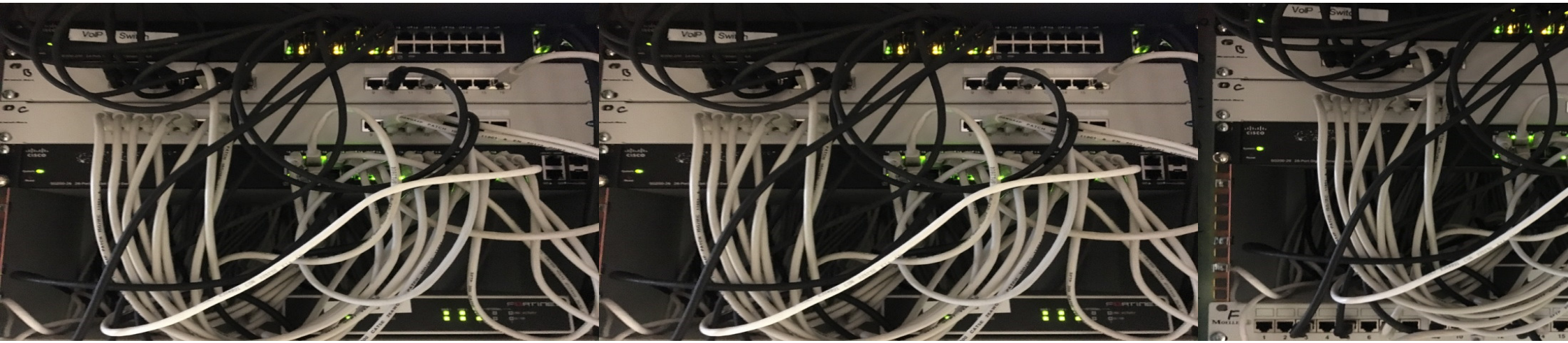
Cyberversicherungen für Unternehmen:

Sinnvoll oder unnötige Kosten?

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN



Anton Alt, Akad. Vkfm.

Graz, 14. November 2022

Von Industrie 1.0 zu Industrie 4.0

Dampfmaschine James Watt
1769

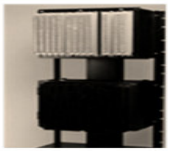
Erste industrielle Revolution durch Einführung mechanischer Produktionsanlagen mithilfe von Wasser- und Dampfkraft

Ende
18. Jhdt

Erstes Fließband,
Schlachthilfe von Cincinnati
1870

Zweite industrielle Revolution durch Einführung arbeitsteiliger Massenproduktion mithilfe von elektrischer Energie

Ende
19. Jhdt



Erste Speicherprogrammierbare Steuerung (SPS), Modicon 084
1969

Dritte industrielle Revolution durch Einsatz von Elektronik und IT zur weiteren Automatisierung der Produktion

Ende
20. Jhdt

Vierte industrielle Revolution auf Basis von Cyber-Physical Systemen

heute

Grad der Komplexität

Datenschutzgesetz (DSG)

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Artikel 1 (Verfassungsbestimmung)

§ 1. Grundrecht auf Datenschutz

(1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personen-bezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

