Cyber

–

Was ist das eigentlich?

Cyber – Risiken

Absicherungsmöglichkeiten deutscher Unternehmen

Einblick & Überblick

Arbeitsgruppe VDVM Stand 01.05.2014

Cyber

Eine Definition

INFORMATION INTERNET COMPUTER

Geografie? **Grenzen?** **Regeln?**

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.

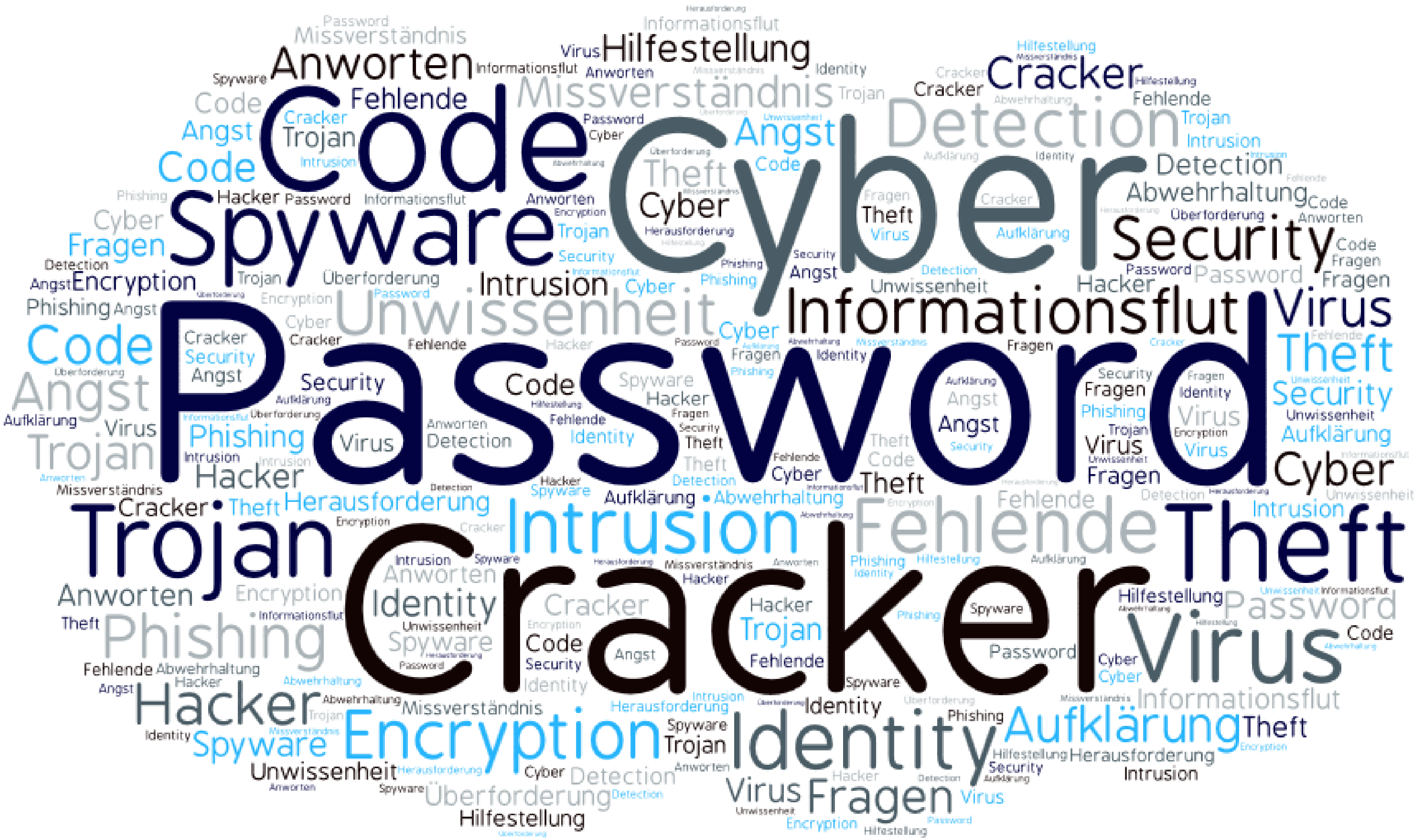
Quelle: Webseite BKA

Deutschland unter Cyber-Beschuss

–

Wo stehen wir?

Bild: Gettyimages


Password
Cracker
Cyber
Code
Spyware
Trojan
Intrusion
Identity
Encryption
Theft
Virus
Informationsflut
Detection
Missverständnis
Unwissenheit
Fehlende
Hilfestellung
Anworten
Security
Hacker
Phishing
Angst
Aufklärung
Fragen
Abwehrhaltung
Herausforderung
Überforderung

03 | Der Schadensfall
Die Cyber-Versicherung

Schadenbeispiele

Die sechs Bausteine

Cyber- und Daten-Eigenschaden

Der Mitarbeiter einer Rechtsanwaltskanzlei öffnet den Anhang einer E-Mail, welcher einen Verschlüsselungstrojaner beinhaltet. Alle Daten auf den Systemen der Kanzlei werden somit unlesbar gemacht. Die Kosten für die IT-Forensik sowie die Entfernung der Schadsoftware und Installation neuer Sicherheitssoftware betragen 26.000 €.

