Datenschutzrichtlinie 2018 sowie Versicherungsmöglichkeiten

Salzburg, 08.09.2017

Cybercrime-Aktivitäten weltweit

Anzahl der jährlichen Cyberangriffe weltweit in den Jahren 2009 bis 2014:

- Die Statistik zeigt die Zunahme der jährlichen weltweiten Anzahl an Cyberattacken von 2009 bis 2014
- Das letztgenannte Jahr markiert mit annähernd 43 Millionen registrierten Angriffen über das Internet zugleich die bis dato höchste Anzahl

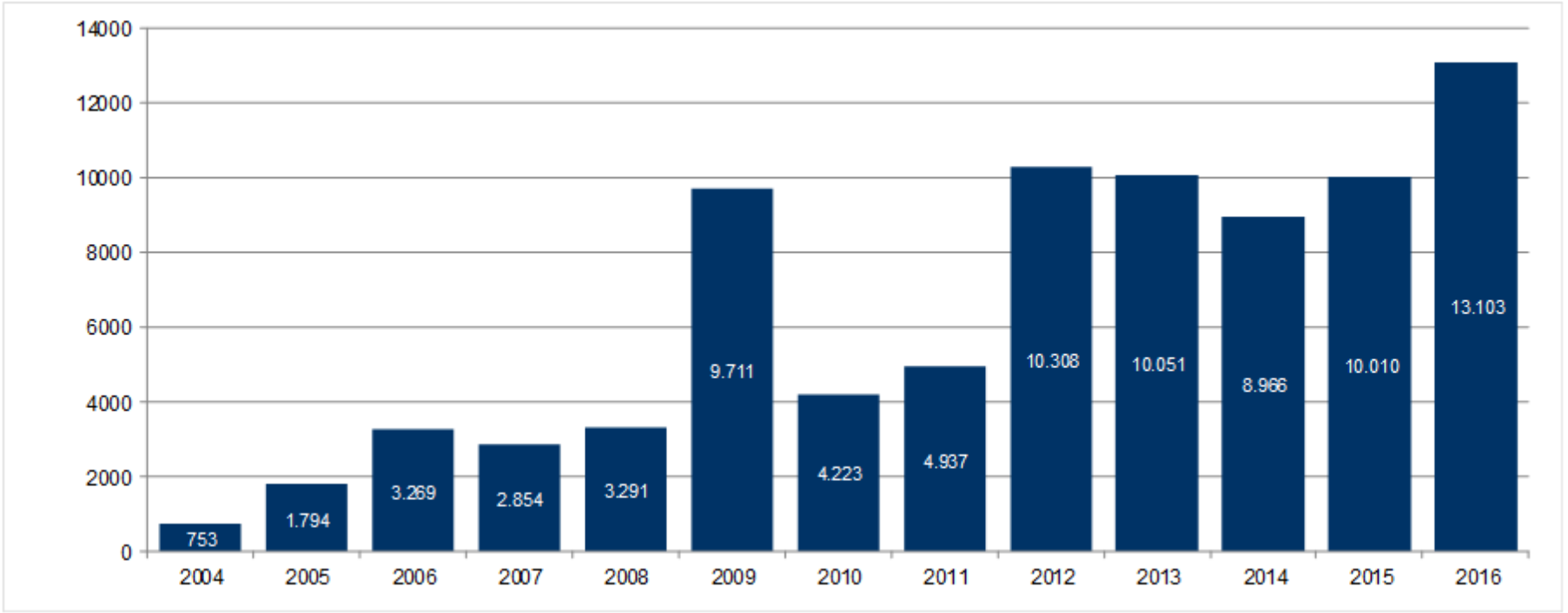
- Dies entspräche über 117.000 Cyberattacken täglich
- 2016 wurden täglich bereits 380.000 neue Varianten von Schadprogrammen festgestellt

Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

Internationale Fälle

- T-Mobile USA → 15 Mio. Kundendaten betroffen (6/2015)
- Der Autobauer Fiat Chrysler ruft rund 1,4 Millionen Fahrzeuge in USA zurück, um Hackerangriffe darauf zu verhindern (7/2015)
- Hacker greifen deutschen Bundestag an (7/2015)
- Hacker greifen US-Regierung an (vermutlich größte Cyber-Attacke in der Geschichte der US-Regierung) 21,5 Millionen Daten von Mitarbeitern betroffen (7/2015)
- Hacker attackieren US-Hotelkette Hyatt (12/2015)
- WannaCry legt in 150 Ländern 240.000 Computer lahm (5/2017)
- Attacke Petya/NotPetya führt zu enormen Schäden weltweit (6/2017)

Angezeigte Cybercrimefälle in Österreich



Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

Was sagt die Regierung 2017 dazu?

