IT- und Cyber-Risiken

Chancen und Risiken

Maßstäbe / neu definiert

Vielfältige und neuartige Bedrohungen für Unternehmen

Einleitung
Die Herausforderung

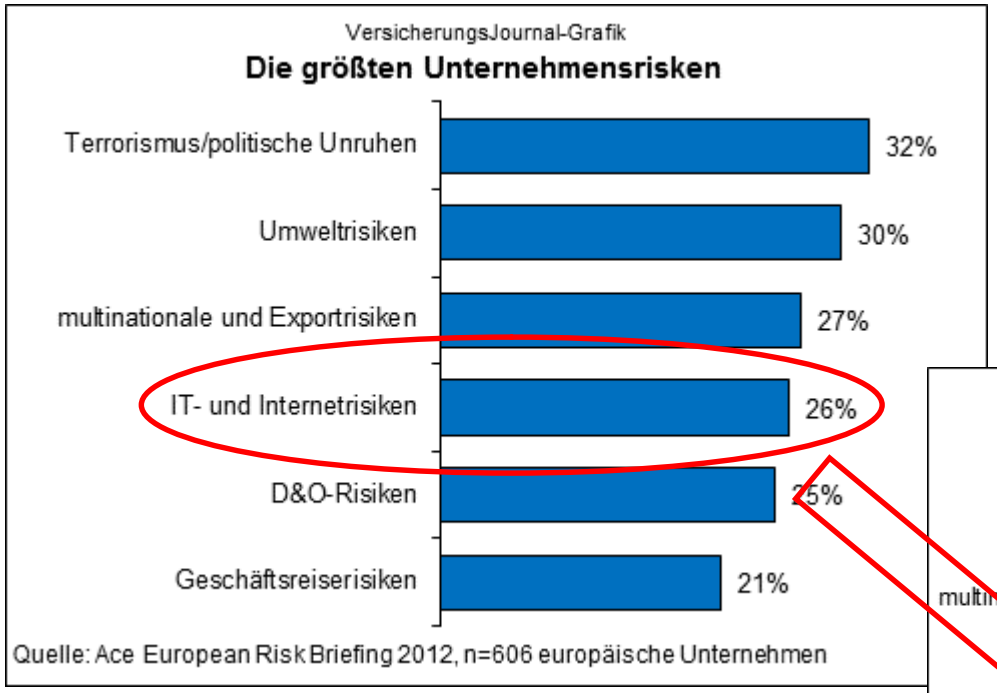
Typische Zeitungsüberschriften

- **Daten sind einer der wichtigsten Rohstoffe des 21. Jahrhunderts**
  (VDI-n, 20.05.2011)
- **Angst vor dem großen Hack – Etablierte IT-Sicherheitssysteme versagen zunehmend**
  (FAZ, 17.05.2011)
- **Angst vor Datendiebstahl wächst**
  (FAZ, 17.05.2011)

➡ **IT-Risiken sind**

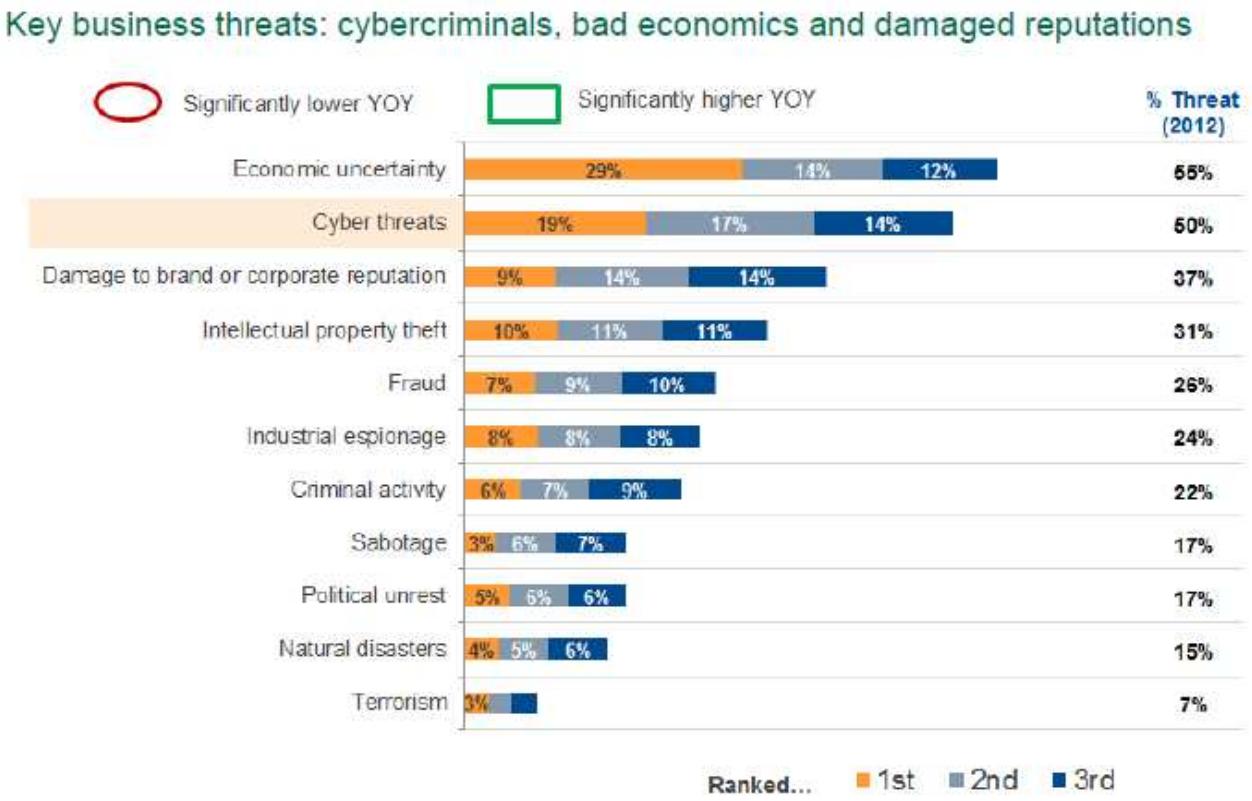
- **neuartig** (mangelnde Schadenerfahrung, fehlendes fachliches Verständnis)
- **teilweise komplex bzw. subtil** hinsichtlich ihrer Ursache/Herkunft
- in ihrer Auswirkung oft nur **schwer einschätzbar**

