Internetkriminalität – wie sich Risiken begrenzen lassen.

17.11.2017

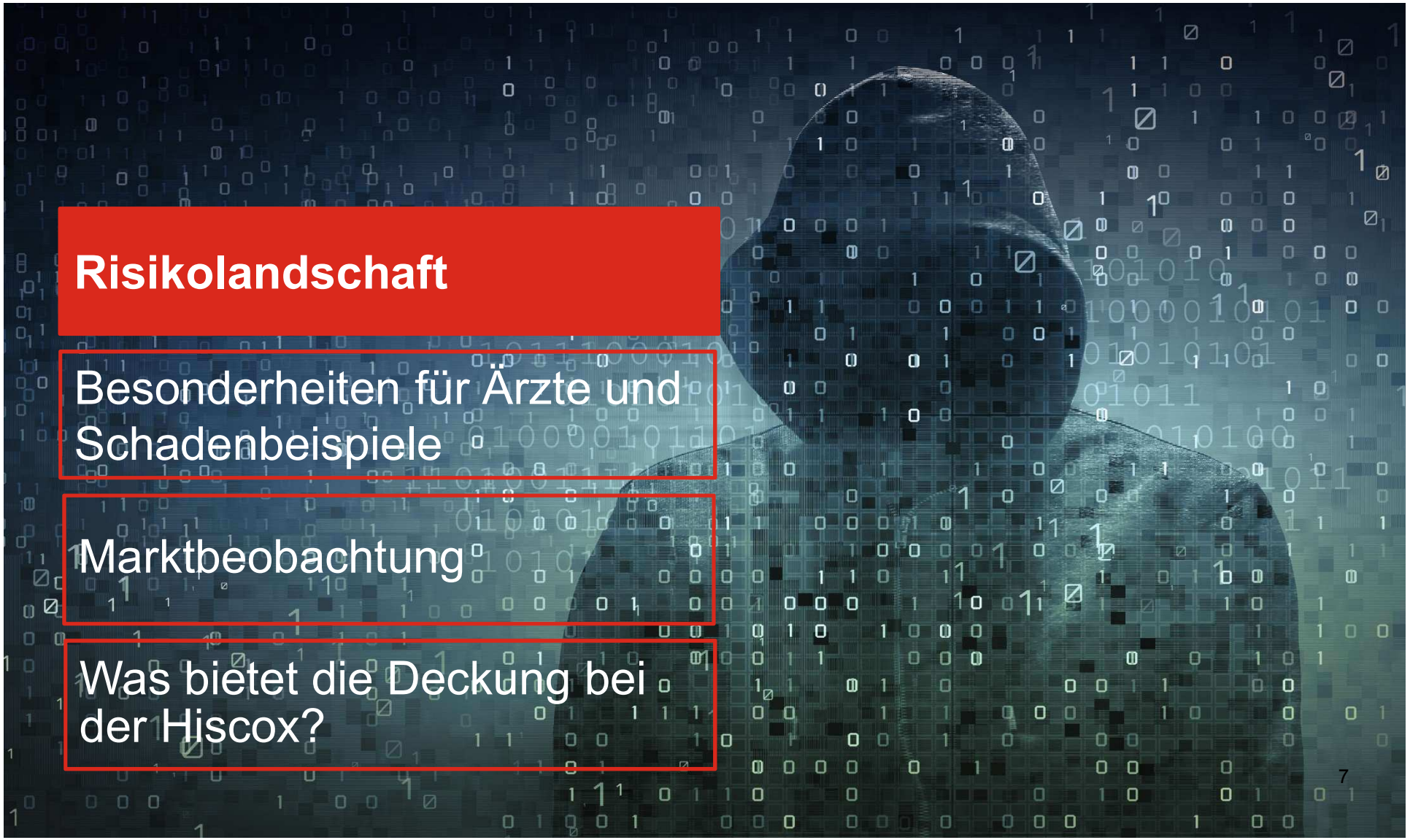
Hartmut Niederle-Renken (Dipl. Kfm.)
Geschäftsführer

Spezielle Versicherungslösung für Hackerangriffe und Datenverluste

Are You Prepared?

- Quelle: ENISA via Youtube

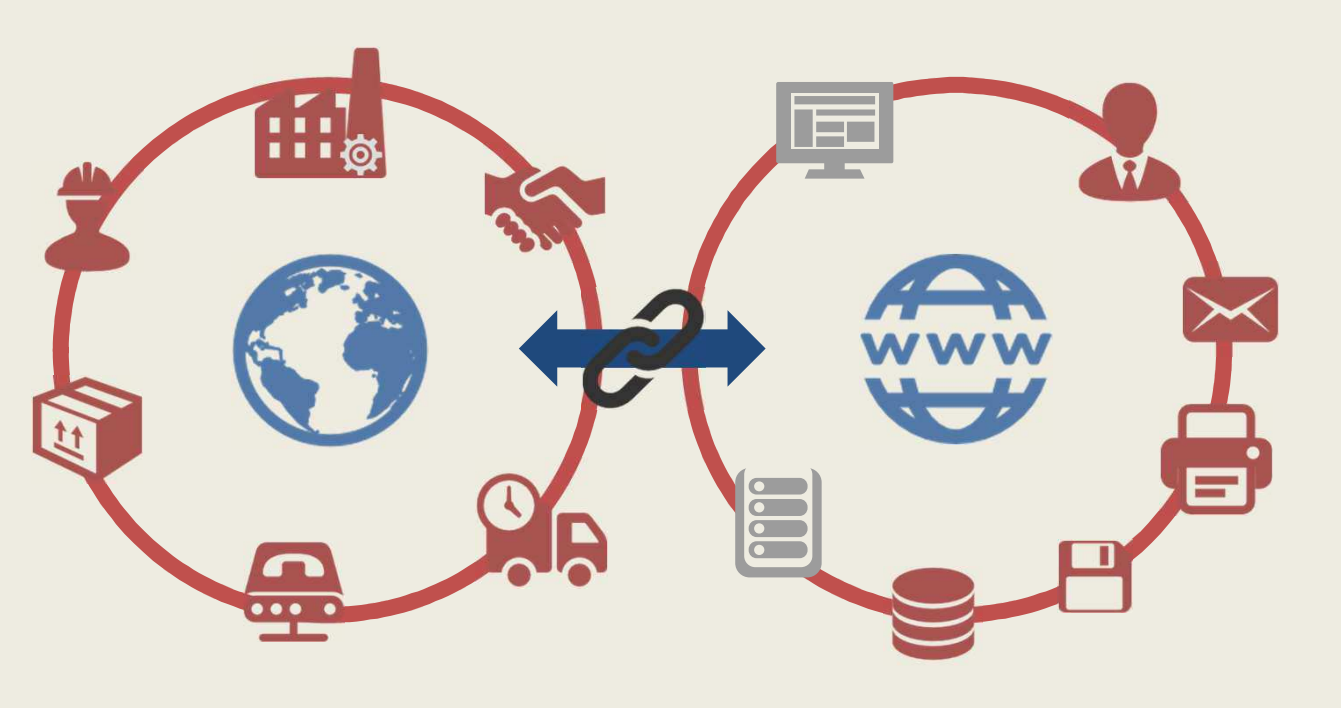
Agenda


Risikolandschaft
Besonderheiten für Ärzte und Schadenbeispiele
Marktbeobachtung
Was bietet die Deckung bei der Hiscox?

