



**ALT+PARTNER**  
VERSICHERUNGSLÖSUNGEN

**Anton Alt**



**HISCOX**

**Tobias Knoll**

Linz, 12.04.2018

- 1992 gegründet / 2018 umgegründet
- Unabhängiger Versicherungsmakler und Berater in Versicherungsangelegenheiten
- Assekurateur
- 10 Mitarbeiter/Innen im Innendienst
- Eigene Schadensabteilung
- Netzwerke
- International tätig





## Was sind unsere Ziele?

- Bindeglied zwischen Versicherungsmakler und Versicherungsgesellschaft
- Marktführende und exklusive Versicherungskonzepte entwickeln
- Unseren Kooperationspartnern Zugang zu außergewöhnlichen Versicherungsprodukten zu ermöglichen
  - Bestehende Kundenbeziehungen absichern
  - Neukunden gewinnen



## Unsere Serviceleistungen – Ihre Vorteile

- Angebotslegung und Polizzierung sowie Verkaufsunterlagen in unserem Online-Portal
- Polizzenkontrolle
- Fachliche Unterstützung (Zeit- und Kostenersparnis)
- Unterstützung bei der Schadensabwicklung
- Bei Großkunden: Wenn gewünscht, gemeinsamer Besprechungstermin beim Kunden
- Laufende Webinare
- Bei Bedarf und auf Anfrage: Schulungen, Vorträge
- 100%iger Kundenschutz!



# Hiscox Group

## Über 100 Jahre Erfolg aus London

Hiscox ist seit vielen Jahren wichtigstes Einzelmitglied des Londoner Versicherungsmarktes "Lloyd's of London".

