Cyber – Risiken

Absicherungsmöglichkeiten deutscher Unternehmen

Einblick & Überblick

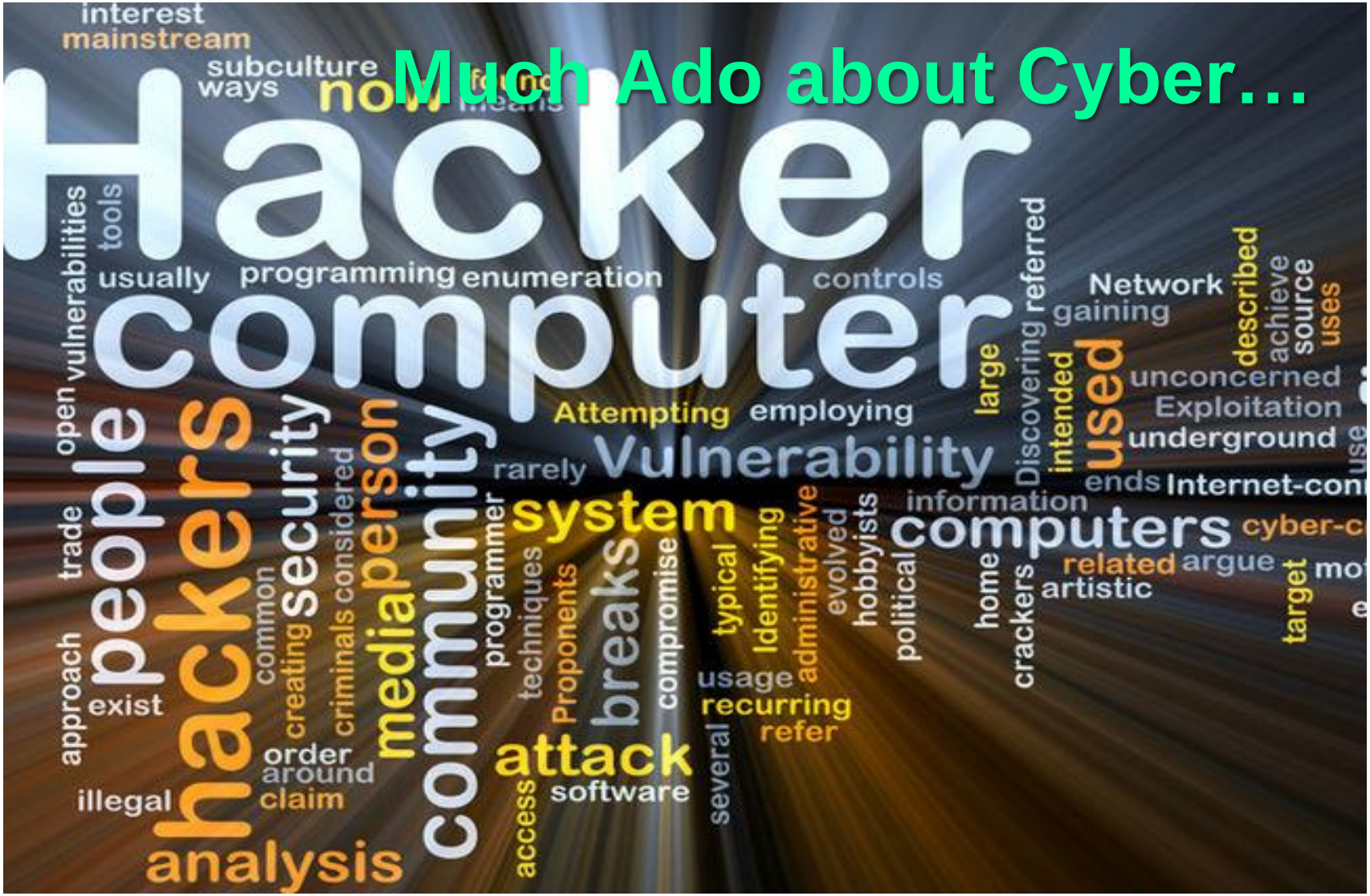
Arbeitsgruppe VDVM Stand 01.05.2014

Agenda

Cyberrisiko – Bedrohung oder Hysterie ?