Was funktioniert heute noch ohne Computer?

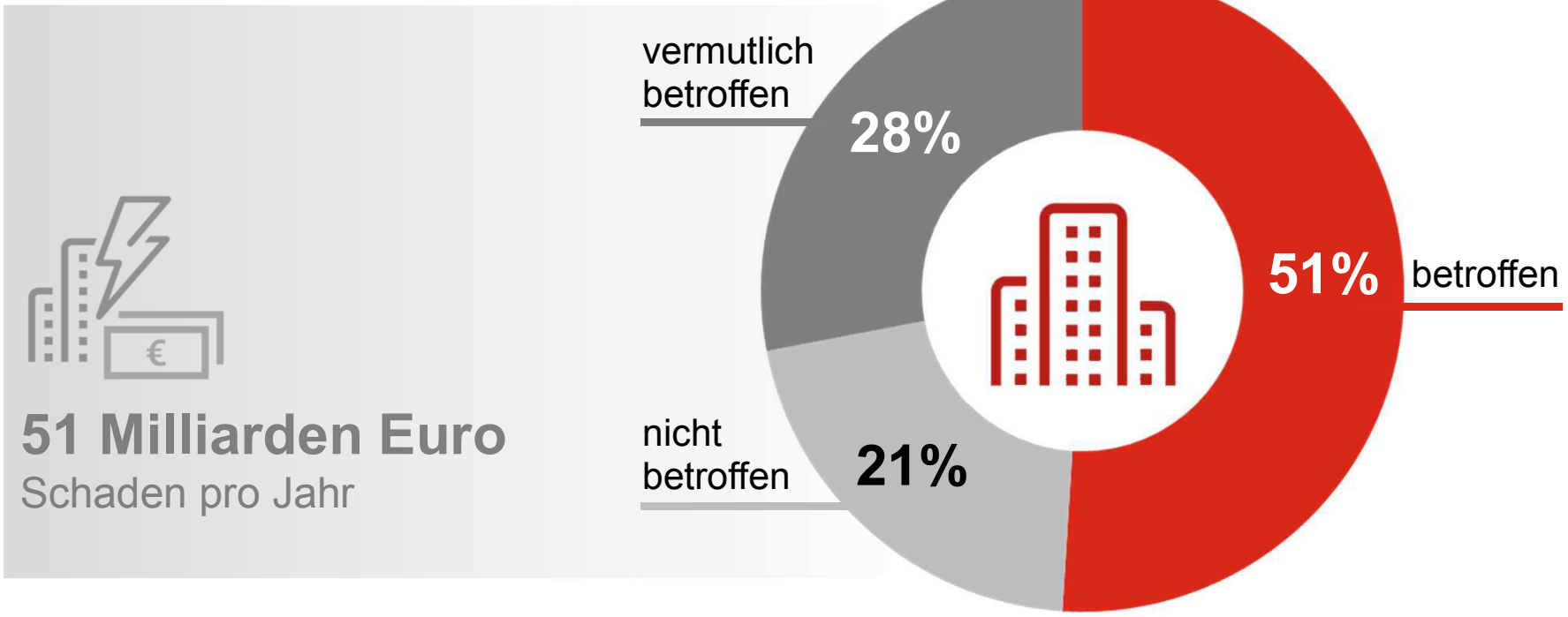
- ! Jede Sekunde treten 8 neue Nutzer dem Internet bei
- ! Jeden Tag gibt es 30.000 neue infizierte Webseiten
- ! Jeden Tag tauchen 250.000 neue individuelle Schadcodes auf

Cyberspace und reale Welt sind mittlerweile fast überall miteinander verbunden.



Aktuelle Risikosituation
Zahlen & Fakten

Anteil Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, digitaler Wirtschaftsspionage oder Sabotage betroffen waren



51 Milliarden Euro
Schaden pro Jahr

Quelle: Bitkom Research 2015

Angreifer und Angreifer-Typologie

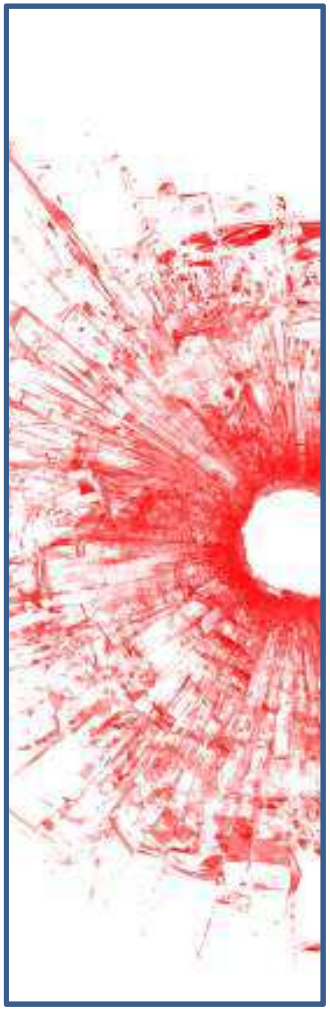
Cyber-Kriminelle
versuchen mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen

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

Cyber-Krisensituation - Was kann dazu führen?



Rechtlicher Hintergrund

- Irrtürmliches Mitschicken von Daten/Unterlagen in einem Brief
- Verlieren eines Laptops, USB Sticks, Smartphone, etc.
- Diebstahl von Computern
- Email oder FAX wird an einen falschen Empfänger verschickt
- Dokumente landen im Papierkorb
- Viren, Trojaner etc.

Rechtlicher Hintergrund

- Hackerangriffe ggf. unterstützt von kriminellen Organisationen
- Denial of Service Attacken

Missverständnisse und Fehleinschätzungen

„Wir sind doch viel zu klein und unbekannt, um Hacker anzulocken.“	Kleine Unternehmen stellen oftmals ein viel interessanteres Ziel dar.
 „Wir sind eine verschworene Gemeinschaft, auf jeden unserer Mitarbeiter können wir uns voll verlassen.“	Bis zu 60% aller Datenverlust-Vorfälle werden durch „Unachtsamkeit“ von Mitarbeiter zumindest begünstigt.
„Cyber Security ist doch ein technisches, keines-falls ein strategisches Problem.“	Ein Datenschutzvorfall kann zu einer Betriebs-unterbrechung, zu immensen Schadenersatz-forderungen sowie irreparablen Reputationsschäden führen.