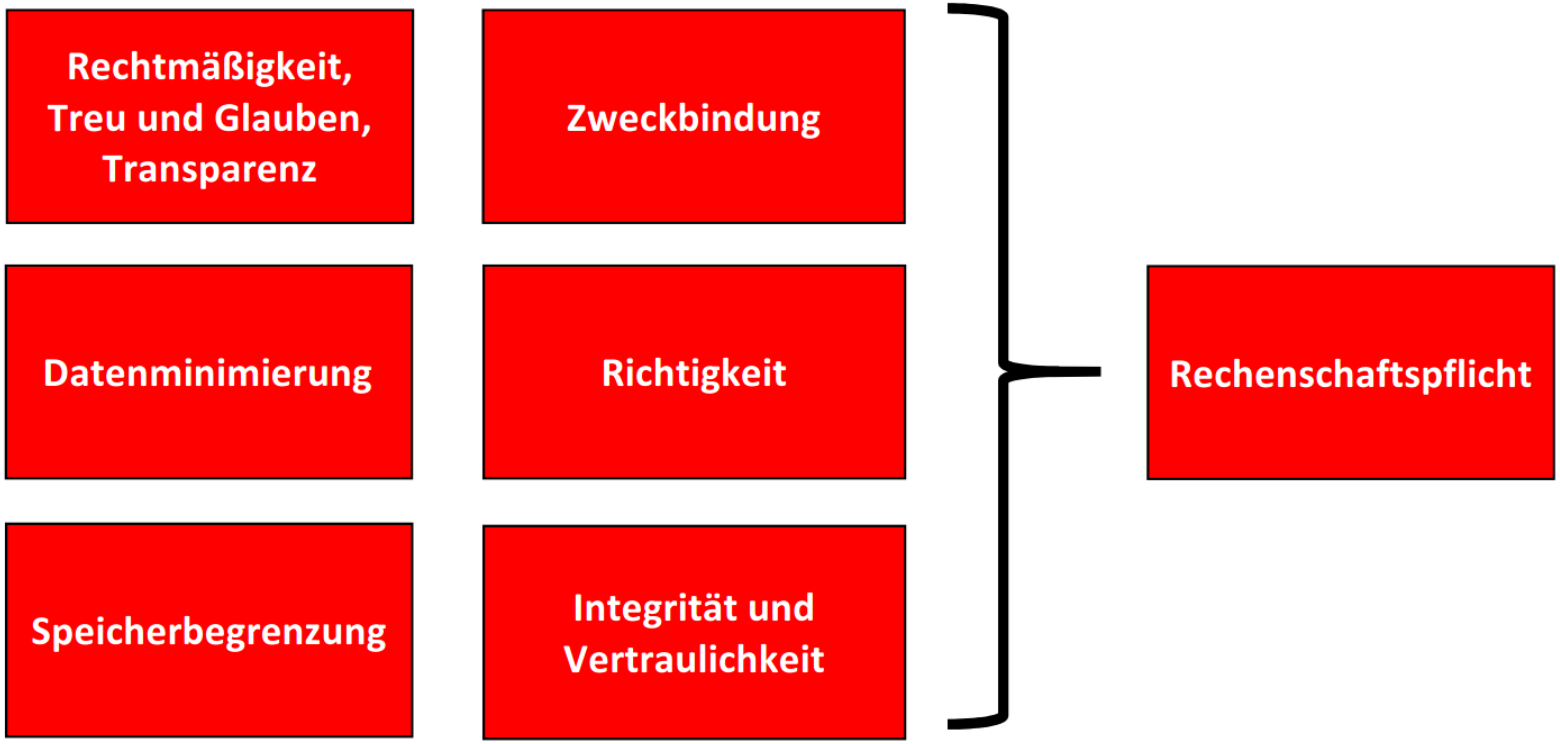
Datenschutzgesetz (DSG)

§ 4. (1) Die Bestimmungen der Verordnung (EU) 2016/679 ….
(im Folgenden: DSGVO) und dieses Bundesgesetzes gelten für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten natürlicher Personen sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten natürlicher Personen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, soweit nicht die spezifischeren Bestimmungen des 3. Hauptstücks dieses Bundesgesetzes vorgehen.