Gründung des **Hiscox Syndicate** in London 1901

Heute **Lloyd's Syndicate 33**

Seit **über 20 Jahren** in Deutschland

## Hiscox – seit 1995 in Deutschland

### Standorte und lokales Underwriting

#### Standorte

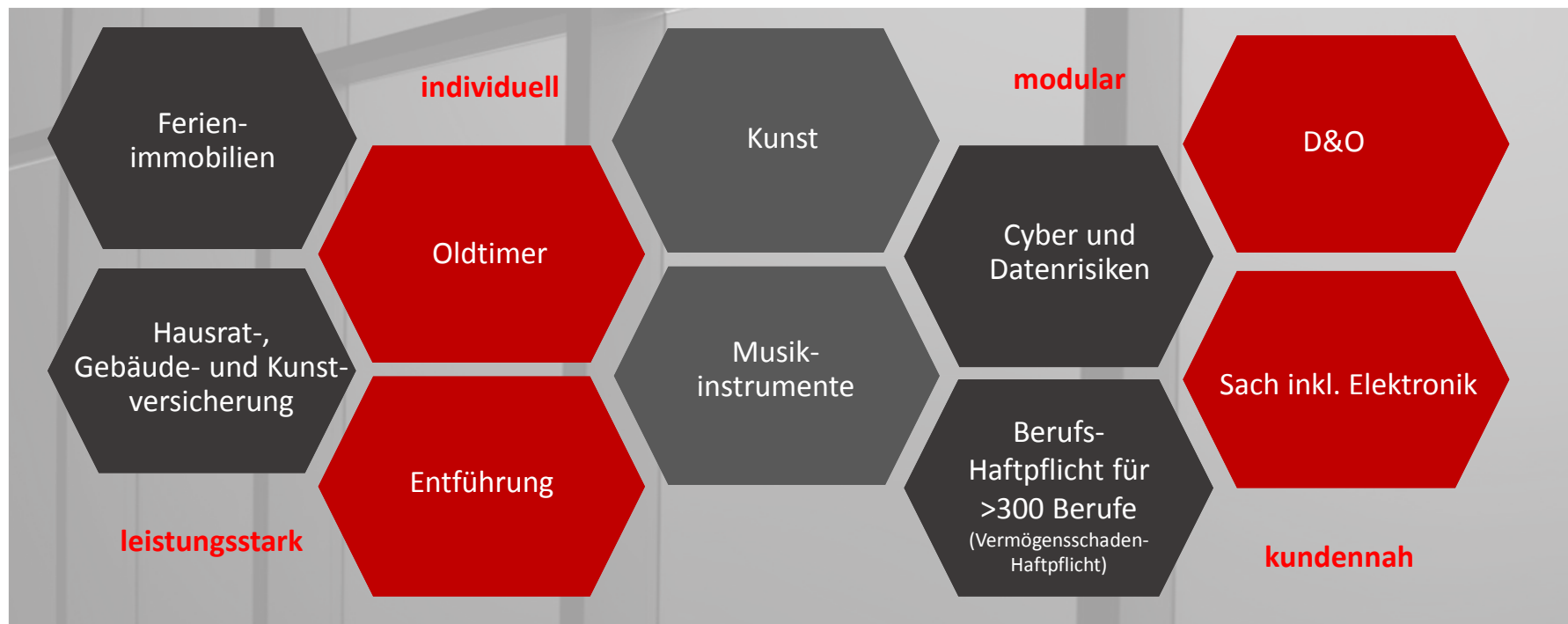
- München
- Köln
- Hamburg
- Frankfurt

#### Lokales Underwriting

- Berlin
- Stuttgart
- Hannover



## Spezialversicherungen für Geschäfts- und Privatkunden



## Highlights der Spezialprodukte

### Sach inkl. Elektronik

1. Haftungssicherheit durch umfassende Allgefahren-Deckung
2. Außenversicherung weltweit auf Allgefahrenbasis
3. Verzicht auf Einwand der groben Fahrlässigkeit bei Schäden bis € 50.000

### D&O

1. Prämienneutrale und unbegrenzte Nachmeldefrist
2. Mitversicherung der gesamten operativen Tätigkeit
3. Abwehrkosten reduzieren nicht die Versicherungssumme

### Berufs- Haftpflicht für >300 Berufe

(Vermögensschadenhaftpflicht)

1. All-Risk Bedingungen
2. Gesetzliche und vertragliche Haftpflichtansprüche
3. Weltweiter Versicherungsschutz
4. Automatische Mitversicherung von Töchtern im EWR

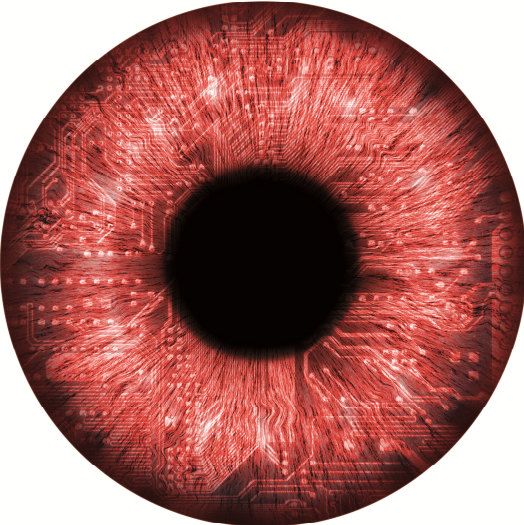
### Betriebs- haftpflicht

1. Offene Deckung
2. Großzügige Sublimits für Schlüsselschäden € 25.000, Mietsachschäden auf Geschäftsreisen € 50.000, Tätigkeitsschäden € 75.000
3. Wird in den VH Vertrag integriert