Cyber-Betriebsunter-brechung

Ein Unternehmen wird mit einer Denial-of-Service-Attacke (DOS) angegriffen. Die Plattform und damit verbundene Dienste, sind 2 Tage für Kunden nicht erreichbar. Die Kosten für die Anmietung zusätzlicher Serverkapazitäten sowie die Kosten der Betriebsunterbrechung und Wiederherstellung der ursprünglichen Homepage belaufen sich auf 80.000 €.

Cyber-Zahlungsmittel-schaden

Versicherungsschutz beim Verlust oder der Beschädigung von Kreditkartendaten und -programmen, Verstöße gegen Kreditkartenverarbeitungsvereinbarungen, Verletzungen der PCI Data-Security-Standards oder Verstöße gegenvertragliche Vereinbarungen im Zusammenhang mit Bezahlsystemen.

Schadenbeispiele

Die sechs Bausteine

Cyber-Vertrauens-schaden

Der Mitarbeiter eines Unternehmens hat Zugang zu mehreren Konten seines Arbeitgebers. Dies nutzt er aus, um sich über einen längeren Zeitraum kleine Beträge auf sein Privatkonto zu überweisen. Der über ein Jahr entstandene Schaden beträgt insgesamt 32.000 €.

Cyber-Haftpflicht

Ein Onlinebuchversand stellt kostenlose Leseproben zum Download zur Verfügung. Trotz aller Sicherheitsmaßnahmen wird eine infizierte Datei zum Download angeboten. Die IT-Systeme mehrerer Kunden werden dadurch infiziert. Der entstandene Gesamtschaden beläuft sich auf 30.000 €.

Cyber-Forderung

Ein Hacker verschafft sich Zugriff auf die IT-Systeme eines Steuerberaters und verschlüsselt wichtige Mandanten-Daten. Kurze Zeit später erhält der Steuerberater eine E-Mail mit der Forderung, den Betrag in Höhe von 8.000 € in Form von Bitcoins zu zahlen.

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 – 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.

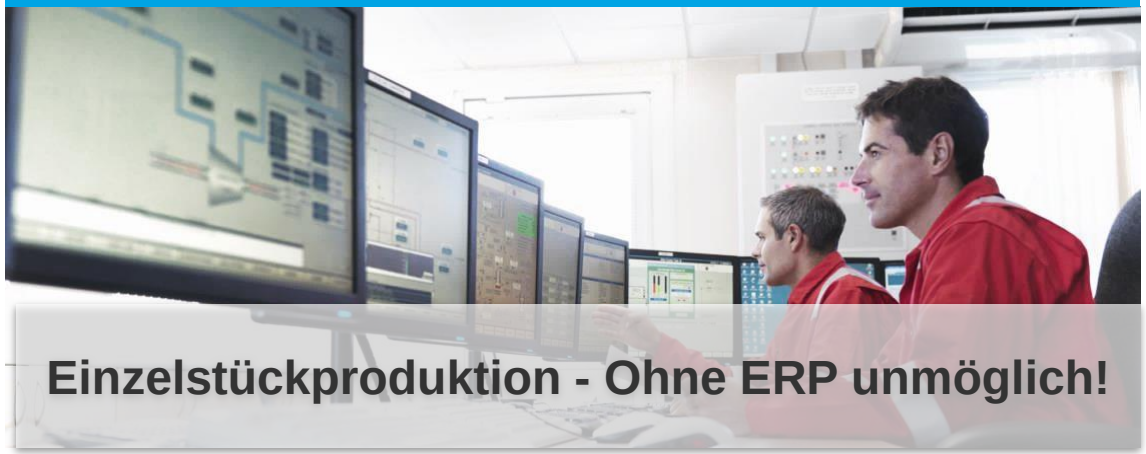
Folgende Kosten sind entstanden:

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

Konsequenzen für den Mittelstand

Potenzielle Auswirkungen

Beispiel | Fensterglasproduzent

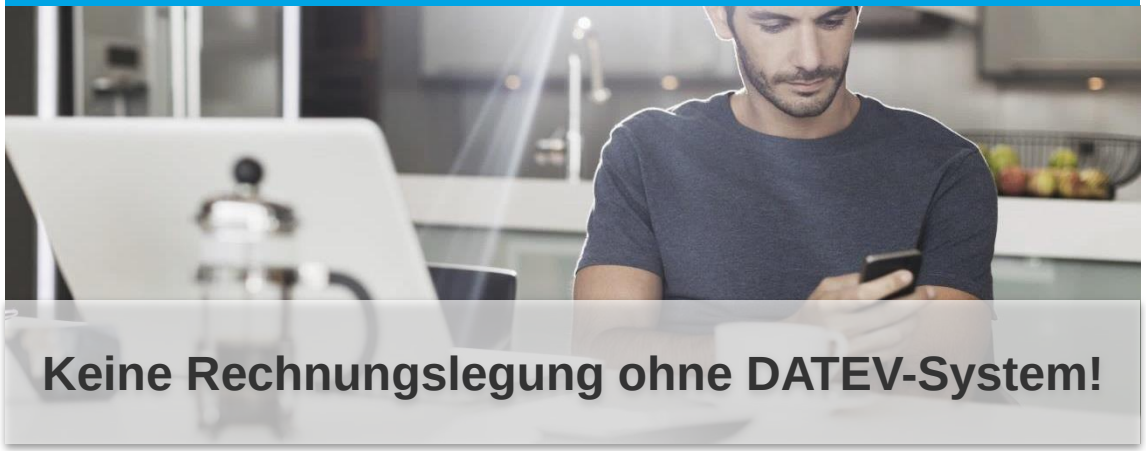


Einzelstückproduktion - Ohne ERP unmöglich!