DSGVO

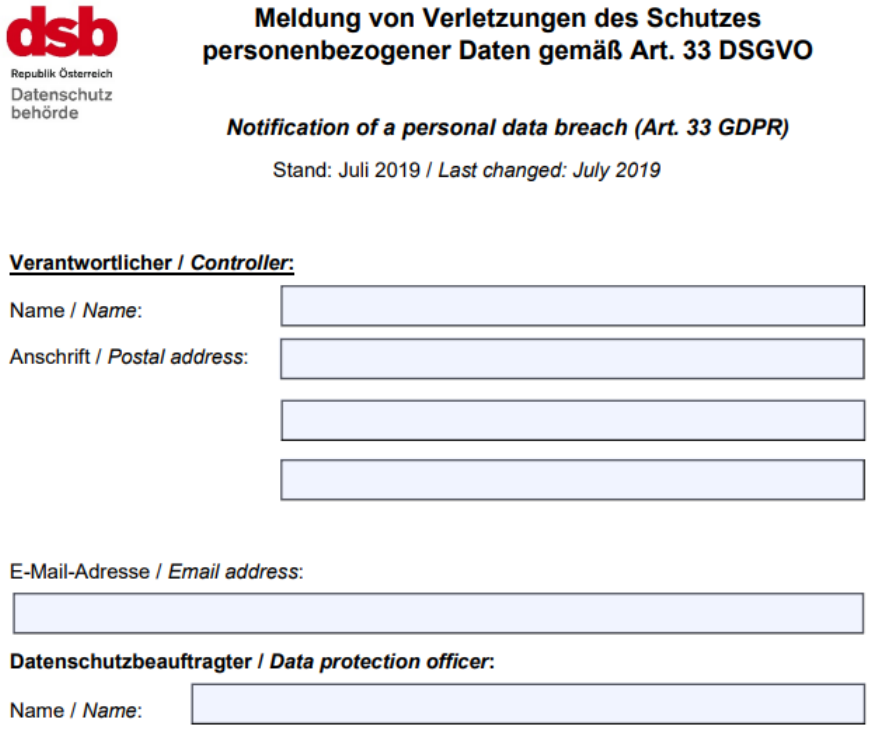
ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten



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

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN



dsb
Republik Österreich
Datenschutz
behörde

Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO

Notification of a personal data breach (Art. 33 GDPR)

Stand: Juli 2019 / *Last changed: July 2019*

Verantwortlicher / *Controller*:

Name / *Name*:

Anschrift / *Postal address*:

E-Mail-Adresse / *Email address*:

Datenschutzbeauftragter / *Data protection officer*:

Name / *Name*:

DSGVO

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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

10.08.2015
Verlag Versicherungswirtschaft GmbH

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Verlag Versicherungswirtschaft

Klosestraße 20-24

76137 Karlsruhe

Mitteilung auf der Homepage www.vvw.de

Herzlich Willkommen beim Verlag Versicherungswirtschaft

Versicherungswirtschaft

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Sehr geehrte Kundinnen, sehr geehrte Kunden,

leider ist unser Webshop (www.vvw.de) Ziel eines kriminellen Datenangriffs geworden.

Die Täter hatten Zugriff auf folgende Angaben: Anrede, Name, Adresse, Geburtsdatum, E-Mail-Adresse, Kundenkonto-Passwort, Bankleitzahl und Kontonummer, Telefon- und Fax-Nummer. Sicher ist, dass die Täter keinen Zugang zu Ihren VISA oder Mastercard-Daten hatten.

Wir können nicht ausschließen, dass auch Ihre Daten davon betroffen waren. Wir bedauern dies sehr und versichern Ihnen, dass die Sicherheitslücke unverzüglich geschlossen wurde.

Was sollten Sie tun?
1. Wir empfehlen Ihnen dringend die Zugangsdaten zu Ihrem Kundenkonto in unserem Shop vvw.de zu ändern. Zum Kundenkonto
2. Beobachten Sie Bewegungen auf Ihrem Bankkonto genau. Sollten Sie unberechtigte Abbuchungen feststellen, lassen Sie diese durch Ihre Bank zurückgeben.

Falls Sie Fragen haben oder Hilfestellung benötigen, zögern Sie bitte nicht, sich bei uns zu melden.

Artikel 32 DSGVO: Sicherheit der Verarbeitung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten…

DSGVO

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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.