1. Beispiele: Risiken, Schäden, Kosten
2. Grundstruktur der Cyberpolicen
3. Marktpotential für Versicherungsmakler
4. Felder für eine Zusammenarbeit

Erichsen


Much Ado about Cyber…
Hacker
computer
people
hackers
community
security
media
person
system
computers
Vulnerability
attack
analysis
breaks
interest
mainstream
subculture
ways
usually
programming
enumeration
controls
Network
gaining
Attempting
employing
rarely
information
related
argue
artistic
home
crackers
political
hobbyists
evolved
administrative
Identifying
typical
usage
recurring
refer
compromise
Proponents
techniques
programmer
software
access
several
order
around
claim
illegal
approach
exist
common
creating
criminals considered
trade
open
vulnerabilities
tools
large
intended
used
Discovering referred
described
achieve
source
uses
unconcerned
Exploitation
underground
ends
Internet-con
cyber-c
target

Was umfasst „Cyber“ eigentlich genau?

Der Cyber-Raum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen.

In Deutschland nutzen sämtliche Bereiche des gesellschaftlichen und wirtschaftlichen Lebens die vom Cyber-Raum zur Verfügung gestellten Möglichkeiten.

Staat, Kritische Infrastrukturen, Wirtschaft und Bevölkerung sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.

Quelle: Webseite BKA

Schadenbeispiele

Februar 14: Barclays Bank meldet den Verlust von 27.000 Datensätzen von Kunden

http://www.theguardian.com/business/2014/feb/09/thousands-of-barclays-customer-files-stolen-and-sold-to-scammers-report

März 14: BSI veröffentlicht 18 Mio. Euro gestohlene Datensätze

http://www.stern.de/digital/online/riesiger-datenklau-16-millionen-e-mail-zugangsdaten-gestohlen-2084591.html

Dezember 13: Datenklau bei Target | Cyber-Versicherer zahlt 71 Mio. Kundendaten / 44 Mio. USD

http://derstandard.at/1392686466949/US-Haendler-Target-befuerchtet-nach-Datenklau-auf-Jahre-Belastungen

August 2012: Datenpanne bei der Allianz

http://www.taz.de/Detektiv-gibt-Kundeninformationen-weiter/!100047/

Kosten

Im Schadenfall entstehen Kosten für :

- Rekonstruktion und Wiederherstellung der Daten
- Schadensersatzansprüche Dritter wegen Vertraulichkeits- und Datenschutzverletzungen
- Betriebsunterbrechung
- Aufklärung des Vorfalles, IT-Forensik
- Sicherheitsberater oder PR-Berater
- Umsatzverluste/Reputationsschaden
- Erpressungsgeld, Belohnungen
- Vertragsstrafen/Bußgelder

…

Kosten – Beispiel „Diebstahl eines Laptops“

Bei einem Einbruch in die Büroräumlichkeiten einer Produktions-Einrichtung wurde unter anderem ein Desktop PC gestohlen.
Auf diesem Rechner befanden sich Daten von ca. 50 Kunden inclusive den Konstruktionsplänen.
Folgende Kosten sind entstanden:

Rechtsberatung und Info.pflichten gegenüber Dateninhabern	**67.368 €**
Forensische Dienstleistungen	**23.747 €**
Kreditüberwachungsdienstleistungen	**11.640 €**
PR	**2.137 €**
Gesamtkosten	**104.882 €**

Kosten – Beispiel „Datenklau im E-Commerce“

Ein Online-Vertrieb mittlerer Größe ist Opfer von Datendiebstahl geworden. Über mehrere Monate konnten sich Hacker rechtswidrigen Zugang zu dem eigentlich streng gesicherten online-basierten Abrechnungssystem für Bezahlkarten verschaffen (Payment Processing Tool). Während dieser Zeit konnten die Hacker über rund 2 Millionen Kundendaten kopieren und unrechtmäßig nutzen. Das Schadensausmaß ist sowohl finanziell als auch reputationsmäßig immens. Die bisher entstandenen Kosten sind wie folgt:

Kosten für diverse forensische Arbeiten	**€ 150.000,00**
Kosten für Rechtsberatung und Rechtsbeistand	**€ 525.000,00**
Kosten für gesetzliche Informationspflichten	**€ 2.170.000,00**
Kosten für Media und PR Arbeiten	**€ 253.000,00**
Geltend gemachter Vermögensschaden der Payment Card Industry	**€ 2.000.000,00**
Gesamtkosten	**€ 5.098.000,00**

Kosten – Betriebsunterbrechung

Durch einen unzufriedenen Mitarbeiter erhalten Hacker Zugriff zum Produktionssteuerungsprozess. Eine Engpassmaschine wird gezielt „verseucht“. Der Hersteller kann den Virus erst nach 4 Tagen und unter Hinzuziehung von IT-Security-Experten entschärfen.

