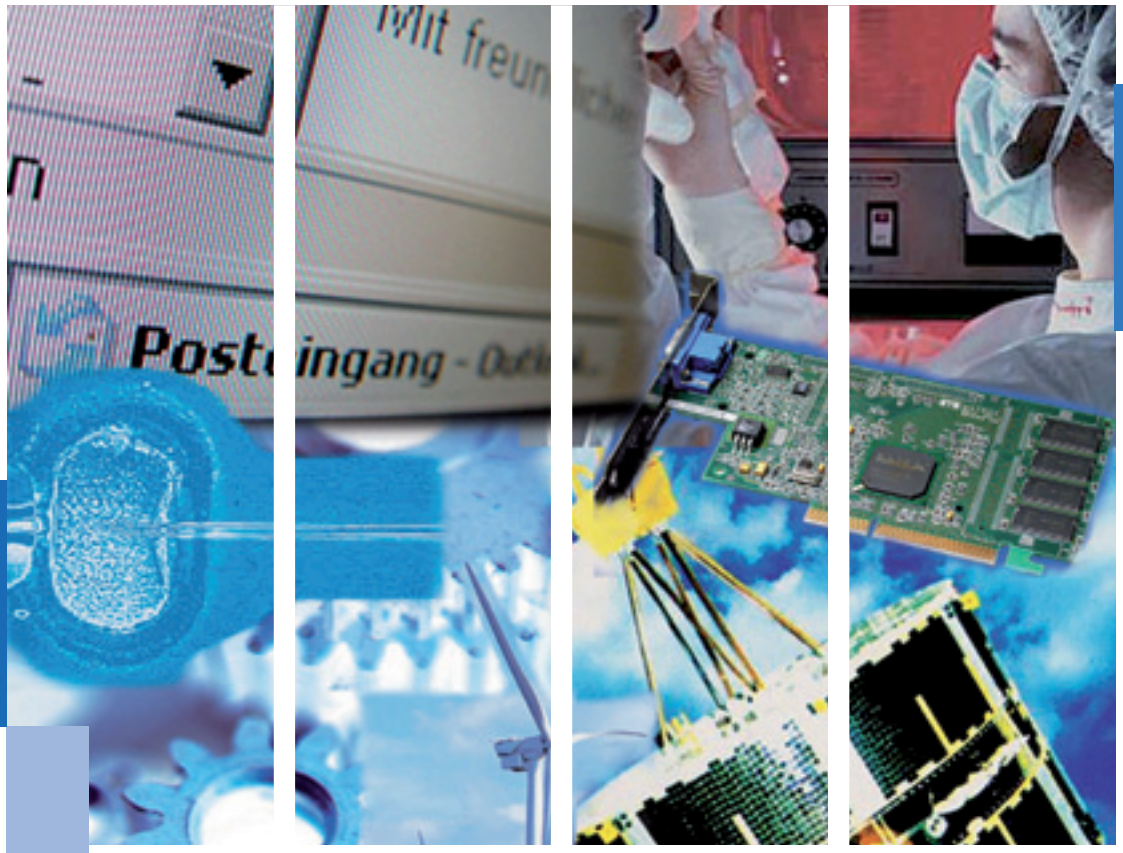
Bundesamt für
Verfassungsschutz

ASW
Zentralorganisation der Wirtschaft

Wirtschaftsschutz: Prävention durch Information

6. Sicherheitstagung des BfV und der ASW am 4. Juli 2012 in Berlin



Tagungsband

„Proaktiver Wirtschaftsschutz: Prävention durch Information“

6. Sicherheitstagung des BfV und der ASW am 4. Juli 2012 in Berlin

Tagungsband

Impressum:

Herausgeber: Bundesamt für Verfassungsschutz
Merianstraße 100
50765 Köln

Tel.: 0221-792-0
Fax: 0221-792-2915
E-Mail: wirtschaftsschutz@bfv.bund.de
Internet: http://www.verfassungsschutz.de

Inhaltsverzeichnis Seite

Einleitung **1**

Begrüßung und Keynote des Abteilungsleiters Spionageabwehr im BfV, **2**
Dr. Burkhard Even

„Trends im globalen Sicherheitsumfeld“ **5**
Dr. Cosima Eggers, CSO Airbus Deutschland GmbH

„Konvergenz von Sicherheit als Antwort auf komplexe Bedrohungen“ **9**
Volker Wagner, Leiter Group Business Security Deutsche Telekom AG/
Vorsitzender der ASW

„Cyberwar, iPads, Facebook, Cloudcomputing: Lässt sich Know-how heute überhaupt noch schützen?“ **25**
Florian Oelmaier, Leiter IT-Sicherheit und Computerkriminalität,
Corporate Trust GmbH

„Proliferationsabwehr – eine Aufgabe des Verfassungsschutzes“ **44**
Edmund Meyer, Referatsleiter im BfV

„Deutschlands Sicherheit – Cybercrime und Cyberwar“ **46**
Arne Schönbohm, Vorstand BSS BuCET Shared Services AG

6. Sicherheitstagung des BfV und der ASW am 4. Juli 2012 in Berlin

Die 6. Sicherheitstagung des Bundesamtes für Verfassungsschutz und der Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V. (ASW) fand unter dem Motto „Proaktiver Wirtschaftsschutz: Prävention durch Information“ statt. Zahlreiche Vertreter von Unternehmen und Wirtschaftsverbänden sowie Mitarbeiter von Ministerien und Sicherheitsbehörden nahmen an dem jährlichen Treffen teil. Die Referate von Sicherheitsexperten aus Behörden und der Wirtschaft zu diversen Aspekten des Wirtschaftsschutzes regten einen vielfältigen Informations- und Meinungsaustausch an.

Die gemeinsamen Sicherheitstagungen sind Teil umfangreicher Maßnahmen im Bereich der Information und Sensibilisierung durch das BfV und seines Kooperationspartners ASW. Ziel von Prävention durch Information ist der Schutz der Unternehmen und des Wirtschaftsstandortes Deutschland. Sie sind zugleich Ausdruck einer guten Zusammenarbeit von Staat und Wirtschaft. Denn:

„Wirtschaftsschutz ist Teamwork!“

Begrüßung und Keynote des Abteilungsleiters Spionageabwehr im BfV, Dr. Burkhard Even

Meine sehr geehrten Damen und Herren,
ich begrüße Sie herzlich zur heutigen Sicherheitstagung, die wir unter das Motto „Proaktiver Wirtschaftsschutz: Prävention durch Information“ gestellt haben. Es handelt sich mittlerweile um die 6. Tagung dieser Art, die gemeinsam von der Arbeitsgemeinschaft für Sicherheit der Wirtschaft und dem Bundesamt für Verfassungsschutz durchgeführt wird.

Diese alljährliche Sicherheitstagung ist für uns ein wichtiger Baustein im Rahmen unserer Wirtschaftsschutzaktivitäten. Der Austausch von Informationen, der gemeinsame Dialog, das Kennenlernen und das Vertiefen bestehender Kontakte ist eine der Grundlagen vertrauensvoller Kooperation zwischen Staat und Wirtschaft und dem soll auch die Tagung heute dienen.

Spionage in Deutschland ist tägliche Realität. Im Fokus stehen neben den sog. klassischen Spionagefeldern Politik und Militär – seit Jahren und mit gestiegener Bedeutung – auch die Bereiche Wirtschaft, Wissenschaft und Forschung.

Die bislang positive wirtschaftliche Entwicklung Deutschlands im Umfeld der anhaltenden Krise der Finanz- und Wirtschaftsmärkte zeigt die Stärke der deutschen Unternehmen im weltweiten Wettbewerb. Ihre Stärke liegt vor allem in ihrer Innovations- und Wettbewerbsfähigkeit.

Es überrascht daher nicht, dass Nachrichtendienste anderer Staaten den Auftrag haben, ihre Volkswirtschaften mit illegal beschafftem Know-how deutscher Unternehmen zu unterstützen. Ziel ist es, Entwicklungsaufwand, Kosten und Zeit einzusparen und sich Wettbewerbsvorteile zu verschaffen. Gleiches gilt auch für konkurrierende Unternehmen, die es auf das Know-how deutscher Wettbewerber abgesehen haben. Unabhängig von der Täterfrage gilt es für deutsche Unternehmen, sich vor den vielfältigen Risiken zu schützen.

Unsere Lageeinschätzung deckt sich mit dem Ergebnis verschiedener wissenschaftlicher Studien sowie auch der Selbsteinschätzung zahlreicher Unternehmen. So ergibt sich aus der Studie „Industriespionage 2012“, die von Corporate Trust im Mai veröffentlicht wurde, dass über 20 % der befragten Unternehmen Schäden durch Spionage und Ausspähung bei sich festgestellt haben.

Schadensverhütung ist stets besser als Schadensbeseitigung. Grundlage effektiver Prävention ist dabei immer ein entsprechendes Sicherheitskonzept, welches erstellt und anschließend auch umgesetzt werden muss. Dabei ist wichtig, dass das Konzept als „Chefsache“ im Unternehmen behandelt wird, die Mitarbeiter einbezieht, technische Lösungen beinhaltet,

ohne sich darin zu erschöpfen, sowie ständig an sich wandelnde Rahmenbedingungen und Bedrohungen angepasst wird.

Dies zu tun ist in erster Linie eine Aufgabe der Unternehmen selbst und nicht des Staates. Gleichwohl ist es der Bundesregierung ein wichtiges Anliegen, Wirtschaftsschutz als gesamtstaatliche Aufgabe zu behandeln. Deutlich wird dies durch die Einrichtung des Ressortkreises Wirtschaftsschutz, in dem die für dieses Aufgabenfeld besonders relevanten Ressorts (insbesondere BK, BMI und BMWi) sowie die zuständigen Sicherheitsbehörden vertreten sind und in dem Aktivitäten gebündelt und koordiniert werden. Zentrale Bedeutung hat dabei die Förderung des Dialogs zwischen Sicherheitsbehörden und der Wirtschaft.

Die Verfassungsschutzbehörden des Bundes und Länder nehmen diese Herausforderungen proaktiv an, d.h. einer der Schwerpunkte unserer Aufgabenwahrnehmung ist die Prävention und hierbei die Kooperation mit Unternehmen und Wirtschaftsverbänden in Deutschland.

Unser Handlungsspektrum reicht von allgemeinen Sensibilisierungen (Vorträge, Broschüren, Homepage) über genauere Hinweise zu bestimmten Themen bis hin zu Hilfe und Beratung im Einzelfall bei konkreten Anhaltspunkten.

Beispielhaft erwähnen möchte ich in diesem Zusammenhang unsere Reihe von Kurzinformationen zu einzelnen Aspekten der Prävention, die wir aktuell um vier weitere Ausgaben ergänzt haben. Diesmal gehen wir u.a. auf die besonderen Risiken während Geschäftsreisen sowie auf die Frage möglicher „Innentäter“ ein. Die Publikationsreihe umfasst mittlerweile zehn unterschiedliche Themen, die in einem handlichen Format vielfältige praxisgerechte Handlungsempfehlungen enthalten. Natürlich sind sie hier und heute erhältlich.

Die Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind zu einer existenziellen Frage unseres Jahrhunderts geworden. Die Gewährleistung von Cyber-Sicherheit wird damit zur zentralen gemeinsamen Herausforderung für Staat, Wirtschaft und Gesellschaft. Die Umsetzung der im letzten Jahr von der Bundesregierung beschlossenen Cyber-Sicherheitsstrategie ist angesichts dessen eine prioritäre Aufgabe.

Beispielhaft nennen möchte ich in diesem Zusammenhang die weitere Konsolidierung des vor einem Jahr gegründeten Cyber-Abwehrzentrums, die vom BKA initiierte Public-Private-Partnership im Bereich Cyber-Kriminalität sowie die von BSI und BITKOM auf der CEBIT im März vorgestellte „Allianz für Cybersicherheit“, eine Internetplattform die noch im Laufe dieses Jahres in Betrieb gehen und die den wechselseitigen Informationsaustausch zwischen Behörden und Unternehmen erleichtern soll.