Beispiel | Lebensmittelproduzent

Ohne Etikett und IT-Warenvoranmeldung keine Annahme im Distributionszentrum!

Beispiel | Naturkosmetikproduzent



Keine Rechnungslegung ohne DATEV-System!

Beispiel | Werbeagentur

Genau die Werbung die sie wollen!

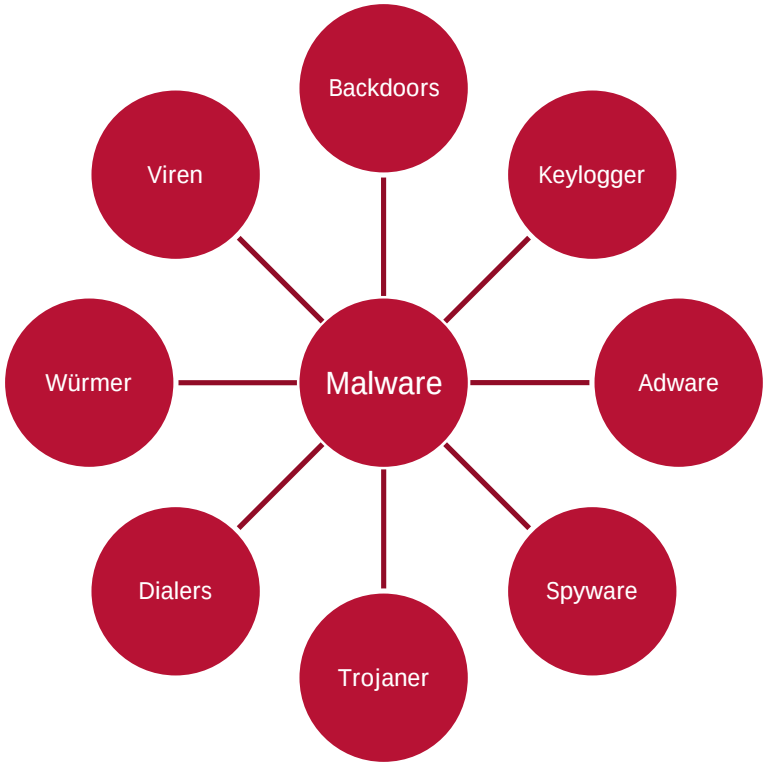
Bilder: Gettyimages

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

Die Cyber Gefahren

Infektion durch Schadsoftware



- **Infektion** der IT Systeme mit Schadsoftware, insbesondere Viren und Trojaner
- Hierdurch können Cyber-Eingriffe auf die **eigenen** IT Systeme ermöglicht werden
- Versehentliche Übermittlung von **Schadsoftware an Dritte kann zu Haftpflichtansprüchen führen**
- Viele Infektionen führen zu Straftaten, manche sind jedoch **willkürlich,** um einfach nur Schaden zu verursachen.

EU DSGVO I

Die neue Datenschutz-Grundverordnung

Am 25.05.2018 endet die zweijährige Übergangsfrist. Ab diesem Zeitpunkt müssen Unternehmen die Anforderungen der EU-DSGVO umgesetzt haben. Die EU-DSGVO erfordert keine Umsetzung in nationales Recht.

Für wen gilt die EU-DSGVO?

- Alle Unternehmen in der EU welche personenbezogene Daten verarbeiten (auch Niederlassungen ausländischer Firmen)

Was sind die Ziele der EU-DSGVO?

- Vereinheitlichung des Datenschutzrechtes innerhalb der EU
- Präzisierung der Rechte von betroffenen Personen
- Mehr Kontrolle über eigene Daten

Was ist neu?

- Neue Difinition besonderer Daten (genetische Daten, Profiling, Daten von Kindern)
- Recht auf Löschung
- Erhöhte Sicherheitsstandards und Zertifizierungen
- Erhohung der Bußgelder auf 4% des weltweiten Umsatzes oder € 20 Mio.!

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.