Folgende Kosten sind entstanden:

Forensische Kosten	**35.000 €**
Daten-Wiederherstellung	**2.500 €**
Betriebs-Unterbrechung	**150.000 €**
Gesamtkosten	**187.500 €**

Versicherbare Cyber- Schadenpositionen

- Schadenersatzansprüche Dritter
  - Abwehr unberechtigter Ansprüche
  - Ausgleich berechtigter Ansprüche
- Ertragsausfall infolge Unterbrechung des Betriebes
- Kosten für forensische Untersuchungen
- Kosten für externe Unterstützung bei Aufklärung
- Kosten für Einschaltung PR-Berater
- Wiederherstellungskosten bei Verlust/Zerstörung eigener Daten und Netzwerke
- Erpressungsforderungen durch Hacker
- Benachrichtigungskosten bei Verstößen gegen Datenschutz-Vorschriften
- Schadenersatzansprüche bei Veröffentlichen vertraulicher Informationen
- Kosten für externe Unterstützung bei Aufklärung
- Kosten für Einschaltung PR-Berater
- Wiederherstellungskosten bei Verlust/Zerstörung eigener Daten

Cyber- Inhalte konventioneller Versicherungssparten

Erichsen

Cyber-Risiken werden teilweise heute schon über Einzelversicherungen, wie Haftpflicht-, Sach- oder Vertrauensschadenversicherung abgedeckt.

Dieser Versicherungsschutz ist jedoch unzureichend, da

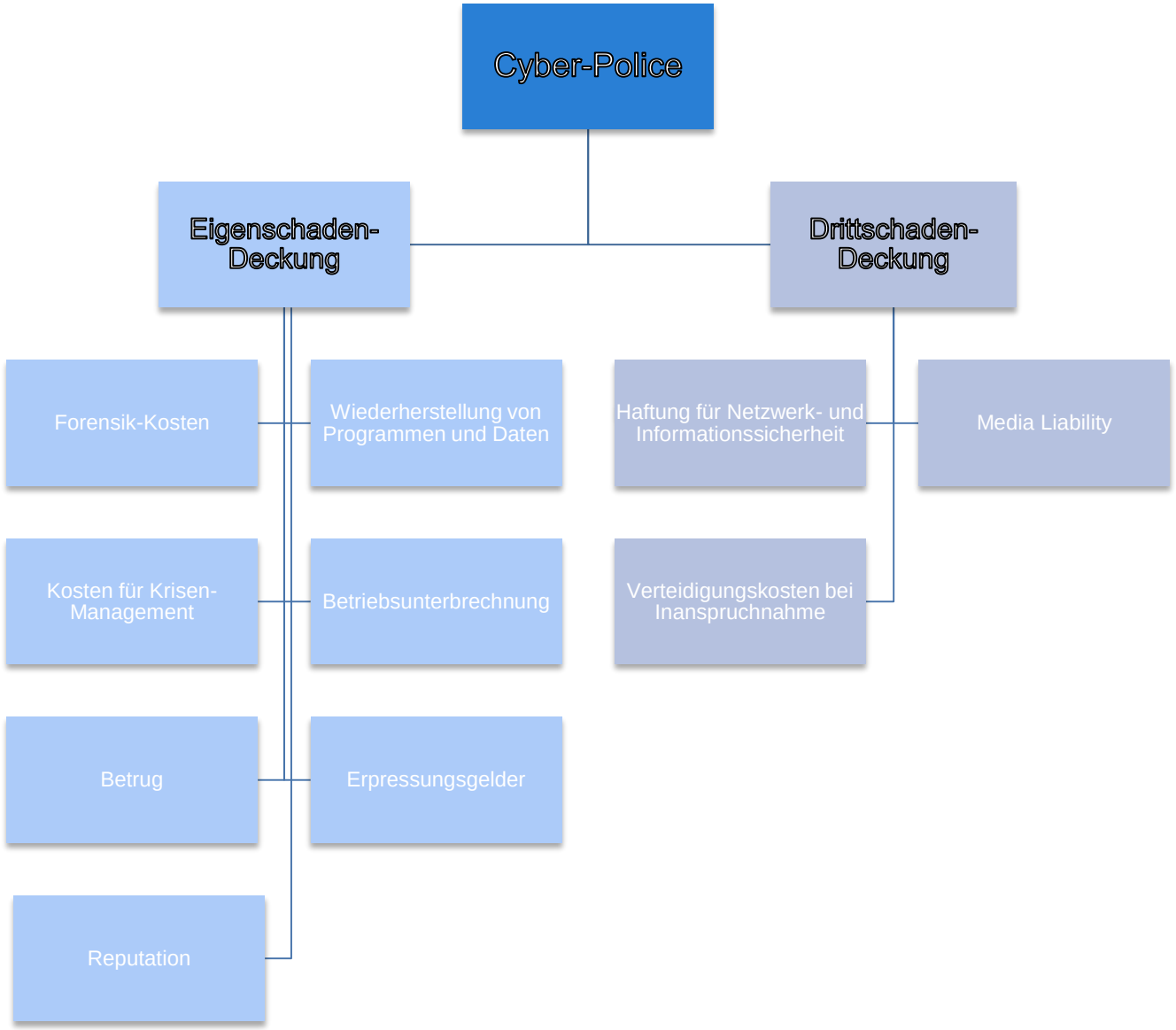
- Ausschlüsse bestehen
- jeweils andere Versicherungsfall-Definitionen zu berücksichtigen
- immer mehrere Versicherer zu involvieren sind.