Effektiven Wirtschaftschutz gibt es nur gemeinsam: in Kooperation von Staat und Wirtschaft. Dem entspricht auch, dass bei der heutigen Tagung Vertreter aus beiden Bereichen teilnehmen und dass sich das auch bei den Referenten widerspiegelt.

Zunächst begrüße ich Frau Dr. Cosima Eggers, Leiterin der Konzernsicherheit von Airbus, die sich in ihrem Vortrag mit den Trends im globalen Sicherheitsumfeld auseinandersetzen und uns über den Umgang eines Unternehmens mit den gestiegenen Herausforderungen berichten wird.

Volker Wagner ist nicht nur neuer Vorsitzender der ASW, sondern gleichzeitig auch Leiter der „Group Business Security“ bei der Deutschen Telekom AG. Sein Thema lautet „Konvergenz von Sicherheit als Antwort auf komplexe Bedrohungen“. Vielen Dank Herr Wagner, dass Sie sich heute mit Ihrer umfassenden Erfahrung und zudem quasi in Doppelfunktion einbringen.

Lässt sich Know-how heute überhaupt noch schützen – in Zeiten von Cyberwar, iPads, Facebook und Cloud Computing ? Auf diese wohl bewusst provokative Frage wird Florian Oelmeier, Leiter der IT-Sicherheit bei der Corporate Trust GmbH eingehen. Wir sind gespannt auf Ihre Analyse und Antworten – seien Sie herzlich willkommen.

Ich begrüße auch Arne Schönbohm, Vorstandsmitglied des Beratungsunternehmens BSS Shared Services AG. In seinem Vortrag „Deutschlands Sicherheit – Cybercrime und Cyberwar“ wird Herr Schönbohm die umfangreichen Auswirkungen der Risken aus dem Cyber-Raum für unser Gemeinwesen thematisieren.

Last but not least möchte ich auch Edmund Meyer Referatsleiter im BfV begrüßen. Seien Sie gespannt auf einen Bericht zu einem sensiblen und wichtigen Teilaspekt des Wirtschaftsschutzes - die Verhinderung der Weitergabe oder Weiterverbreitung von Massenvernichtungswaffen, ihren Trägersystemen oder den dafür notwendigen Produkten und das Know-how hierzu. Auch hier ist die Sensibilisierung von und Kooperation mit Unternehmen eine wichtige Aufgabe der Verfassungsschutzbehörden.

Ich möchte nicht versäumen, an dieser Stelle ganz besonders herzlich auch einige Vertreterinnen und Vertreter unserer Partnerdienste zu begrüßen. Ihre Anwesenheit und Ihr Interesse an dieser Tagung zeigt, dass Wirtschaftsschutz nicht nur eine Herausforderung in Deutschland ist. Wir teilen das Problem mit anderen und auch in diesem Bereich sind wir dankbar für den Erfahrungsaustausch im internationalen Rahmen.

Meine Damen und Herren,
uns allen wünsche ich eine interessante Tagung, eine abwechslungsreiche Diskussionsrunde sowie rege Gespräche.

Trends im globalen Sicherheitsumfeld

Referentin: Dr. Cosima Eggers, CSO Airbus Deutschland GmbH

Abstract

Im Rahmen der Veranstaltung „Wirtschaftsschutz: Prävention durch Information“ ist der Fokus dieses Vortrages Informationsschutz in einem internationalen Konzern mit besonderer Berücksichtigung des folgenden Sicherheitsumfeldes:

- Internationales Business
- Reisen
- Konkurrenz
- Netzwerksicherheit
- Sicherer Produktionsprozess
- Politik

Airbus

Airbus ist der weltweit führende Flugzeughersteller. Als internationales Unternehmen unterhält Airbus neben seinen Produktionsstätten in Frankreich, Deutschland, Spanien, Großbritannien, China und (ab 2015) den USA noch weltweit Ersatzteilzentren, Kundenbüros und Entwicklungsbüros.

Airbus S.A.S. ist eine Tochtergesellschaft des EADS-Konzerns mit Hauptsitz in Toulouse. Airbus erzielte im Jahr 2011 einen Umsatz von 33,1 Milliarden Euro und beschäftigt derzeit 55,600 Mitarbeiter. Im Jahr 2011 verzeichnete das unternehmen einen Bestellungseingang in Höhe von 117,9 Milliarden Euro.

Im April 2009 wurde „Airbus Military“ mit Sitz in Madrid gegründet.

Diese Tochtergesellschaft umfasst alle zum Airbus-Konzern gehörigen militärischen Luftfahrzeugprogramme. Im Jahr 2003 hat Airbus Boring als führenden Flugzeughersteller überholt. Gemeinsam sind diese beiden Unternehmen die zwei führenden (und faktisch weltweit einzigen) Produzenten von modernen Großraumflugzeugen. Marktanalysen beider Duopolisten sagen für die nächsten 20 Jahre eine Nachfrage von rund 28,000 neuen Flugzeugen voraus. Um diesen Markt werben vor allem Boeing und Airbus, es ist jedoch zur Mitte des Jahrzehnts mit neuen Wettbewerbern aus Russland, China, Kanada gerade im unteren Größensegment (100-150 Sitze) zu rechnen.

Die Flugzeugproduktion von Airbus ist über die Grenzen der vier Kernländer (Deutschland, Frankreich, England, Spanien) hinweg transnational und arbeitsteilig organisiert. Sowohl die Schaffung der technischen Voraussetzungen einer harmonisierten Produktion sowie der sichere Transport der Flugzeugteile per Luft, Land und Wasser gehören zu den grundlegenden

Herausforderungen. Gleichzeitig verfügt Airbus über eine tief gestaffelte Lieferkette, mit der die Produktionsprozesse eng verwoben sind. So unterstützen zum Beispiel alleine über 200 Vertragsfirmen den Bau der A350. Diese Firmen arbeiten miteinander und mit Airbus.
Airbus denkt bereits heute über die Zukunft des Fliegens im Jahr 2050 nach. Die innovativen Zukunftsprojekte von Airbus für neue Flugzeug- und Kabinenkonzepte, öko-effiziente Antriebe und neuartige Treibstoffe sind Teil des zu schützenden k*now-how*.
Das Sicherheitsumfeld von Firmen der Größenordnung von Airbus ist vielschichtig. Objektsicherheit, Produktsicherheit und Informationsschutz sind Kernsicherheitsthemen. Der Fokus dieses Vortrages ist die Informationssicherheit. Hierbei sind die Hauptherausforderung die Internationalität von Unternehmen und die Sicherheit des IT-Netzwerkes.

- Internationales Business

Internationale Geschäftstätigkeit umfasst immer eine Anpassung an die nationalen Anforderungen des Geschäftsumfeldes. Während in Lateinamerika Korruption die Kernherausforderung für europäische Firmen darstellt, ist es Terrorismus im Nahen Osten und der Schutz des geistigen Eigentums in Asien. Firmen schützen sich auf diverse Arten vor diesen Bedrohungen. Der Gefahr des Terrorismus wird durch erhöhten Schutz entgegengewirkt. Korruption wird zunehmend durch *compliance*-Strategien und klare *policies* bewältigt. Der Bereich des Produktschutzes gehört weiterhin zu den schwierigsten Bereichen des Selbstschutzes von Firmen. Um defensive Maßnahmen so gering wie möglich zu halten, wählen viele Firmen einen offensiven und offenen Weg - jenen der Markenanbindung von Kunden und Qualitätssicherung. Mit einer schnellen und effektiven Marktdominanz durch schnelle Umsetzung von Innovationen und Verlässlichkeit durch Qualität stellen sich große Konzerne gegen diese Form der Bedrohung. Kleinen und mittelständischen Betrieben fehlt oft das Kapital für diese Strategie.

- Reisen

Im Rahmen der Reisetätigkeiten der Mitarbeiter ist vor allem der Verlust des *know-how* im Fokus der Sicherheitsmaßnahmen. Sowohl der Diebstahl von Laptops als auch Informationsabfluss im Rahmen von Gesprächen sind Standardherausforderungen aller international agierender Firmen.
Verschlüsselung der Hardware der Laptops als auch der Kommunikation im Falle wichtiger Geschäftsverhandlungen oder Produktenwicklungsprozesse gelten als Standardmaßnahme. *Awareness*-Programme für Mitarbeiter sollen sensibilisieren und auf mögliche Gefährdungen aufmerksam machen.

- Konkurrenz

Im Flugzeugbau unterhalten Boeing und Airbus ein Duopol bei Flugzeugen mit mehr als 100 Sitzen. Beide Unternehmen haben sich am Markt platziert. Eine strategische oder taktische Neuausrichtung impliziert eine 15 bis 20 jährige Umsetzungsphase. Die Entwicklungskosten

sind hoch und der Kernbereich der Informationen ist zu schützen. Besonders hart trifft Informationsabfluss Unternehmen, deren Produktspektrum klein ist und die sich als Marke noch nicht etablieren konnten. Gegen Informationsabfluss an Konkurrenz wird der Schwerpunkt der Schutzaktivitäten auf die Klassifizierung der Informationen und auf *awareness*-Programme für Mitarbeiter gelegt.

- Netzwerksicherheit

Mit Stuxnet hat die IT-Sicherheit einen neuen Stellenwert erhalten. Kernaufgabe ist die Gestaltung einer Netzwerkstruktur, welche die Verbreitung von *malware* erschwert. Hierbei wird der Schwerpunkt auf *stand-alone*-Systeme gelegt und *compartmentalisation* zum bereichsspezifischen Schutz zur Gewährleistung des *business recovery* im Falle eines erfolgreichen Angriffes. Der Schutz nach außen, sprich die Implementierung einer *firewall*, ist keineswegs ausreichend. Verbreitung intern durch USB-Sticks oder gezielte Platzierung muss ebenso detektiert werden.

- Sicherer Produktionsprozess

Der gezielte Angriff auf die Steuerung des Produktionsprozesses durch *malware* ermöglicht Sabotagehandlungen. Entsprechend ist die Netzwerksicherheit auf einen effektiven *business recovery* Plan auszurichten und die bereits angesprochene Netzwerkstruktur an diese Gefährdung zu adaptieren. Eine besondere Herausforderung stellen in diesem Zusammenhang die Vielzahl von Zulieferern, Fremdfirmen und IT-Servicedienstleistern dar.
Die Sicherheitsstandards werden vertraglich festgelegt und durch regelmäßige Audits verifiziert.

- Politik

Know-how Abgabe ist manchmal auch Teil von Gegengeschäften, besonders in geschäftlichen Beziehungen mit Staaten und Regierungen. Dies kann der Erringerung von Marktanteilen in ansonsten verschlossenen Märkten förderlich sein. Hierbei ist bewusste und gezielte *know-how* Abgabe Teil der Geschäftsstrategie.