⇨ **Beweislastumkehr!**

DSGVO

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

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.

⇨Datenschutz-Deregulierungs-Gesetz 2018

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

DSGVO Art. 83 – Geldbußen seit 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 %	-

Beispiel für Geldbußen

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- 23.10.2019: Die Österreichische Post hat im Datenskandal um die Speicherung von Parteiaffinitäten von Millionen Post-Kunden und dem Verkauf dieser Daten an wahlwerbende Parteien eine Verwaltungsstrafe von 18 Mio. Euro + 10% Verfahrenskosten von der Datenschutzbehörde erhalten.
- 2.12.2020: Das Bundesverwaltungsgericht bestätigte nun zwar grundsätzlich, dass das Verhalten der Post illegal gewesen sei. Doch entdeckte das Gericht im Strafbescheid gegen die Post einen Formfehler.

Beispiel für Geldbußen

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Die österreichische Datenschutzbehörde verhängte gegenüber der Unser Ö-Bonus Club GmbH eine Geldbuße in Höhe von 2 Millionen Euro. Dies geht aus dem am 2. August 2021 von der Behörde veröffentlichten Bescheid hervor.

Beispiel für Geldbußen

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Das Kundenbindungsprogramm von Rewe, der jö Bonus Club, ist erneut im Visier der Datenschutzbehörde. Die Behörde verhängte eine Strafe in Höhe von 8 Mio. Euro gegen das Unternehmen wegen Verstößen gegen die Datenschutzgrundverordnung (DSGVO), berichten die "Salzburger Nachrichten" am Freitag, dem 14.1.2022.

Erfolgreiche Cyber-Angriffe häufen sich

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Freitag, 19. Dezember 2014

Cyber-Angriff auf Stahlwerk

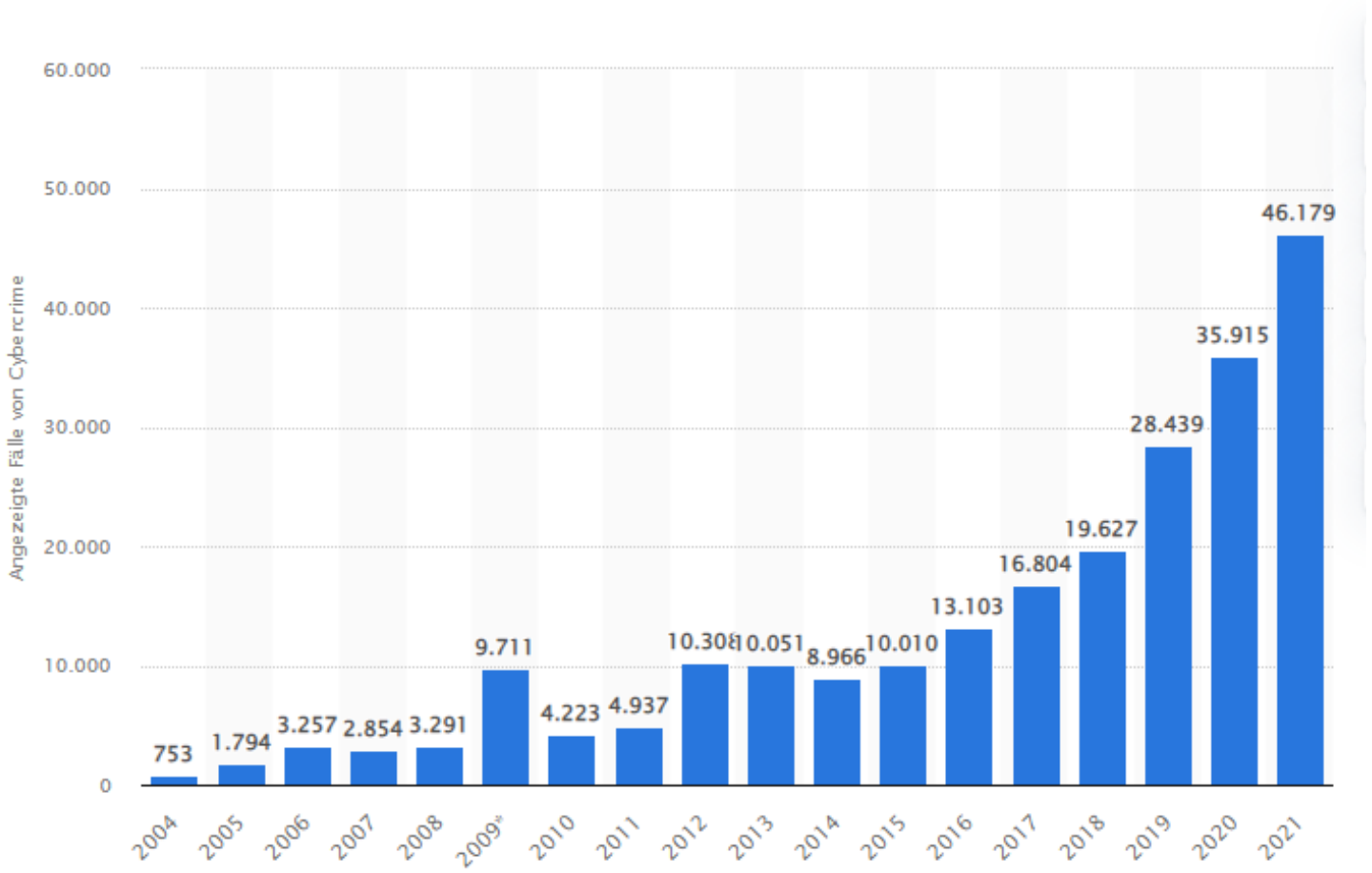
Hacker bringen Hochofen unter ihre Kontrolle