So ist einer Haftpflichtversicherung zum Beispiel der Schadensersatzanspruch eines Dritten erforderlich. Ob dieser Anspruch allerdings bei einem Hacker-Angriff gegeben ist, dürfte fraglich sein.

Eigenschäden	Sach / TV	Haftpflicht	K&R	VSV	Cyber
Wiederherstellungskosten Daten / Programme	✓	⊘	⊘	⊘	✓
Benachrichtigungskosten	⊘	⊘	⊘	⊘	✓
Betriebsunterbrechungsschäden	?	⊘	⊘	⊘	✓
Kosten für IT-Forensik	⊘	⊘	⊘	✓	✓
Wiederherstellungskosten nach Hackerangriff	?	⊘	⊘	✓	✓
Kosten Sicherheitsberater	⊘	⊘	⊘	?	✓
Kosten PR-Berater	⊘	⊘	⊘	?	✓
Erpressung / Bedrohung	⊘	⊘	✓	⊘	✓
Belohnung für Hinweise, die zur Ergreifung des Erpressers führen	⊘	⊘	✓	⊘	?
Diebstahl Geld oder Vermögenswerte in elektronischer Form	⊘	⊘	⊘	?	?

Drittschäden	Sach / TV	Haftpflicht	K&R	VSV	Cyber
Ansprüche Datenverlust	⊘	✓	⊘	⊘	✓
Ansprüche Datenschutz	⊘	✓	⊘	⊘	✓
Forderungen der PaymentCard-Industrie	⊘	⊘	⊘	⊘	✓
Ansprüche Persönlichkeitsrechtsverletzungen	⊘	?	⊘	⊘	✓
Ansprüche aus Verletzung Rechte des geistigen Eigentums	⊘	?	⊘	⊘	?

Bausteine einer Cyber-Versicherungslösung



Nachfrage nach Versicherungsschutz (1)

Allianz Risk Barometer: Geschäftsrisiken 2014*: Veröffentlichung zu einer Umfrage bei großen Industrieunternehmen u. mittelständischen Firmen

„Laut Allianz Experten ist die Risikowahrnehmung was **Cyberkriminalität** und **Reputationsverlust** angeht am stärksten gestiegen. Weltweit sind Risikomanager aufgrund der sich schnell entwickelnden High-Tech-Risiken in höchster Alarmbereitschaft. Dieses Jahr wurden Cyberrisiken am stärksten in die Höhe katapultiert, vom 15. auf den achten Platz.“

* Veröffentlichung Januar 2014: Für die „Risk Barometer“-Studie wurden mehr als 400 Allianz Experten für Firmen- und Industrieversicherung in mehr als 30 Ländern nach ihrer Einschätzung befragt, welche Risiken für ihre Kunden am wichtigsten sind.