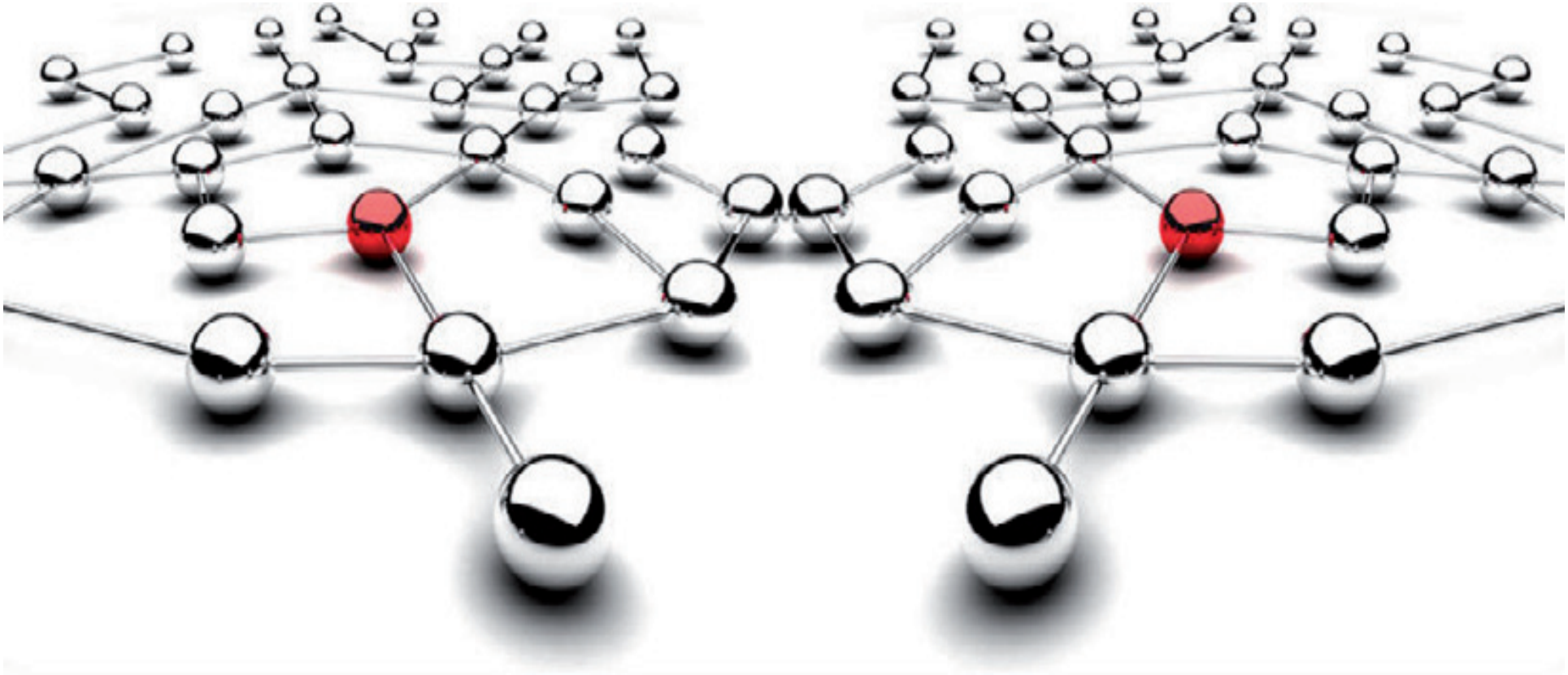
Maßnahmen

Die Maßnahmen, die einem Großkonzern zur Verfügung stehen, sind in Summe vielfältig. Erster Ansatz ist die Schaffung klarer Richtlinien für die Standards von Sicherheitsmaßnahmen. Basis dafür ist die Prävention durch rechtzeitige Information. Ein konkretes Regelwerk und Vorgaben für die Klassifizierung von Informationen dienen auch der harmonisierten Zusammenarbeit mit Fremdfirmen. Vor allem die Klassifizierung von schützenswerten Informationen und *know-how* werden *top-down* von den Bereichen selbst definiert. Auditierung gewährleistet die Einhaltung der Maßnahmen.
Eine sicherheitsbezogene Netzwerkstruktur wird zukünftig zu den Standardinvestitionen von

Unternehmen gehören. Die Cyberdrohungen gehören zu den dynamischsten und unberechenbarsten Gefahrenquellen der Zukunft. Innerhalb der Netzwerkstrukturen muss eine flexible Reaktion auf gefahren möglich sein, gekoppelt mit Detektionssystemen, die ungewöhnliche Verhaltensmuster wahrnehmen. Zur Gewährleistung eines sicheren Produktionsprozesses muss der Fokus auf *business recovery management* liegen und die vertraglichen Voraussetzungen dafür auch bei Fremdfirmen geschaffen werden. Verschlüsselung von schützenswerten Informationen und *stand-alone* Systeme für geheime Information sind ebenso Teil der Schutzmechanismen wie *awareness* Kampagnen für die Mitarbeiter.

Zusammenfassung

Großkonzerne wie Airbus richten ihre Sicherheitsmaßnahmen entsprechend der Firmenstrategie und dem bestehenden Sicherheitsumfeld aus. Die Maßnahmen müssen an die Beschaffenheit der Produkte, den Produktionsprozess und an die Zielsetzungen der Geschäftsinteressen angepasst werden. Prävention durch rechtzeitige Information und die Ausgestaltung von Richtlinien sind das Fundament. Während die klassischen Gefährdungen für ein Unternehmen auf Basis langjähriger Erfahrung bewältigt werden, stellt *cybercrime* die Sicherheitsexperten vor neue Herausforderungen. Hier steht der Schutz versus kostengünstige IT-Lösungen. Eine hundertprozentige Sicherheit kann kein Sicherheitskonzept leisten. Dennoch muss in eine effektive und schnelle Reaktionsfähigkeit sowie Prävention und *business recovery* investiert werden.

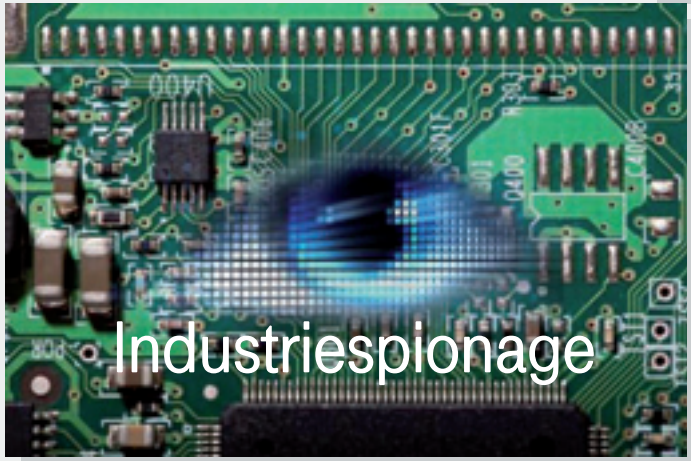


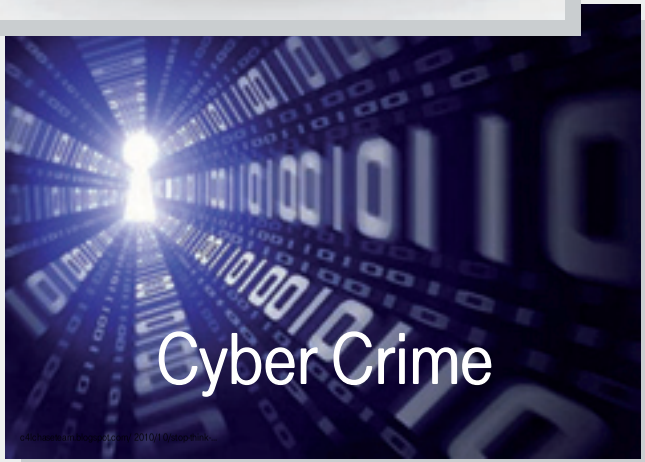
Konvergenz von Sicherheit als Antwort auf komplexe Bedrohungen

Volker Wagner, Deutsche Telekom AG, Leiter Group Business Security
Vorstandsvorsitzender ASW

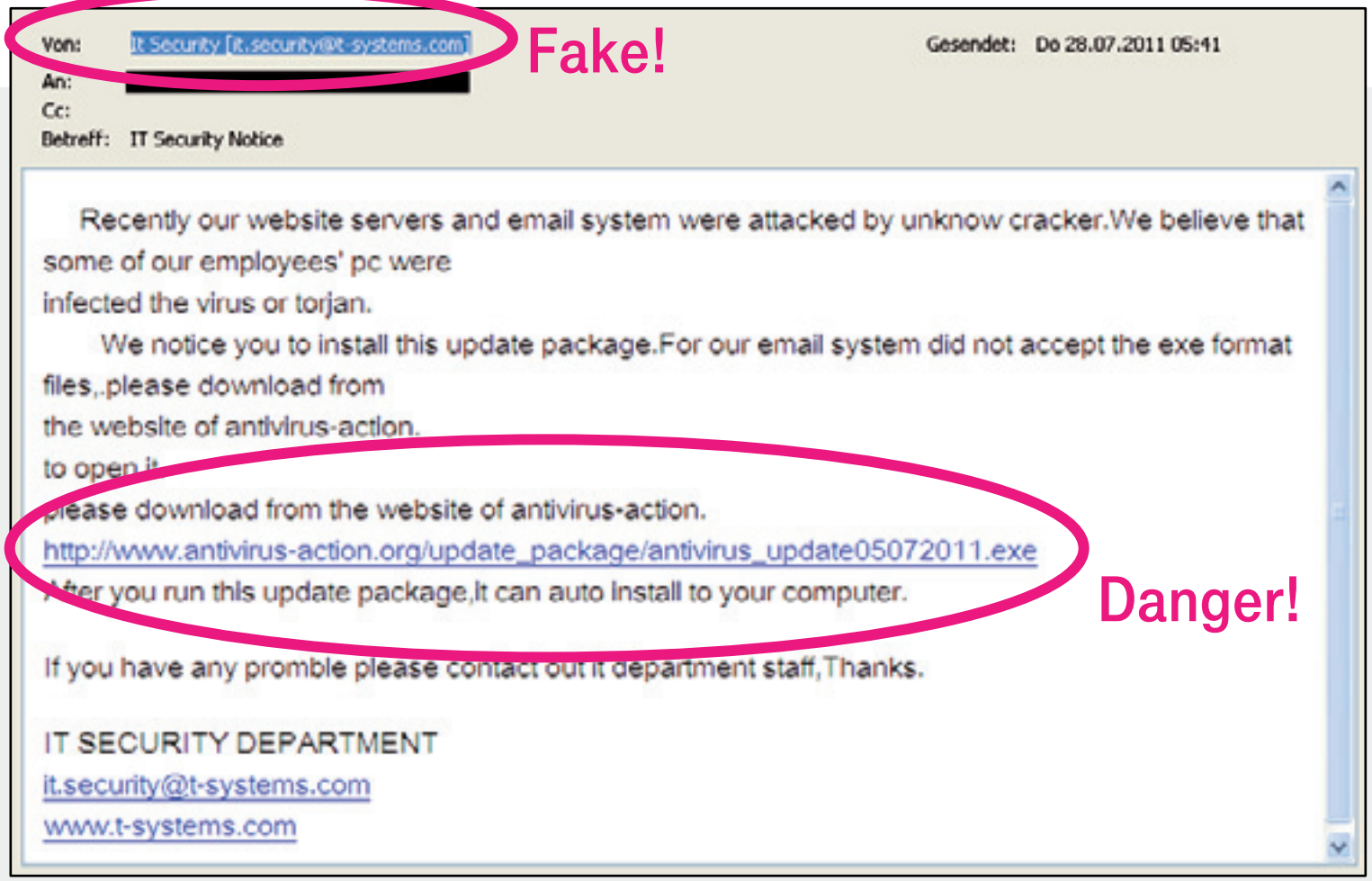
04. Juli 2012

Attacken haben in den letzten Jahren an Anzahl, Geschwindigkeit und „Intelligenz“ zugenommen.





Eine E-Mail von unserer Sicherheitsabteilung?