Sicherheitslage aus Sicht der Unternehmen
Befragung der ACE-Versicherung



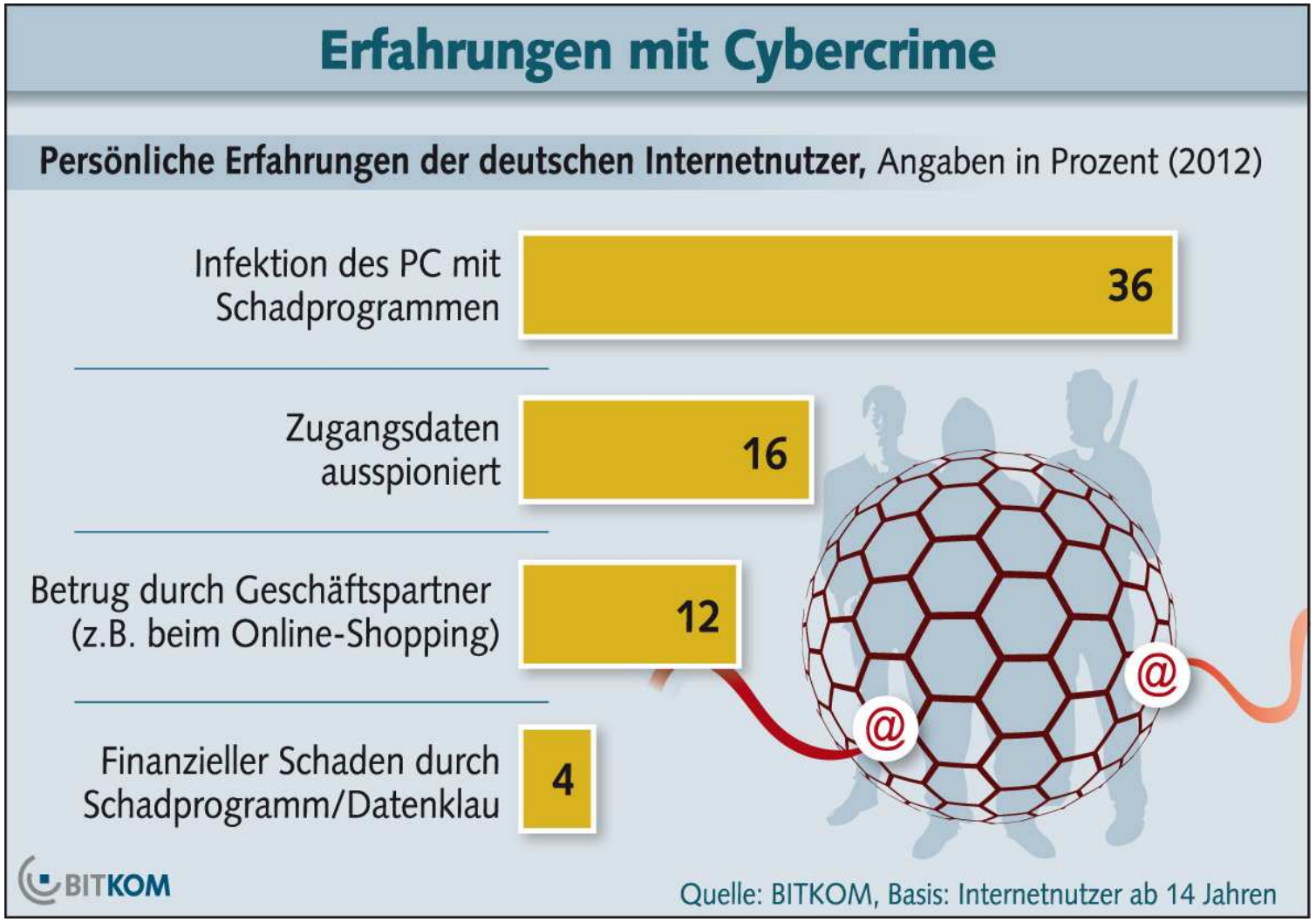
Sicherheitslage aus Sicht von Unternehmen