# Cyber-Versicherung



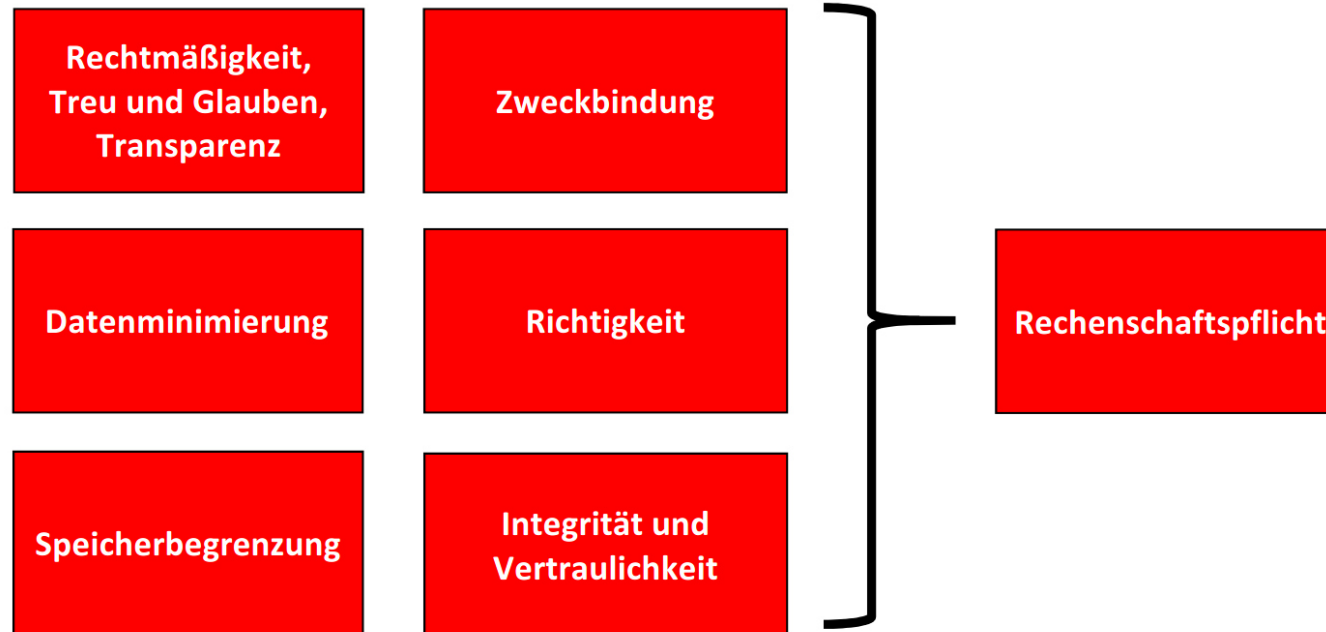


ALT+PARTNER  
VERSICHERUNGSLÖSUNGEN



## DSGVO

### Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten



## DSGVO

**Artikel 13:** Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

**Artikel 30:** Verzeichnis von Verarbeitungstätigkeiten

**Artikel 33:** Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

**Artikel 34:** Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

## DSGVO

### Artikel 82: Haftung und Recht auf Schadenersatz

- Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz...
- Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

## DSGVO Art. 83 – Geldbußen ab 25.5.2018

Verstoß	Höchstbuße	bisher
Grundsätze	20 Mio., bzw. 4 %	€ 25.000,-
Informationspflicht	20 Mio., bzw. 4 %	€ 500,-
Sicherheit der Verarbeitung	10 Mio., bzw. 2 %	€ 10.000,-
Verarbeitungsverzeichnis	10 Mio., bzw. 2 %	€ 10.000,-
Meldepflicht gegenüber Behörde	10 Mio., bzw. 2 %	-
Benachrichtigung Betroffener	10 Mio., bzw. 2 %	-

## DSGVO

### Artikel 83: Allgemeine Bedingungen für die Verhängung von Geldbußen

- Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen für Verstöße gegen die DSGVO in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** ist.

## Erfolgreiche Cyber-Angriffe häufen sich - auch in Österreich: Studie 13.9.2017 von KPMG

- 236 österreichische Unternehmen wurden befragt
- 72 % waren in den letzten Monaten Opfer von Cyber-Angriffen (im Vorjahr waren es noch lediglich 49 %)
- Angriffsquote von 84 % auf Produktionsbetriebe
- Jedes 2. Unternehmen musste in Folge seine Geschäfte unterbrechen
- Fast ein Viertel der Angriffe waren zielgerichtete Cyber-Attacken (Verschlüsselungstrojaner)
- Größtes Sorgenkind: Das Internet der Dinge



**Es gibt keine sicheren Systeme!**

# CyberClear - Versicherung

## Der Aufbau unserer Polizza



### **CyberClear Versicherungsschutz:**

umfassende Hiscox-Leistungen – vorbeugend, mitten in der Krise, bei der Schadenregulierung und bei der anschließenden Sicherheitsanalyse

#### **Cyber-Eigenschadenversicherung:**

- Unterstützung durch IT-Krisenexperten, PR-Berater, Datenschutzanwälte
- Wiederherstellung des IT-Systems und der Daten
- Benachrichtigung der Betroffenen
- uvm.