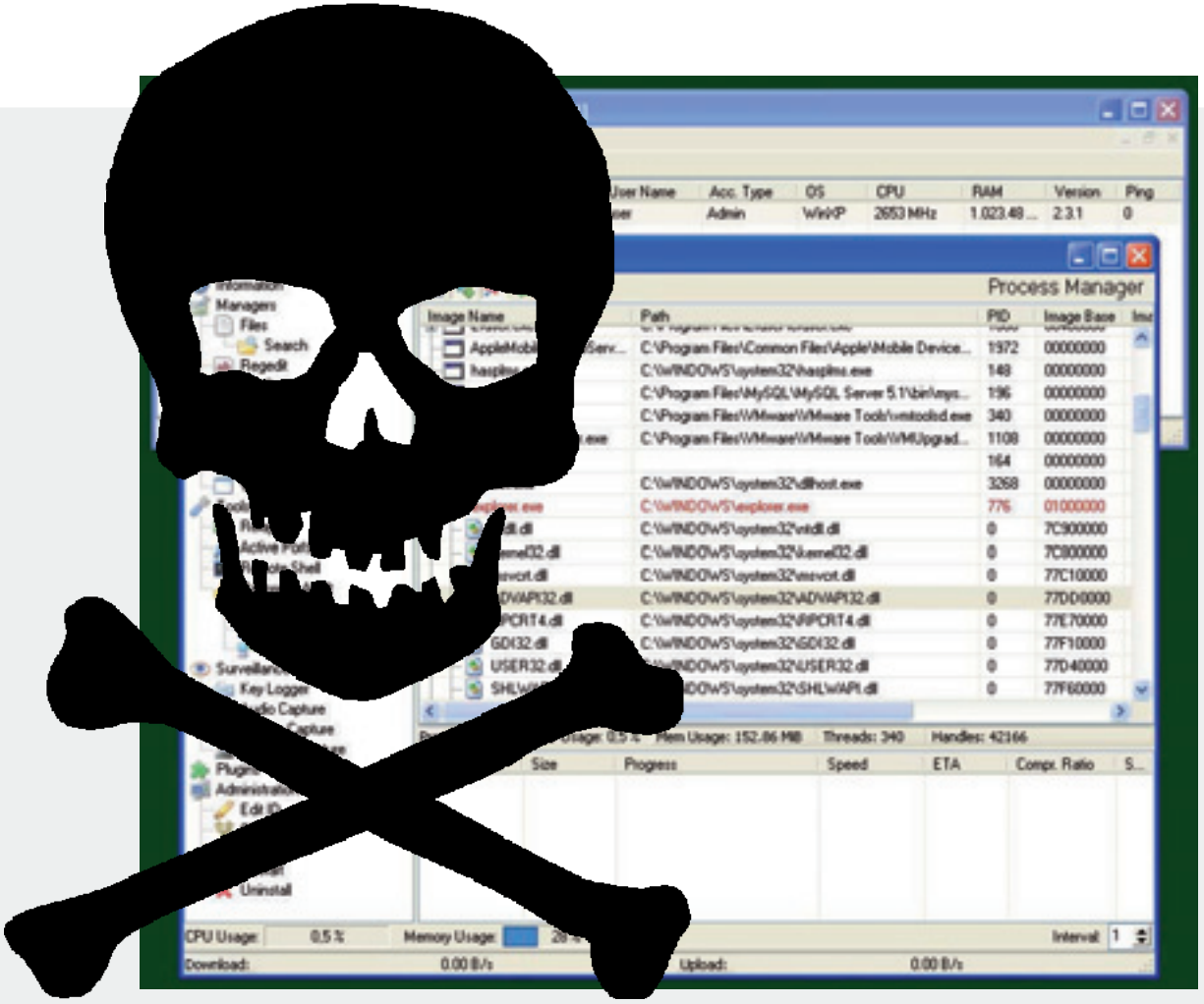


Laboranalyse: Mail User Agent

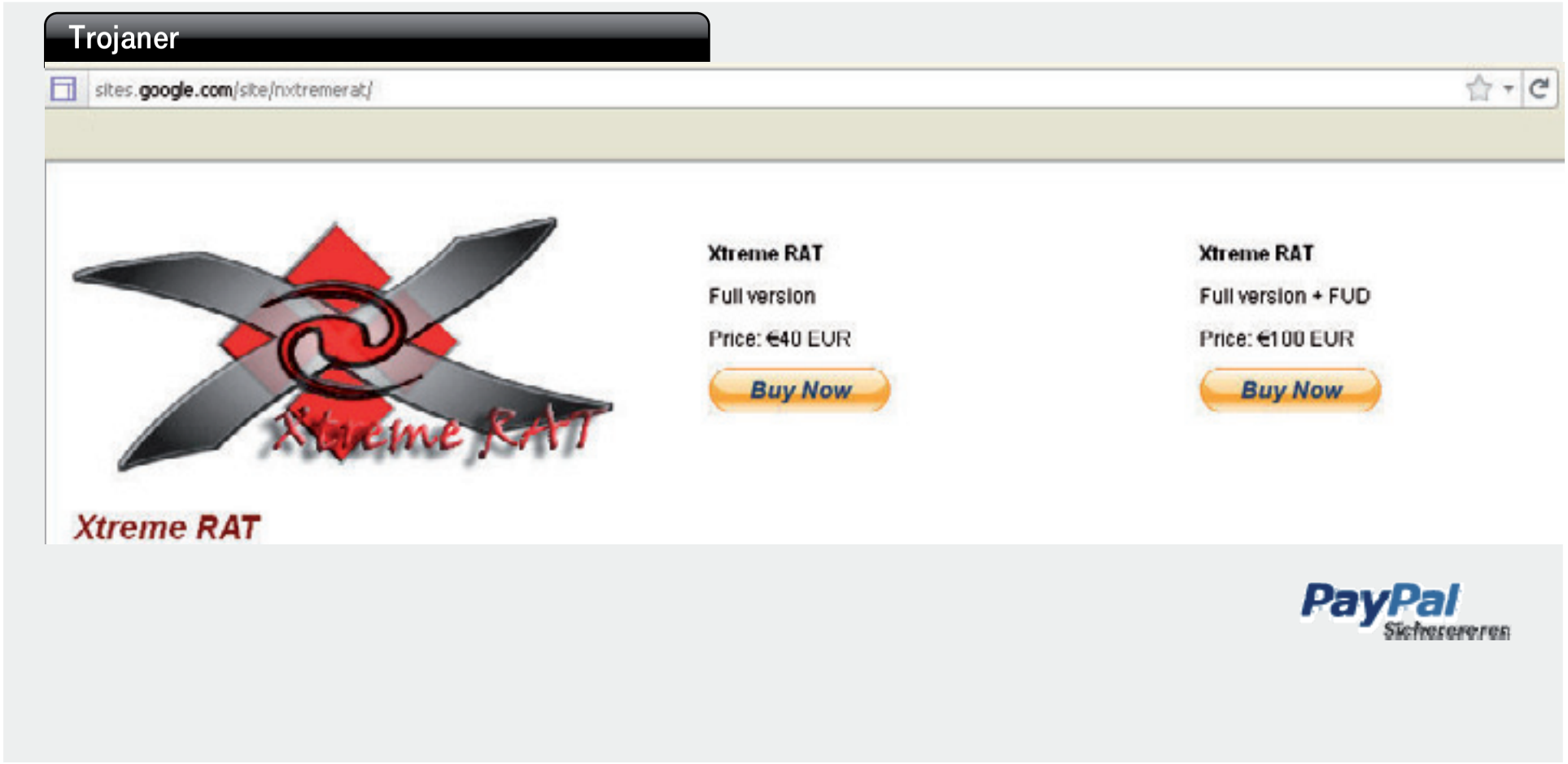
Ergebnis: Poison Ivy

„Remote Administration Tool”

- infects standard browser for communication
- system data collector
- screen shots
- audio / video capture
- keylogger
- registry editor
- process monitor
- communication tunnels
- file transfer
- proxy to intranet systems
- plugin API
- live updates w/o restart
- manage „clients” on server



Marktplatz Internet: Trojaner und Schwachstellen auf Bestellung



Unsere Antwort auf diese Sicherheitsherausforderungen ist ein umfassendes Sicherheitsmanagement.

Früherkennung von Gefahren

Umgang mit Sicherheitsvorfällen

Prävention

Audit und Monitoring

Lösungsansatz:

Konvergenz der Sicherheit

Früherkennung von Gefahren – rechtzeitig die Lage im Blick

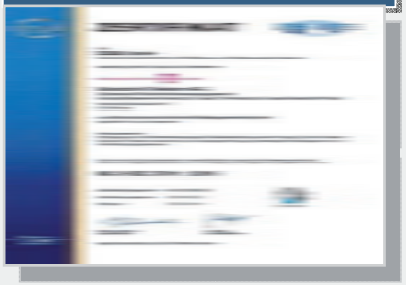
Lagemanagement

Zusammenarbeit
national / international

Prävention – Vertrauen schaffen

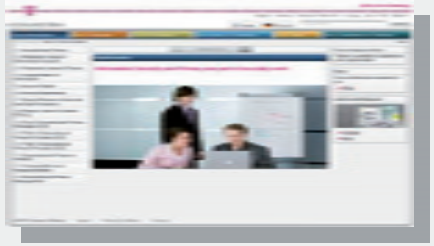
Prävention

Sicherheits-management

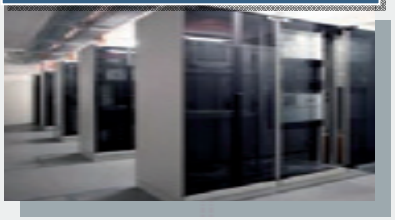


IT-Sicherheit

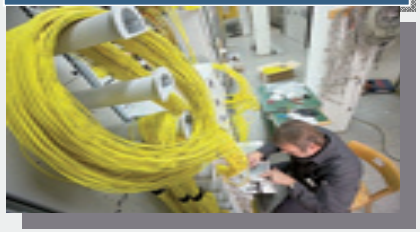
Security Awareness - Ganzheitliches mySecurity Concept



Physikalische Sicherheit



Incident-Handling-Prozesse



Computer Emergency Response Team – CERT

Audit und Monitoring – Risiken abschätzen und erkennen

Sicherheitsuntersuchungen

Missbrauchserkennung

Umgang mit Sicherheitsvorfällen – effiziente Kommunikation

Ermittlungen

Krisenmanagement

Konvergenz von Sicherheit - unsere strategische Antwort

Nur gemeinsam können wir die Risiken abwehren!