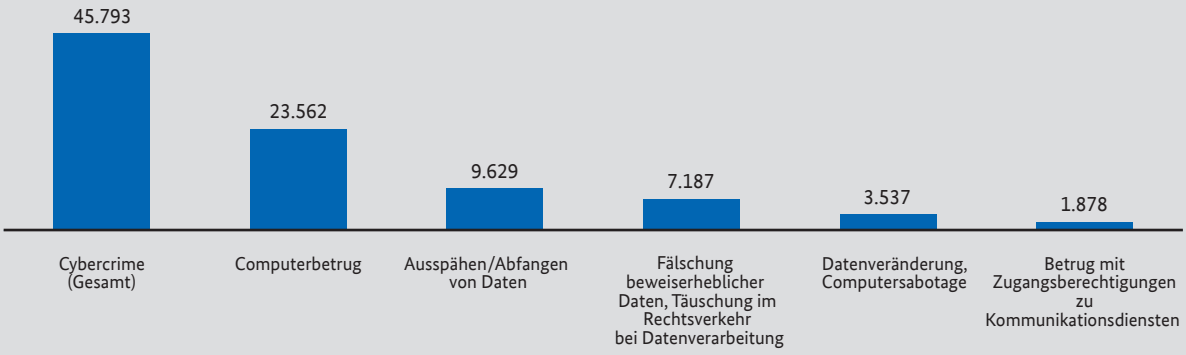
Eigenschäden	Sach / TV	Haftpflicht	K&R	VSV	Cyber
Wiederherstellungskosten Daten / Programme	✓	⊘	⊘	⊘	✓
Benachrichtigungskosten	⊘	⊘	⊘	⊘	✓
Betriebsunterbrechungsschäden	?	⊘	⊘	⊘	✓
Kosten für IT-Forensik	⊘	⊘	⊘	✓	✓
Wiederherstellungskosten nach Hackerangriff	?	⊘	⊘	✓	✓
Kosten Sicherheitsberater	⊘	⊘	⊘	?	✓
Kosten 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	⊘	?	⊘	⊘	?

Fallzahlen

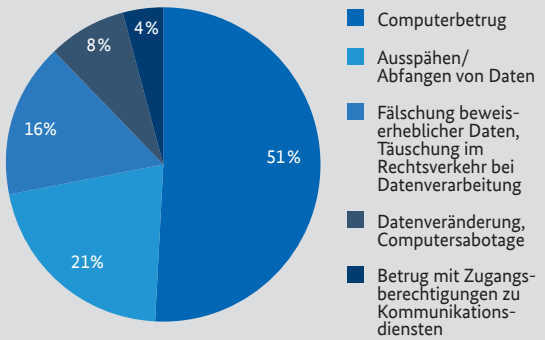
Für das Jahr 2015 registrierte die PKS insgesamt 45.793 Straftaten im Bereich Cybercrime im engeren Sinne.

Cybercrime im engeren Sinne 2015



Für die einzelnen Phänomenbereiche ergibt sich daraus folgende prozentuale Verteilung:

Cybercrime im engeren Sinne 2015 (prozentuale Verteilung)



Der **Computerbetrug** (§ 263a StGB) erfasst insbesondere die Verwertungshandlungen des Phishing (beispielhaft: Initiierung missbräuchlicher Transaktionen im Online-banking unter Nutzung von Schadsoftware), Trans-aktionen unter Nutzung missbräuchlich erlangter Kreditkartendaten und den Einsatz gestohlener oder gefälschter Zahlungskarten am Geldautomaten oder Point-of-Sale (POS)-Terminal.

Das **Ausspähen und Abfangen von Daten** (§§ 202a, 202b StGB) erfasst den „Diebstahl" digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden in der Regel als Handelsware in der „Underground Economy"[02] zum Kauf angeboten und täterseitig missbräuchlich einge-setzt. Die Verwertung erfolgt damit in zwei Stufen, dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.

Der Straftatbestand der **Fälschung beweiserheblicher Daten bzw. der Täuschung im Rechtsverkehr** (§ 269 StGB) erfasst die Täuschung (einer Person) durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies geschieht z. B. durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten oder Firmen. Mit überzeugenden Legenden soll das Opfer z. B. zur Preisgabe von Account-Informati-onen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Ebenso erfasst ist das Zusenden von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.

Bei dem Delikt **Datenveränderung / Computersabotage** (§§ 303a, 303b StGB) handelt es sich um eine Art digitale „Sachbeschädigung". Es wird die Veränderung von Daten in einem Datenverarbeitungssystem bzw. das Verändern des Systems durch andere als den Dateninhaber unter Strafe gestellt. §§ 303a, 303b StGB umfassen typischer-weise die Denial of Service-Angriffe (DoS-, DDos-An-griffe[03]), ebenso fällt darunter die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art (Trojanische Pferde, Viren, Würmer usw.).

02 Überregionale Online-Schwarzmärkte, oft im sogenannten Darknet, über die Anbieter und Käufer ihre kriminellen Geschäfte rund um die digitale Welt anbahnen und abwickeln können.

03 Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern (Quelle: BSI – Die Lage der IT-Sicherheit in Deutschland 2015 - Glossar).

Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2015

Fallbeispiel Botnetze:

Anfang Dezember 2016 konnte durch eine zeitgleich erfolgte Beschlagnahme von 39 Servern und mehreren Hunderttausend Domains nach mehr als vier Jahren intensiver Ermittlungsarbeit von Cyber-Experten aus Polizeien und anderen Behörden in 41 Staaten die wohl weltweit größte Infrastruktur zum Betrieb sogenannter Botnetze aufgedeckt und analysiert werden. Dadurch ist Cyberkriminellen allein in Deutschland die Kontrolle über mehr als 50.000 infizierte Computer entzogen worden.

Mindestens seit 2009 haben Täter die weltweit vernetzte Botnetz-Infrastruktur „Avalanche“ für das Versenden von E-Mails, die schadhaften Code enthalten haben, genutzt. In 180 Staaten wurden Opfer festgestellt. Bei „Avalanche“ handelte es sich nach bisheriger Einschätzung um die weltweit größte Infrastruktur zum Betrieb eines Botnetzes.