Umfrage Kaspersky Lab 2012



- **60 % der KMU weltweit beklagen Malware-Infektionen**
- **Großkonzerne eher Industriespionage, Phishing und DDos-Attacken**
- **KMU sind bezüglich IT-Sicherheit tendenziell schlechter aufgestellt**

Persönliche Erfahrungen mit Cybercrime



Datensicherheit ist größtes Risiko für KMU

McAfee-Umfrage 2012

Über 1.000 Entscheidungsträger von KMU in Deutschland, Frankreich und Großbritannien wurden befragt zum Status quo der Datensicherheit

Die KMU-Geschäftsführer in allen drei Ländern waren in zwei zentralen Punkten einig:

1) **Dem Verlust vertraulicher Informationen gilt die größte Sorge, wobei zwei Drittel der Unternehmen besonders das Hacken vertraulicher Daten fürchten.**
2) **Die beiden herausragenden Probleme für KMU sind die mögliche Kompromittierung von Informationen und die drohende Verweigerung von Krediten.**

Größte IT-Risiken 2013

- **71 % der Unternehmen nennen Hackerangriffe als größte IT-Bedrohung 2013**
- **61 % nennen „Social Networking“**
- **Den dritten Platz teilen sich Software-as-a-Service (SaaS) und Cloud Computing (58 Prozent)**
- **Weitere Themen:**
  - Datensicherung und Datenarchivierung (41 %)
  - Abschottung vor den Gefahren mobiler Geräte (16 %)
  - Aufstellung und Einhaltung von Compliance-Regeln (16 %)
  - Schutz vor den eigenen Mitarbeitern etwa gegen Datenklau (9 %)

Quelle: Studie „IT-Sicherheit und Datenschutz“
Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS)

Symantec Sicherheitsbericht 2013

- **Anstieg der Cyber-Angriffe um 81 Prozent auf insgesamt 5,5 Milliarden weltweit**
- **Deutschland belegt den europäischen Spitzenplatz bei Malware-Aktivitäten noch vor Russland und Großbritannien**
- **Zudem findet sich Deutschland als Quelle webbasierter Angriffe sowie Netzwerkattacken jeweils auf dem zweiten Platz wieder - gleiches gilt für die Anzahl bot-infizierter Rechner in Europa**
- **Trend zu gezielten Angriffen: Ende 2011 82 Attacken pro Tag. Die Täter setzen Social-Engineering-Techniken ein und passen ihre Schadprogramme so an ihr Ziel an.**
- **Mehr als die Hälfte dieser Angriffe trafen weltweit Unternehmen mit weniger als 2500 Mitarbeitern, 18 % der betroffenen Organisationen beschäftigten sogar weniger als 250 Angestellte. Gründe:**
  - Häufig sind kleinere Firmen als Zulieferer oder Partner an große Firmen gebunden und bieten so einen idealen Ausgangsort, um von dort aus das eigentliche Ziel - den Großkonzern - zu attackieren.
  - Außerdem verfügen mittelständische Firmen über wertvolles Know-how und wiegen sich tendenziell eher in Sicherheit.
  - Sie sind im Vergleich zu großen Organisationen oftmals schlechter geschützt.
- **Pro Datendiebstahl wurden 2011 durchschnittlich 1,1 Millionen personenbezogener Daten entwendet. Hackerangriffe sind für den Großteil der Diebstähle verantwortlich**
- **Am häufigsten fielen die Daten aber durch Diebstahl oder Verlust mobiler Geräte wie Smartphones oder USB-Sticks in falsche Hände**

Quelle: 17. Auflage des Sicherheitsberichts Internet Security Threat Report von Symantec