Missverständnisse und Fehleinschätzungen

„Wir haben eine Top-IT-Abteilung, die hat Störungen immer schnell im Griff.“	Vielfach verfügen selbst sehr gute IT-Abteilungen nicht über das spezifische Equipment und/oder Know-how, ferner sind sie keine Krisenmanager.
„Ich habe meine Daten an einen externen Dienstleister ausgelagert, deshalb trage ich keine Verantwortung.“	Verantwortung für Datensicherheit kann nicht vollständig ausgelagert werden. Verantwortliche Stelle im Sinne des BDSG ist das Unternehmen, welches die Daten erhebt (§ 3 Abs. 7 BDSG)

Auszug: Haftungsrechtliche Grundlage BDSG

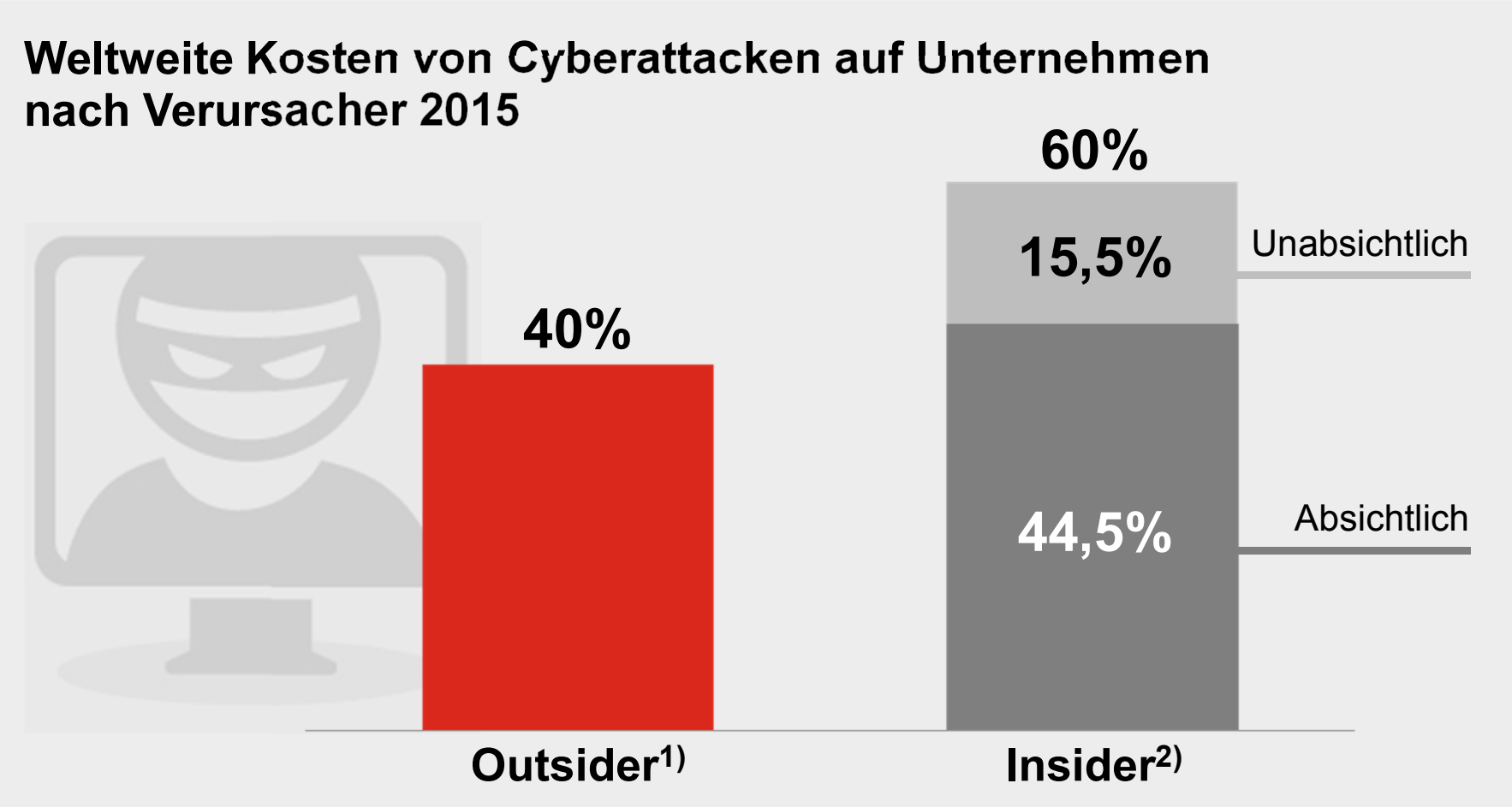
BDSG

- Verbotsprinzip mit Erlaubnisvorbehalt
- Schadenersatzansprüche für Geschädigte
- Datenschutzbeauftragter bei mehr als 9 MA
- Meldepflicht bei bestimmten Datenschutzverstößen
- Bußgelder von 50.000 bis 300.000 EUR
- D&O-Aspekt: Verantwortung bleibt beim Unternehmen, das die Daten verarbeitet / speichert

