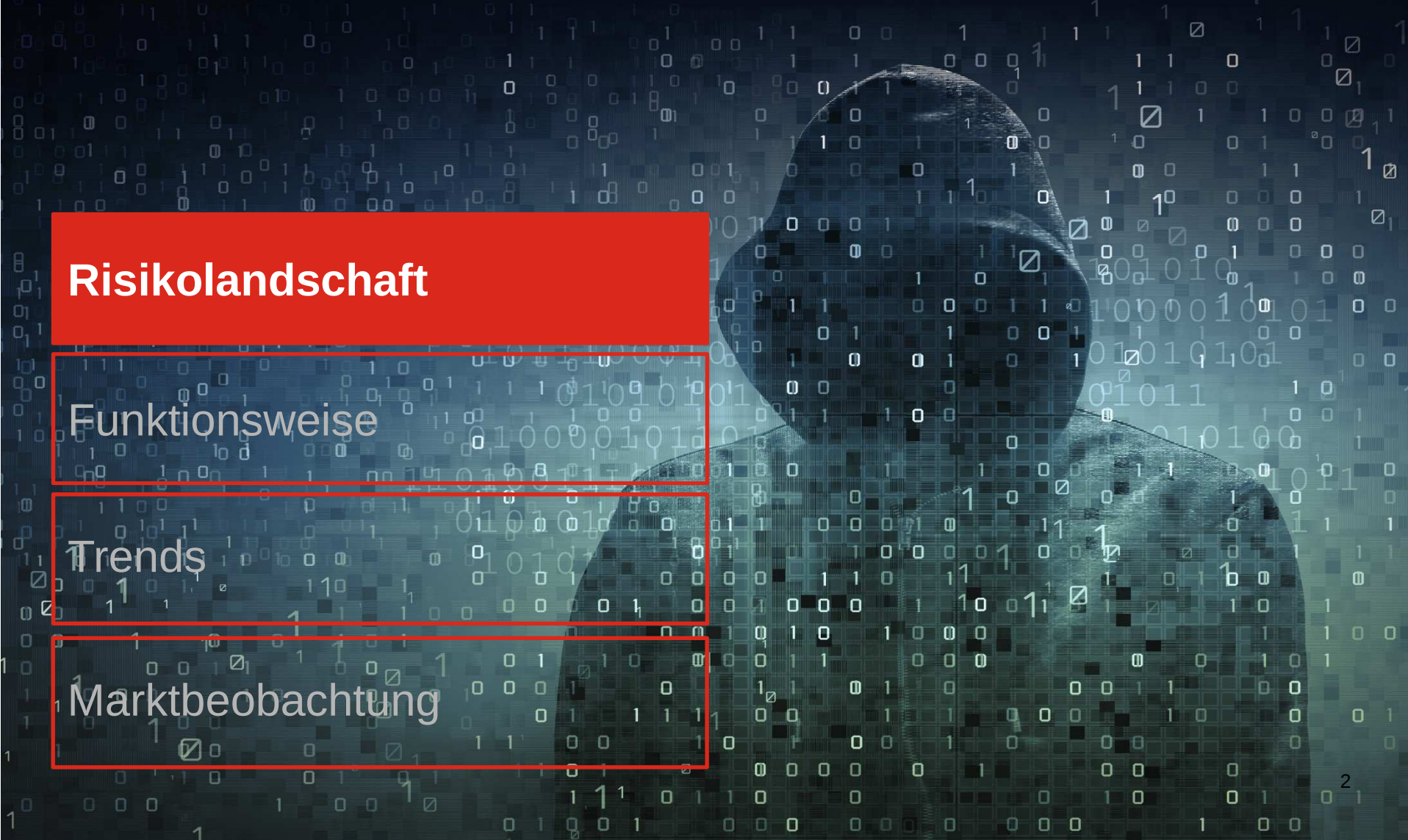


40. Versicherungswissenschaftliches Fachgespräch: Absicherung von IT-Sicherheitsrisiken durch moderne Cyber-Versicherungen



17. September 2018 / *Roman Potyka*

Agenda



Risikolandschaft

Funktionsweise

Trends

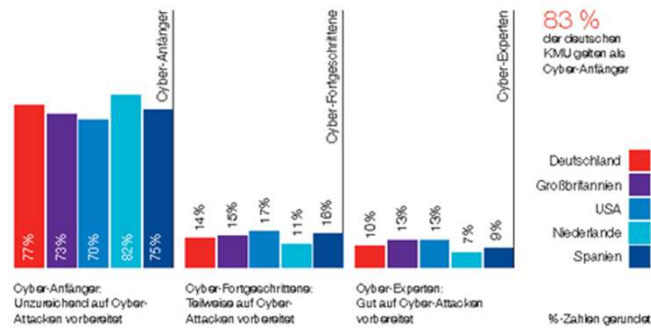
Marktbeobachtung

Unternehmer sind durch die Cyber-Gefahren verunsichert – aktives Risikomanagement & Experten Hilfe sind gefragt!