Nachfrage nach Versicherungsschutz (2)

„Die Cyber-Bedrohung steigt exponentiell. Die wachsende Beteiligung der organisierten Kriminalität, unzureichende interne Prozesse, das sich schnell verändernde aufsichtsrechtliche Umfeld, das immer mehr zu Strafen neigt, sowie eine Erfolgsrate beim Hacken, von der Spammer nur träumen können, haben dazu geführt, dass Cyberrisiken 2014 mehr denn je als große Bedrohung wahrgenommen werden. Schätzungen zufolge tragen US-amerikanische Unternehmen mit durchschnittlich rund 5,4 Millionen US Dollar pro Verstoß die weltweit höchsten Kosten für Datenschutzverletzungen.**

Risikowahrnehmung bei den Unternehmen steigt.

** Cost of Cyber Crime 2013 study, Ponemon Research Institute

Marktpotential - Anbieter

- Ace
- AGCS/Allianz
- AIG
- Axa und Axa Corso
- Chubb
- CNA
- HDI Gerling
- Hiscox
- XL
- Zürich

Kapazitäten zw. 5 und 50 Mio. Euro

In Vorbereitung:

- Ergo
- R+V
- Württembergische

- Reine Eigenschaden-Deckung:
  Torus

Marktpotential – Prämie (1)

Schätzung AGCS für Europa bis 900 Mio. Euro in 7 Jahren

Expertenmeinung: schnellere Entwicklung als D& O

USA über 1,3 Mrd. USD Prämie in 2013

Risiko-Bewusstsein durch NSA und BSI-Information deutlich gestiegen

D: Schätzungen der Arbeitsgruppe / Dr. Sven Erichsen:

- ►200 Mio. Euro in 5-7 Jahren (Hiscox-Schätzung 700 Mio. Euro)
- ►Z.Zt. Ca. 100 Abschlüsse (überwiegend in 2013/ 1. Quartal 2014)
- ►Marktprämie z.Zt. 3-5 Mio. Euro
- ►Steigende Tendenz

Marktpotential – Prämie (2)

Prämien pro Vertrag:

Aussage Hiscox Euroforum 16.01.2013 Prämie pro Mio. DS:

- ►Umsatz bis 100 Mio. Euro: 5.000 Euro bis 7.000 Euro
- ►Umsatz 100 Mio. bis 500 Mio. 10.000 – 13.000 Euro
- ►Umsatz grösser 500 Mio. Euro 15.000 Euro

Eigene Marktbeobachtungen

4.000 – 10.000 Euro pro Mio. Deckungssumme unabhängig von Größe

Unterschiedliche Fragebögen, unterschiedliche technische Expertise

Für welchen Ihrer Kunden ist eine Cyber- Versicherung wichtig?

Grundsätzlich für jeden Kunden, der

1. sensible Daten (personenbezogene oder sonstige vertrauliche) seiner Kunden, Mitarbeiter, Patienten, Vertragspartner speichert, bearbeitet oder verwaltet

   und / oder

2. wichtige Prozesse und Transaktionen seines Unternehmens IT-und / oder Web-gestützt steuert oder durchführt.

Beispiele für sensible Aktionsfelder potentieller Versicherungsnehmer (1)

Erichsen

1. Umgang mit personenbezogenen oder sonstigen sensiblen Daten

- Risiko Datenschutzverletzungen, Vertraulichkeitsverletzungen
- Risiko CyberCrime
- Risiko Reputationsverlust

2. Transaktionen durch IT-gestützte Systeme

- Risiko Verfügbarkeit / Betriebsunterbrechung
- Risiko Folgenschaden aus „Fehltransaktionen“
- Risiko CyberCrime

Beispiele für sensible Aktionsfelder potentieller Versicherungsnehmer (2)

Erichsen

3. Bereitstellen von Online-Portalen

- Risiko Verfügbarkeit (Eigenschaden BU, Schadenersatz)
- Risiko Datenschutzverletzungen, Vertraulichkeitsverletzungen
- Risiko CyberCrime
- Risiko Reputationsverlust

4. Produktion durch IT-gestützte Systeme

- Risiko Betriebsunterbrechung
- Risiko Vertraulichkeitsverletzungen
- Risiko CyberCrime

Kundenbedarf –
es darf auch etwas mehr sein…

Erichsen

Was kann/ sollte die Versicherungslösung auch gewährleisten?!

Optionen für das Krisenmanagement, z.B.

Prävention und Krisenbewältigung durch die Einbeziehung eines professionellen Unternehmens insbesondere zum strategischen, forensischen und juristischem Management von IT-Security-Krisen

Erstreaktion & Hotline
Krisenpläne
Forensik
Penetrationstests
Schulungen, Trainings & Übungen