Cyberkriminalität sei mittlerweile ähnlich lukrativ wie Menschen- oder Drogenhandel, so Kanzleramts-Staatssekretärin Mag. Muna Duzdar. Im Jahr 2015 ist durch Cyberkriminalität weltweit ein volkswirtschaftlicher Schaden von 500 Milliarden Euro entstanden.

Das hat der weltgrößte Rückversicherer, die Munich Re, errechnet. In Österreich sei Ransomware ein großes Problem geworden, so die Staatssekretärin. Aktuell gibt es rund 30 neu angezeigte Vorfälle pro Woche. Ransomware gilt mittlerweile als der profitabelste Malware-Typ in der Geschichte der IT.

futurezone.at 1/2017

KPMG-Studie 4/2016

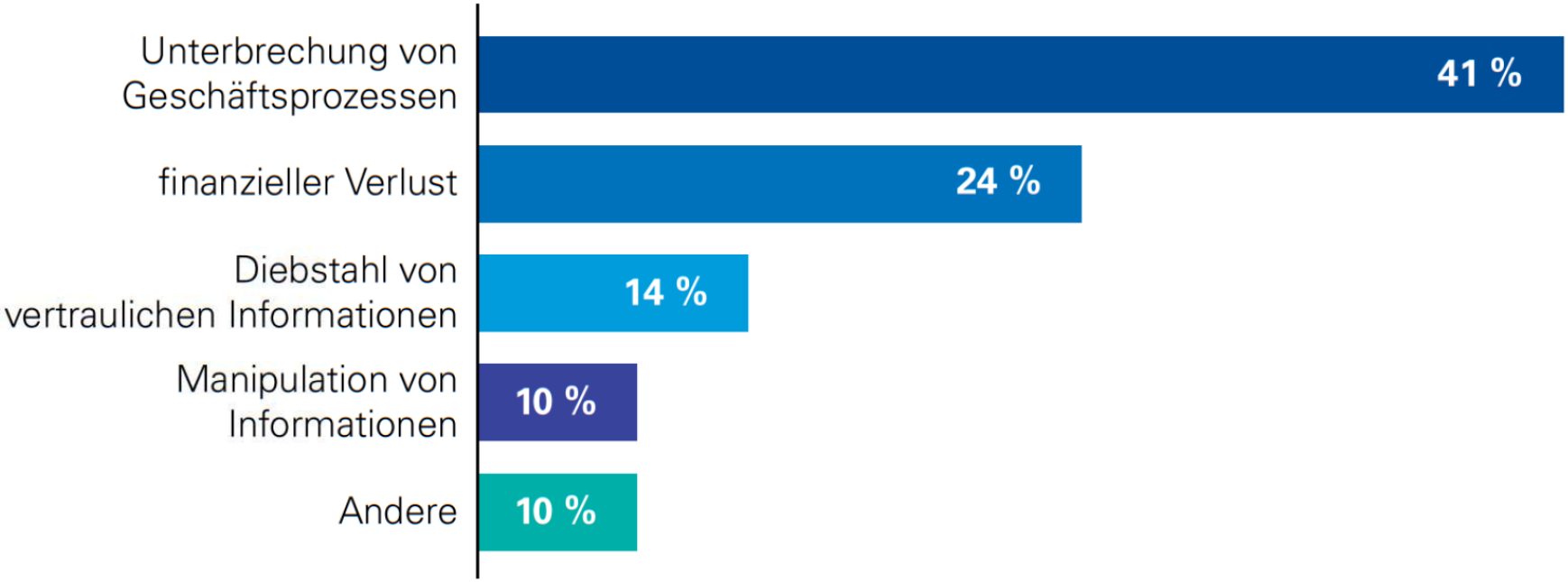
Fakten aus der Studie von KPMG:

- 92% meinen, dass Cyber-Security Alltag ist
- 49% waren bereits Ziel eines Cyber-Angriffs
- 30% haben bereits einen finanziellen Schaden erlitten
- 71% können Angriff nicht verhindern und nur 18% können wirksam reagieren
- 16% können ihre Kronjuwelen schützen
- 76% haben Defizit in Mitarbeiter Awareness

KPMG-Studie 4/2016

Auswirkungen von Cyberangriffen

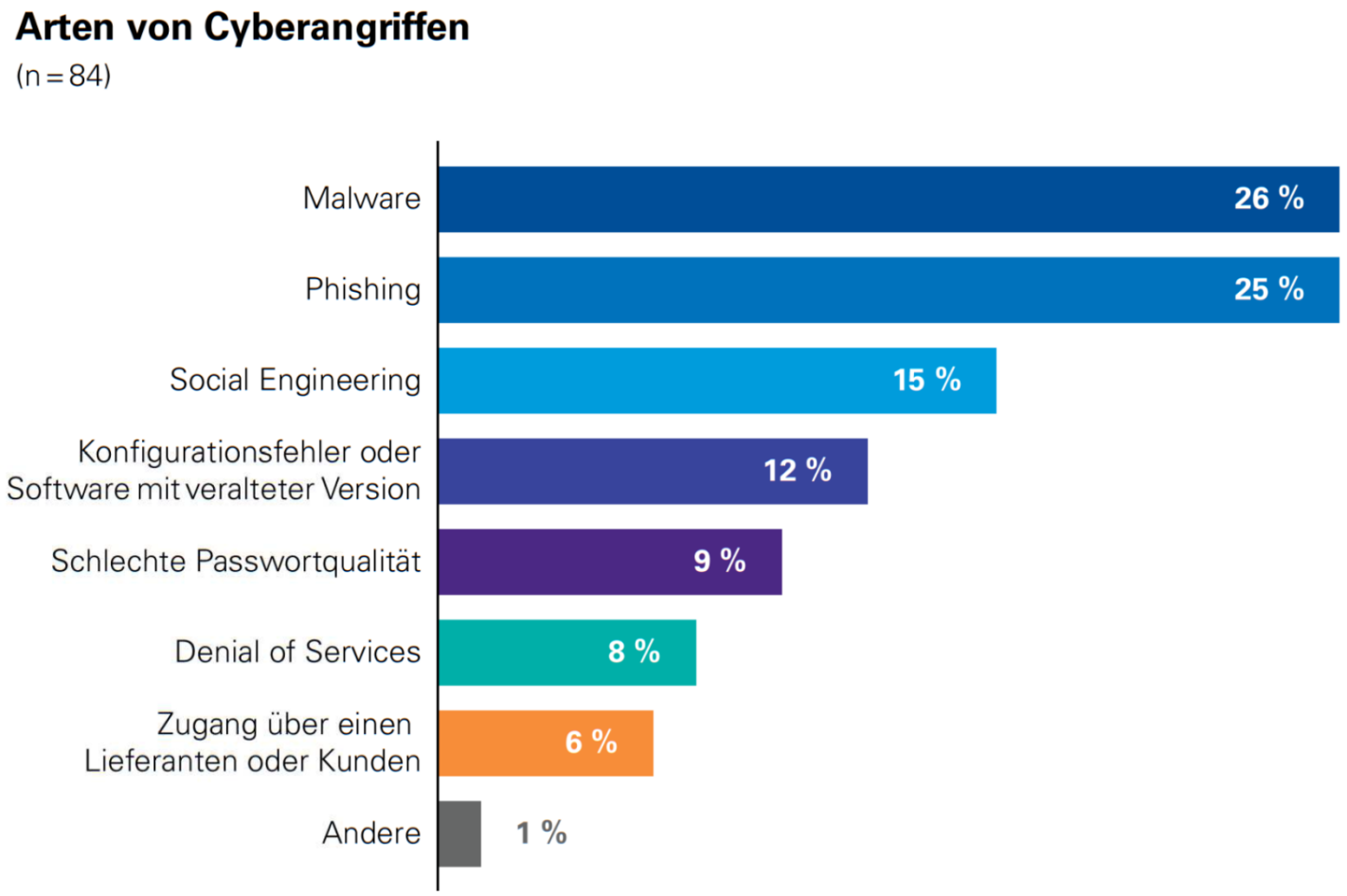
(n = 84)



Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

KPMG-Studie 4/2016

KPMG-Studie 4/2016

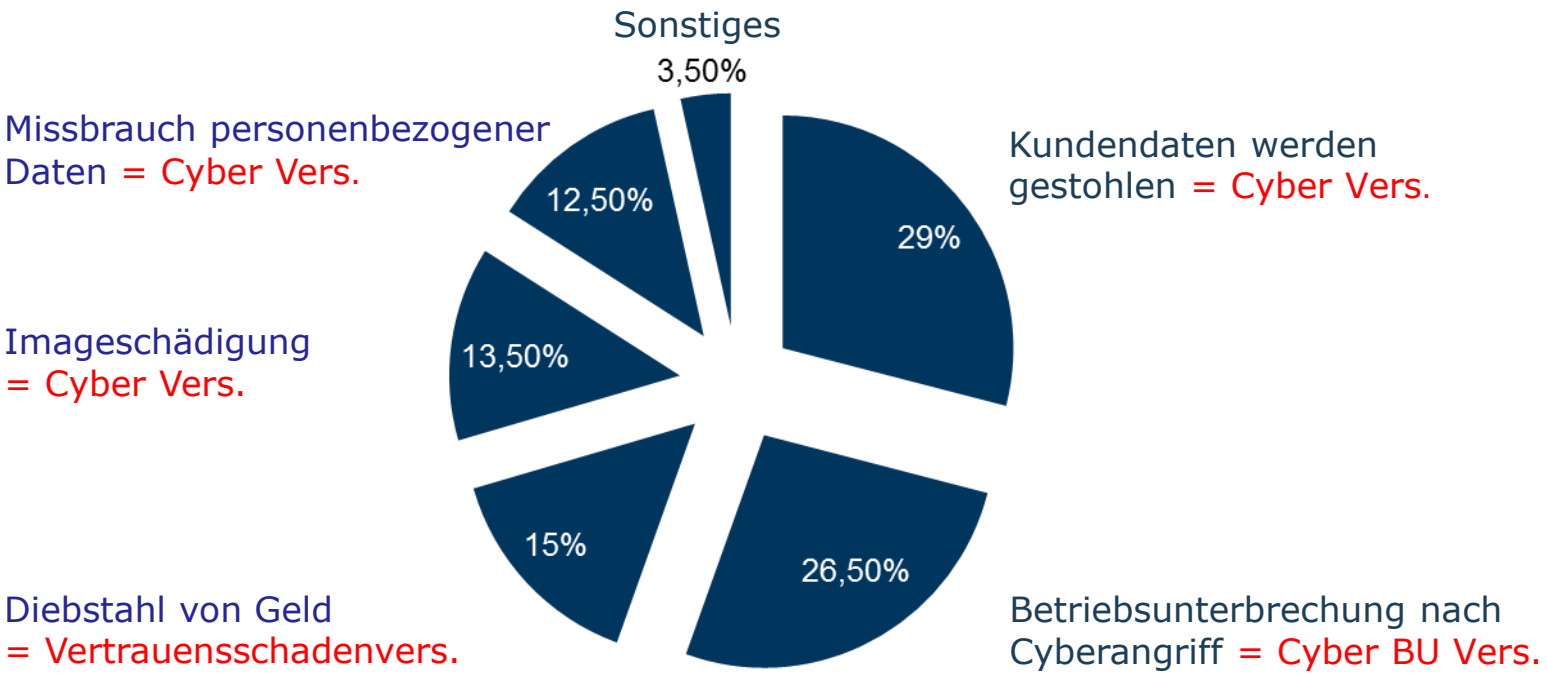


Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

KPMG-Studie 4/2016

Veränderung des Risikobewusstseins

Gemäß einer Meinungsumfrage bei österreichischen Unternehmen:

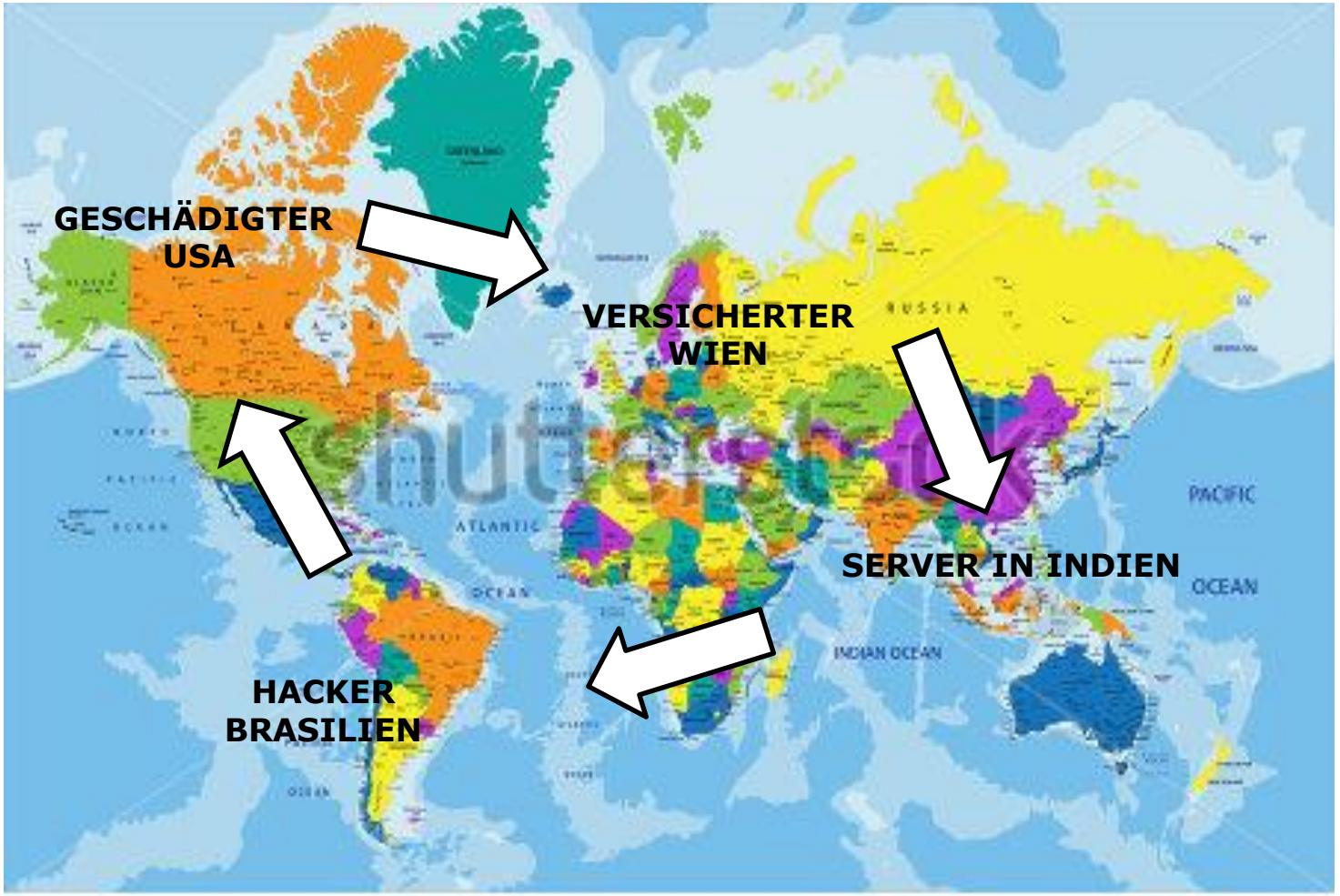


Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

Fotos Papstwahl 2005 / 2013

Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

Neue Versicherungswelt ohne Grenzen



Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

Datenschutzanpassungsgesetz zum Datenschutzgesetz (DSG) 2018

Highlights

- **Sehr weiter Verarbeitungsbegriff**
  (jeder mit oder ohne automatisiertem Verfahren ausgeführter Vorgang)