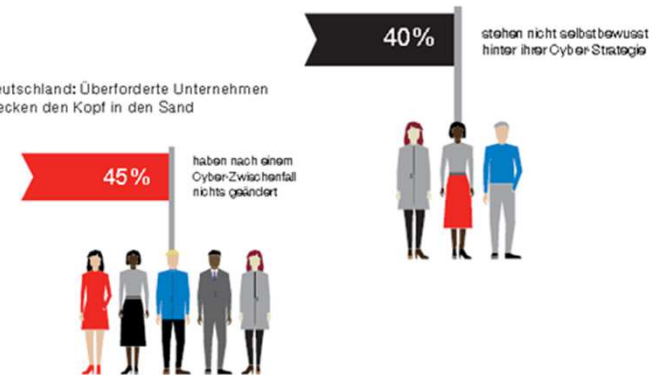
Cyber Readiness im Ländervergleich

Cyber Readiness im Ländervergleich



Kopf in den Sand: Cyber-Zwischenfälle & die eigene Strategie

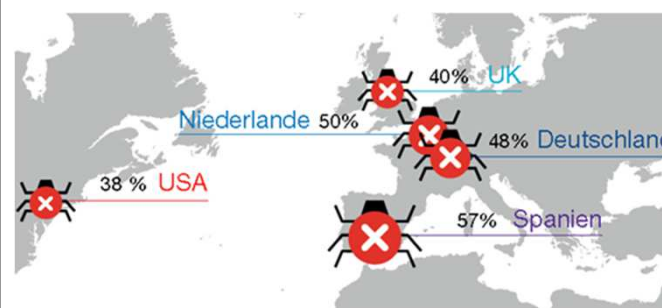
Deutschland: Überforderte Unternehmen stecken den Kopf in den Sand



Ausgaben für Cyber-Sicherheit



48% der deutschen Unternehmen geben an selbst im letzten Jahr einen Cyber-Vorfall erlebt zu haben



Cyberversicherung rückt in den Fokus der Unternehmer

Cyber-Versicherungsschutz – Agendapunkt in deutschen Chefetagen

33%

der deutschen Unternehmen verfügen über eine Cyber-Versicherung

25%

der deutschen Unternehmen planen innerhalb von 12 Monaten eine Cyber-Police abzuschließen

Angreifer und Angreifer-Typologie



Cyber-Kriminelle

versuchen mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen



Nachrichtendienste

Spionage und Wirtschaftsspionage



Hacktivismus und Cyber-Aktivisten

nutzen Computersysteme und Netzwerke vorgeblich als Protestmittel, um politische oder ideologische Ziele zu erreichen

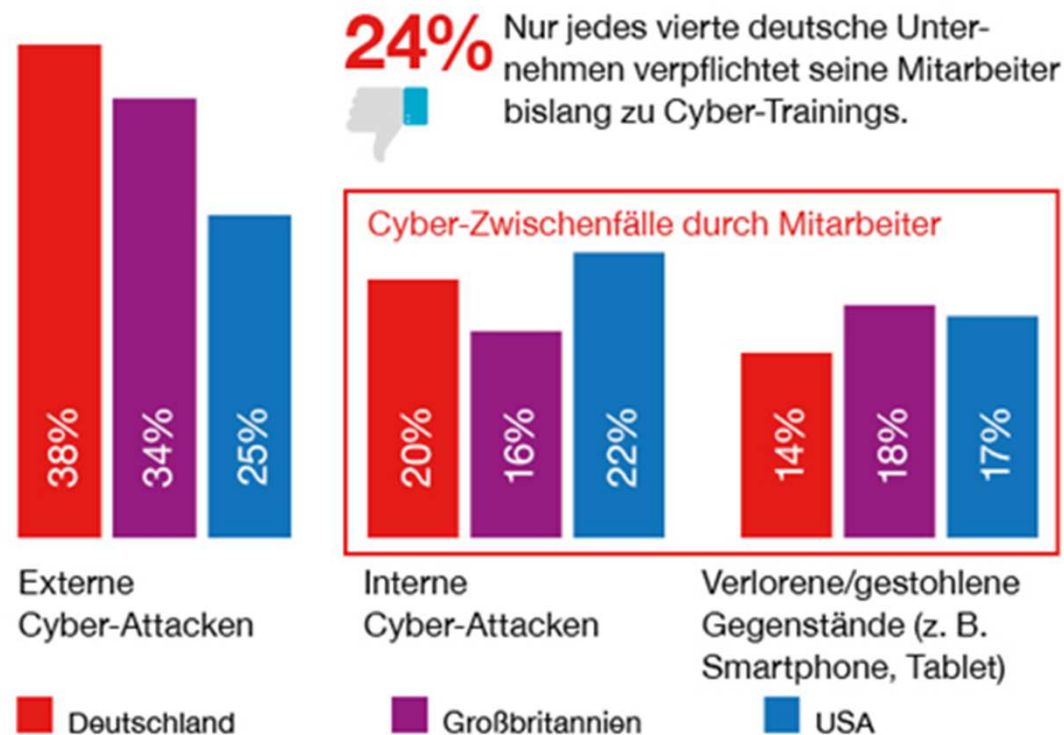


Innentäter

Tätergruppe, die für Angriffe auf firmeninterne oder vertrauliche Informationen sowie Sabotage in Frage kommt