Top 10 der größten Internet-Gefahren 2013

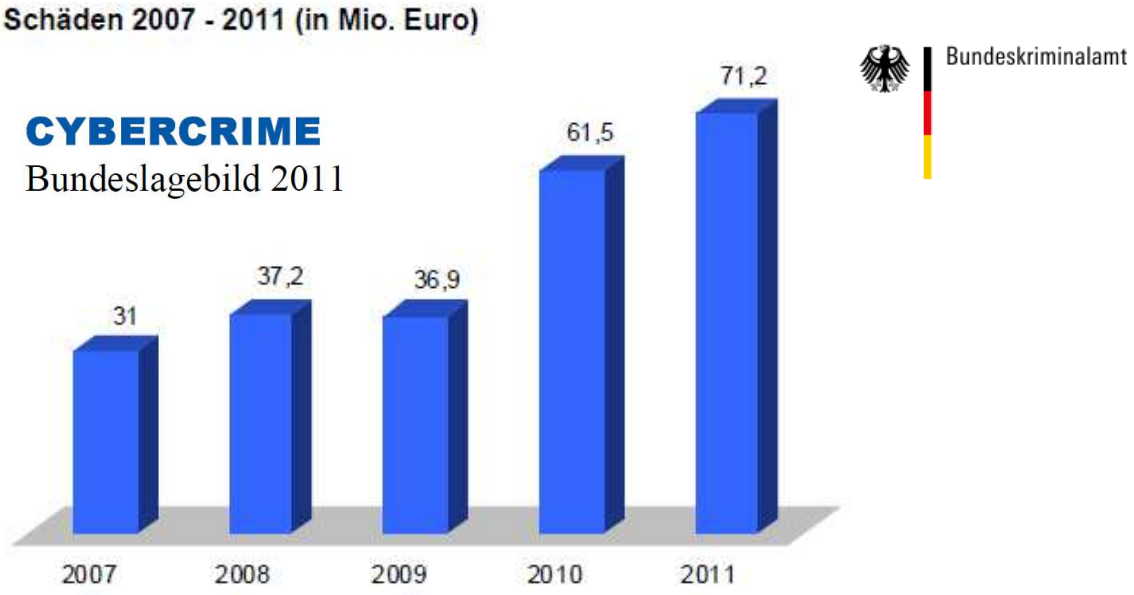
	Bedrohung	Gefährdung
1	Drive-by-Downloads von Schadsoftware	steigend
2	Trojaner/Würmer	steigend
3	Attacken auf Datenbanken und Websites	steigend
4	Viren-Baukästen	steigend
5	Botnetze	steigend
6	Denial-of-Service-Attacken	stabil
7	Phishing	stabil
8	Datenverluste	steigend
9	Rogueware/Scareware	stabil
10	Spam	sinkend

steigend
stabil
sinkend

BITKOM

Quelle: ENISA, BITKOM

Zunahme der Cybercrime-Schäden aus Sicht des BKA



Im Jahr 2012: 64.000 Fälle von Internet-Kriminalität

Besonders stark angestiegen sind Fälle im Bereich Datenveränderung/ Computersabotage.

Im Jahr 2011: 60.000 Fälle mit

71,2 Mio € Schadensumme (+ 16%)

Höchster Anteil: Computerbetrug/Kreditkartenmissbrauch

In der Kriminalstatistik erfasst werden nur die Taten, bei denen der Verdächtige an einem Computer in Deutschland saß.

Sicherheitslage aus Sicht von IT-Unternehmen und dem BSI

Gefährdungstrends

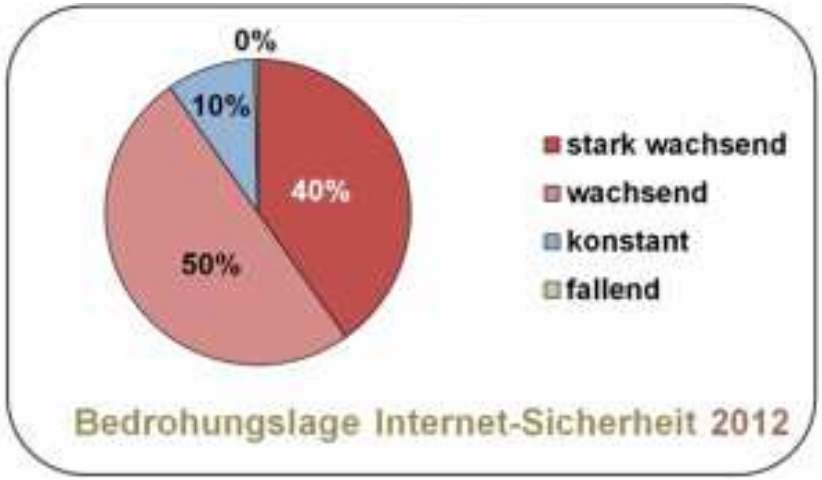
Bedrohung	2009	2011	Prognose
DDoS-Angriffe	↑	→	→
Unerwünschte E-Mails (Spam)	↑	→	→
Botnetze	↑	↑	↑
Identitätsdiebstahl	↑	↑	↑
Sicherheitslücken	–	↑	↑
Drive-By-Exploits	–	↑	→
Schadprogramme	–	↑	↑

Quelle: BSI

Entwicklung von IT-Bedrohungen nach Einschätzung des BSI [7]

↑ steigend ↓ sinkend → gleichbleibend

Bundesamt für Sicherheit in der Informationstechnik



Umfrage eco-Verband 2011 (www.eco.de)

eco
Verband der deutschen Internetwirtschaft e.V.