#### **Cyber-Haftpflichtversicherung:**

- Schutz bei Ansprüchen Dritter in Zusammenhang mit Cyber-Schäden

#### **Werbe-Haftpflicht:**

- Schutz bei Rechtsverletzung durch Werbung und Marketing

#### **Cyber-Betriebsunterbrechung:**

- Schutz und Kostenübernahme bei Unterbrechung des Geschäftsbetriebes durch den Ausfall von IT-Systemen infolge eines Cyber-Vorfalles



#### **Service-Leistungen**

1. Soforthilfe im Notfall
2. Cyber-Training
3. Cyber-Krisenprävention

#### **Rechtsschutz:**

- Abwehrkosten in Bezug auf behördliche Datenschutzverfahren
- Kosten der Wahrnehmung der rechtlichen Interessen bei Einleitung eines Strafverfahrens

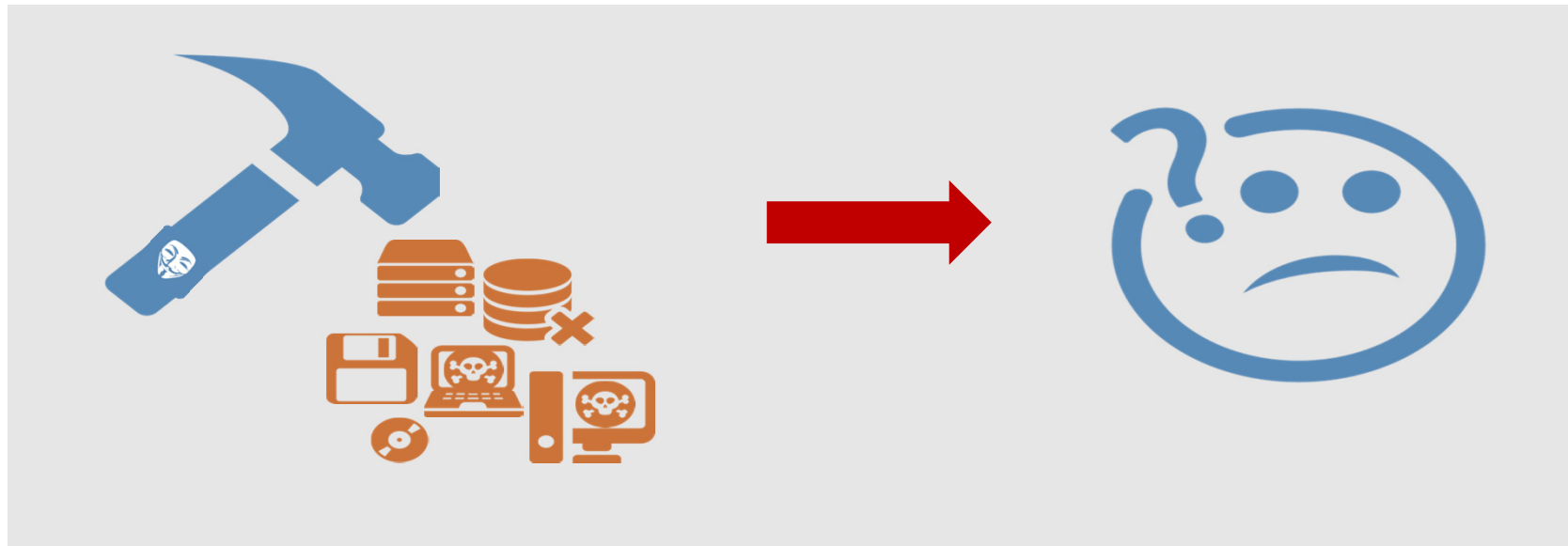




ALT+PARTNER  
VERSICHERUNGSLÖSUNGEN

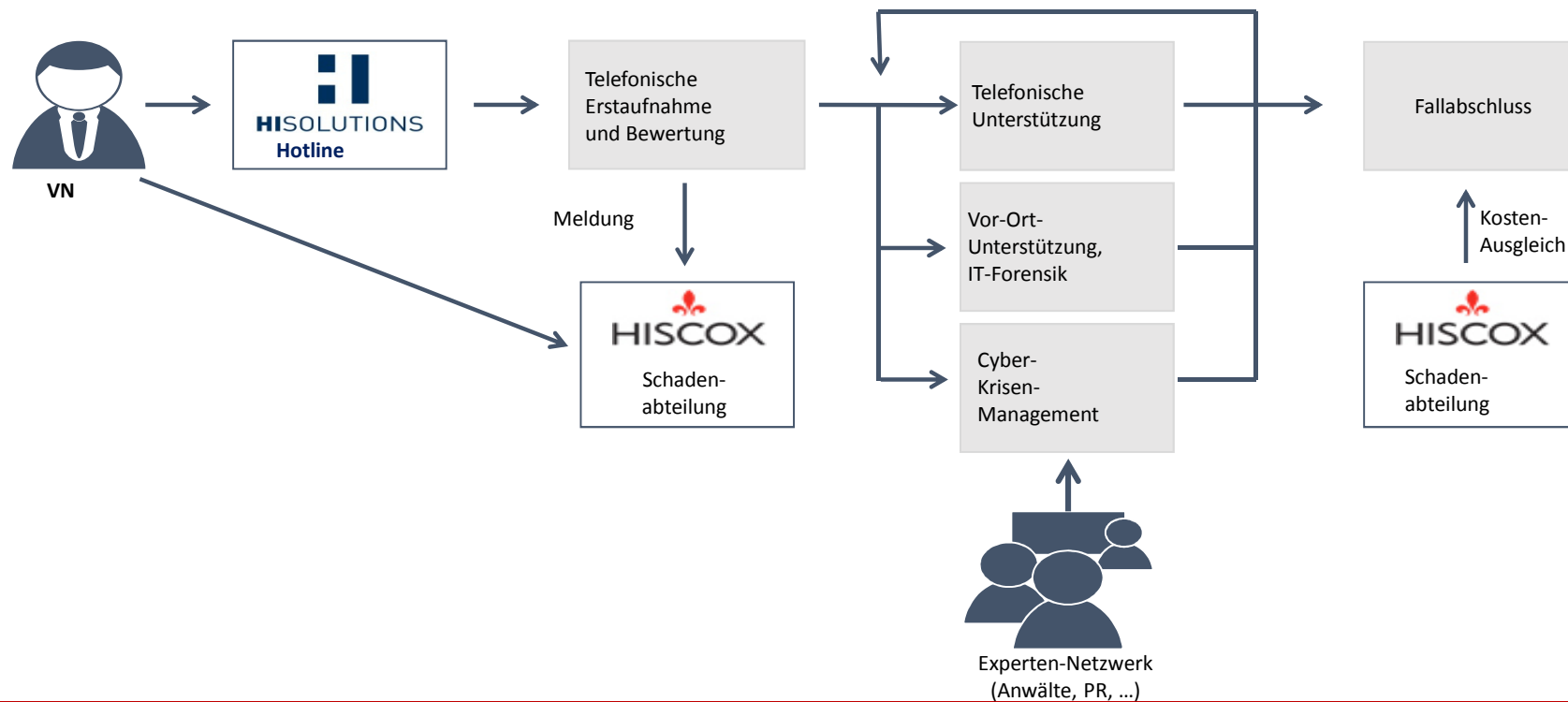


Stellen Sie sich vor, Sie kommen Montagmorgen  
ins Büro und nichts geht mehr...