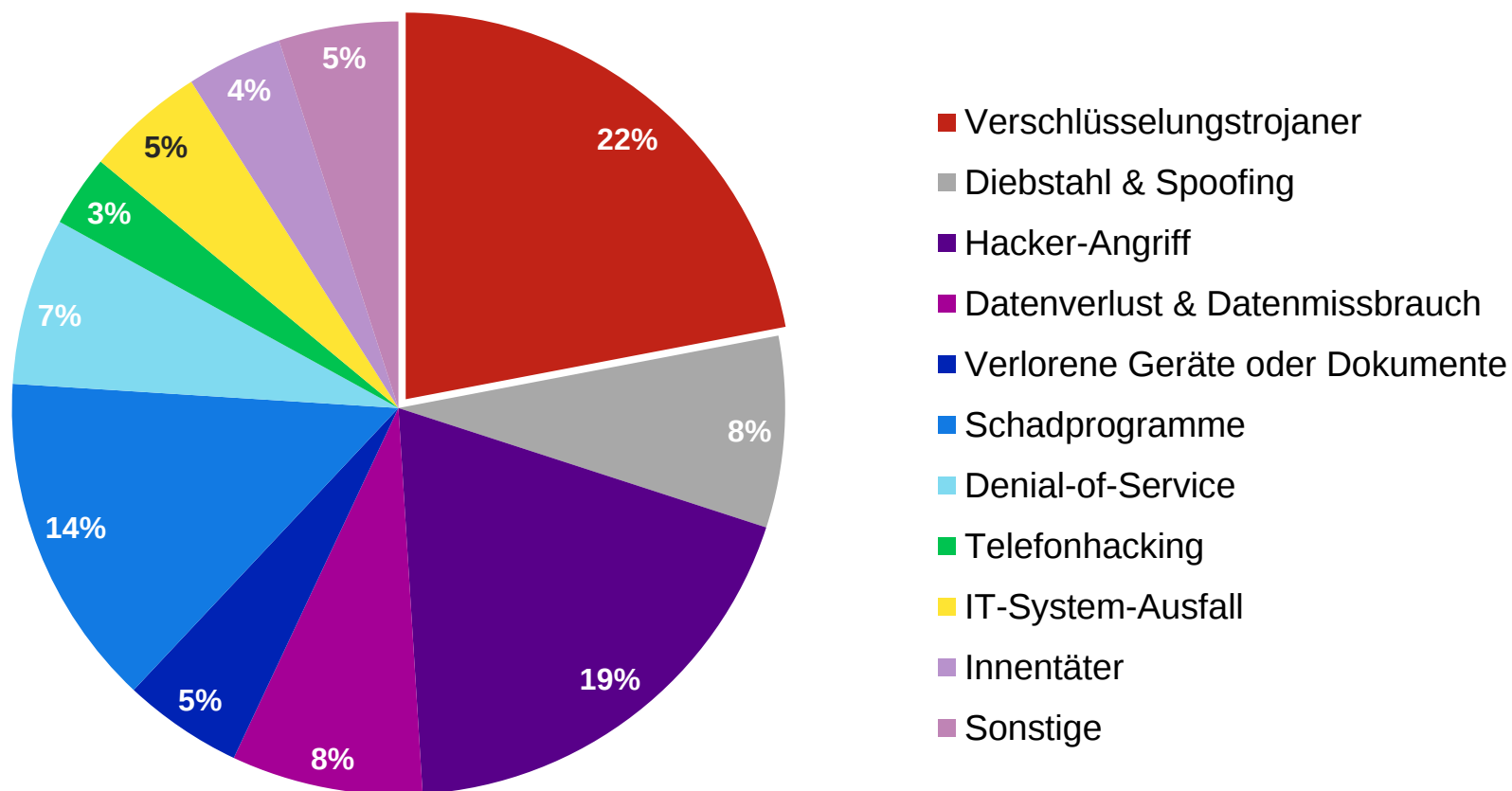
Wer steckt hinter Hackerangriffen? Eigene Mitarbeiter