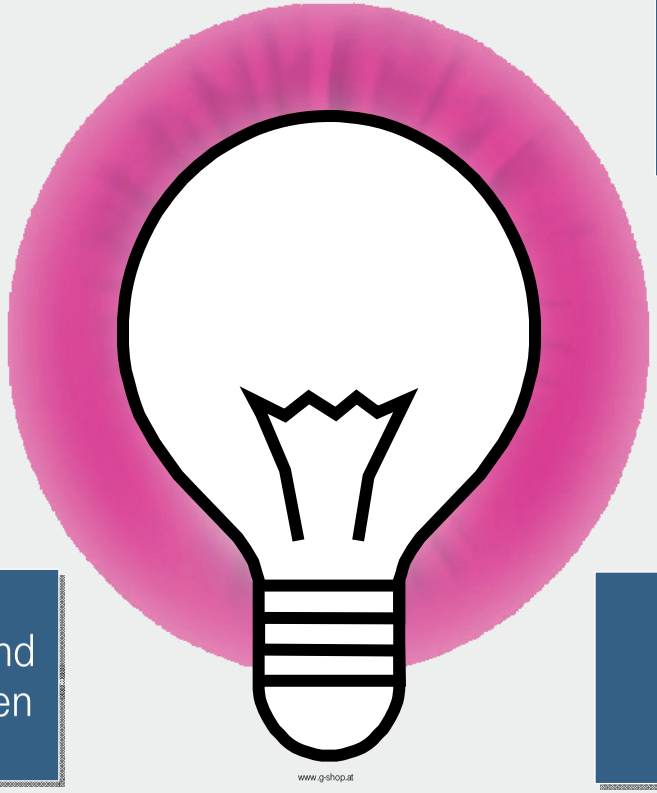
- indem wir ganzheitlich und konvergent denken, über Organisationen und Funktionen hinaus
- indem wir Sicherheit in der Planung und im Tagesgeschäft verankern
- indem wir alle wichtigen Interessengruppen einbeziehen

Konvergentes Denken – es beginnt bei uns selbst

Fachübergreifende Maßnahmen annehmen

Professionelle Einstellung & enge Beziehungen aufbauen

Informationen teilen

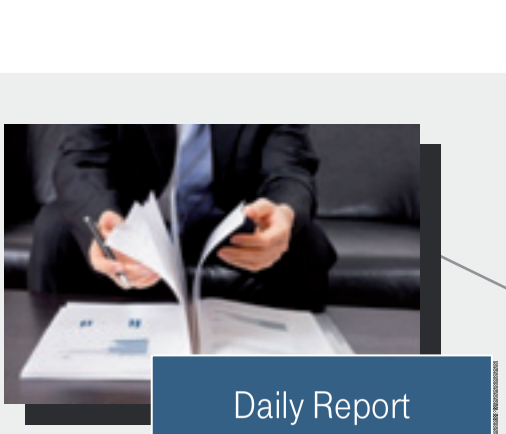


Bescheiden sein und andere Risikoprioritäten akzeptieren

Prozesse integrieren und Reporting rationalisieren

Verständnis in allen Funktionen fördern

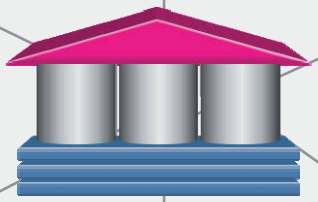
Strategische Ausrichtung - Sicherheit als Design-Prinzip des Daily Business

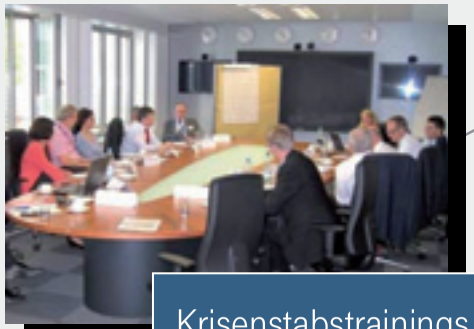


Daily Report

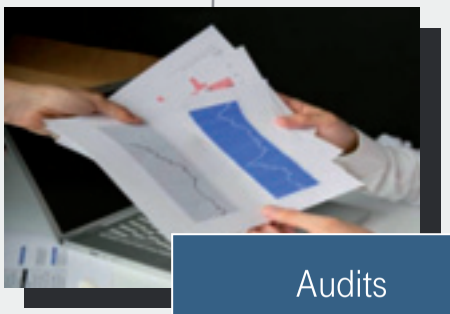
Missbrauchs-
erkennungssystem

BCM

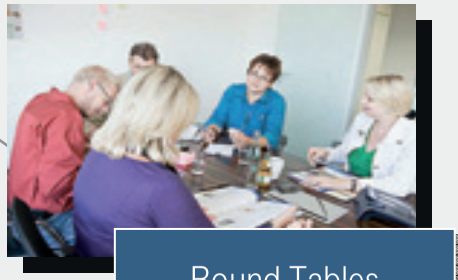




Krisenstabstrainings



Audits



Round-Tables

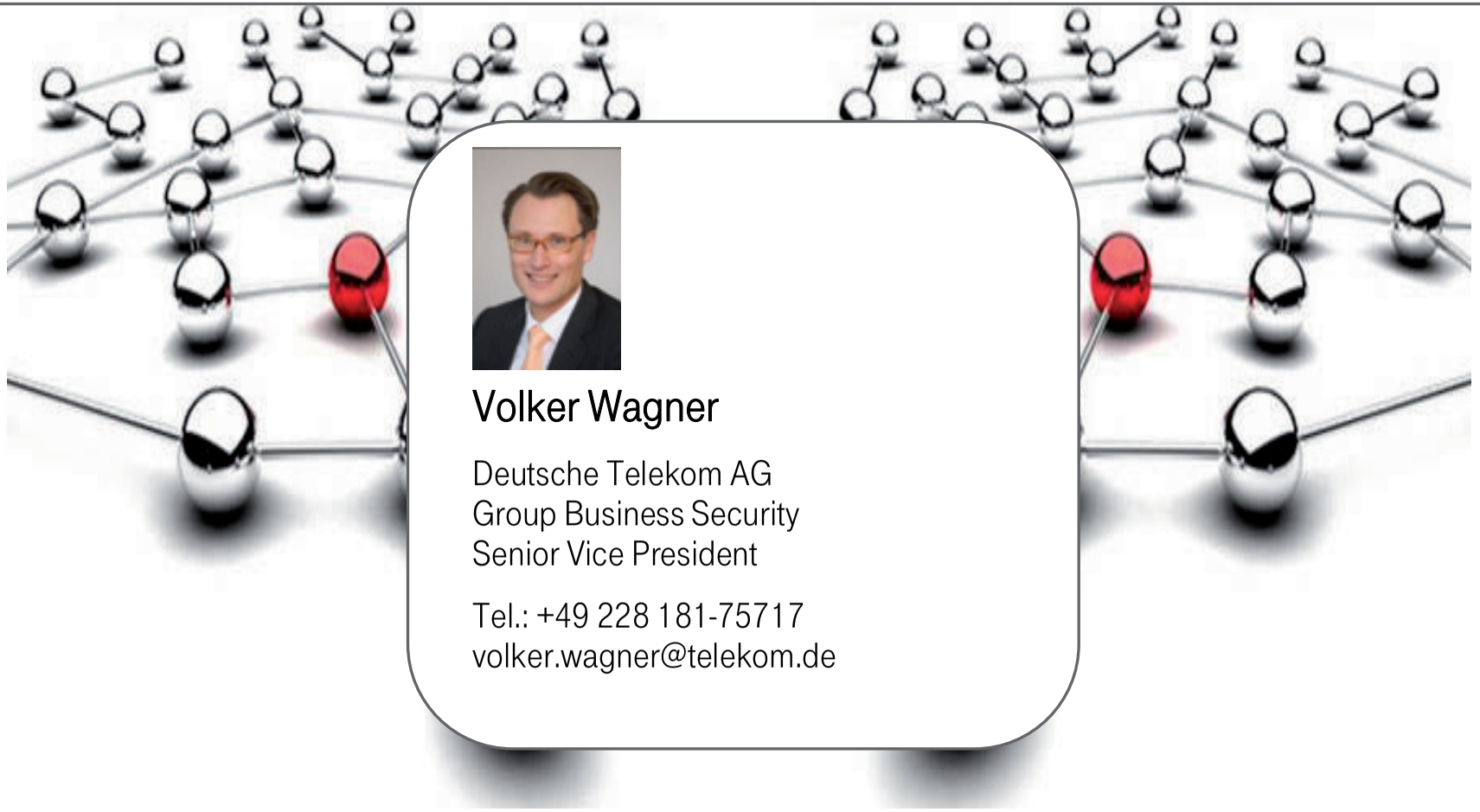
Kooperation schafft Stärke – wir alle tragen Verantwortung

Einbindung der Stakeholder.

- Unternehmensintern
- Staatliche Stellen
- Unternehmensübergreifend
- Geschäftspartner & Kunden

Alle ziehen an einem Strang.

Vielen Dank für Ihre Aufmerksamkeit!



Volker Wagner

Deutsche Telekom AG
Group Business Security
Senior Vice President

Tel.: +49 228 181-75717
volker.wagner@telekom.de

Bildquellen: Telekom-Medienarchiv und andere (siehe Quellenangaben auf Bildern)