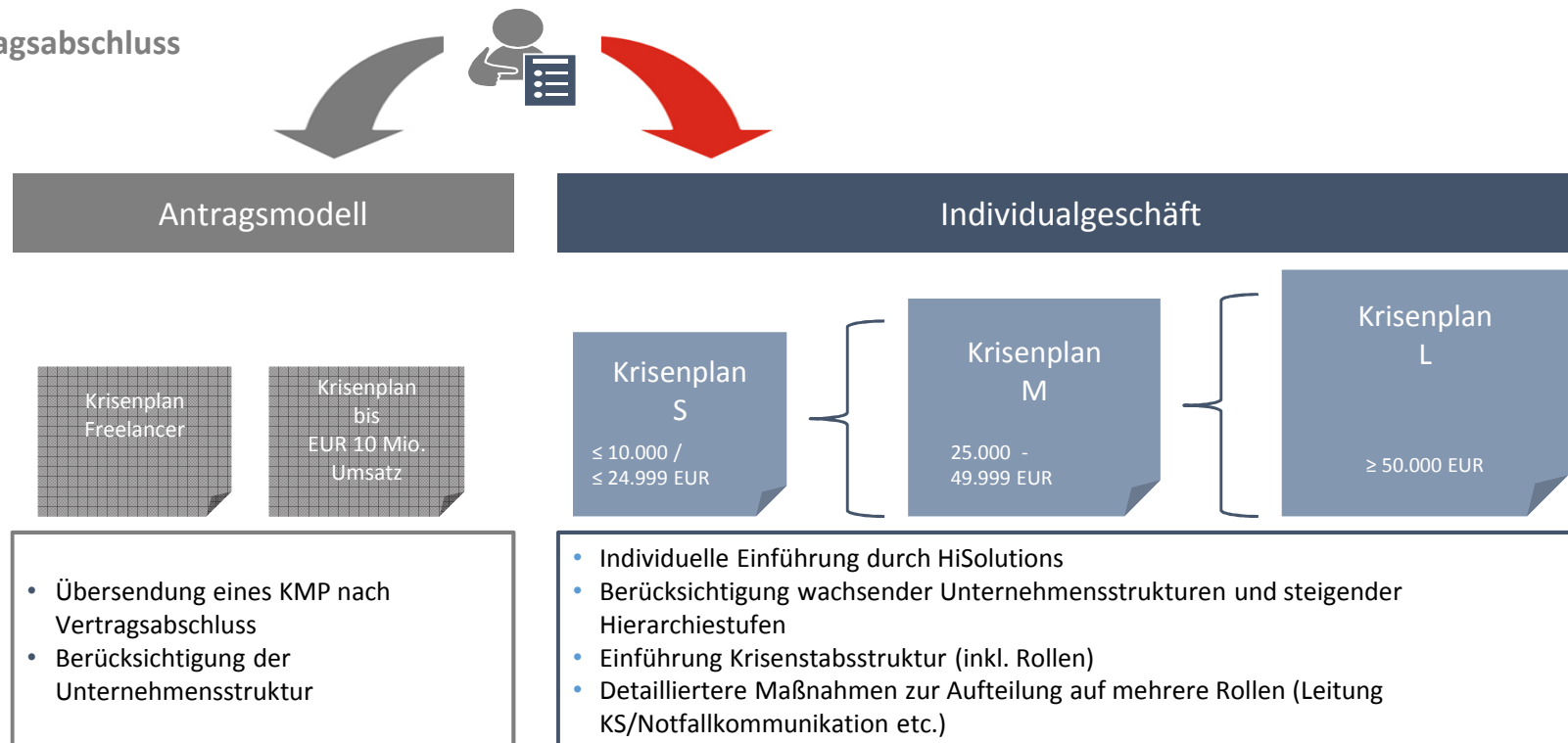
## Soforthilfe in der IT-Krise

### Fallbezogene Unterstützung von Experten







## Mehrere Leistungsstufen: Vom Freelancer bis zum Großunternehmen

Vertragsabschluss



## Der Krisenmanagementplan befähigt die leitenden Mitarbeiter Krisen strukturiert managen zu können

2 CHECKLISTE KRISENSTAB UND -BEWÄLTIGUNG		Bedr.	Dringl.
<b>Sofortmaßnahmen</b>			
Diese Checkliste wird beim ersten Treffen des Krisenstabs verwendet und soll eine allgemeine Struktur vorgeben und die wichtigsten Punkte für alle Vorfälle abdecken.			
<b>Checkliste Krisenstab</b>			
1. Sammeln Sie alle bekannten Fakten zu dem Vorfall.			
• Was ist betroffen?			
• Seit wann?			
• Welche Fehler liegen vor?			
• Was wurde bei dem erstmaligen Auftreten des Fehlers getan?			
2. Treffen Sie alle notwendigen Sofortmaßnahmen, um weitere Schäden abzuwenden.			
• Trennen Sie betroffene Systeme vom Internet und vom Intranetnetz.			
• Schalten Sie betroffene Systeme nicht auf! Das kann die Beweissicherung erschweren.			
• Verändern Sie das betroffene System nicht weiter!			
3. Stellen Sie die Prozessbeurteilung mit Hilfe der Prozessbeurteilung sicher.			
• Notieren Sie alle relevanten Entscheidungen und die Entscheidungsgrundlage.			
• Notieren Sie alle relevanten Informationen.			
• Notieren Sie die Kontakte/Kontaktversuche zu relevanten Dienstleistern und Behörden.			
4. Nehmen Sie Kontakt zur HISOLUTIONS auf. Ggf. auch zur Polizei oder anderen Dienstleistern.			
• Informieren Sie auf jeden Fall Ihren IT-Dienstleister oder IT-Beauftragten.			
<b>Organisation</b>			
5. Verpfändung aller Beschäftigten mit zur Gefahrenhaltung.			
• Die unkontrollierte Verbreitung von Informationen und Gerüchten sollte vermieden werden.			
6. Legen Sie erste Maßnahmen fest, um den Geschäftsbetrieb aufrechtzuerhalten.			
7. Legen Sie mithilfe der Checkliste Krisenkommunikation & Fragen und Antworten* und den Textbausteinen (Fragen & Antworten) fest, wie und von wem kommuniziert wird.			
8. Informieren Sie alle Mitarbeiter über den Vorfall und über die Kommunikationsstrategie.			
• Informieren Sie die Mitarbeiter so umfassend wie nötig (Was ist passiert? Welche Systeme sind betroffen? Was wird mit dem Problem umgegangen?). Als Hilfestellung können die Checkliste Krisenkommunikation verwendet.			
9. Legen Sie langfristige Maßnahmen fest, um den Geschäftsbetrieb aufrechtzuerhalten, bis z.B. die IT wiederhergestellt ist.			
10. Fordern Sie die Wiederherstellung der IT-Systeme. Prüfen sie dabei alle denkbaren Optionen.			
* Cyber-Krisenmanagementplan		Seite 8 von 19	
HISOLUTIONS AG © 2017		Stand: 19. Dezember 2017	