Allein auf der Führungsebene dieser kriminellen Vereinigung konnten 16 Beschuldigte identifiziert werden. Gegen sieben Tatverdächtige in Deutschland wurden Haftbefehle wegen des Verdachts der Bildung einer kriminellen Vereinigung, des banden- und gewerbsmäßigen Computerbetrugs und anderer Straftaten erlassen.

Die Exekutivmaßnahmen wurden von den deutschen Dienststellen koordiniert und durch Eurojust und Europol zeitgleich in zehn Staaten unterstützt. An den Ermittlungen beteiligt waren neben dem US-amerikanischen Federal Bureau of Investigation (FBI) weitere US-amerikanische sowie europäische und außereuropäische Behörden.

Kurzbewertung:
Die quantitative wie qualitative Ausgestaltung von kriminellen Infrastrukturen erreicht ein immer größeres Ausmaß. Der Fall verdeutlicht die Erforderlichkeit von internationalen Kooperationen im Phänomenbereich Cybercrime, um derartige Infrastrukturen erfolgreich bekämpfen zu können.

Angriffe auf die Verfügbarkeit von Webseiten, Internetdiensten und Netzwerken (DDoS-Angriffe[24])

Eng verknüpft mit der Thematik Botnetze sind die „DDoS-Angriffe“. Die in einem Botnetz zusammengeschlossenen Rechner sind die zentrale Ressource zur Durchführung von DDoS-Angriffen. Ziel dieser ist es, die Verfügbarkeit von Webseiten, einzelner Dienste oder auch von ganzen Netzen in der Regel zu sabotieren.

DDoS-Angriffe gehören zu den am häufigsten beobachteten Sicherheitsvorfällen im Cyber-Raum. Kriminelle haben hieraus entsprechende Geschäftsmodelle entwickelt und vermieten Botnetze verschiedener Größen.

Statistische Daten zu Anzahl und Dauer von DDoS-Angriffen in Deutschland liegen im BKA nicht vor. Das BSI berichtet in seinem Jahresbericht 2016, dass sich die maximale Bandbreite von Einzelangriffen gesteigert hat[25].

Die Nichterreichbarkeiten von Vertriebsportalen wie beispielsweise Online-Shops in Folge eines DDoS-Angriffs kann gerade im wettbewerbsintensiven Marktsegment Internet erhebliche wirtschaftliche Schäden nach sich ziehen. Die Motivlagen der Täterseite reichen von rein monetären Interessen (Erpressung) oder dem Erlangen von Wettbewerbs-

24 Vgl. Fußnote 5.

25 BSI – Bericht „Die Lage der IT-Sicherheit in Deutschland 2016“.

Bundeskriminalamt

BKA

Cybercrime

Bundeslagebild 2016

Cybercrime-Straftaten in Deutschland

82.649 Fälle von Cybercrime im engeren Sinne (+80,5 %*)

253.290 Fälle mit dem Tatmittel Internet unter allen in der PKS erfassten Straftaten (+3,6 %)

972 Fälle von Ransomware (+94,4 %)

2.175 Fälle von Phishing im Onlinebanking (-51,4 %)

22 OK-Verfahren im Deliktsbereich Cybercrime (4 % aller OK-Verfahren)

Cybercrime ist transnationale Kriminalität

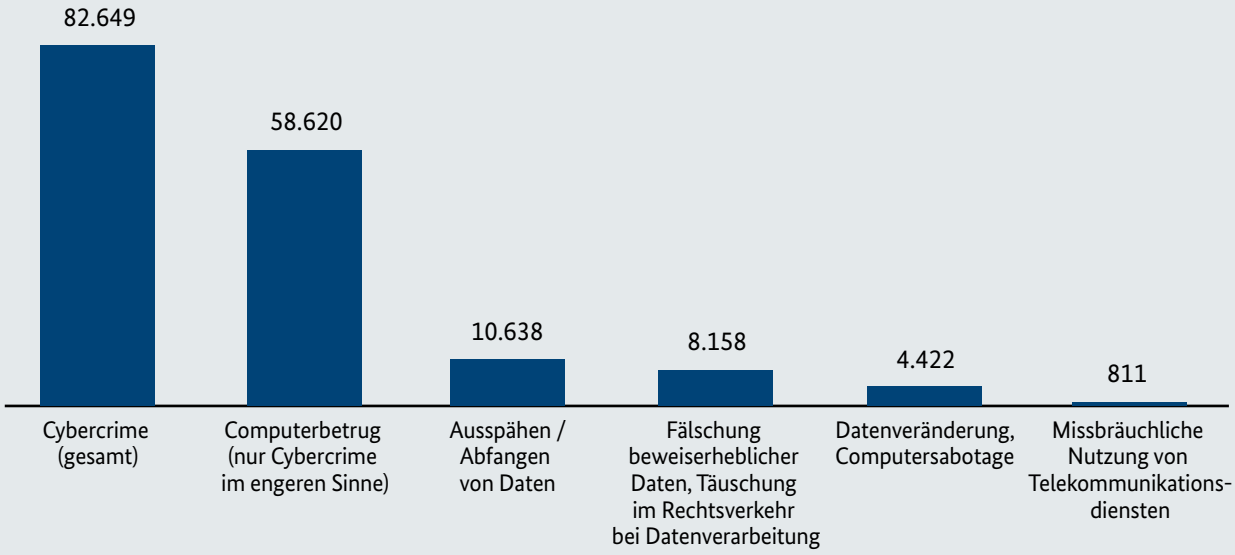
Zunehmende Professionalisierung der Täter, neue Tatgelegenheiten und Modi Operandi