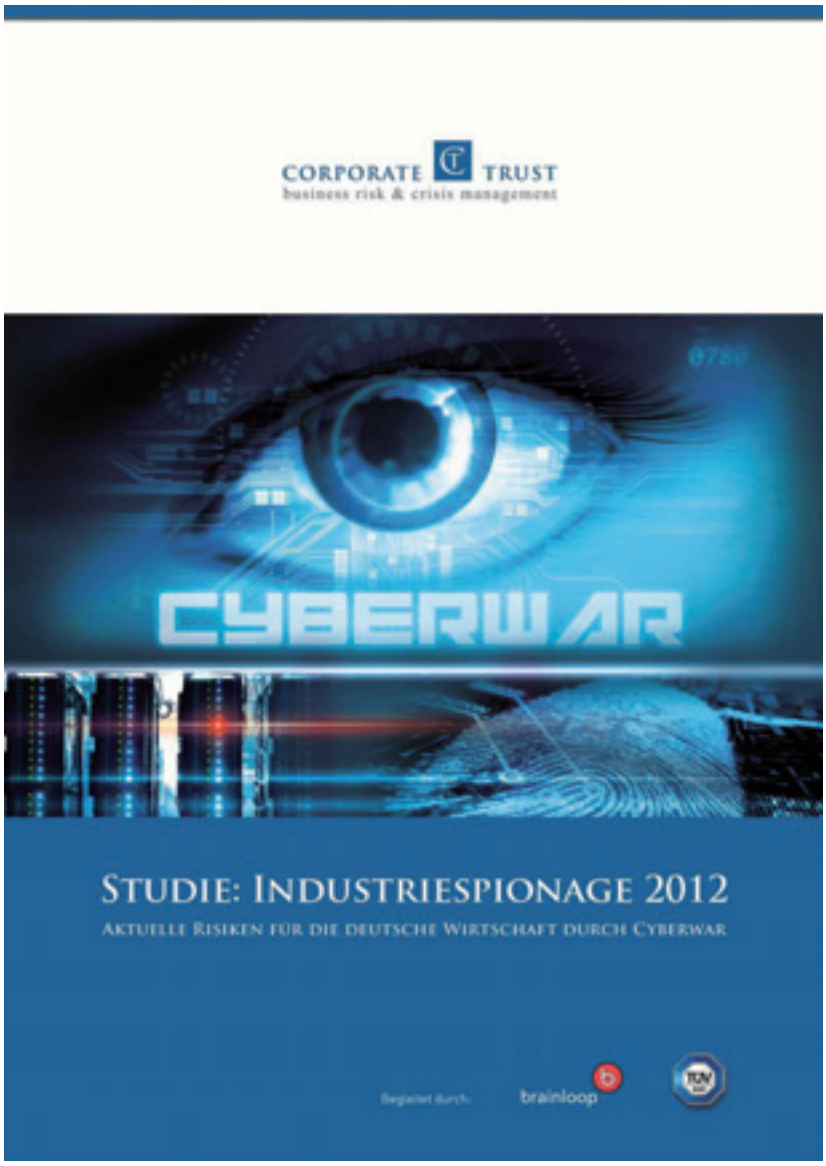
Vortrag Oelmaier

ASW - BfV Tagung

CORPORATE TRUST
business risk & crisis management

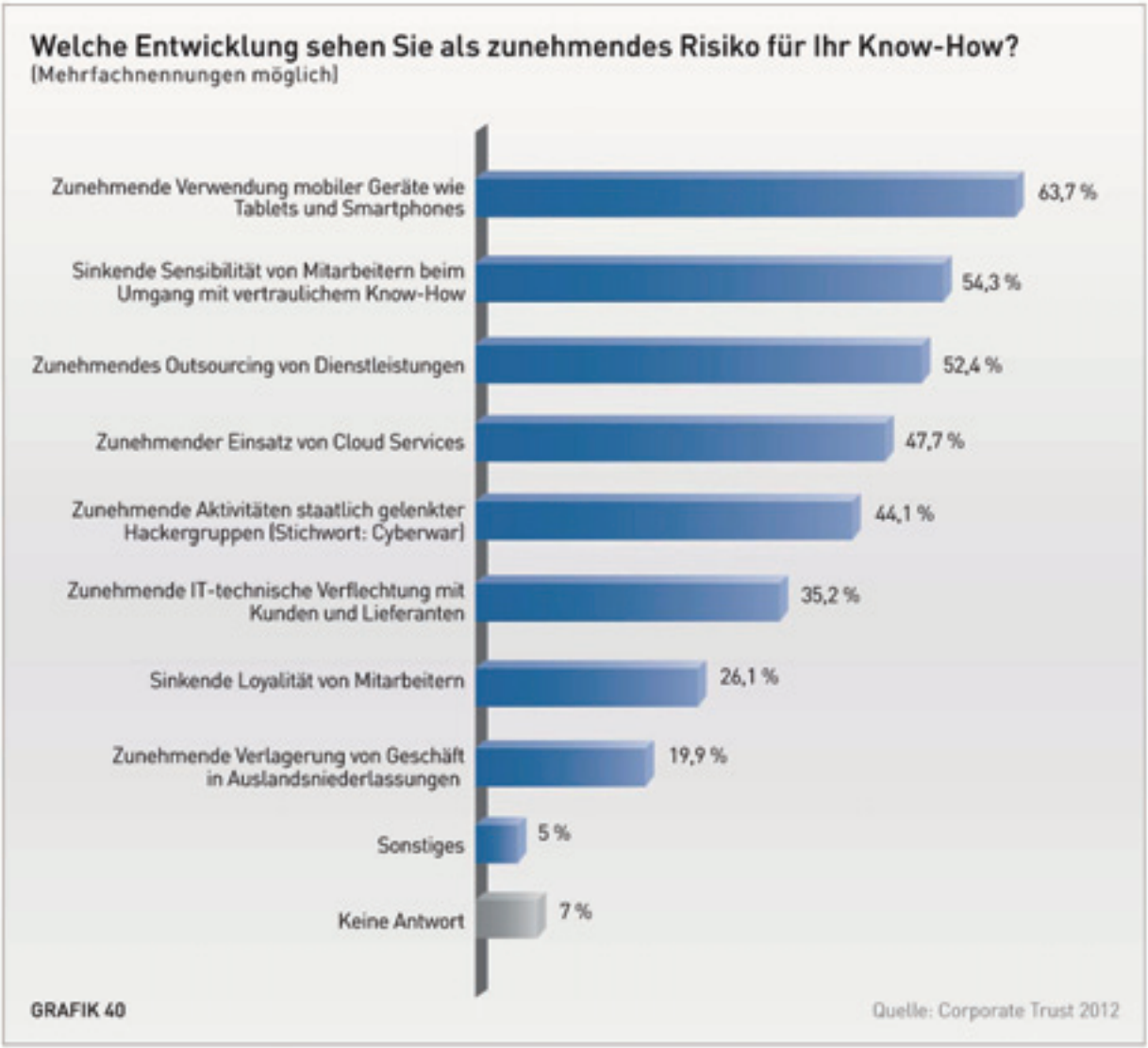
Cyberwar, iPads, Facebook, Cloud Computing: Lässt sich Know How überhaupt noch schützen?

Die Corporate Trust hat Anfang 2012 eine Studie „Industriespionage 2012 – Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar“ in Zusammenarbeit mit der Brainloop AG und der TÜV SÜD AG auf der Grundlage einer Befragung von 6.924 deutschen Unternehmen erstellt. Für die Studie wurde ein repräsentativer Querschnitt aus ca. 65.000 Unternehmen nach dem Zufalls-prinzip ausgewählt und befragt.



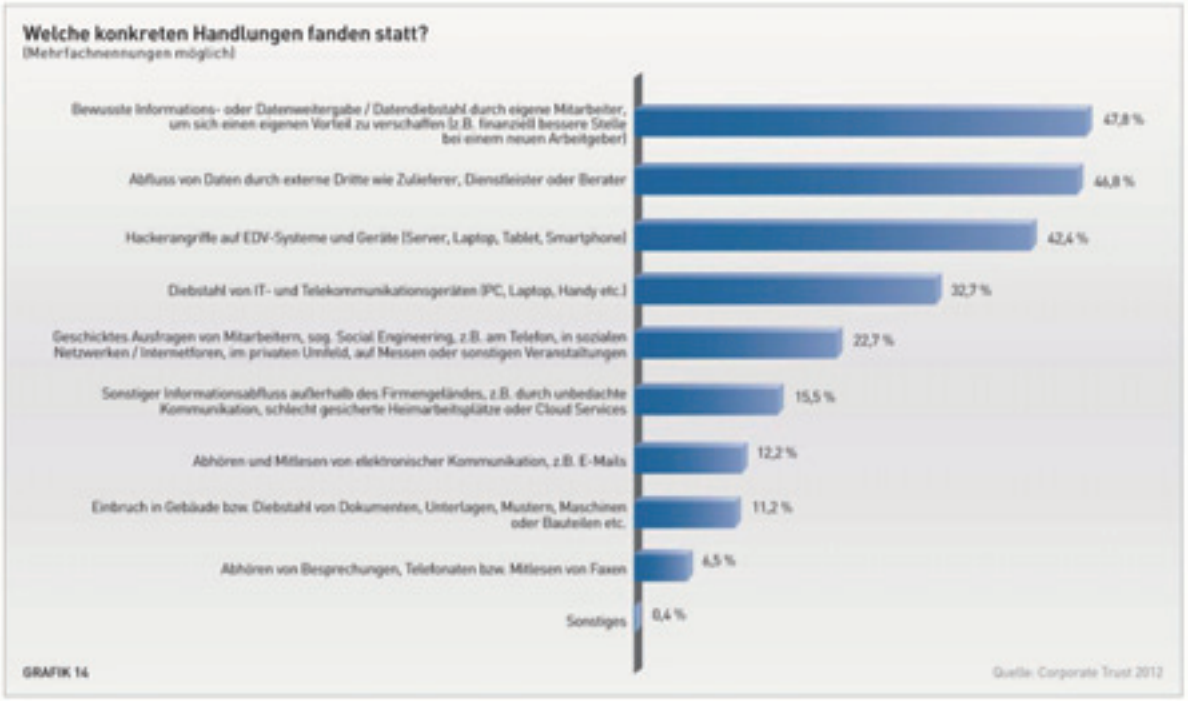
Um ein möglichst umfassendes Bild der aktuellen Bedroung zu erhalten, wurde großer Wert darauf gelegt, die Befragung branchenübergreifend durchzuführen und sämtliche Unternehmensgrößen zu berücksichtigen, vom Kleinunternehmen bis zum Konzern, jeweils gemessen an Umsatzvolumen und Anzahl der Mitarbeiter. Es wurden allerdings nur Unternehmen mit mindestens zehn Mitarbeitern bzw. einem Umsatz über einer Million Euro berücksichtigt. Aus den vorangegangenen Studien der letzten Jahre wurde deutlich, dass sich viele Unternehmen trotz ihres hohen Umsatzes und der Vielzahl ihrer Mitarbeiter noch zum Mittelstand zählen. Daher wurde vor allem berücksichtigt, zu welcher Kategorie sich die Unternehmen selbst zugehörig fühlten. Die Befragung wurde im Januar und Februar 2012 durchgeführt.

1 Interessante Ergebnisse



Als bedrohlich wird mit 63,7 Prozent vor allem die zunehmende Verwendung von mobilen Geräten wie Tablets und Smartphones bewertet. Die sinkende Sensibilität von Mitarbeitern im Umgang mit vertraulichen Informationen ist wohl auch ein Effekt der Verbreitung von sozialen Medien und Web 2.0 Angeboten. Auch die Informationsverarbeitung durch Dienstleister wird kritisch beurteilt. 52,4 Prozent nennen das zunehmende Outsourcing von Dienstleistungen und 47,7 Prozent die Verwendung von Cloud-Services als zunehmendes Risiko. Fast die Hälfte der Unternehmen sehen die zunehmenden Aktivitäten staatlich gelenkter Hackergruppen (also die Bedrohung, die gemeinhin unter dem Begriff „Cyberwar“ zusammengefasst wird) als künftiges Problem für ihr Know-how.

Generell sehen die Unternehmen Ihren eigenen Schutz nicht optimistisch. Viele Nennungen und hohe Prozentzahlen zeigen eine enorme Verunsicherung in der Wirtschaft.



Die Frage nach konkreten Vorfällen zeichnet ein anderes Bild. Hier zeigt sich, dass die bewusste Informationsweitergabe durch Vertrauenspersonen sehr häufig ist.

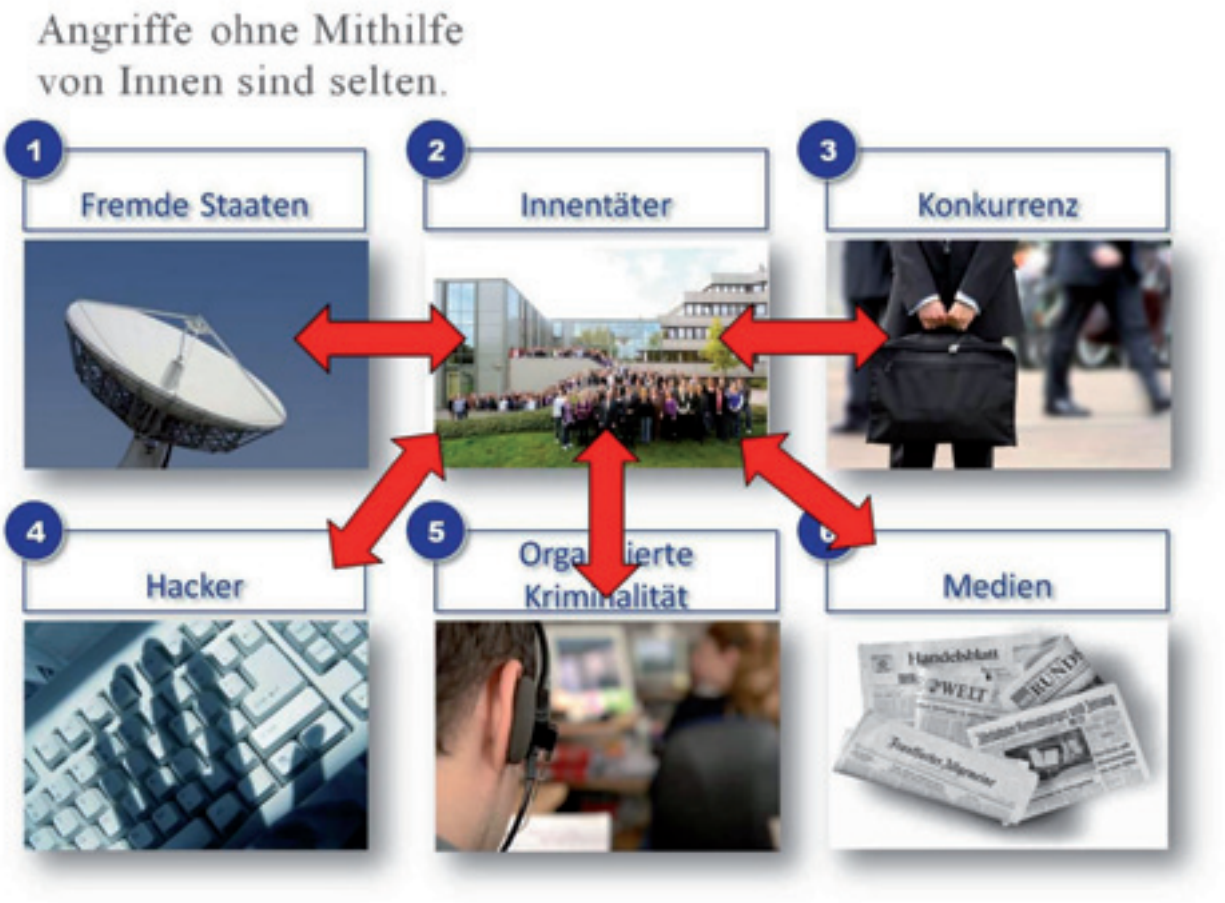
2 Soziale Netzwerke

Facebook steht nur stellvertretend für eine ganze Reihe sozialer Netzwerke, die fast jeder nutzt. Dabei ist grundsätzlich klar:

Vertrauen in der mobilen Welt:
Ihre Mitarbeiter schützen ihre Daten

Autor: Chr-nan, Wikimedia

Die Erfahrung der Corporate Trust zeigt dabei:



Dabei ist in einer modernen Welt nicht nur das erleichterte Social Engineering durch soziale Netzwerke ein Problem. Die zunehmende Portabilität riesiger Informationsmengen erleichtert den Datenabfluss, z.B.:

Angriffe in der mobilen Welt:
Datenabfluss in der Öffentlichkeit

Informationsabfluss auf Messen, in Zügen, Hotels, Lounges, etc.