### Rollen und Aufgaben

- Alarmierung und Eskalation
- Aufbau Krisenstab
- Aufgaben der Krisenstabsmitglieder

### Reaktion auf Krisenszenarien

- Checkliste Sofortmaßnahmen
- Checkliste Krisenstabsarbeit (Führungszyklus)

### Unterstützung Krisenkommunikation

- Checkliste Krisenkommunikation
- Wichtige Stakeholder
- Fertige Textbausteine

### Hilfsmittel

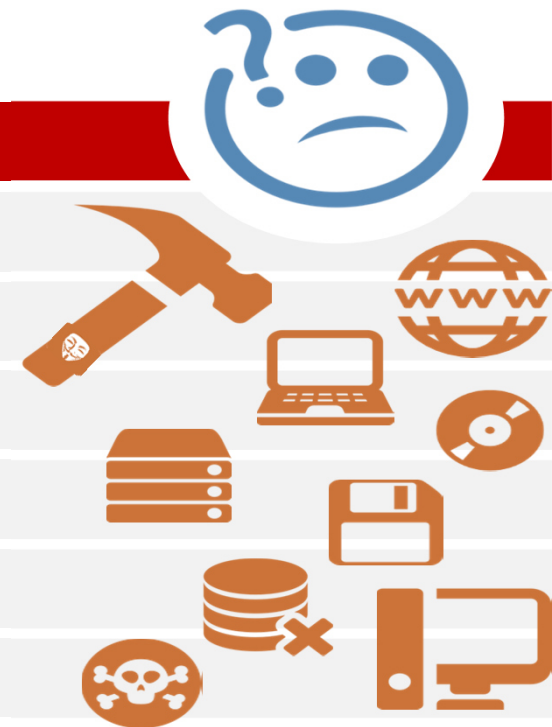
- Weitere Checklisten
- Protokollvorlagen
- Notfallkontakte

# Cyber-Training

Sensibilisierung der eigenen Mitarbeiter zur Cyber

Online-Cyber-Training in Kooperation mit der HvS-Consulting AG

- Phishing erkennen und abwehren
- Sichere Passwörter erstellen und merken
- Social-Engineering-Angriffe erkennen und abwehren
- Sicheres Verhalten am Arbeitsplatz
- Sicher unterwegs
- Umgang mit mobilen Geräten





# Wie kann die Cyber-Versicherung abgeschlossen werden?



ALT + PARTNER ist Ihr Ansprechpartner in allen Fragen



Antragsmodelle bis 10 Mio. EUR



Individualquotierungen



Vereinfachte Anhaltsquotierungen

## Welche Unternehmen können versichert / nicht versichert werden?

### II. TÄTIGKEITSBEREICH DES VERSICHERUNGSNEHMERS

- |   |  |
|---|--|
| <input type="checkbox"/> Hersteller                   | <input type="checkbox"/> Gesundheits- & Heilwesen                                |
| <input type="checkbox"/> Handwerk                     | <input type="checkbox"/> Unternehmensberater, Agenturen                          |
| <input type="checkbox"/> Baugewerbe                   | <input type="checkbox"/> IT-Dienstleister  |
| <input type="checkbox"/> Logistik, Spedition          | <input type="checkbox"/> Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Notare |
| <input type="checkbox"/> (Einzel-)Handel              | <input type="checkbox"/> Architekten, Ingenieure                                 |
| <input type="checkbox"/> Fahrzeughandel und Werkstatt | <input type="checkbox"/> Hausverwalter, Immobilienmakler                         |
| <input type="checkbox"/> Hotel und Gastronomie        | <input type="checkbox"/> Bildung, Schulen  |
| <input type="checkbox"/> Sonstige: _____              | <input type="checkbox"/> Verbände, Vereine                                       |