Vermehrte Nutzung von Anonymisierungsdiensten

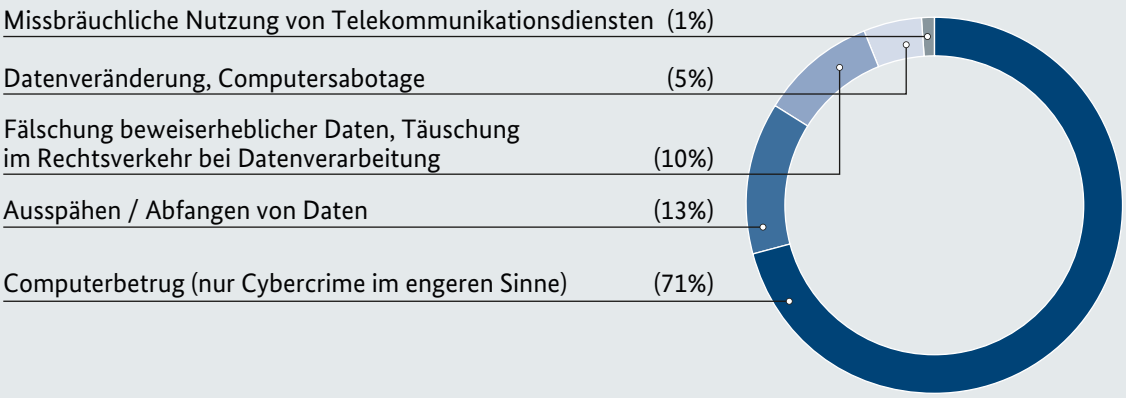
* Siehe hierzu Anmerkungen auf S. 5

zung von Telekommunikationsdiensten intendiert, wurden mit zunehmender Bedeutung des Internets im Wirtschaftsleben tatsächlich darunter auch viele andere Betrugsdelikte erfasst, bei denen Kommunikationsdienste zwar eine Rolle spielten, deren Nutzung alleine aber keine strafbare Handlung begründete und mithin ein anderer Erfassungsschlüssel einschlägig gewesen wäre.

Cybercrime im engeren Sinne (2016)



Cybercrime im engeren Sinne - prozentuale Verteilung (2016)



Was kostet Cyberschutz?

Machen Sie den Vergleich!

2016 bereits 36.000 Cyberattacken
und 50 Mrd. Euro Schaden!
2017 ist die Zahl um 500% gestiegen.

B-Haftpflicht + Cyber Spezial

Anderen immer einen Schritt voraus!
Fragen Sie nach einem Angebot!

G|O|V
Versicherungsmakler

VEMA PARTNER

Weitere Informationen am Messestand!
www.gov-mbh.de

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 (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.

Cyber-Risiko steuern

Risikoanalyse

- Kritische IT-Abhängigkeiten?
- Angriffsfläche für Cyber-Kriminelle?
- Technische Schwachstellen?

Maßnahmen und Vorbereitung

- Maßnahmen machen Risiko beherrschbar!
- Vorbereitung auf den Ernstfall!

Versicherungsbedarf

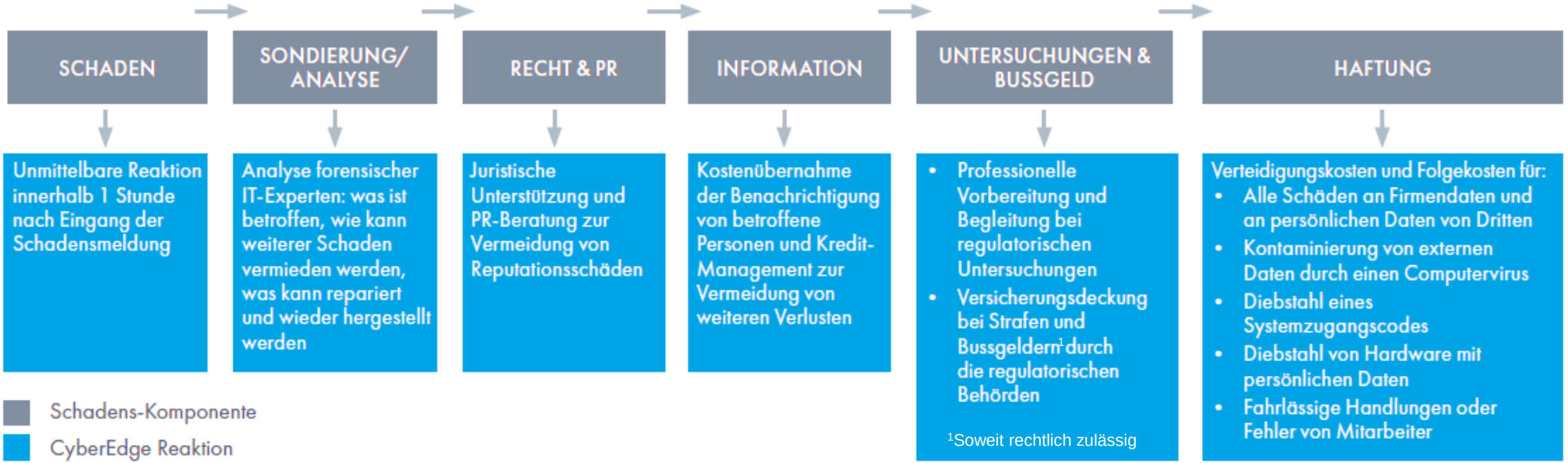
- Transfer angemessener Cyber-Risiken
- Assitance-Leistungen – Hilfe im Ernstfall

AIG

AIG CyberEdge – Ablauf eines Cyberschadens

Deckungsbausteine in Anlehnung an die verschiedenen Stationen eines Cybervorfalles

Wir helfen Ihnen, schnell und umfassend auf einen Vorfall zu reagieren.