Angriffe in der mobilen Welt:
Kommunikationsüberwachung im Ausland

Im Mobilfunk gilt: die SIM Karte vertraut dem Provider. Im Roamingfall wird dieses Vertrauen an den ausländischen Mobilfunkbetreiber delegiert. Gerechtfertigt?

Angriffe in der mobilen Welt:
Sichere Aufbewahrung / Diebstahl

Wenn Sie die PIN eines deutschen Hotelsafes vergessen: kein Problem, die Rezeption kann Ihnen den Safe wieder öffnen. Wenn ein deutsches Gericht eine Durchsuchung eines Hotelsafes anordnet, dann wird jedes Hotel in Deutschland diesem Ersuchen nachkommen. Im Ausland ist das ähnlich - vielleicht mit Ausnahme des notwendigen Gerichtsbeschlusses.

Informationsverlust im privaten Bereich

Durch zunehmende Vermischung von Privat- und Arbeitsleben gewinnt aber auch der Informationsabfluss im privaten Bereich an Bedeutung.

Schlimmstes Problem dabei ist aber eine sehr geringe Mitarbeiterloyalität:

Mangelnde Mitarbeiterbindung
ist ein Sicherheitsrisiko.

Quelle: http://eu.gallup.com/berlin/146030/praesentation-zum-gallup-eei-2010.aspx

Diese Mitarbeiter sind die Personen, die unsere Daten schützen.

3 Vertrauen

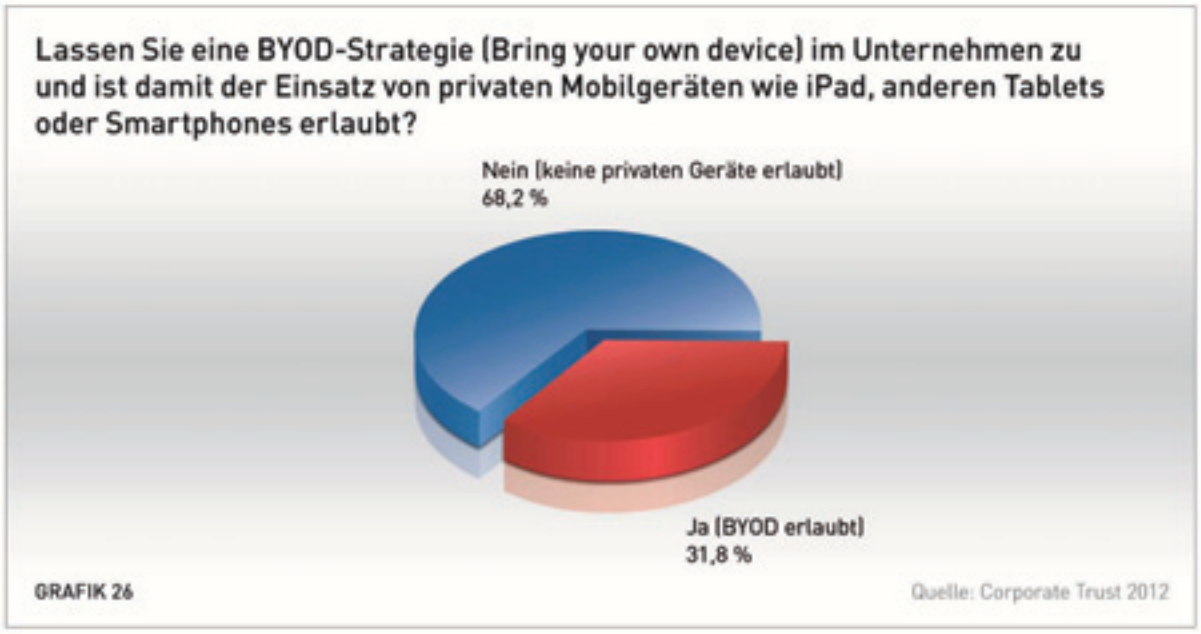
Zusätzlich gibt es in einer arbeitsteiligen Welt aber natürlich Partnerfirmen und Zulieferer denen man Vertrauen muss:

Dies ist im klassischen Bereich der Hausverwaltung schon schlimm genug. Im Bereich der IT potenziert sich das Problem. Eine Verteidigung gegen den Hersteller einer Software oder gegen den Anbieter eines Dienstes ist nur sinnvoll möglich, wenn auf die Software oder den Dienst verzichtet wird. Mangels deutscher IT-Firmen vertraut fast jede deutsche Firma implizit mindestens einem der folgenden Unternehmen:

Hat Windows eine Backdoor? Kann Apple Gespräche abhören? Erlaubt Cisco Fernzugriffe? Und wie viel weiß ich über Ihr Unternehmen, wenn ich alle Google-Suchanfragen aller Ihrer Mitarbeiter in den letzten 2 Monaten analysiere?

Dennoch ist die Situation nicht hoffnungslos. Moderne mobile Geräte bringen ganz neue Sicherheitsfunktionen mit:

- Es kann nur autorisierte Software aus definierten Quellen installiert werden
- Statt on-access Virenschutz wird Software einer viel intensiveren Prüfung bei der Aufnahme in den Distributionsprozess unterworfen
- Geräte können ferngelöscht werden
- Installierte Programme laufen in getrennten Umgebungen. Schnittstellen zwischen installierten Programmen sind nur noch über das Betriebssystem möglich (keine seltsamen Plugin- oder Extensionkonzepte mehr)
- Benutzer können untereinander über die Qualität von Applikationen diskutieren



Andererseits dürfen bereits in 31,8% der Unternehmen eigene Geräte dienstlich benutzt werden. Kein Wunder: Wenn ein Unternehmen 1000 Mitarbeiter mit iPhones ausstattet, bekommen diese Mitarbeiter die exakt gleiche Hard- und Software wie ein Mitarbeiter, der das Gerät privat kauft. Die Mitarbeiter, die die Unternehmensgeräte bekommen haben, dürfen damit ihre Kontakte und Kalender synchronisieren, Firmen-E-Mails lesen und eventuell auf Unternehmensdateien zugreifen. Warum sollte das mit einem baugleichen Privatgerät nicht möglich sein? Es gibt drei einfache Regeln für „Bring Your Own Device“:

- Regel #1: BYOD ist nur zulässig für Geräte, die exakt baugleich zu den Geräten sind, die die Firmen-IT ausgibt.
- Regel #2: Die Geräte im BYOD-Programm werden technisch und organisatorisch exakt gleich behandelt wie Firmengeräte.
- Regel #3: Die Teilnahme am BYOD-Programm ist vollkommen freiwillig und kann jederzeit beendet werden. Beim Eintritt und Austritt in das BYOD-Programm wird das Gerät jeweils komplett gelöscht. Es empfiehlt sich daher für den Eigentümer des Geräts, vor dem Eintritt in das BYOD-Programm ein Geräte-Backup anzulegen.

Wenn ein Unternehmen diese drei Regeln einhält, dann spricht aus rein technischer IT-Sicherheitssicht nichts gegen BYOD. Dennoch gibt es Kontraindikation:

- Es gibt im Umfeld von BYOD rechtliche Unsicherheiten. Diese rechtlichen Unsicherheiten dürfen auf keinen Fall dazu führen, dass Regel #2 aufgeweicht wird und zum Beispiel Fernlöschungen oder Gerätekontrollen im BYOD-Programm nicht mehr zulässig sind. Wenn die Rechtsberatung / Rechtsabteilung

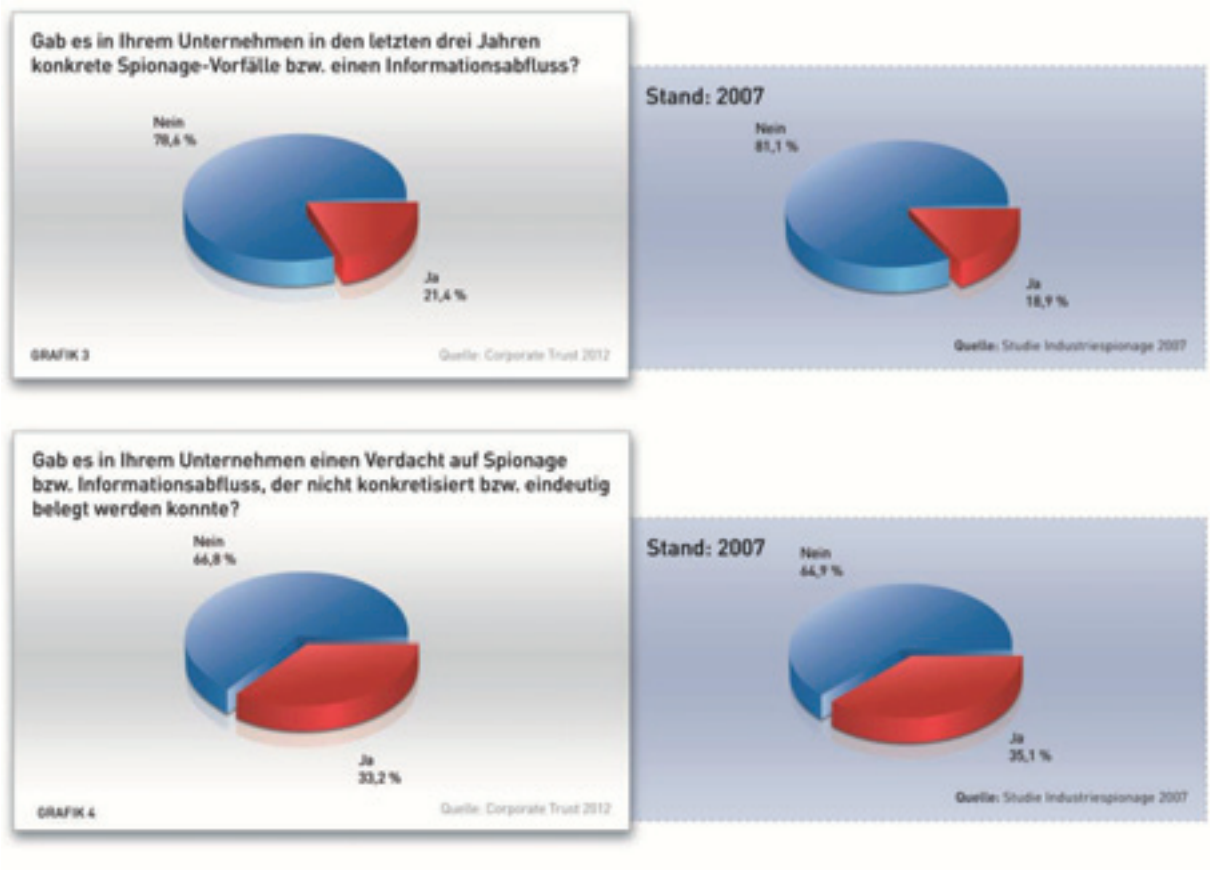
Ihres Unternehmens die Rahmenbedingungen für Regel #2 nicht schaffen kann, dann muss man auf BYOD verzichten.