Die deutsche Industrie vernetzt sich immer stärker - und wird sensibler für Cyber-Attacken. Ein Beispiel zeigt, wie dramatisch die Folgen sein können: Hacker haben den Hochofen eines Stahlwerks unter ihre Kontrolle gebracht. Die Schäden sind massiv.

Hacker sind nach einem Bericht des Bundesamtes für Sicherheit in der Informationstechnik in das Netzwerk eines Stahlwerks eingedrungen, haben die Steuerung des Hochofens übernommen und die Anlage massiv beschädigt. Das geht aus dem Bericht "Die Lage der IT-Sicherheit in Deutschland 2014 (https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html)" hervor. Demnach führte der Einbruch der Hacker zum Ausfall ganzer Systeme der Anlage. Die Verantwortlichen in dem Stahlwerk seien nicht mehr in der Lage gewesen, den Hochofen herunterzufahren.

Es gibt keine sicheren Systeme!

Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2021



Quelle: Statista

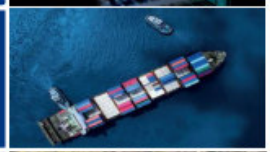
ALLIANZ RISK BAROMETER 2022

Top 10 Geschäftsrisiken weltweit

1 44%

Cybervorfälle
(z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen)

2021: 40% (3)



2 42%

Betriebsunterbrechung
(inkl. Lieferkettenunterbrechung)

2021: 41% (1)

3 25%

Naturkatastrophen
(z.B. Sturm, Überschwemmung, Erdbeben)

2021: 17% (6)

4 22%

Ausbruch einer Pandemie
(z.B. Gesundheits- und Arbeitskräfteprobleme, Einschränkungen der Bewegungsfreiheit)

2021: 40% (2)

5 19%

Rechtliche Veränderungen
(z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)

2021: 19% (5)