CyberEdge Wording

–

Kleinigkeiten machen den Unterschied

AIG Cyber

Unser Wissen ist ihr Vorteil

1 Fachkompetenz

- Cyber seit 1999
- Lokalisierte Policen
- Sehr großes Portfolio weltweit
- Schadenerfahrung
- Produktevolution und Innovation
- Unterstützung für Broker

2 Risikoappetit

- alle Branchen
- Kapazität bis 25 Mio. €
- Unternehmen jeder Größe

3 Erprobte „proaktive Maßnahmen“

- Sofortige Verfügbarkeit
- IT- / Krisenmanagement
- Juristische Beratung
- Multijurisdiktional
- Ohne Selbstbehalt (48h/72h)

AIG KPMG

Norton Rose Fulbright

AIG

F. VERSICHERTER ZEITRAUM

1. Vorwärtsversicherung, Rückwärtsversicherung und Ausschluss bekannter Verstöße

Der Versicherungsschutz umfasst für die Bausteine A.1 - A.5 alle während der Dauer des Versicherungsvertrags eintretenden Versicherungsfälle.

Für die Cyber-Haftpflicht gemäß A.6 bezieht sich der Versicherungsschutz auf Versicherungsfälle, die während der Dauer des Versicherungsvertrags eintreten und auf Verstößen beruhen, welche während der Dauer des Versicherungsvertrags begangen wurden.

Versicherungsschutz besteht auch für Versicherungsfälle, die während der Dauer des Versicherungsvertrags eintreten und auf Verstößen beruhen, die vor Beginn des Versicherungsvertrags begangen wurden, ausgenommen wenn dem Versicherungsnehmer und/oder einer versicherten Person der Verstoß zum Zeitpunkt der Abgabe der Vertragserklärung des Versicherungsnehmers bekannt war oder hätte bekannt sein müssen.

2. Nachmeldefrist für die Cyber-Haftpflicht

Versicherungsschutz besteht nur für Haftpflichtversicherungsfälle gemäß dem Baustein A.6., die dem Versicherer nicht später als 10 Jahre nach Beendigung des Versicherungsvertrags gemeldet werden.

1.7 Verstöße gegen Namens- und Persönlichkeitsrechte

Der Versicherer gewährt dem Versicherungsnehmer Versicherungsschutz für die Verletzung von Namens- und Persönlichkeitsrechten sowie daraus entstehende immaterielle Vermögensschäden.

1.8 Verstöße durch Werbung und Marketing

Der Versicherer gewährt dem Versicherungsnehmer für Rechtsverletzungen durch Werbung und Marketing, insbesondere Marken-, Urheber-, Lizenz- und Domainrechte, wenn im Zusammenhang mit Veröffentlichungen zu Werbe- und Marketingzwecken für die Produkte oder die Dienstleistungen des Versicherungsnehmers Rechte Dritter verletzt werden.

MARKEL®

HISCOX

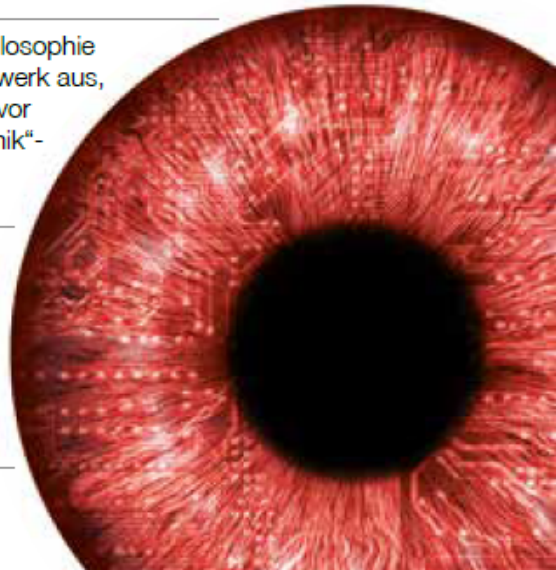
Hiscox CyberClear

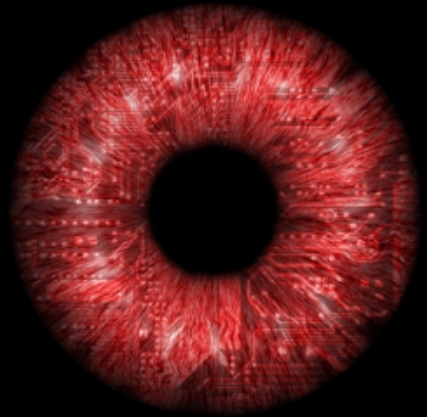
Rundum-Schutz und außergewöhnliche Assistance-Leistungen bei Hacker-Angriffen und IT-Ausfällen

Bereits seit 2011 bietet Hiscox eine umfassende Cyber-Versicherung für Geschäftskunden und war damit der erste Versicherer mit einer solchen Deckung auf dem deutschen Markt. Hiscox schützt kleine und mittelständische Unternehmen – vorbeugend, mitten in der Krise, bei der Schadenregulierung und einer nachgelagerten Sicherheitsanalyse.