Weitere Normen

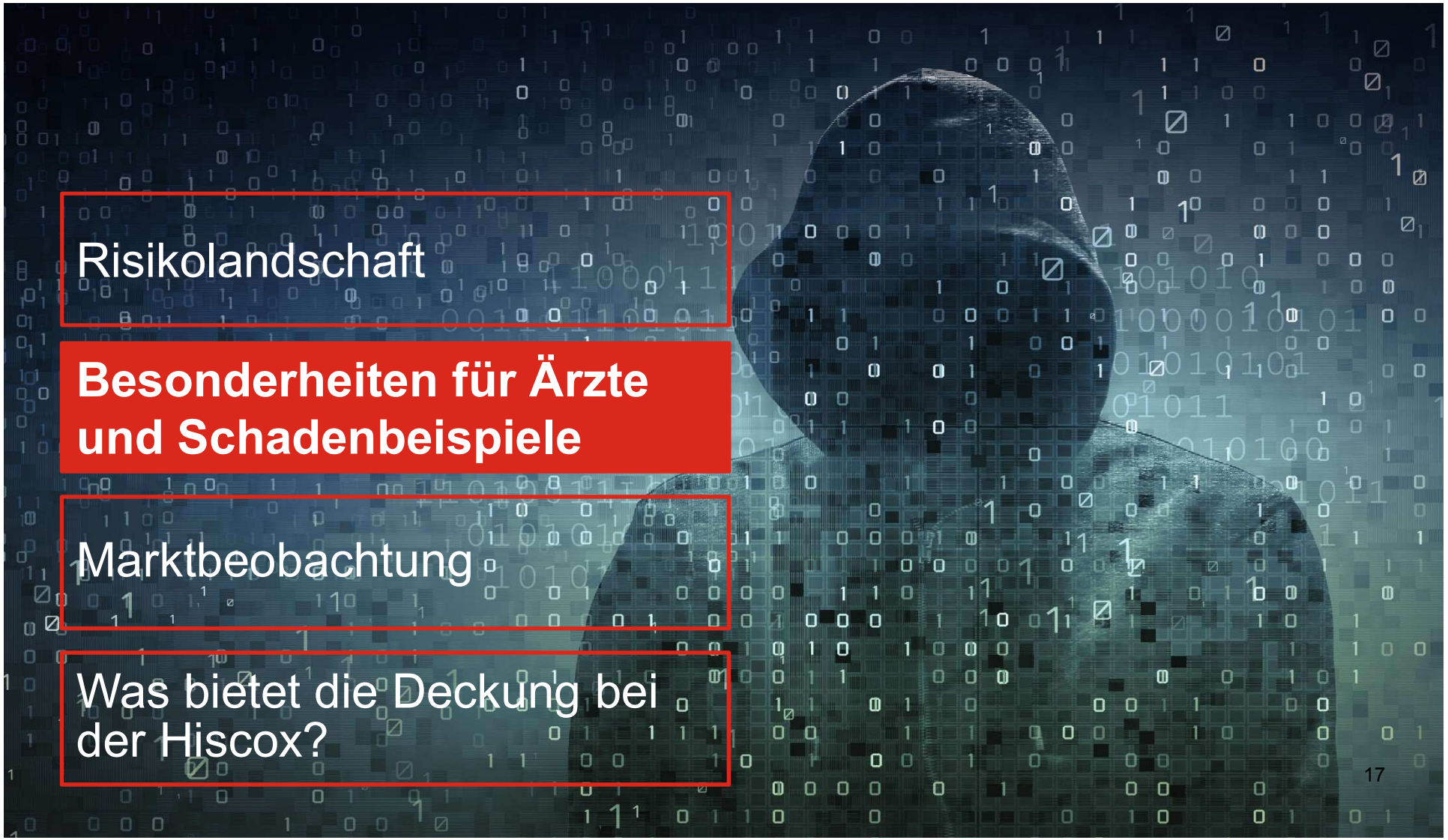
- Privatrechtliche Vereinbarungen
- Vertragliche Haftung
- 2018 EU Datenschutz-richtlinie

Cyber-Attacken oft auf Insider zurückzuführen



1) Angreifer ohne Zugriffsrechte
2) Angestellte, Dritte mit Systemzugriff
Quelle: IBM X-Force Cyber Security Intelligence Index 2016

Agenda


Risikolandschaft
Besonderheiten für Ärzte und Schadenbeispiele
Marktbeobachtung
Was bietet die Deckung bei der Hiscox?

Aktuelle Risikosituation
Besonderheiten für Ärzte

Arztpraxen generieren und verarbeiten eine hohe Anzahl personenbezogener Daten, insbesondere Gesundheitsdaten der Patienten. Diese Daten sind aus-gesprochen sensibel; sie bilden eine sehr private Sphäre der Patienten ab.
Eine Datenschutzverletzung – z.B. die ungewollte Veröffentlichung von Patientendaten bei Datenklau durch Hacker & Co – ist eine Krise, die jede Praxis nachhaltig in eine finanzielle Schieflage bringen kann.

§ Rechtlicher Hintergrund

- Datenvorfall kann Schadensersatzanspruch des Betroffenen gemäß § 7 BDSG begründen
- Das Unternehmen/Praxis haftet auch dann als verantwortliche Stelle im Sinne des BDSG, wenn ein Datenverlust auf einem Handeln von Mitarbeitern oder einem externen Dienstleister (z. B. Hosting von Daten in externem Rechenzentrum) beruht
- Informationspflicht nach **§ 42a** BDSG
- Verantwortlichkeit kann nicht delegiert werden
- Die jüngsten Datenvorfälle zeigen, dass Aufsichtsbehörden harten Verfolgungskurs einschlagen

Aktuelle Risikosituation
Schadenbeispiele aus den Medien

Süddeutsche Zeitung
SZ.de Zeitung Magazin

Wirtschaft Panorama Sport München Bayern Kultur

ital > Hackerangriff - Computervirus legt Klinik in Neuss lahm

12. Februar 2016, 16:36 Uhr Hackerangriff

Computervirus legt Klini lahm

- Ein Computervirus legt das städtische Krankenh Neuss lahm. Es werde gearbeitet wie vor 15 Jahr Sprecherin.
- Cyberangriffe auf Krankenhaus-IT nähmen zu, Fälle von Erpressung, teilt die Krankenhausgese

Ein Computervirus hat die Arbeit eines Krankenha Neuss bei Düsseldorf stark eingeschränkt. Vor zwe festgestellt worden, dass sich eine Schadsoftware Informationssystem ausbreite, bestätigte die Spre Klinik. Ob es sich um einen gezielten Angriff hand war unklar.

Protokoll einer Cyberattacke

Eine Bonner Praxis wird Opfer eines Hacker

Blutdruckmessen ohne Elektronik: Bei anderen Geräten, wie dem Ultraschall, ist der Bilder notwendig. Ein Hackerangriff kann auch eine Hausarztpraxis empfindlic

BONN. Ein Virus in der Arztpraxis. Ausgerechnet. der Computerschädling „Wannacry" Mitte Mai welt 230.000 Rechner lahmlegte, machte ein Bonner Ar Erfahrung. Das Protokoll eines Hackerangriffs.

Von Delphine Sachsenröder, 27.05.2017

Patientendaten gestohlen: Hacker übernahmen Server

Patientendaten gestohlen: Hacker übernahmen Server / Bild: (c

Der Server eines Softwaredienstleisters, der Ziel von Angriffen. Vermutlich sind 2000 Pat

25.09.2013 | 17:44 | (Die Presse)

Wien. Digital gespeicherte Daten landen durch einfa einmal dort, wo sie eigentlich nicht hingehören. Es is die falsche Person den richtigen Mausklick macht.

Karneval vs. Datenschutz: Patientenakten aus der Konfetti-Kanone

heise online 11.02.2016 15:05 Uhr vorlesen

Patientendaten sind attraktives Diebesgut

Schadenbeispiele I

Datenverlust durch Computervirus

Ein Arzt öffnet den Anhang einer E-Mail.
Der darin befindliche Virus verschlüsselt alle Daten auf den Computern im Büro und fordert Lösegeld für die Wiederherstellung und Nichtveröffentlichung der Daten. Die Wiederherstellung dauert mehrere Tage in denen in der Praxis nur teilweise gearbeitet werden kann. Gesamtschaden: 100.000 EUR.