Sie sind in **keinem** der folgenden Bereiche tätig:

- Finanzdienstleistungssektor (zB Vermittlung von und Beratung zu Versicherungen und Bankprodukten, Vermögensverwaltung, Zahlungsabwicklung, Inkassodienstleistungen)
- Agentur für Kredit-Rating, Direktmarketing, Call Center, Datensammlung und -speicherung (Hauptgeschäftszweck)
- Behörden und sonstige staatliche Einrichtungen, öffentliche Versorgungsunternehmen
- Produzent und/oder Anbieter von pornografischen Inhalten oder Glücksspiel
- Hersteller und Betreiber von mobilen Applikationen und Online-Spielen (Hauptgeschäftszweck)
- Betreiber von Online-Shops, sozialen Netzwerken und Dating-Plattformen
- Franchisenehmer, Franchisegeber
- Flughäfen, Fluggesellschaft

## Nur noch 6 Fragen bis zum Anbot...

2. Sie erwirtschaften maximal 25%, höchstens aber € 500.000 Ihres jährlichen Gesamtumsatzes in U.S.A. oder Kanada.

3. Sie (einschließlich aller Ihrer rechnergestützten Geräte und Computer) bearbeiten, speichern oder übermitteln im Jahr nicht mehr als 20.000 Kreditkartendaten und bestätigen hiermit, dass Sie die Standards gemäß PCI DSS (Payment Card Industry Data Security Standard) einhalten (sofern Kreditkartendaten vorhanden sind)

4. Sie betreiben mindestens die folgenden IT-Schutzmaßnahmen:

- Virenschutz auf allen Servern und Systemen mit aktuellen Virensignaturen
- Firewallstrukturen an allen Netzübergängen zu externen Netzen
- Abgestuftes Rechtekonzept mit administrativen Kennungen ausschließlich für IT-Verantwortliche
- Regelmäßige, (mindestens tägliche) Datensicherung auf separierten Systemen oder Datenträgern

5. Keine Aufsichtsbehörde, staatliche Stelle oder Verwaltungsbehörde hat Klage gegen Sie oder eine mitversicherte Person eingereicht, Ermittlungen eingeleitet oder Auskünfte angefordert, was den Umgang mit sensiblen Daten angeht

6. Sie haben bei Ihren Telefonanlagen und Anrufbeantwortern die Passwörter & PINs von der Werkseinstellung geändert.  
**Diese Frage ist nur zu beantworten, wenn die Zusatz-Deckung Cyber-Diebstahl gewünscht wird.**

7. Aus den letzten 5 Jahren sind keine Schäden durch eine Daten- oder Cyberrechtsverletzung, Hacker-Angriff, Denial-of-Service-Angriff oder Cyber-Erpressung bekannt und Ihnen sind auch keine Umstände bekannt die zu einem Cyber-Versicherungsfall führen könnten



## Welche Obliegenheiten gibt es?

- klares und einfaches Bedingungsmerk
- keine versteckten Klauseln
- Verzicht auf marktübliche Obliegenheiten vor Eintritt des Versicherungsfalles
- keine „Stand der Technik“ oder „Erprobungs“ Klausel

## Beispiele für primäre Obliegenheiten bei anderen Versicherern

- VN hat insbesondere Cyber Angriffe, oder den unerlaubten Zugriff auf Daten und Software zu verhindern
- VN hat sämtliche zumutbaren Vorkehrungen zu ergreifen, um Betriebsunterbrechungsschäden gering zu halten
- Der VN hat alle Herstellerempfehlungen einzuhalten
- VN hat insbesondere Cyber Angriffe, oder den unerlaubten Zugriff auf Daten und Software zu verhindern ⇨ Schadensfall RZ!



**Vielen Dank für Ihre Aufmerksamkeit!**

**Fragen?**