Auswirkung eines IT-Schadens

<kes>/Microsoft-Sicherheitsstudie 2010

	Ausfallzeit		Kosten	
	Durchschnitt	Max.	Durchschnitt	Max.
Virus	17 h	400 h	18.990 €	1 Mio. €
Fehlalarm	9 h	150 h	1.318 €	20.000 €
Gezielter Angriff	130 h	4.000 h	12.716 €	350.000 €

Durch Internetkriminalität weltweit verursachter Schaden wird auf 81 Mrd. € geschätzt, davon in Deutschland 23,5 Mrd. €
(Norton Cybercrime Report 2011)

Europas Datennetze sind ein Sicherheitsrisiko

Enisa-Bericht zu Internetstörungen 2011:

- **11 Länder der EU haben 51 Bericht zu Störungen gemeldet**
- **Mindestens 15 % der Nutzer müssen über mehr als 8 h betroffen sein**
  - 70 % Software- oder Hardwarefehler bzw. Ausfall des Providers
  - 12 % Naturkatastrophen (durchschnittlich 45 h Ausfall!)
  - 12 % menschliches Versagen
  - Am häufigsten Stromausfälle, da Notstromversorgung meist nur 4 h überbrücken können (Dominoeffekt!)
  - Konfigurationsfehler eines Administrators führte zum Ausfall sämtlicher Mobilfunkkommunikation in Westeuropa. Es dauert 4 h bis Konfiguration neu aufgesetzt war!
  - Weil ein früherer Mitarbeiter eines Providers einen Vermittlungsrechner in Brand gesetzt hatte (Sabotage), hatten 10.000 Kunden 36 h kein Internet.

Markt für Cyber-Versicherungen

- In den USA bieten mehr als 30 Versicherer Cyber-Deckungen an, 2012 soll der Markt ca. 1 Mrd. US$ betragen haben, was einem Wachstum von 25 % entspräche.
- In UK sind ca. 15 Versicherer aktiv
- In Deutschland nur wenige Versicherer (Chubb, Hiscox, XL, CNA und Chartis), damit überwiegend ausländische, die ihre Produkte bereits in den USA oder UK anbieten
- Wichtigster Wettbewerber: Hiscox mit Bausteinprodukt DataRisk und breiter Kundenansprache (KMUs) – BU-Deckung nur für e-Commerce
- Neuer Wettbewerber: dataVERS mit Torus Insurance!?
- Aktivität von Makler, insbesondere Marsh und AON, aber auch Willis, Schunck u. a. – eher auf Großkundenbedarf ausgerichtet (Global Clients)
- Wachstumsimpuls wird durch die Verschärfung des Datenschutzgesetzes erwartet: Einführung einer EU Datenschutz-Grundverordnung vermutlich Ende 2014.
- Corporate executives are more concerned about cyberattacks and data breaches than property damage and investment risk, according to a survey commissioned by insurer AIG. The poll found 85% of the survey participants - a group that included risk managers, senior executives and insurance brokers in the U.S. and Canada - were very or somewhat concerned with cyber risks.

Ganzheitliches Risikomanagement

Was kann man versichern?

Potentielles Risiko	Versicherungsmöglichkeit
Ausfall der IT durch einen Sachschaden (z. B. Brand, Fehlbedienung, Vandalismus)	Sachversicherung, z. B. Elektronik-versicherung inkl. Betriebsunter-brechungsversicherung
Zielgerichtete DoS- bzw. Hacker-Attacke Geheimnisverrat	VertrauensschadenV: Kosten für Wiederherstellung und Mehrkosten sowie unmittelbarer Schaden (Beispiel: Telefonhacking)
Löschung oder Veränderung von Daten	Elektronik- (bzw. Software-)V Bei Vorsatz: VertrauensschadenV
Verstoß gegen Datenschutzgesetz	RechtsschutzV HaftpflichtV (auf Ausschlüsse achten!)

Ganzheitliches Risikomanagement
Wo sind die Grenzen der Versicherbarkeit?

- Kosten durch **nicht zielgerichtete** Schadsoftware
- **Mittelbare Kosten** durch Hackerangriffe wie z. B. Kreditkartenmissbrauch
- **Betriebsunterbrechung** durch Hackerangriffe, DoS-Attacken, Schadsoftware ohne einen vorausgehenden Sachschaden
- Ausfall des **Internetzugangs** (aber mögliche Haftung Dritter beachten!)
- **Zugangserpressung**

Einzelheiten zur Technischen Versicherung

Technische Versicherung

- Entschädigung für den Sachschaden an der Informationstechnik (Hardware) des Unternehmens
- Entschädigung für den Betriebsunterbrechungsschaden durch Sachschäden an der Informationstechnik (Hardware) des Unternehmens
- Übernahme der Kosten für Wiederherstellung und Wiederbeschaffung bei Verlust, Veränderung oder Nichtverfügbarkeit von Daten oder Programmen (Software) durch Schäden an der Informationstechnik des Unternehmens