Leistungen unter der Cyber Risk Management by Hiscox

- ✓ Sofortberatung von HiSolutions 24/7 Hotline
- ✓ Kosten für IT-Forensik
- ✓ Kosten der Wiederherstellung des Systems
- ✓ Kosten der Wiederherstellung der Daten
- ✓ Kosten für Sicherheitsverbesserungen
- ✓ Informationskosten der Dateninhaber
- ✓ Kosten PR-Maßnahmen
- ✓ Betriebsunterbrechnung (sofern vereinbart)
- ✓ Haftpflichtansprüche von Dateninhabern

Schadenbeispiele II

Datenverlust nach Hackerangriff

Nachdem sich ein Hacker Zugriff auf die Computer einer Praxis verschafft hatte, löschte er alle Daten und damit alles Patientenakten von aktuellen und archivierten Patientenakten. Die Akten müssen mühsam wiederhergestellt werden und die Praxis kann drei Tage nur teilweise arbeiten.
Gesamtschaden: 280.000 EUR.

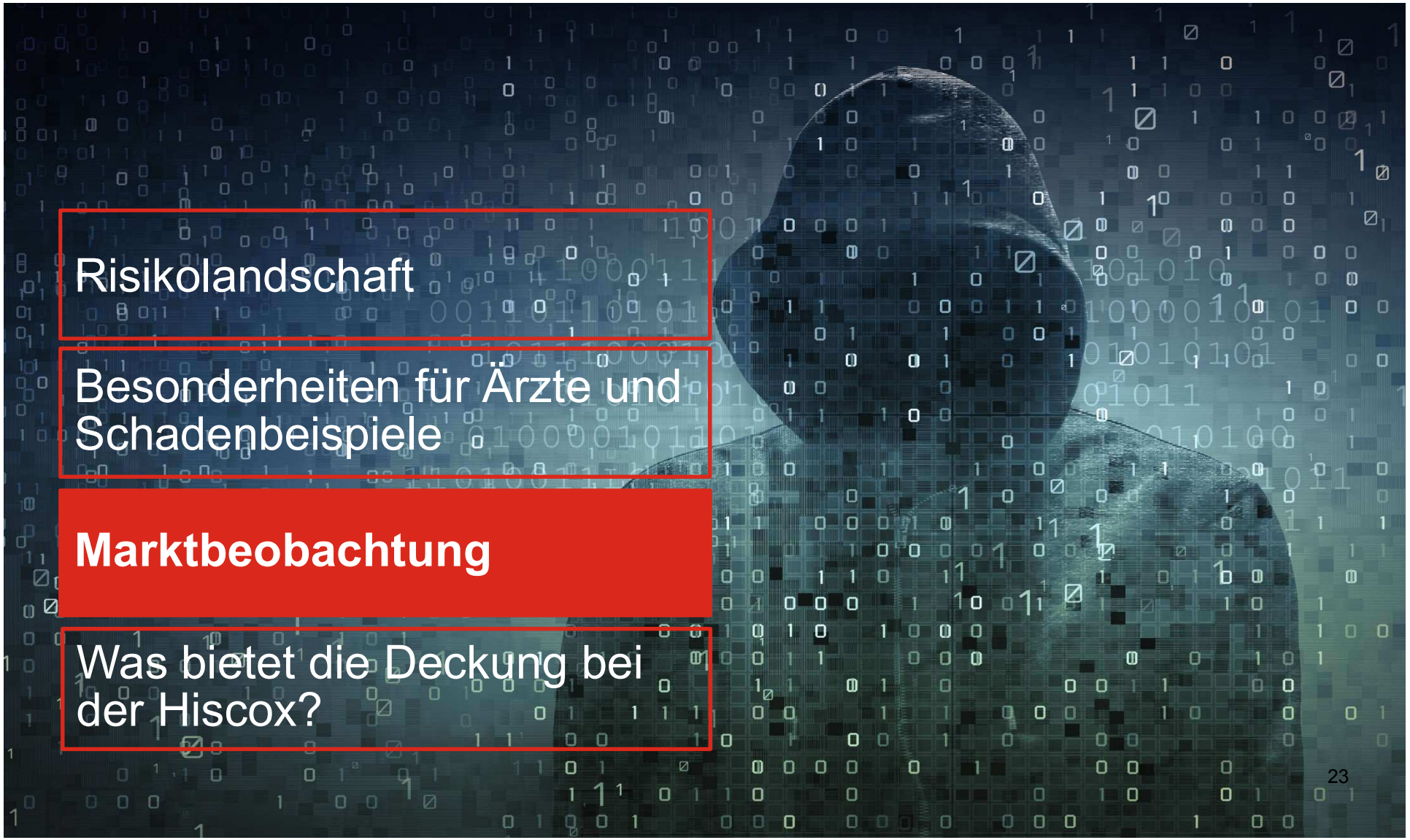
Leistungen unter der Cyber Risk Management by Hiscox

- ✓ Sofortberatung von HiSolutions 24/7 Hotline
- ✓ Kosten für IT-Forensik
- ✓ Kosten der Wiederherstellung des Systems
- ✓ Kosten der Wiederherstellung der Daten
- ✓ Kosten für Sicherheitsverbesserungen
- ✓ Kosten PR-Maßnahmen
- ✓ Betriebsunterbrechnung (sofern vereinbart)

Was können Sie tun, um Ihr Risiko zu minimieren?

- **Krisen- und Business Continuity Plan**
  - Krisenstab unter Einbeziehung externer Ressourcen
  - Wer ist zu informieren? Wie können wir weiterarbeiten?
  - Dokumentierung und Kommunikation
- **Faktor Mensch**
  - Risikobewusstsein
  - Training / Übung
- **Technik**
  - Implementierung von Sicherheitssoftware
  - Herausforderung: Balance zwischen Investition und Sicherheit
- **Versicherung**
  - Restrisiken transferieren

Agenda


Risikolandschaft
Besonderheiten für Ärzte und Schadenbeispiele
Marktbeobachtung
Was bietet die Deckung bei der Hiscox?

Bedingungswerke noch nicht konsistent in Qualität und Praxistauglichkeit

Worauf sollten Sie achten:

- Jede Art von Daten sollten mitversichert gelten
- Keine Obliegenheiten vor Eintritt des Versicherungsfalls / Ausschlüsse
- Sinnvolle Assistance-Leistung
- Sinnvolle Repräsentanten-Klausel
- Klar geschriebenes Bedingungswerk
- Keine Subsidiaritätsklauseln
- Basis des Deckungsschutzes muss stimmen

Klauseln aus der Praxis

Subsidiarität
Ist ein zu diesem Versicherungsvertrag gemeldeter Schadensersatzanspruch auch unter einem an-deren Versicherungsvertrag versichert, so besteht kein Versicherungsschutz über diesen Vertrag. [...]