TOP 3 der folgenschwersten Cyber-Angriffe



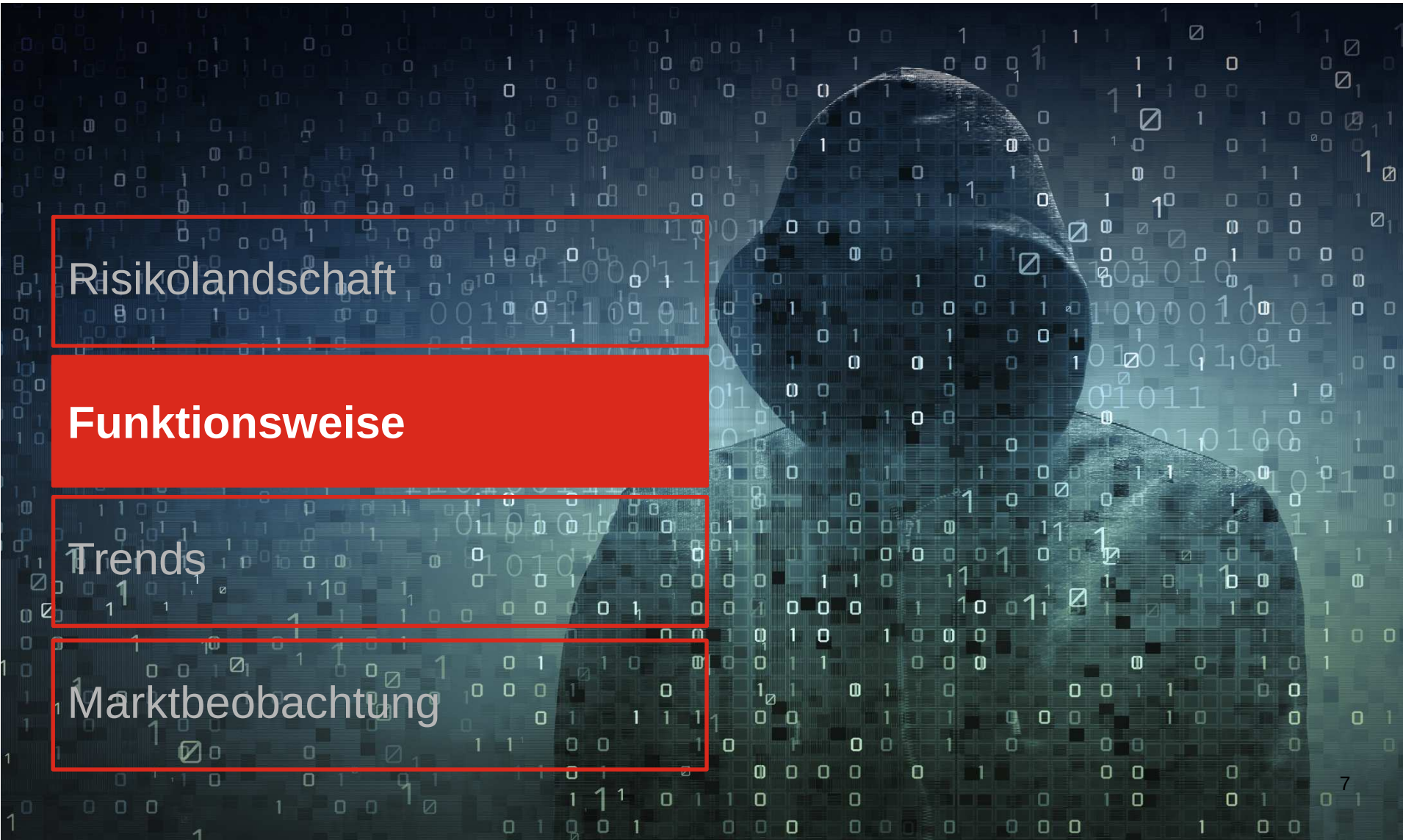
Die Art der **Cyber-Schäden** ist sehr divers – es überwiegen jedoch Fälle durch Ransomware

Schadenart



Auswertung der Cyber-Schäden im Jahr 2017

Agenda



Risikolandschaft

Funktionsweise

Trends

Marktbeobachtung

Der nachgelagerte Kostenersatz greift viel zu kurz!

Prävention



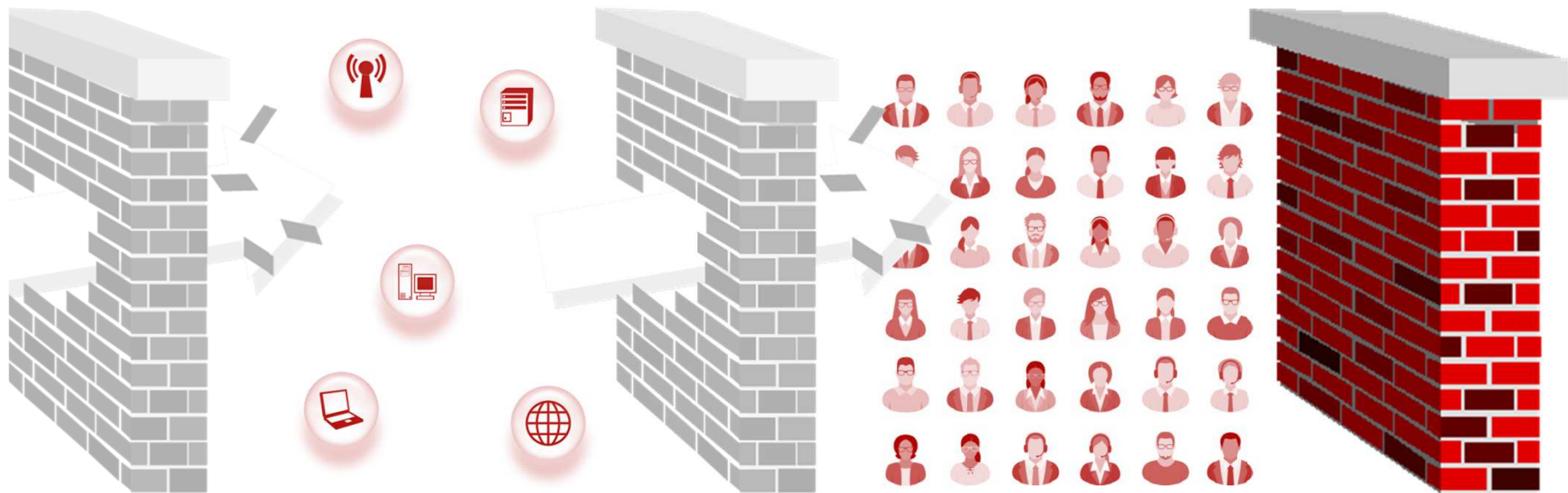
Versicherung



Assistance



IT-Sicherheit: Cyber-Versicherung ist die 3. Linie der Verteidigung



Technische Maßnahmen, z.B.