- Wenn Ihr Unternehmen versucht, die Anzahl der Mobilgeräte mit Unternehmenszugriff gering zu halten, um die möglichen Angriffspunkte zu reduzieren, dann sollten es von BYOD absehen. BYOD hat das Potenzial, die Anzahl der Mobilgeräte im Firmeneinsatz massiv zu erhöhen.

Die Frage, ob Mitarbeiter mit eigenen Geräten im BYOD-Programm sorgsamer umgehen oder ob Mitarbeiter mit vom Unternehmen gestellten Smartphones sicherheitsbewusster agieren, wird oft diskutiert. In der Erfahrung der Corporate Trust ist das eine sehr individuelle Fragestellung, die sich nicht allgemein beantworten lässt. An sinnvollen Schulungs- und Awareness-Maßnahmen rund um den Einsatz von Mobilgeräten führt – unabhängig von BYOD oder nicht – in keinem Fall ein Weg vorbei.

Aber auch für Cloud-Aktivitäten gibt es einfache Regeln:

4 Cyberwar & Industriespionage



Mehr als 50% der Firmen hatten bereits konkrete Spionage-Vorfälle oder zumindest einen Verdacht.Dabei haben wir in Deutschland bisher Glück: die großen und gefährlichen Angriffe wie Stuxnet oder Flame gehen von unseren Alliierten aus und haben uns nicht betroffen, wie z.B. die Verbreitung von Flame zeigt:

Dabei werden Firmen - wie der RSA-Hack zeigt - nicht mehr nur direkt angegriffen. Manchmal wird eine Firma nur angegriffen um damit den Angriff auf dritte Firmen zu erleichtern. Diese Angriffskaskaden sind teilweise generalstabsmäßig geplant und orchestriert.

Dass die zuständigen Behörden dabei in Deutschland mit wesentlich weniger Mitteln ausgestattet sind, als dies in anderen - größeren - Ländern der Fall ist, schafft eine zusätzliche Gefährdung.

Dass die Wirtschaft dabei - aufgrund der befürchteten Rufschädigungen - sehr geheimniskrämerisch mit Vorfällen umgeht hilft der Entwicklung eines guten Lagebilds nicht:

Hilfreich wäre in diesem Kontext ein sinnvolles Versicherungsangebot, wie dies z.B. von der Enisa gefordert wird:

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/

5 Fazit

Lässt sich Know How heute überhaupt noch schützen?

Ja! Aber dazu müssen wir liebgewordene und geübte Praktiken über Bord werfen und uns für die künftigen Realitäten neu erfinden. Schaffen wir das?

6 Autor

Florian Oelmaier

Leiter IT-Sicherheit und Computerkriminalität

Corporate Trust

Business Risk & Crisis Management GmbH
Tel.: +49 89 599887580
oelmaier@corporate-trust.de
www.corporate-trust.de

Florian Oelmaier leitet das Fachgebiet IT-Sicherheit und Computerkriminalität bei der Corporate Trust, Business Risk & Crisis Management GmbH. Seine Spezialgebiete sind aktuelle Angriffe auf Applikationen und Netzwerke sowie Sicherheitskonzeptionen in Softwareprojekten.

Nach seinem Informatikstudium war er an der Entwicklung von Sicherheitstechnologien am Fraunhofer Institut für Integrierte Schaltungen beteiligt und in der Folge als IT-Sicherheitsspezialist bei einer deutschen Großbank tätig. Als Sicherheitsberater konzipierte er Sicherheitsarchitekturen für eine Vielzahl von großen IT-Projekten bei namhaften Unternehmen und leitete die Durchführung von Security Source Code Reviews und Penetrationstests. Neben diesen präventiven Maßnahmen war Herr Oelmaier als IT-Experte bei der Aufklärung von vielen Fällen im Bereich der Computerkriminalität beteiligt.

Florian Oelmaier ist Autor des Buches „Apple´s iPad im Enterprise-Einsatz", erschienen im Springer Verlag. Außer-dem ist er Herausgeber einer Vielzahl von Artikeln zum Risiko durch Hackerangriffe.

Proliferationsabwehr – Eine Aufgabe des Verfassungsschutzes

Referent: Edmund Meyer, Referatsleiter im BfV

Abstract

Eine der größten Gefährdungen der internationalen Sicherheit ist die Proliferation.
Daher ist die Aufklärung und Verhinderung illegaler Beschaffung von Gütern, Technologien und Know-How in Deutschland, die zur Entwicklung und Herstellung von Massenvernichtungswaffen Verwendung finden kann eine wichtige Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder.

Das Bundesamt für Verfassungsschutz sieht sich als Unterstützer der Exportkontrolle und arbeitet daher eng mit dem Bundesamt für Wirtschaft und Ausfuhrkontrolle, dem Bundesnachrichtendienst, dem Zollkriminalamt und dem Bundeskriminalamt zusammen.

Erfahrungen der Sicherheitsbehörden haben gezeigt, dass die Wissenschaft und die Industrie die proliferationsrelevanten Absichten ihrer „Geschäftspartner“ oftmals nicht erkennen können. So laufen sie Gefahr, sich strafbar zu machen, indem sie z.B. gegen das Außenwirtschaftsgesetz oder gegen § 99 Strafgesetzbuch (geheimdienstliche Agententätigkeit) verstoßen. Zusätzlich ist die Aufnahme der eigenen Firma in eine Sanktionsliste denkbar, möglicherweise verbunden mit großem wirtschaftlichem Schaden. Meistens ist mit der illegalen Handlung auch ein großer Reputationsverlust verbunden.

Somit birgt der proliferationsrelevante Export von Gütern und Know-how neben der Wirtschaftsspionage und der Konkurrenzausspähung für deutsche Firmen ein erhebliches Gefährdungspotential.

Die Verfassungsschutzbehörden haben ein Sensibilisierungsprogramm entwickelt, mit dem sie Unternehmen und Forschungseinrichtungen nach dem Opportunitätsprinzip individuelle und vertrauensvolle Zusammenarbeit anbieten.

Anm.:
Das Opportunitätsprinzip gestattet dem Verfassungsschutz einen Ermessensgrundsatz, der wenn es zweckmäßig erscheint, eine Strafverfolgung nicht zwingend erforderlich macht.

Das Kooperationsgespräch mit dem Bundesamt für Verfassungsschutz ersetzt jedoch nicht die nach dem deutschen Ausfuhrrecht bestehenden rechtlichen Verpflichtungen, sich umfassend über die aktuelle Rechtslage zu informieren.

Trotz hervorragender interner Exportkontrollsysteme sind Güter deutscher Firmen in der Vergangenheit in falsche Hände gelangt, ein Vorgang, der durch ein rechtzeitiges Gespräch mit dem Bundesamt für Verfassungsschutz hätte vermieden werden können.

Wegen der ausgefeilten und immer häufiger verschleierten Beschaffungsmethodik der proliferationsrelevanten Länder Iran, Syrien, Nordkorea und Pakistan appelliert der

Verfassungsschutz bei Zweifelsfällen für eine rechtzeitige Kontaktaufnahme unter:
non-proliferation@bfv.bund.de
zur Terminierung eines persönlichen Gespräches. Die bisherigen Erfahrungen mit deutschen Firmenvertretern sind durchweg positiv. Die zum Teil sehr wertigen Rückmeldungen führen zu wachsendem Erkenntnisaufkommen des Bundesamtes für Verfassungsschutz über Beschaffungsorganisationen und deren angewandter Methodik in Deutschland.

Deutschlands Sicherheit – Cybercrime und Cyberwar

Referent: Arne Schönbohm, Vorstand BSS BuCET Shared Services AG

Abstract

Herausforderung „Cybersecurity“

Trends: Einfluss „Social Media“

- Sozialleben konzentriert sich zunehmender auf das Internet
- Unternehmen stoßen in die VR vor
- Datenschutz und Privatsphäre wird immer schwieriger zu garantieren
- Wirtschaftsspionage nimmt zu
- Sicherheit wird teurer

Wissensverdopplung:

- 1750 – 1900: 150 Jahre
- Heute: 5 Jahre
- 2020: 72 Tage

Verwundbarkeit der Unternehmen nimmt mit dem Grad der Nutzung der IT zu.
Immer komplexere Szenarien:
Nutzen von Sozialen Netzwerken (Schwarmverhalten).

- Bundesminister zu Guttenberg innerhalb von 12 Tagen
  von allen Ämtern zurückgetreten.
  - Einführung eines GuttenPlagWIKI
  - Umfangreiche Investition an Zeit in diese Plattform durch Freiwillige
  - Nutzen „virtueller social media“ Accounts zur Meinungsverstärkung

- Im September 2008 bewarb sich die hundertprozentige Post-Tochter „DHL“ als Logistikdienstleister der Bundeswehr
  - Aktivisten nutzen das Internet, um aktiv eine Kampagne zu starten
  - Kosten der Kampagne relativ gering
  - dhl.blogsport.de

„Social Media“ (Negativ-) Nutzung in Deutschland:
Im Mordfall „Lena“ wird in Emden ein doch unschuldiger 17-jähriger Jugendlicher bedroht. Der nun zu Jugendarrest verurteilte 18-Jährige hetzte auf seiner Facebook-Seite: „Aufstand! Alle zu den Bullen. Da stürmen wir. Lasst uns das Schwein tothauen!“
Danach versammelten sich Dutzende Menschen vor der Emdener Polizeiwache und forderten die Herausgabe des 17-Jährigen.
Auch in Deutschland kommt es zu „Protestbewegungen“ durch Social Media.

Cybercrime – warum ist es so erfolgreich?

Anonymität der Angreifer.
Operation aus Ländern mit fehlender oder mangelhafter Gesetzgebung.
Stetig wachsende Möglichkeiten für Cybercriminals:

- 2 Mrd. Internetbenutzer
- 6 Bill. Internetseiten weltweit
- 2,2 Mrd. Google-Abfragen im Monat
- 12% des globalen Handels werden online durchgeführt
- 388 Mrd US$ Schaden durch Cybercrime inkl. des entstandenen Zeitverlustes

Im Vergleich zu Großunternehmen sind KMU nur unzureichend gegen Cyber-Attacken gewappnet!

Virusattacken, Trojaner und Malware werden von KMU als wichtigste Gefahrenquellen eingeschätzt!
Cybercrime stellt eine zunehmende Gefährdung für Unternehmen mit vielen Facetten (Wettbewerb, Markenruf etc.) dar.

Cybercrime Gefahr für KMU

Aufgrund ihrer Ausrichtung und Innovationskraft sind KMU den Gefahren des Cybers in besonderem Maße ausgesetzt.
Kriminalitätslage in Deutschland:

Straftaten insgesamt:	2009:	6.054.330
	2010:	5.933.078
	2011.	5.990.679

Rückgang um 2,1 % in drei Jahren

Malware - die größte Herausforderung im Cyber

Ziel: Passwörter und Kundendaten stehlen / PIN und TAN auszuspionieren / Kundendaten an Dritte weiterzuverkaufen / unter gestohlenen Identitäten Geschäfte abzuwickeln / Unternehmen zu diskreditieren.

Cybergremien in der EU und Deutschland.

Fazit:

- Cyberkriminalität gewinnt auch in Zukunft an Bedeutung.
- Starker Innovationsdruck und Veränderungen.
- Der Staat alleine kann unterstützen, Unternehmen sind für den Eigenschutz zuständig!
- Vorsorge ist billiger als Nachsorge

Wie können Sie sich schützen?

- Ist-Analyse
- Security Policy
- Awareness
- Compliance
- Risk-Analysis

Wirtschaftsschutz
ist
Teamwork

BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Referat Wirtschaftsschutz
Merianstr. 100
50765 Köln
Telefon: 0221/792-0
Fax: 0221/792-2915
E-Mail: wirtschaftsschutz@bfv.bund.de