6 17%

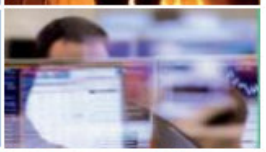
Klimawandel
(z.B. Sachschaden-, Betriebs-, Finanz- oder Reputationsrisiken als Folge der Erderwärmung)

2021: 13% (9)

7 17%

Feuer, Explosion

2021: 16% (7)



8 15%

Marktveränderungen
(z.B. Volatilität, verstärkter Wettbewerb/ neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)

2021: 19% (4)

9 13%

Fachkräftemangel

2021: 8 % (13)

10 11%

Makroökonomische Entwicklungen
(z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation)

2021: 13% (8)

Aufsteiger | Absteiger | Stabil

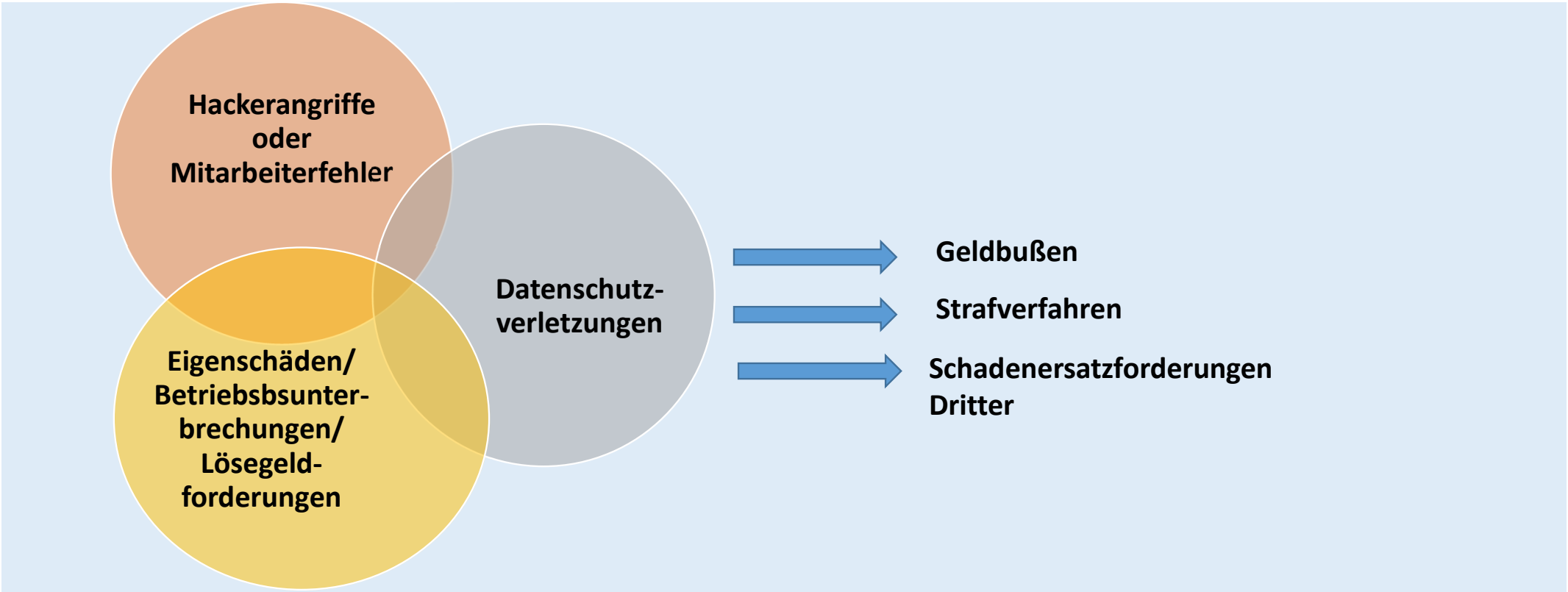
2,650 respondents

89 countries and territories

22 industry sectors

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Digitale Gefahren



Sicherstellung einer IT-Security

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Haftung der Unternehmensleitung

IT-Security ist nicht Selbstzweck, sondern rechtliche Verpflichtung der Unternehmensleitung.