- Virenschutz
- Firewall
- Intrusion-Detection-System
- Penetrations-Tests

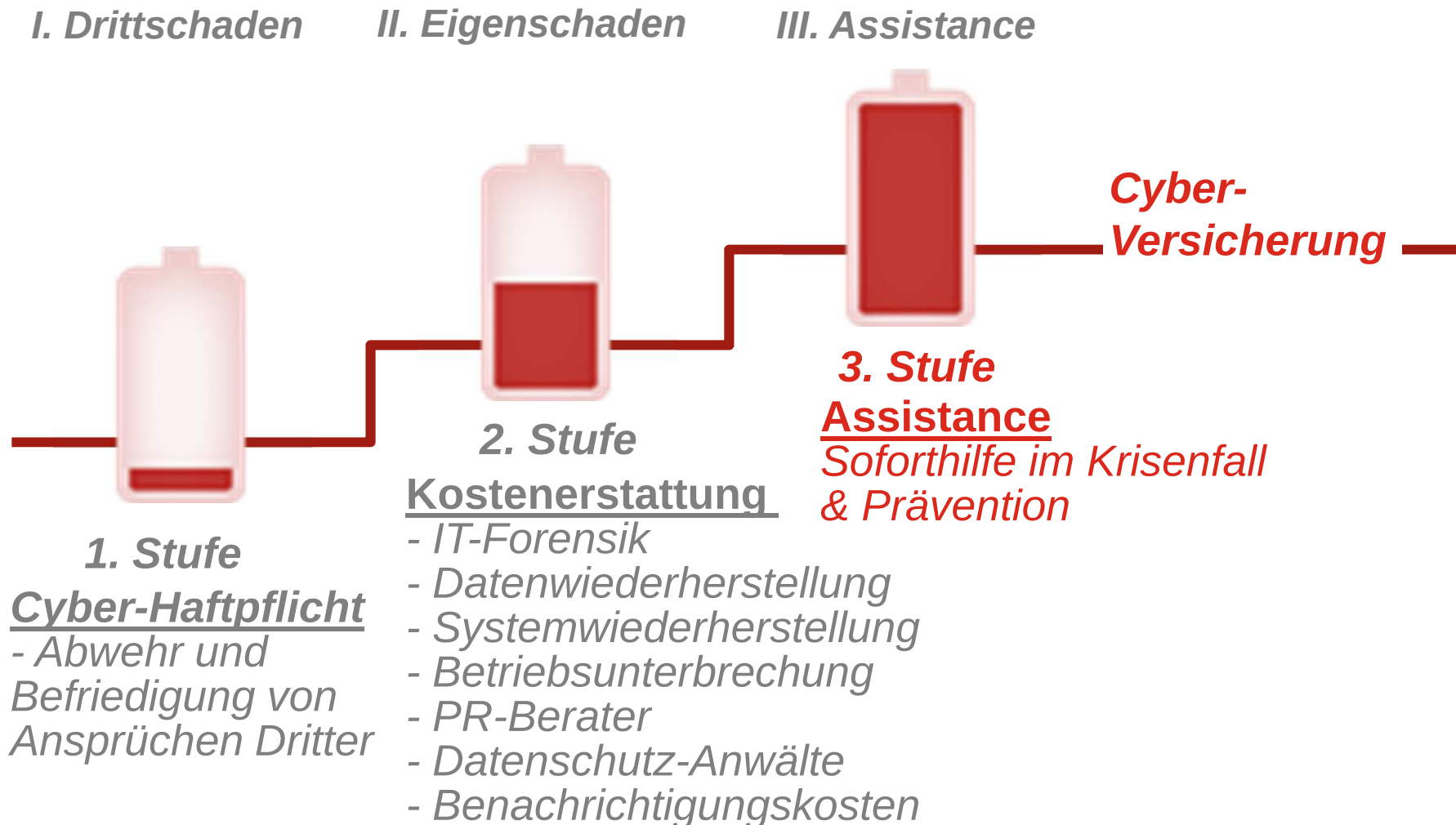
Organisatorische & personelle Maßnahmen, z.B.

- Benennung Verantwortliche
- Mitarbeitersensibilisierung
- Krisenstabsübungen

Cyberversicherung

- **Soforthilfe**
- **Risikotransfer**
- **Bilanzschutz**

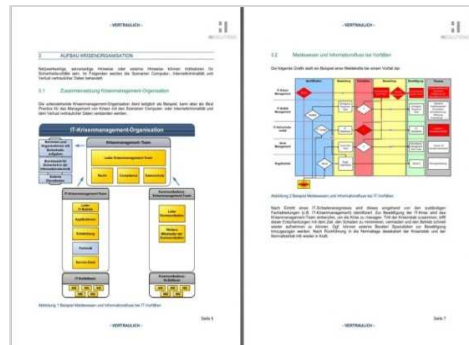
Aufbau einer Cyber-Versicherung mit den wichtigsten Komponenten



Beispiele für sinnvolle Krisen-Assistance + Prävention

Krisenplan

- Kurze übersichtliche Darstellung der Rahmenanweisungen.
- Beschreibung der Grundsätze, Richtlinien und Verfahrenselemente.



Notfallhotline

- Direkter Zugriff auf Experten.
- Kompetenter Sparringspartner.
- Direkte Hilfestellung und Schadenbearbeitung im Krisenfall.