Produkt-Highlights

- **Cyber-Eigenschaden, Cyber-Haftpflicht und Cyber-Betriebsunterbrechung in einer Allround-Deckung:** Hiscox CyberClear umfasst eine Cyber-Eigenschadendeckung, eine Cyber-Haftpflicht- und Werbe-Haftpflichtversicherung sowie Schutz bei einer Cyber-Betriebsunterbrechung. Optional ist die Police um die Betriebsunterbrechung bei Cloud-Ausfall, Cyber-Diebstahl und Vertragsstrafen bei verzögerter Leistungserbringung erweiterbar.
- **Außergewöhnliche Assistance- und Service-Leistungen:** Hiscox kooperiert exklusiv mit dem IT-Sicherheitsexperten HiSolutions AG, PR-Spezialisten und spezialisierten Datenschutzanwälten. Sie unterstützen präventiv und agieren im Ernstfall wie ausgelagerte Cyber-Krisenabteilungen. Kostenfreie Cyber-Schulungen und ein Cyber-Krisenplan sind integrale Bestandteile der vielseitigen Hiscox Services.
- **Erstattung von Ertragsausfall und Mehrkosten:** Ertragsausfälle und Mehrkosten werden übernommen, wenn eine Netzwerksicherheitsverletzung (z. B. durch einen Hacker-Angriff, eine Infektion durch ein Schadprogramm oder einen Denial-of-Service-Angriff), ein Bedienfehler, eine Datenrechtsverletzung oder eine Cyber-Erpressung zum teilweisen oder kompletten Stillstand des Betriebs führen.
- **Umfassender Schutz physischer und elektronischer Daten:** Ob Laptop, Smartphone oder Papierakte – Hiscox leistet, wenn physische oder elektronische Daten abhandengekommen, nicht mehr verfügbar sind oder missbraucht wurden. Der Versicherungsschutz umfasst personenbezogene, persönliche und auch geschäftliche Daten.
- **Übernahme von Cyber-Eigenschäden und Kosten:** Hiscox erstattet seinen Kunden u. a. Eigenschäden wie Kosten für Krisenberatung, IT-Forensik, begleitende PR-Maßnahmen, die Wiederherstellung der Daten und des IT-Systems (inkl. Wiederherstellungskosten für IT-Hardware), die Kosten für die Benachrichtigung der Betroffenen sowie die Aufwendungen für Datenschutzanwälte, Strafrechtsschutz und eine nachgelagerte Sicherheitsanalyse.
- **Abwehr unberechtigter und Erfüllung berechtigter Haftpflichtansprüche:** Der Versicherungsschutz bietet die Abwehr unberechtigter Forderungen (passiver Rechtsschutz) sowie die Erfüllung berechtigter Ansprüche, die von Dritten aufgrund einer Netzwerksicherheitsverletzung, eines Bedienfehlers, einer Datenrechtsverletzung oder einer Cyber-Erpressung erhoben wurden.
- **Schutz bei Abmahnungen und Urheberrechtsverletzungen:** Mit der eingeschlossenen Werbe-Haftpflicht hilft Hiscox im Falle einer Verletzung von Urheber- und Persönlichkeitsrechten. Dies ist z. B. der Fall, wenn eine Bildrechtsverletzung auf der eigenen Internetseite abgemahnt wird.
- **Einfaches Bedingungswerk im Sinne des Kunden:** Gemäß der Hiscox Philosophie zeichnet sich Hiscox CyberClear durch ein klares und einfaches Bedingungswerk aus, das keine versteckten Klauseln enthält und auf marktübliche Obliegenheiten vor Eintritt des Versicherungsfalles verzichtet – so gibt es keine „Stand der Technik"- oder „Erprobungs"-Klausel. Ebenso verzichtet Hiscox auf eng gefasste Definitionen – beispielsweise des IT-Systems.
- **Umfassendes Deckungskonzept:** Die Grunddeckung von Hiscox CyberClear enthält alle elementaren Deckungsbausteine und leistet vorrangig vor anderen Versicherungsverträgen. Der einheitliche Versicherungsfall des tatsächlichen Schadeneintritts bietet eine unbegrenzte Rückwärtsdeckung. Eine fünfjährige Nachhaftung sorgt für zusätzliche Sicherheit. Außerdem gilt im Versicherungsfall eine Beweiserleichterung für den Versicherungsnehmer.





Hiscox Cyber-Training

Profitieren Sie als Hiscox-Kunde von unserem kostenlosen Cyber-Training und erhöhen Sie die digitale Sicherheit in Ihrem Unternehmen.

Exklusiv für die Kunden, die eine Cyber-Versicherung oder ein Cyber-Modul im Rahmen ihrer Berufshaftpflicht abgeschlossen haben.

Fragen?