Mindestsicherungen für den Abschluss einer Cyberversicherung

- Abgestuftes Berechtigungskonzept mit administrativen Kennungen, die ausschließlich durch IT-Verantwortliche verwendet werden

- Alle vorhandenen Cloud-Administrationskonten sind mit einer Zwei-Faktor-Authentifizierung abgesichert

Mindestsicherungen für den Abschluss einer Cyberversicherung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Die Datensicherung erfüllt folgende Anforderungen:

- Vollständige wöchentliche Datensicherung
  - Aufbewahrung der vollständigen Datensicherung über mind. 30 Tage*)
  - Nutzung einer Offline-Datensicherung mit dauerhafter physischer Trennung von den IT-Systemen ODER Nutzung einer unveränderbaren Online-Datensicherung, auf welche die Administratoren nur mit einer von der betreffenden Domäne unabhängigen Zwei-Faktor-Authentifizierung oder aus einer separaten Domäne zugreifen können.

*) von VR zu VR unterschiedlich

Mindestsicherungen für den Abschluss einer Cyberversicherung

- Einspielen von Sicherheitsupdates auf Servern und Clients (Mobilen Geräten, Desktops und Terminals) sowie auf Netzwerkgeräten und Sicherheitssystemen (z.B. Firewalls, Virenschutz) innerhalb von 30 Tagen nach Veröffentlichung des Updates durch den Hersteller.
- Es dürfen keine Betriebssysteme, für die keine Sicherheitsupdates mehr bereitgestellt werden (Altsysteme wie z.B. Windows XP), genutzt werden ODER der Betrieb dieser Altsysteme erfolgt ausschließlich in einer isolierten Netzwerkumgebung ohne direkten Internetzugang und mit durchgehender Kontrolle des Datenverkehrs
- Die automatische Ausführung von Makros in Office-Dokumenten ist deaktiviert

Mindestsicherungen für den Abschluss einer Cyberversicherung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Die Werkeinstellung der Passwörter und PINs von digitalen Telefonanlagen muss geändert worden sein

- Bei Überweisungen von mehr als EUR 10.000,- *) muss ein verpflichtendes 4-Augen-Prinzip eingeführt sein

