ideen, wie z. B. Tätigkeiten auf dem Bausektor erleichtert werden können. So wurde schon nach wenigen Jahren mit der Entwicklung eigener Produkte begonnen. Eines der ersten Produkte war ein Schalungsmagnet, der auf Füßen steht. Dieser Magnet erlaubt die exakte Platzierung von Schalungen, mit denen Betonfertigteile produziert werden. Die Füße halten den Magneten soweit auf Abstand vom Schaltisch, auf dem Betonfertigteile produziert werden, dass der Magnet ohne großen Kraftaufwand milimetergenau platziert werden kann, ehe er durch Druck so nah an den Schaltisch gebracht wird, dass er zuschnappen kann und anhaftet. Durch diese Technologie wurde die Effizienz von Betonfertigteilwerken erhöht. Dieser Magnet wurde überarbeitet und 2009 in der heute erhältlichen Fassung erstmalig angeboten. Bei einem Gewicht von 5,4 kg und einer Haftkraft von über 22 000 N stellt dieser Magnet den derzeit an Haftkraft zu Masse gemessenen besten Magneten für Betonfertigteilwerke dar.

Die Magneten mit der „MagFly-Technologie“ wurden zum Patent angemeldet. Dies hinderte jedoch eine estnische Firma nicht, dieses von der B. T. innovation GmbH patentierte Gerät von einem chinesischen Unternehmen nachbauen zu lassen und die Plagiate selbst zu vermarkten. Sie schreckten, wie alle Teilnehmer der Veranstaltung sich überzeugen konnten, auch nicht davor zurück, das Design vollständig zu kopieren. Die Plagiateure waren jedoch nicht in der Lage, die Leistungsstärke des Magneten auch nur annähernd zu erreichen. Die B. T. innovation GmbH selbst konnte nachweisen, dass die estnische Firma die Plagiate u. a. in Deutschland vertrieben hat, was gegen den Patentschutz verstieß. Ein Gerichtsverfahren mit Unterlassungsklage wurde eingeleitet und gewonnen. Die Kosten für das Gerichtsverfahren belaufen sich auf ca. 15.000 Euro, bei einem geschätzten

Umsatzverlust von mehreren 10.000 Euro. Herr von Limburg erläuterte an diesem praktischen Beispiel wie er es erreichte, seine Innovation patentieren zulassen, wie die Produkte modifiziert werden mussten und mit welchem Aufwand dies verbunden war. Er gab den Zuhörern den Rat gute Ideen schützen zu lassen und dabei einen kompetenten Patentanwalt einzusetzen.

Herr Dr. Heesemann ergänzte die Ausführungen von Herrn von Limburg, indem er erläuterte, welche Schutzrechte es gibt, welchen Risiken ein Unternehmer unterliegt und welche bürokratischen Hürden er überwinden muss, um seine Patente im In- und Ausland durchzusetzen. Schon die Anmeldung von Schutzrechten unterliegt besonderen Anforderungen und nimmt Zeit in Anspruch. Finanzielle Mittel sind einzuplanen, Märkte zu evaluieren und abzuwägen, wo ein Schutz sinnvoll und auch durchsetzbar ist. In Abhängigkeit von der Größe eines bestimmten Marktes kann auf Beantragung von Schutzrechten verzichtet werden, insbesondere wenn man nicht beabsichtigt dort tätig zu werden.

Das stärkste Schutzrecht für eine technische Erfindung stellt das Patent dar. Patentfähige Erfindungen müssen nach § 1 Abs. 1 Patentgesetz besondere Voraussetzungen erfüllen. Sie müssen neu sein, ihnen muss eine erfinderische Tätigkeit zugrunde liegen und sie müssen gewerblich nutzbar sein. Sind diese Voraussetzungen erfüllt, kann beim deutschen Patent- und Markenamt (DPMA) ein Patent beantragt werden. Die Kosten für diesen Prozess belaufen sich oft auf mehrere Tausend Euro und setzen sich aus optionalen Kosten für den Patentanwalt und den obligatorischen Kosten für die eigentliche Anmeldung zusammen. Wird das Patent nach Prüfung gewährt, hat der Patentinhaber vom Anmeldetag an bis zu 20 Jahre lang das alleinige Recht die Erfindung zu verwerten – praktisch ein Monopolrecht mit dem Zweck die wirtschaftliche Nutzung der Erfindung zu vereinfachen. Die Nutzungsdauer des Patents hängt davon ab, ob der Patentinhaber die kontinuierlich steigenden Jahresgebühren bezahlt. Die Nutzung der Erfindung kann sich in der alleinigen Vermarktung widerspiegeln oder aber durch Lizenzvergabe oder gar Verkauf des Patents. Vorteil des Patentschutzes besteht auch darin, dass dieser nach nationaler Anmeldung im Prioritätsjahr auch auf andere Länder bis hin zum weltweiten Schutz ausgeweitet werden kann. Die Frist kann durch eine PCT-Anmeldung[1] im Prioritätsjahr auf bis zu 30 Monate verlängert werden. Oft werden aber nur die wichtigsten Märkte geschützt, um unnötige Kosten für viele Länder zu sparen.