Haftzeit BU:
Lediglich 1 Monat.

Wartefrist nach Vertragsabschluss

Erprobungsklauseln:
Kein Versicherungsschutz besteht für Versicherungsfälle, die dadurch entstehen, dass die Versicherten Hardware oder Software benutzen, die in ihrer Entwicklung noch nicht abgeschlossen oder deren Testverfahren noch nicht beendet und daher noch nicht erfolgreich erprobt ist.

Ausschluss Daten im Arbeitsspeicher

Datenwiederherstellung
Kosten werden für die Wiederherstellung getragen, jedoch nicht für die Systemverbesserungen.

Stand der Technik:
Der Versicherungsnehmer hat aktuelle technische Schutzmaßnahmen zu ergreifen, die unvorhergesehene Verluste, nachteilige Veränderungen an oder die Nichtverfügbarkeit von Daten und Programmen sowie unerlaubten Zugriff auf Daten und Programme verhindern.

Bezug auf Personengebundene Daten:
Es gelten personengebundene Daten als versichert nicht jedoch sonstige Daten. .

SB-Regelung
Der Versicherer erbringt Versicherungsleistungen erst dann, wenn der im Versicherungsschein dokumentierte anwendbare Selbstbehalt durch Zahlung der Versicherten verbraucht ist. (Verzögert die Hilfeleistung enorm!)

Wartung von Systemen:
Im Rahmen der Systemwartung / Abschaltung gilt kein Versicherungsschutz.

Erpressungshandlungen
Nur versichert, wenn Fremde / Dritte erpressen. Dazu gehören die eigenen Mitarbeiter nicht. Jedoch hier ein hohes Schadenpotential.

Notfallpläne als Obliegenheit:
Vorliegen eines aktuellen **Notfallplans** für den Fall des Eintritts der unter Ziffer XXX beschriebenen und versicherten Gefahren, der unter anderem einen Wiederanlaufplan umfasst.

Art der Daten
Verletzung von Daten die maschinenlesbar und maschinenverarbeitbare Informationen in elektronischer Form auf Datenträgern darstellen. Somit keine klassischen physischen Daten.

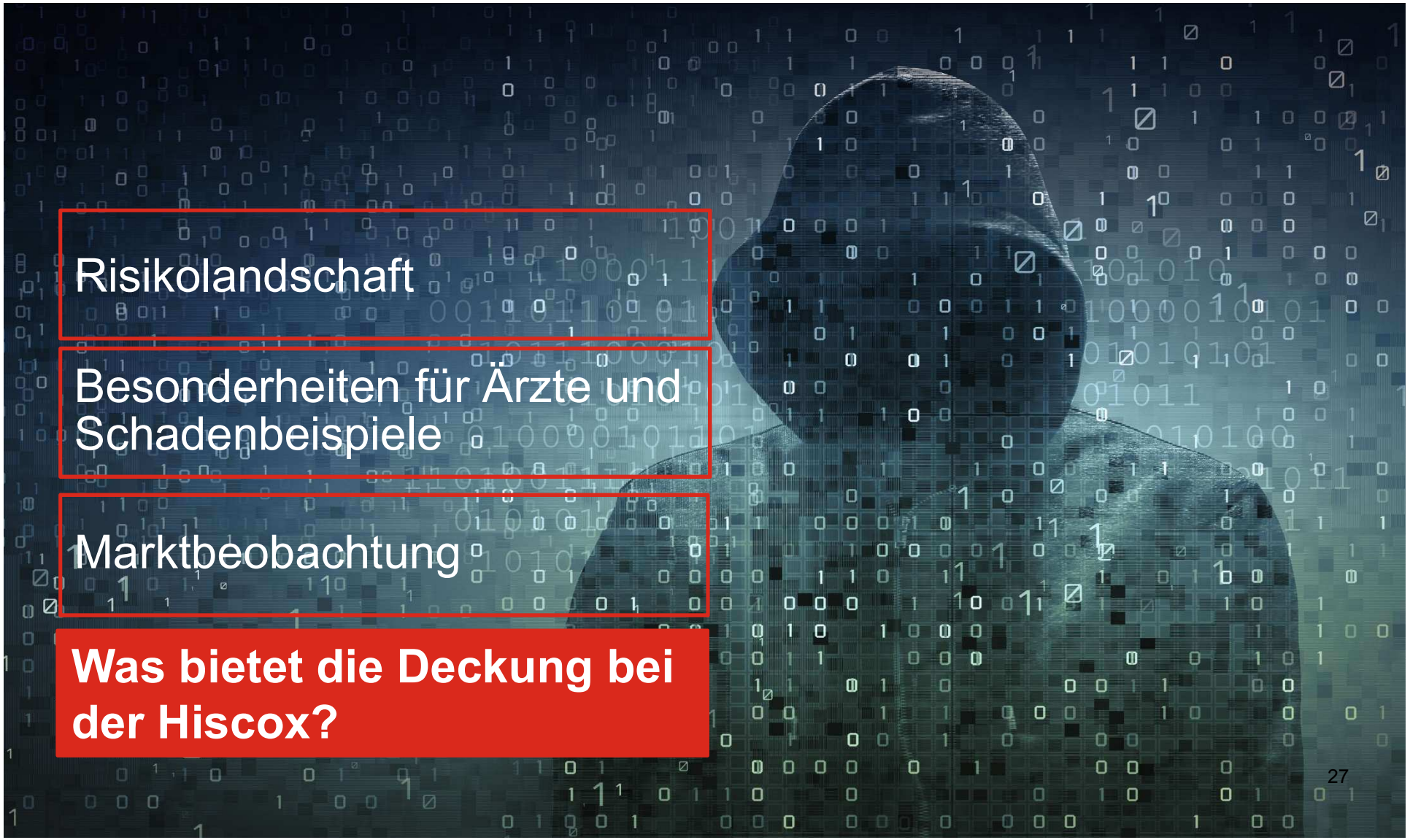
Obliegenheit Datensicherung:
Datensicherung. Der Versicherungsnehmer nimmt mindestens eine tägliche Datensicherung vor, d.h. Duplikate der versicherten Daten und Programme werden angefertigt.

Risikoort:
Versicherungsschutz besteht für die im Versicherungsschein benannten Betriebsgrundstücke.