- **Besondere Kategorien personenbezogener Daten / sensible Daten**
  (Informationen über Rasse, religiöse oder politische Meinung, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Gesundheitsdaten, Daten zu Sexualleben oder sexueller Orientierung)

- **Einwilligungserklärung**
  (Muss künftig vom Betroffenen eingeholt werden und von diesem aktiv bekundet werden – versteckt in AGBs ist zu wenig)

- **Recht auf Löschung der Daten**
  (Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten, auf Auskunft über die Verarbeitung solcher Daten sowie auf Richtigstellung unrichtiger Daten und auf Löschung unzulässigerweise verarbeiteter Daten)

Strafrechtliche Komponenten

Datenschutzgrundverordnung EU

Highlights

Strafen

Art 83 Ziff. 4. DSGVO

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von **bis zu 10.000.000,- Euro** oder im Fall eines Unternehmens von **bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) Die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) Die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) Die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

Datenschutzgrundverordnung EU

Highlights

Strafen

Art 83 Ziff. 5. DSGVO

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von **bis zu 20.000.000,- Euro** oder im Fall eines Unternehmens von **bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) Die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) Die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c) Die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) Alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

Versicherbare Risiken Cyber Insurance

Verlust, Beschädigung oder Zerstörung von Daten (Eigenschadendeckung) durch:

- Mut- oder böswillige Handlungen durch AN oder Dritte (Malicious Acts)
- Programme oder Programteile mit Schadfunktion (Malicious Codes), wie Viren, Trojaner und logische Bomben
- Menschliches Versagen (bei manchen Versicherern)
- Verlust, Beschädigung der Hardware (bei manchen Versicherern)
- Ausfall oder Störung der Hardware (bei manchen Versicherern) durch:
  - Elektrostatische Entladung oder elektromagnetische Störung
  - Überspannung, Spannungsabfall
  - Ausfall der Stromversorgung oder des Datennetzes

Versicherbare Risiken Cyber Insurance

Versicherbare Kosten

- Kosten zur Wiederherstellung der Software
- Beschleunigungskosten
- Sachverständigenkosten, Forensikkosten, Nachforschung, Sachverständige
- Kosten für Regresse, Rechtsanwälte, PR-Agenturen, Benachrichtigung
- Vertragsstrafen, Lösegeld (wenn mit Versicherer vereinbart), Krisenmanager
- PCI Strafen (bei manchen Versicherern optional)
- Leistungen bei Schäden durch externe Dienstleister
  (Cloud, IaaS, PaaS, SaaS)
- Cyber - Betriebsunterbrechungsversicherung

Versicherbare Risiken Cyber Insurance

Cyber-Haftpflichtversicherung (Drittschadendeckung)

- Vermögensschäden der versicherten Unternehmen wegen Schadenersatzansprüchen Dritter aufgrund einer Datenschutzverletzung
- Abwehrkosten (gerichtlich und außergerichtlich) wegen der Haftbarmachung von zu unrecht gestellten Forderungen Dritter
- Anwaltskosten
- Sachverständigenkosten
- Gerichtskosten

Wie tickt eine Cyberversicherung?

- Im Vordergrund steht Risk-Management für IT-Systeme
- Nicht jeder Kunde ist versicherbar
- Risikoprävention im IT-Bereich macht versicherbar
- Technologische Aufrüstung hinsichtlich Datensicherheit ersetzt die Cyber-Insurance nicht sondern ist als Assistance-Produkt mit Elementen von diversen gebündelten Versicherungssparten zu sehen
- Optimale IT-Sicherheit ist ein Muss um das Restrisiko eines Cyber-Events überhaupt versicherbar zu machen

Was ist eine Vertrauensschaden-versicherung?