Ein kostengünstigeres, nationales Schutzrecht für technische Erfindungen stellt das Gebrauchsmuster dar, das eine Geltungsdauer von bis zu 10 Jahren haben kann, vorausgesetzt, es werden die notwendigen Gebühren gezahlt. Da bei Eintragung des Gebrauchsmusters nicht geprüft wird, ob die Erfindung neu, gewerblich anwendbar sowie auf einer erfinderischen Tätigkeit beruht, stellt das Gebrauchsmuster eher eine Art Registerrecht dar. Hier gilt es sich im Vorfeld durch sorgfältige Recherche zu vergewissern, dass die Voraussetzungen für ein wirksames Schutzrecht bei der Anmeldung tatsächlich vorliegen. Liegen die Voraussetzungen nicht vor, können Sie letztendlich auch keine Rechte aus dem Gebrauchsmuster geltend machen.

Eine wichtige Rolle bei der Kaufentscheidung von Kunden stellt das Design dar. Bei immer kürzer werdenden Produktzyklen, ist das Design ein wahrnehmbares Unterscheidungsmerkmal. Ein schutzfähiges Design muss neu sein und infolgedessen auch entwickelt werden, sodass auch das Design, früher Geschmacksmuster genannt, als eingetragenes Schutzrecht angemeldet werden kann. Der Schutz für zum Zeitpunkt der Anmeldung neue Designs kann für weniger als 100 Euro beim DPMA eingetragen werden und gilt bei Zahlung der anfallenden Gebühren für bis zu 25 Jahre ab dem Anmeldetag. Dieses Schutzrecht kann auch international beantragt werden.

Das letzte, aber nicht zu vernachlässigende Schutzrecht stellt die Marke dar. Nach § 3 Abs. 1 MarkenG gilt: „Als Marke können alle Zeichen, insbesondere Wörter einschließlich Personennamen,

1 Der „Patent Cooperation Treaty“ ermöglicht die gleichzeitige Patentanmeldung in 148 Vertragsstaaten

Abbildungen, Buchstaben, Zahlen, Hörzeichen, dreidimensionale Gestaltungen einschließlich der Form einer Ware oder ihrer Verpackung sowie sonstige Aufmachungen einschließlich Farben und Farbzusammenstellungen geschützt werden, die geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden." Das Eintragen einer Marke kostet ca. 300 Euro für einen Zeitraum von 10 Jahren und ist im Anschluss verlängerbar. Durch eine Marke kennzeichnen Unternehmen ihre Produkte und Dienstleistungen, erkennbar an dem ®-Zeichen, welches zum wirksamen Schutz angehängt werden darf. Die Marke dient dem Kunden zur Unterscheidung sowie Herkunftsnachweis, stärkt bei positiver Verknüpfung das Image des Markeninhabers und sorgt beim Kunden für eine Art Gütenachweis. Die Marke ist folglich wichtig für das Marketing eines Unternehmens, da sie beim Kunden Vertrauen weckt und die Kaufentscheidung beeinflusst. Höchstes Ziel einer Marke ist es, dass das Produkt in den Sprachgebrauch übergeht, wodurch eine notorische Marke entsteht; Beispiele sind Tempo oder Coca Cola. Eine starke Marke stellt somit einen Vermögenswert dar.