Marktüberblick –
ein qualitativer volatiler Markt!

rpc VORSORGE KONZEPTE GmbH & Co. KG

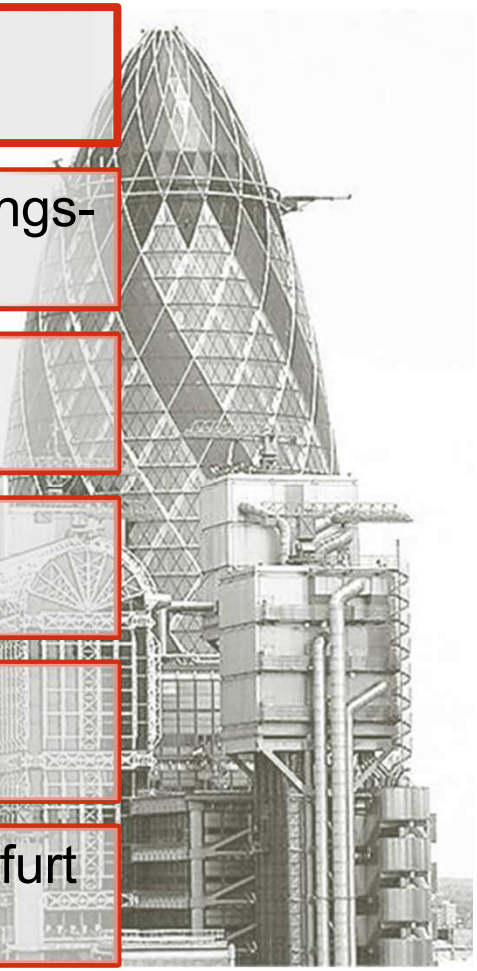
Agenda


Risikolandschaft
Besonderheiten für Ärzte und Schadenbeispiele
Marktbeobachtung
Was bietet die Deckung bei der Hiscox?

Über Hiscox
Hiscox Europe Underwriting Ltd.

Inzwischen eine mehr als 100-jährige Erfolgsgeschichte

- 1901 in London gegründet
- Wichtigstes Einzelmitglied des Versicherungsmarktes „Lloyd‘s of London“
- Hohe Bonität
- Expansion nach Europa und Nordamerika seit den 70er Jahren
- In Deutschland seit 1995
- Niederlassungen in München, Köln, Frankfurt und Hamburg



Wie hilft Hiscox Cyber Risk Management?

VORSORGE KONZEPTE GmbH & Co. KG

Rundum-Versicherungsschutz in einer Police!

Cyber-Haftpflichtversicherung zur Absicherung bei Ansprüchen von Dritten, auch bei Verletzung von vertraglichen Geheimhaltungs-pflichten

Cyber-Eigenschadenversicherung zur Abdeckung intern entstandener Schäden/Kosten (inkl. Klausel med. Geräte)

Umfassende **Assistance** im Versicherungsfall, in Zusammenarbeit mit der HiSolutions AG

Cyber-Haftpflichtversicherung – Was ist versichert?

Schadenersatzansprüche (Vermögensschäden) aufgrund ...

- eines Verstoßes gegen eine **gesetzliche** Bestimmung, die den Schutz von Daten bezweckt
- eines Verstoßes gegen Geheimhaltungspflichten
- eines Verstoßes gegen eine **vertragliche** Datenschutzbestimmung, wie dem BDSG
- der Weitergabe eines Virus (an Dritte)
- ein Denial-of-Service-Angriff auf Dritte
- einer Persönlichkeitsrechtsverletzung

Cyber-Eigenschadenversicherung – Was leistet Hiscox?

Kosten für IT-Forensik	Kosten für PR-Beratung
Rechtsberatung	Betriebsunterbrechungs-schäden (optional)
Benachrichtigungskosten	Vertragsstrafen (PCI)
Kreditüberwachungs-dienstleistungen	Wiederherstellungskosten
Kosten für Krisenmanagement	Sicherheitsverbesserungen

Assistance Dienstleistungen - Was bedeutet das genau?

Assistance Dienstleistungen – Warum ist das wichtig?

Recht	• Ist Ihre Rechtsabteilung für einen Cyber-Vorfall fachlich und personell ausreichend vorbereitet? • Welche externe Expertise wird benötigt und wie stellen Sie sicher, dass diese für Sie jederzeit zur Verfügung steht?
Kommunikation	• Welche Informationspflichten haben Sie nach einem Cyber-Vorfall und wie würden Sie diese konkret erfüllen? • Sind all Ihre Kommunikationskanäle auf einen Krisenfall vorbereitet? • In welcher Form wird im Krisenfall externe Expertise benötigt und in welcher Form ist der Zugang zu diesen Ressourcen organsiert?
Technik	• Wie abhängig sind Sie von Ihrem IT System? • Ist Ihre IT-Abteilung zu jeder Zeit in der Lage, das System wiederherzustellen und eventuelle Probleme zu beheben? • Besteht jederzeit die Fähigkeit in angemessener Zeit zu reagieren? • Bestehen neben dem fortlaufenden Tagesgeschäft auch Kapazitäten das System zu überprüfen und Beweise zu sichern?

Über HiSolutions

HISCOX

HISOLUTIONS

HISOLUTIONS

1992 gegründet | gründergeführt und unabhängig

Hauptsitz Berlin | Zweigniederlassungen in Köln, Bonn und Frankfurt

Über 100 Mitarbeiter

Fokussierter Beratungsspezialist für Security Management und Service Management

Über 300 Kunden in D/A/CH

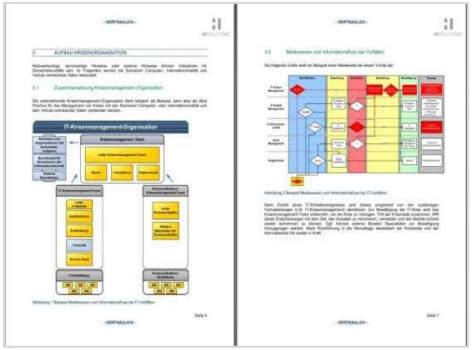
50 % der DAX-Unternehmen | 75 % der deutschen Top20-Banken |
starke Kundenbasis im Mittelstand

Cyber Risk Management by Hiscox
Fokus Assistance Leistungen

rpc VORSORGE KONZEPTE GmbH & Co. KG

Krisenplan

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



Notfallhotline

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

HISOLUTIONS

Mitarbeiter Webinar

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

Cyber Krisenplan - Inhalt

1 **Allgemeiner Teil**
Ziele, Alarmierung, Krisendefinition

2 **Krisenorganisation**
Rollen, Aufgaben, Schnittstellen

3 **Methodik im Krisenstab**
Führungssystem, Lagearbeit, Prinzipien

4 **Erstreaktion**
Checkliste Sofort-maßnahmen

5 **Krisenkommunikation**
Stakeholder, Strategie, Texte

6 **Anhang**
Alarm-/ Gebäudepläne, Templates, Kontaktdaten

Was leistet Hiscox sonst noch? – Cybersecurity Training

Kooperation mit dem Spezialisten für Informationssicherheit, Cybersecurity und Datenschutz – IS-FOX Awareness Programm

Hiscox stellt jedem seiner Kunden kostenlos ein konzipiertes Cyber eLearning Tool für alle Mitarbeiter zur Verfügung.