Mitarbeiter Webinar

- Schulungstool für alle Mitarbeiter des Kunden ohne Begrenzung der Verfügbarkeit.
- Sensibilisierung für Verhaltensweisen bei der Nutzung moderner Kommunikationstechnologien.



The background of the slide is a dark, abstract image of glowing green and yellow circuit lines, resembling a complex electronic circuit board or a digital network. The lines are sharp and angular, creating a sense of depth and complexity.

***„Krise ist ein produktiver Zustand.
Man muss ihm nur den
Beigeschmack der Katastrophe
nehmen.“***

(Max Frisch)

Agenda

Risikolandschaft

Funktionsweise

Trends

Marktbeobachtung

Security > 7-Tage-News > 05/2018 > Drupal-Lücken: Lenovo versäumt Webseiten-Update und fängt sich...

Drupal-Lücken: Lenovo versäumt Webseiten-Update und fängt sich Krypto-Miner ein

08.05.2018 12:02 Uhr – Dennis Schirmacher



(Bild: Pixabay)

Ein Sicherheitsforscher warnt, dass Angreifer gegenwärtig ungepatchte attackieren, um dort einen Kryptogeld-Miner zu platzieren. Sicherheitslängen verfügbar.

Security > 7-Tage-News > 04/2018 > Statt Erpressungstrojaner: Krypto-Miner auf dem Vormarsch

Statt Erpressungstrojaner: Krypto-Miner auf dem Vormarsch

20.04.2018 11:42 Uhr – Dennis Schirmacher



(Bild: Pixabay)

Malware-Autoren setzen vermehrt auf bösartige Mining-Software. Dieses Jahr hat es einem Sicherheitsunternehmen zufolge erstmals mehr Infektionen dieser Art als mit Ransomware gegeben.

Sachschäden durch Cyber-Angriffe



Fake President Fraud

Supply chain – Rück- und Wechselwirkungsschäden



Agenda



Risikolandschaft

Funktionsweise

Trends

Marktbeobachtung

Der globale Cyber-Markt wächst

PwC schätzt das weltweite Marktwachstum von US\$ 2,5 Mrd. in 2015 auf US\$ 5 Mrd. in 2018 und US\$7,5 Mrd. Prämieineinnahmen in 2020.

Stand Alone Cyberprämien weltweit

Rest of World | ca. \$65 Mio.

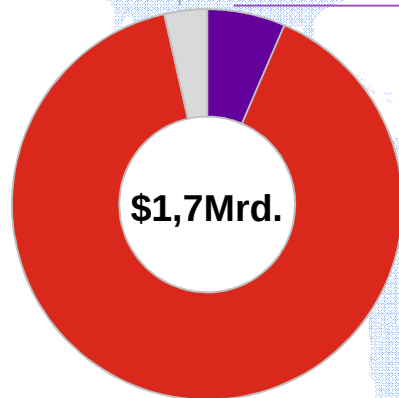
- Weniger entwickelt als der europäische Markt
- Haupttreiber sind APAC, Kanada und der mittlere Osten

Europa | ca. \$135 Mio.

- UK, Deutschland, Spanien & Frankreich machen > 70% der Prämieineinnahmen aus
- UK ist der größte Markt mit \$42 Mio.

LLOYD'S | ca. \$425 Mio.

- Lloyd's schätzt den eigenen weltweiten Marktanteil auf 25%
- Die Cyber-Prämie übersteigt schon heute den größten Terrorism risk code



USA ca. \$1.5 Mrd.

- Weltweit größter Cybermarkt (ca. 90% GWP)
- Wachstumsschub ab 2003 aufgrund von 49 neuen Data Breach Laws und eine Reihe von Großschäden

Quelle:
Lloyd's report Aon In-Point study;
Inga Beale, CEO of Lloyd's

Welche Branche kauft heute Cyber?



Handel



Gesundheit



Bildung



Finanzinstitute



Telko und Media

Kaufen **standalone Cyber** Policen mit Fokus auf Datenschutz. Inzwischen wird die Absicherung der Betriebsunterbrechung zum Haupttreiber

Kaufen sowohl **standalone Cyber** als auch **Add-Ons zur bestehenden Deckung**

Cyber wird oft mit der Vermögensschadenhaftpflicht oder anderen Financial Lines Produkten kombiniert.

- Diese 5 Branchen machen ca. ¾ des Marktes aus
- Marktdurchdringung in den USA ca. 30%
- Noch große Unterschiede zwischen Branchen und Unternehmensgröße
- Ca. ¾ der Krankenhäuser in den USA haben eine Cyberdeckung – größte Käufergruppe in 2015

Welche Unternehmensgröße kauft heute Cyber?