Einzelheiten zur Softwareversicherung

Softwareversicherung

- Versichert sind Kosten für die Wiederherstellung von Daten sowie betriebsfertigen und funktionsfähigen Standardprogrammen und individuell hergestellten Programmen

- Entschädigung für den Verlust, die Veränderung oder die Nichtverfügbarkeit von Daten oder Programme durch:
  - Ausfall oder Störung der Hardware der Datenverarbeitungsanlage, der Hardware der Datenfernübertragungseinrichtungen und -leitungen, der Stromversorgung/Stromversorgungsanlage oder der Klimaanlage
  - Bedienungsfehler
  - vorsätzliche Programm- oder Datenveränderung durch Dritte in schädigender Absicht
  - Über- oder Unterspannung
  - elektrostatische Aufladung oder elektromagnetische Störung
  - höhere Gewalt

Einzelheiten zur Vertrauensschadenversicherung

Vertrauensschadenversicherung

- Entschädigung für Schäden von außenstehenden Dritten durch unmittelbare und rechtswidrige Eingriffe in die EDV **mit** Bereicherungsabsicht!
- Entschädigung für zielgerichtete Angriffe auf die EDV **ohne** Bereicherungsabsicht

  Ersetzt werden folgende Kosten:
  - Wiederherstellungs- und Wiederbeschaffungskosten der beschädigten Software, Daten und Dateien
  - Mehrkosten

Die Vertrauensschadenversicherung (VSV)

Über 80 % aller Unternehmen sehen die Gefahren durch Wirtschaftskriminalität,
ABER: **nur ca. ein Drittel aller Unternehmen besitzen Versicherungsschutz**

- Die VSV ist keine Haftpflichtversicherung, sondern eine Vorsatzversicherung
- Zweck: Schutz des Unternehmens vor innerbetrieblichen Verlusten durch kriminelle Mitarbeiter und Vertrauenspersonen (sowie zum Teil auch durch Dritte wie z. B. Hacker)
- Die Deckung umfasst:
  Verrat von Betriebsgeheimnissen durch Vertrauenspersonen
  - Entschädigungsvoraussetzung: notarielles Schuldanerkenntnis

  Zielgerichtete Hackerschäden (Software) von Außenstehenden, Dritten auch ohne Bereicherungsabsicht
  - Entschädigungsvoraussetzungen: Firewall, individuelle Passwörter, Sicherung von Daten, etc.

  Erstattung interner und externer Schadenermittlungs- und Rechtsverfolgungskosten
  Erstattung von Täuschungsschäden durch außenstehende Dritte
  - Entschädigungsvoraussetzung: Erstattung Strafanzeige

Nach einer Studie der KPMG sind Betrugstäter überwiegend männlich (87 %), Mitte 30 bis Mitte 40 und bekleiden eine Führungsposition (82 %), vor allem im Finanzsegment oder im Vertrieb.

Der durchschnittliche Schaden pro Fall liegt bei 1 Mio €

Einzelheiten zu Profi-Schutz

Profi-Schutz

Haftpflichtversicherung:

- Entschädigung von Vermögensschäden aus der Verletzung von Datenschutzgesetzen und der Nutzung des Internets (Ausschluss: Urheberrechtsverletzungen!)

Sachversicherung:

- Versichert sind Kosten der Wiederherstellung von Geschäftsunterlagen, individuellen Programmen und individuellen Daten sowie Kosten des Aufgebotsverfahren und der Wiederherstellung von Wertpapieren und sonstigen Urkunden

Rechtsschutzversicherung (Strafrecht!):

- Versichert sind Kosten von Ermittlungsverfahren wegen des Vorwurfs eines strafrechtlich relevanten Verstoßes gegen das UWG und sogenannte Hackerparagrafen

Der Risiko-Check IT

Der Risiko-Check IT der AXA

- Leitfaden für die Identifizierung von IT-Risiken im eigenen Unternehmen
- Konkretisierung durch Abschätzung der möglichen Schadenhöhe
- Hilfestellung zur Auswahl des optimalen Versicherungsschutzes
- Gesprächsleitfaden für die Beratung mit einem Versicherungsvermittler

Der Risiko-Check IT

Gliederung des Risiko-Check IT:

1. Ausfall der IT bzw. des Netzzugangs
2. Datenverlust
3. Verstoß gegen Datenschutz- oder andere Schutzgesetze
4. Missbrauch und Manipulation
5. Schäden Dritter durch vom Unternehmen verbreiteter Schadsoftware
6. Zugangserpressung

Beispielhafter Auszug aus dem Risiko-Check IT:

Potentielles Risiko		Mögliche Schadenhöhe	Versicherungsmöglichkeit
A	Löschung eigener Daten aufgrund eines Sachschadens am Datenträger		Sachinhalts- bzw. Elektronikversicherung (mit Daten- oder Softwareversicherung): Kosten für Datenwiederherstellung

Übersicht Absicherungsmöglichkeiten gegen IT-Risiken

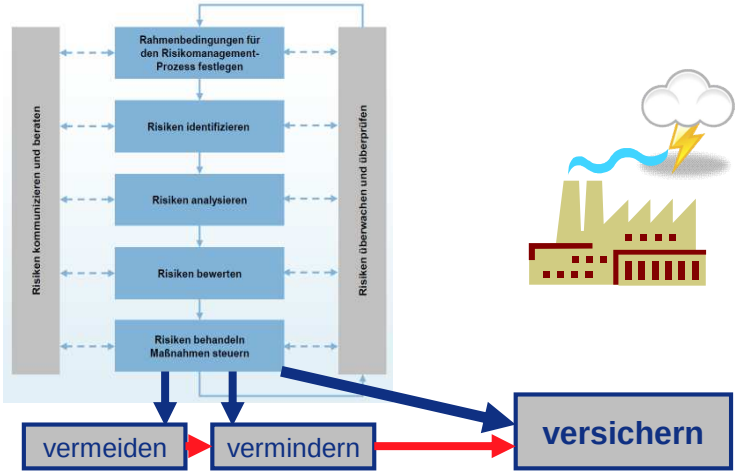
Versicherungsmöglichkeit	Potentielle Risiken
Rechtsschutzversicherung inkl. Strafrechtsschutz	Unzulässiges Löschen oder Kopieren fremder Daten (Strafrechtsschutz!)
Elektronikversicherung mit Softwareversicherung	Versicherung von Kosten für die Wiederherstellung von Daten unabhängig von einem vorangegangenen Sachschaden
Vertrauensschadenversicherung	Unterschlagung durch eigene Mitarbeiter Vermögensschaden durch Hackerangriff
Sachversicherung, z. B. Elektronikversicherung	Löschung eigener Daten aufgrund eines Sachschadens am Datenträger
Haftpflichtversicherung (Zusatzbedingungen für Nutzer von Internettechnologien)	Schäden wie Datenverlust, Ausfall der IT, Sachschäden etc. bei Dritten durch Schadsoftware

Haupt-Risikofelder

- **Betriebsunterbrechung ohne vorausgehenden Sachschaden (z. B. durch Cyber-Attacke)**
  - Gefährdete Branchen: Versorger, Chemieanlagen, Serienproduktion (z. B. Kfz-Zulieferer), Groß- und Einzelhandel (e-Commerce)
- **Internetbetrug (z. B. Online-Banking)**
  - Gefährdete Branchen: Finanzdienstleister, Groß- und Einzelhandel, KMUs allgemein (niedrigerer Schutzgrad)
- **Datenschutzverletzung (Personally Identifiable Information PII Breach)**
  - Gefährdete Branchen: Finanzdienstleister/Makler, Internetprovider/Soziale Netzwerke, Hotels, Handel (e-Commerce), Bildungseinrichtungen, Rechtsanwälte/Notare, Gesundheitsdienste/Ärzte/Kliniken, Medien und Verlage

Versichern ist nicht genug!
Lifecycle of Information Security

- **Ganzheitlicher IT-Risikomanagement-Ansatz:**
  - **Risiken erkennen**
  - **Risiken bewerten**
  - **Risiken mindern (technisch / organisatorisch)**
  - **Risiken übertragen: versichern**
  - **Risiken selber tragen**
  - **Überprüfen und verbessern**



Versichern ist nicht genug!
Lifecycle of Information Security

- **Ganzheitlicher IT-Risikomanagement-Ansatz durch Kooperation der AXA Versicherung AG mit IT-Beratungsunternehmen:**

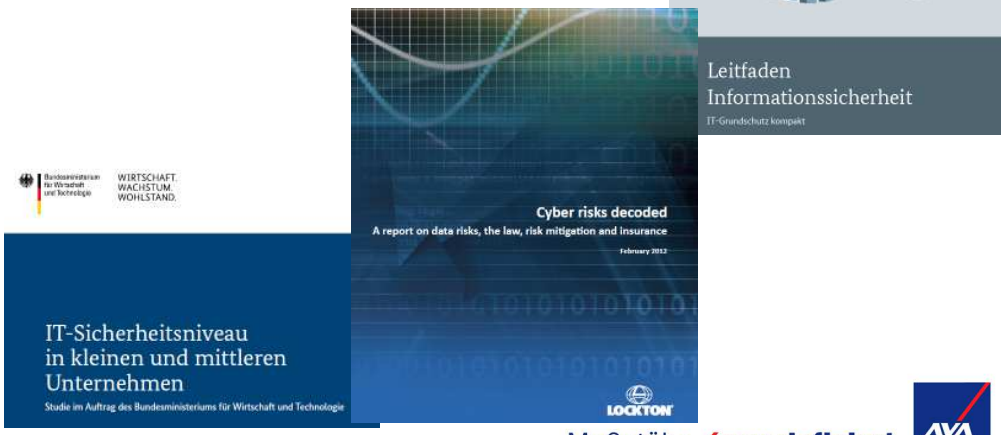
  - **SIZ GmbH**
    (Informationsmanagementsysteme, Zertifizierung, Business Continuity etc.)