Cyber-Training für Hiscox-Kunden

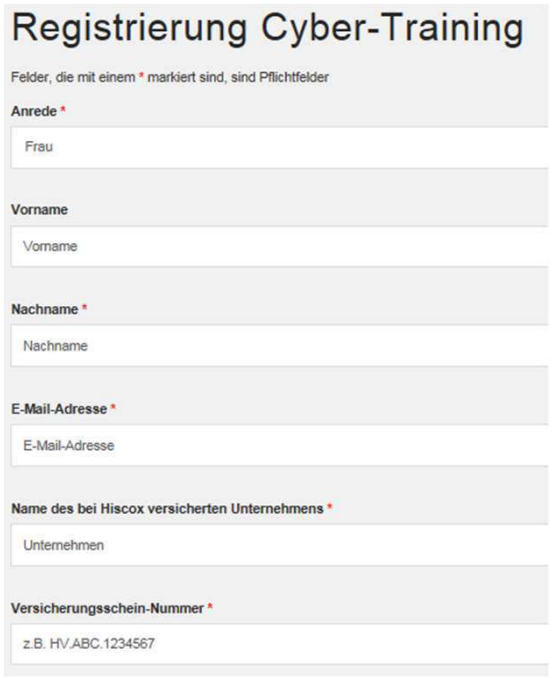
- **Kostenloses Cyber-Training für Hiscox-Kunden:** www.hiscox.de/cybertraining.

Die Inhalte des Cyber-Trainings wurden von der HvS-Consulting AG erstellt, einem spezialisierten Beratungsunternehmen im Bereich „Business Security".

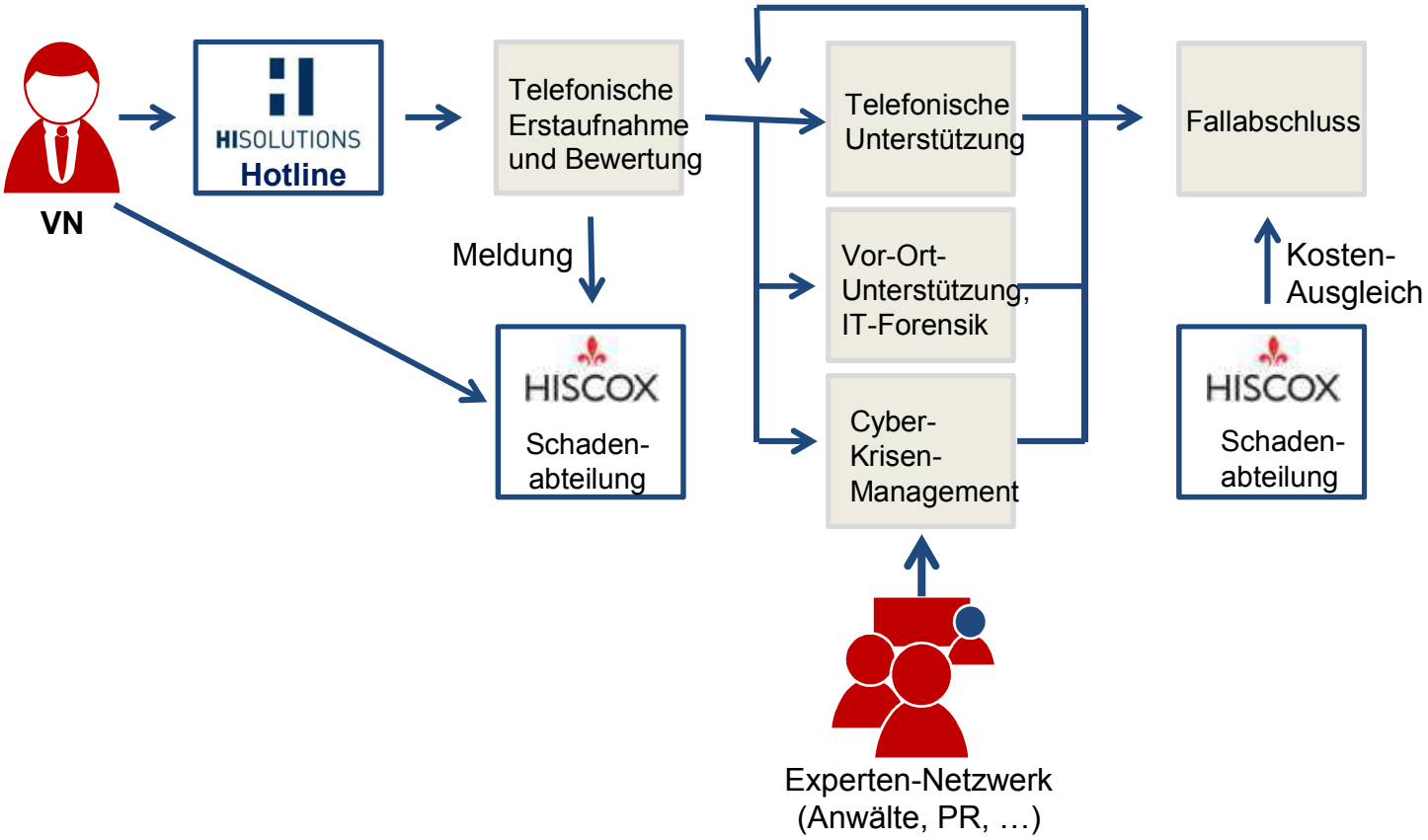
- Phishing erkennen und abwehren
- Sichere Passwörter erstellen und merken
- Social Engineering Angriffe erkennen und abwehren
- Sicheres Verhalten am Arbeitsplatz

Ihre Vorteile

- Sensibilisierung aller Mitarbeiter für digitale Daten-Risiken
- Kostenloses Training
- Spannende Videos und Übungen garantieren hohe Aufmerksamkeit
- Zeit- und Kostenersparnis durch online Training am eigenen PC
- Abschlusstest mit Zertifikat
- Sie brauchen sich nur einmal zu registrieren, die Log-In Daten gelten für alle Mitarbeiter Ihres Unternehmens



Was passiert im Schadenfall? – Die Krisenhotline



Sorgen Sie vor! – Nutzen Sie Ihre Vorteile als Verbandsmitglied!

Bei Fragen und Interesse kontaktieren Sie uns:

Tel: 05347-94968-69

E-Mail: renken@rpc-vorsorgekonzepte.de