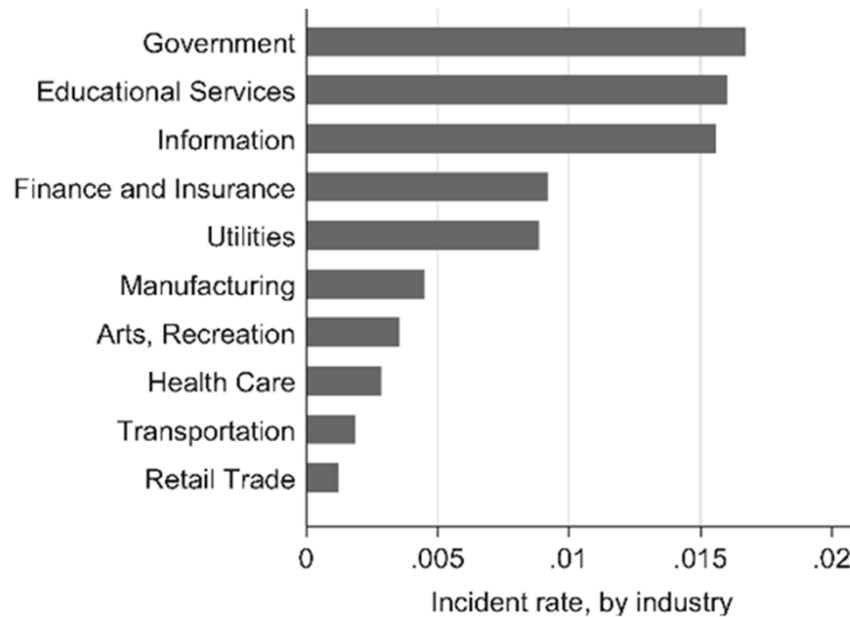


SMEs <= \$50 Mio. Umsatz; Mid-Market > \$50 Mio. <= \$1 Mrd. Umsatz; Large Corporate: >\$1 Mrd. Umsatz

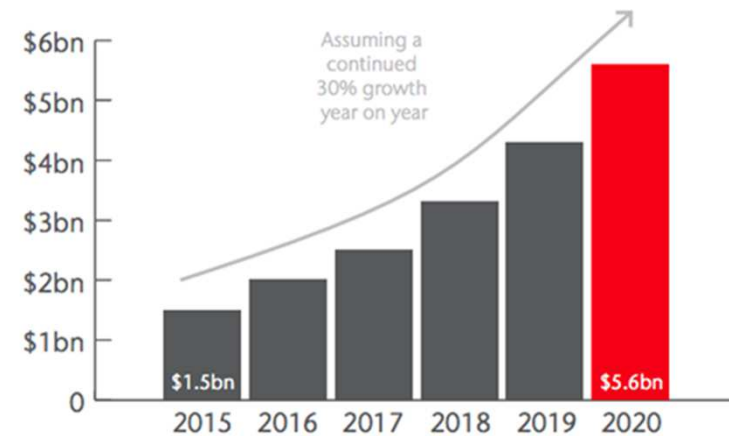
Der globale Cyber-Markt wächst

Ist allerdings kein Selbstläufer – die Schadenquoten der großen Player in den USA lag 2015 zwischen 0% und 160% - Ø 49%*