- Versichert gelten **Vermögensschäden wegen vorsätzlich strafbarer Handlungen** durch eigene Mitarbeiter.
- Mitversicherung von unbefugtem Eingriff in eigene IT-Datensysteme
- Teilweise mit Sublimit versicherbar sind Täuschungsschäden durch Dritte (Fake President Fraud oder CEO Fraud)
- Mitversicherung von nicht identifiziertem Schadenstifter
- Teilweise versicherbar ist Geheimnisverrat
- Achtung auf Obliegenheiten in den Bedingungen (Passwörter etc.)
- Achtung je mehr Definitionen in den Bedingungen, desto schlechter der Versicherungsschutz

Deckungsvergleich

Elektronik-, Cyber-, Vertrauensschadenversicherung

	Elektronik-versicherung	Elektronik-BU	Cyber-versicherung	Cyber-BU	Vertrauens-schadenvers.
Deckung:	Sachschäden durch	BU-Schäden	Kosten durch	BU-Schäden	Reine Vermögens-schäden wegen strafbarer Handlung
Versicherte Gefahren bzw. Versicherte Kosten:	▪ Bedienungsfehler ▪ Ungeschicklichkeit ▪ Mechanische Gewalt ▪ Wasser, Feuchtigkeit ▪ Elementarschäden ▪ Indirekter Blitz, Überspannung ▪ Software je nach Deckungsumfang	▪ nach vorgenannten versicherten Sachschäden	▪ Evaluierung Datenleck ▪ Wiederherstellung Daten nach Hackerangriff ▪ Verlust physischer Datenträger ▪ Krisenmanagement ▪ PR-Kosten ▪ Lösegeld ▪ Cyber Haftpflicht-versicherung	▪ Nach Hacker-angriff aufgrund vorgenannter Schäden	▪ Betrug eigener Mitarbeiter ▪ Verrat von Betriebs-geheimnissen ▪ Computer-missbrauch ▪ Täuschungs-schäden durch Dritte

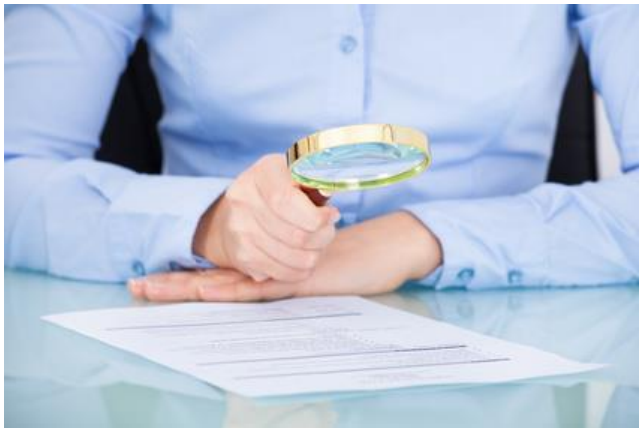
Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer

Die Cyber und VSV Versicherer

ZURICH VERSICHERUNG

R+V

CHUBB



AIG

DUAL

EULER HERMES

WIENER STÄDTISCHE
VIENNA INSURANCE GROUP

TOKIO MARINE KILN

HISCOX

HDI

XL CATLIN

Fazit

- Floriani-Prinzip und Wegschauen wird nicht mehr all zu lange funktionieren.
- Cyber-Insurance und Vertrauensschadenversicherung werden demnächst in Österreich zum Standard gehören.
- Schäden werden für mittelständische Unternehmer auf Dauer schwer leistbar sein. Sie können auch Auslöser für D&O-Schäden werden, wenn das Management nicht die notwendigen Absicherungsmöglichkeiten prüft/ nützt.
- Nur IT-Sicherheit durch Technik in Verbindung mit geschultem Personal, Risk-Management und Cyber-Insurance wird das Paket der Zukunft sein.
- Industrie 4.0 wird dieses Thema weiter beschleunigen.

Bitte denken Sie daran

Fremde Daten sind keine herrenlosen Sachen sondern haben Eigentümer und diese Eigentümer haben Rechte daran!

Danke für Ihre Aufmerksamkeit!

Norbert Jagerhofer
Prokurist
Tel.: +43(0)732/6596-25690
Mobil: +43(0)676/8141-5690
E-Mail: jagerhofer@rvm.at

Quelle: 9/2017, RVM, Prok. Norbert Jagerhofer