  - **8com GmbH & Co. KG**
    (insb. Penetrationstests, Awareness, Schulung)

www.lifecycle-of-is.de

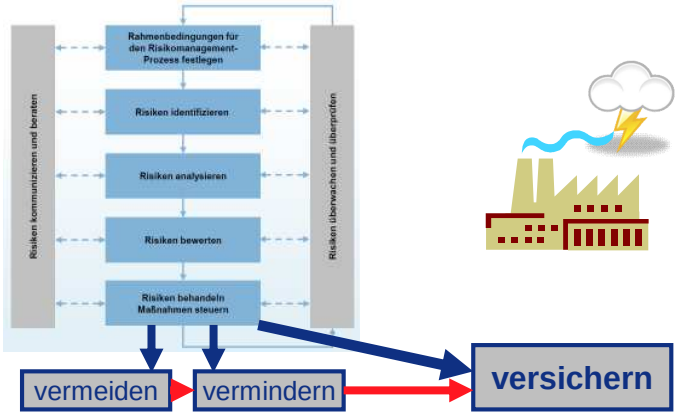
Weiterführende Informationen

- **IT-Sicherheitsniveau in KMU (Bundesministerium für Wirtschaft, 09/2012)**
- **Leitfaden Informationssicherheit (BSI, 2012)**
- **Cyber Risks Decoded (Lockton, 02/2012)**
- **Informationssicherheitsmanagement – Leitfaden für Manager (TeleTrusT, 2012)**
- **Internet-Seiten:**
  - Bundesamt für Sicherheit: www.bsi.de
  - www.kompass-sicherheitsstandards.de
  - www.heise.de
  - Bundesdatenschutzbeauftragter: www.bfdi.bund.de
  - Internet-Verband: www.eco.de



Versichern ist nicht genug!
Lifecycle of Information Security

- **Risikobewältigung durch Outsourcing**
  - **Tätigkeiten auf IT-Dienstleister übertragen**
  - **Vertragliche Regelungen**
  - **Nachweis eines umfassenden Versicherungsschutzes (IT Police Haftpflicht)**



IT Dienstleister

- **IT typische Tätigkeiten**
  - Software-Programmierung
  - Support (Systemhäuser)
  - Access-Provider
  - Cloud-Anbieter (z. B. Software as a Service)
  - Hosting (z. B. Internetseiten)
  - Web-Design
  - Beratung / Zertifizierung
  - Externer Datenschutzbeauftragter
  - Etc.

IT-Police Haftpflicht Highlights

- **Offene Vermögensschadenversicherung**
- **Versichert ist ... die gesetzliche Haftpflicht ... wegen Personen-, Sach- und Vermögensschäden**
- **Alle IT-Tätigkeiten versichert**
- **Schäden durch**
  - **Austausch, Übermittlung, Bereitstellung elektron. Daten**
  - **Beschädigung, Verlust fremder Daten (als Sachschaden!)**
  - **Installation, Wartung**
  - **Mehrkosten nach fehlgeschlagener Installation**
  - **Rechtsverletzungen (auch Urheber- und Persönlichkeitsrechte)**
  - **Verzug durch definierte Gefahren (z. B. Brand, aber auch Ausfall von Schlüsselpersonen)**
  - **Viren und unbefugter Zugriff**
  - **Erfüllungsfolgeschäden**
  - **Strafrechtsschutz**
- Günstige **Kompaktpolice** (580 EUR) für Betriebe bis 500 T€ Umsatz
- **Komfortpolice** für höheren Risikobedarf

IT-Police Haftpflicht

- **Deckung Kompakt-Police**
  - DS
    - 2 Mio. EUR P/S
    - 250.000 EUR V

> günstiges Produkt für Start Ups und Unternehmen bis 500.000 EUR Umsatz
> Wording kann nicht verändert werden

- **Deckung Komfort-Police**
  - DS
    - 2 Mio. EUR P/S
    - variable Deckungssummen für Vermögensschäden
    - Hardwaredeckung (erweiterte Produkthaftpflicht)

> höhere Deckungssummen möglich
> Wording kann individuell angepasst werden
> US-Deckung möglich

Vielen Dank
für Ihre Aufmerksamkeit

Visitenkarte

AXA Versicherung AG
Dirk Kalinowski
Produktmanager IT und Cyber

Colonia-Allee 10 – 20, 51067 Köln
Tel.: +49 (0)221 / 148- 21330
Email: dirk.kalinowski@axa.de