* Quelle: National Association of Insurance Commissioners (NAIC) 4/21/16



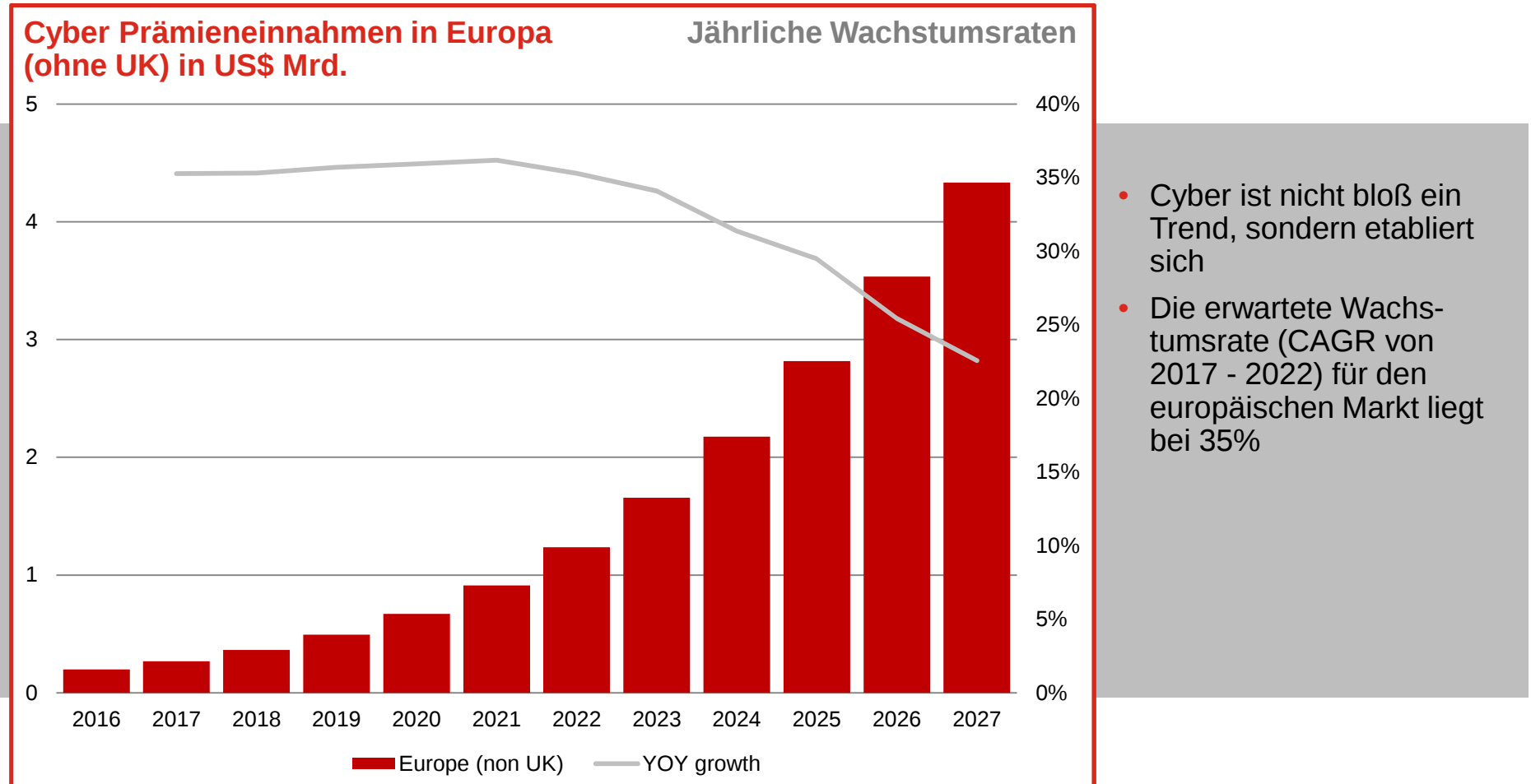
US standalone cyber market projection



Die hohen Abschlusszahlen korrelieren mit den Infektionsraten der einzelnen Branchen

Aon geht von einem jährlichen Wachstum von 30% aus – Kann Deutschland das toppen?

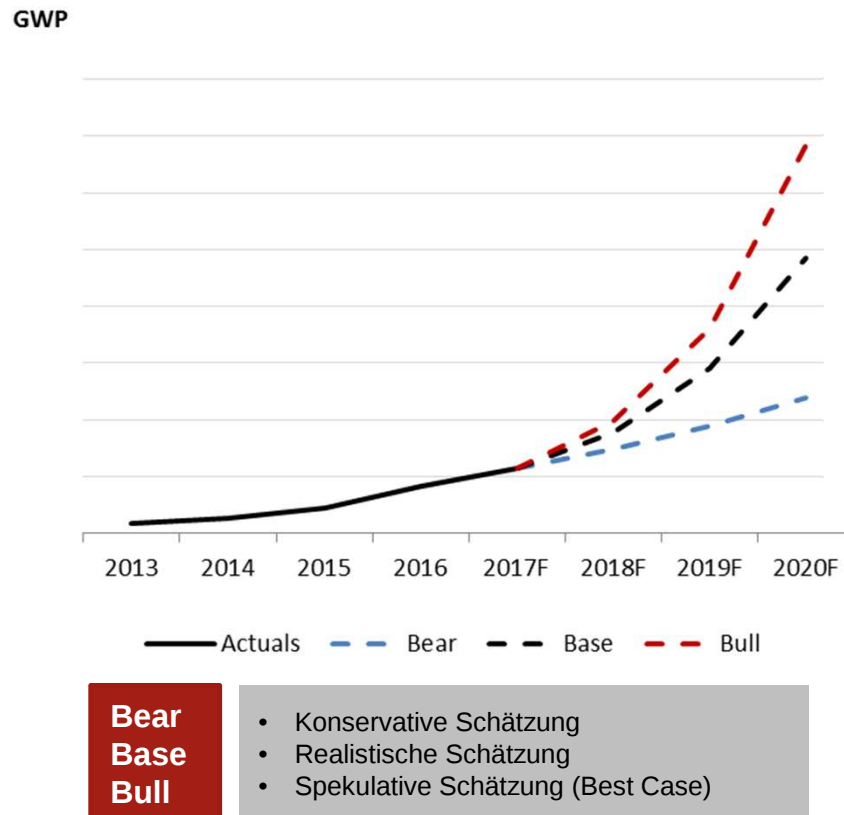
Wir stehen am Anfang einer großen Entwicklung –
der Markt hat enormes Potential und zieht deutlich an



Die EU-DSGV treibt den europäischen Cyber-Markt

Die Datenschutzanforderungen werden mit hohen Bußgeldern europaweit ca. auf BDSG Standard gehoben

Wachstumstreiber



EU Gesetzgebung

EU-Datenschutzgrundverordnung Mai 2018 – Verpflichtung Datenschutzvorfälle zu melden – Bußgelder bis zu 4% des weltweiten Umsatzes*

Sensibilisierung

Cyber erreicht zunehmend die Vorstandsetage
Mit der EU-DSGV werden noch mehr Fälle verpflichtend gemeldet und erreichen die Medien

Frequenz

Cyber-Angriffe nehmen zu
Unternehmen sind immer noch nicht gut vorbereitet.
50% Anfragenzunahme in der Woche nach WannaCry

Benachrichtigungskosten

EU-DSGV wird die Kosten treiben–
Mit der Verpflichtung Vorfälle nachzuverfolgen und die Behörden innerhalb 48 Stunden zu informieren

* Maximales Bußgeld (zB bei fehlender Zustimmung des Kunden zu Datenverarbeitung oder der groben Verletzung des Datenschutzes). Hohe Bußgelder können fällig werden, wenn die Behörden nicht rechtzeitig informiert werden oder andere Regelungen nicht eingehalten werden



Kontakt:
Roman Potyka
Senior Underwriter Berlin
Tel: 0172 8425397
roman.potyka@hiscox.com