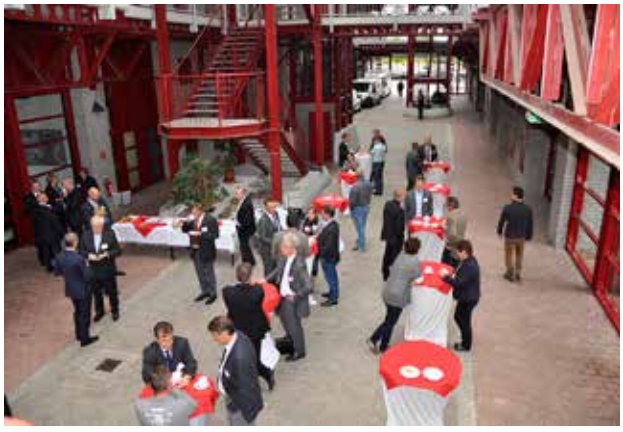
Das beste Schutzrecht hält Produktpiraten leider nicht davon ab, Geschütztes zu kopieren. Daher gilt es den Markt aufmerksam zu beobachten und Nachahmer frühzeitig aufzufinden. Ist ein Plagiateur ausfindig gemacht, sollten Sie frühzeitig aktiv werden. Der geschädigte Unternehmer sollte sich nicht damit begnügen, dass Recht und Gerechtigkeit in der Praxis voneinander abweichen, sondern die Märkte, auf denen er engagiert ist, kontrollieren und beim Auffinden von Plagiaten die Entscheidung vor Gericht suchen. Klagen Sie ihr Schutzrecht ein und untersagen Sie den Vertrieb der Kopie. Wenn Sie die Möglichkeit haben, versuchen Sie die Patentstreitigkeiten auf einen Gerichtsstand zu ziehen, wo ein Durchsetzen Ihrer Rechte auch schnell von Erfolg gekrönt ist – z. B. Deutschland. Plagiatoren muss mit allen zur Verfügung stehenden legalen Mitteln das Handwerk gelegt werden und der Know-how-Schutz, den eine Patentierung entfaltet, rechtfertigt die Mittel.

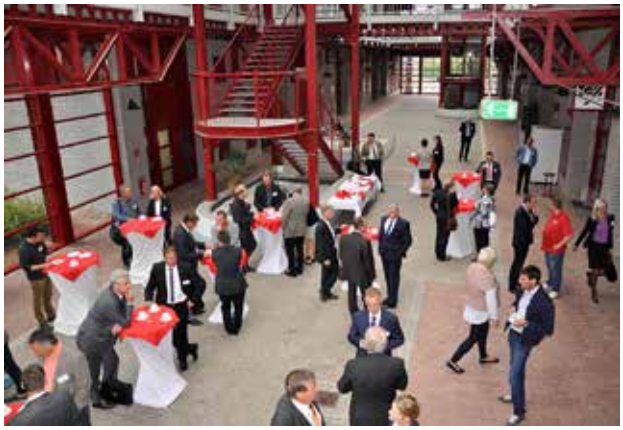
Alles Wissenswerte rund um Schutzrechte und auch damit verbundene Kosten können direkt beim DPMA unter www.dpma.de eingesehen werden.


WEN BEOBACHTET
DER VERFASSUNGSSCHUTZ?


WEN BEOBACHTET
DER VERFASSUNGSSCHUTZ?


INNOVATIONS- UND
GRÜNDERZENTRUM
MAGDEBURG GMBH






Wirtschaftsschutztag Sachsen-Anhalt
Effizienter Schutz für Unternehmen
im In- und Ausland


Perspektiven für die Informationssicherheit
in Kleinen und Mittleren Unternehmen


10 Punkte zum Know-how-Schutz
Effizientes Informationsschutzmanagement:
Identifizierung der benötigten 5% Kronjuwelen
Risiko- und Schwachstellenanalyse
Zugriffsschutz
BYOD-Regelungen
„Need to Know"
„clean-desk-policy"
IT-Sicherheit
Notfallpläne u. a. für IT
Ausland: Datensparsamkeit
Ausland: Kommunikation begrenzen


Begriffsbestimmung
„Sicherheit" umfasst vielfältige Aspekte
1. Soziale Sicherheit
2. Gesundheitsschutz („Health & Safety")
3. Schutz vor Kriminalität und Spionage


Von netten und anderen Menschen


Wirtschaftsschutztag Sachsen-Anhalt
Effizienter Schutz für Unternehmen
im In- und Ausland

Fotos: © ra2 studio - Fotolia.com
© Kurhan - Fotolia.com

Impressum

Herausgeber:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt Halberstädter Straße 2/am „Platz des 17. Juni“ 39112 Magdeburg
Redaktion:	Referat 44 – Parteiverbote, Extremismusprävention, Wirtschaftsschutz – Nachtweide 82 39124 Magdeburg www.mi.sachsen-anhalt.de/verfassungsschutz
Gesamtgestaltung/Druck:	Fachhochschule Polizei Sachsen-Anhalt – Wissenschaftlicher Dienst/Medien –