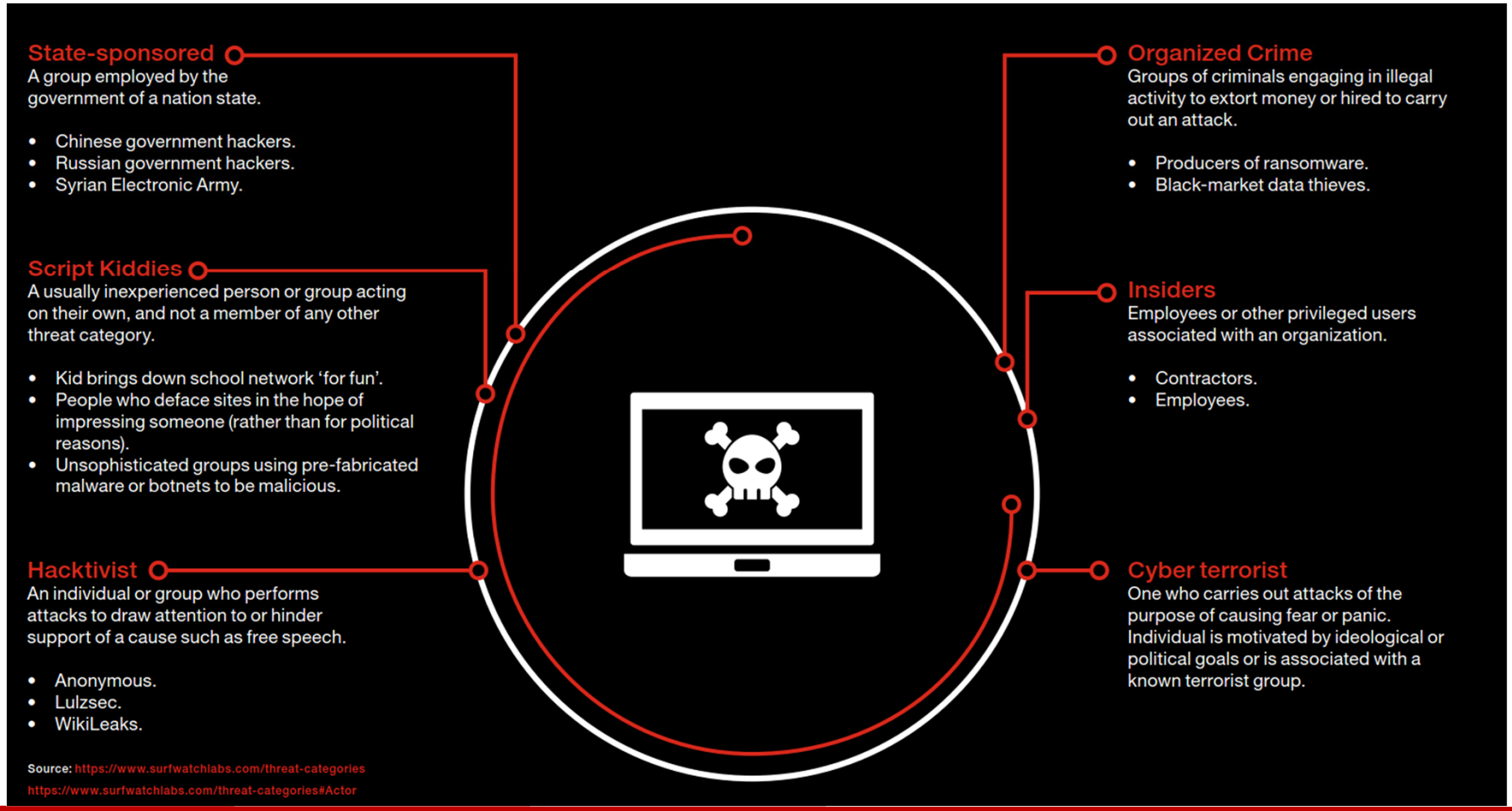
- Mind. Zwei-Faktor-Authentisierung für Fernzugriffsmöglichkeiten (Remote-Zugänge) auf Remote-Desktops für Homeoffice / Telearbeit oder Remote-Zugriffe auf E-Mails

*) von VR zu VR unterschiedlich

Mindestsicherungen für den Abschluss einer Cyberversicherung

- Externe Rechenzentrums- oder Cloud-Services werden entgeltlich genutzt und es ist vertraglich vereinbart, dass der dritte Dienstleister permanent mindestens eine ISO27001 Zertifizierung vorzuhalten hat sowie eine Einstufung in mindestens Tier Level 3 gem. TIA-942 vorliegt

Wozu eine Cyberversicherung?
Es gibt keine 100% sicheren IT-Systeme



Cyberversicherung:
Mögliche Schadensauslöser (Trigger)

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

1. Netzwerkssicherheitsverletzung
2. Bedien- und Programmierfehler
3. Datenrechtsverletzung
4. Cyber-Erpressung

Cyberversicherung:
Mögliche Deckungsbausteine / Leistungen des VR

Cyber-Eigenschadenversicherung:
- Krisenmanagement
- IT-Forensik
- für Rechtsberatung
- PR-Maßnahmen
- Wiederherstellungskosten
- Behördliche Anzeigepflicht
- Benachrichtigung der Betroffenen
- Anfragen der Betroffenen
- Call-Center
- Cyber-Diebstahl
- Cyber-Betrug
- Lösegeld
- Kreditüberwachungs-DL

Cyber-Haftpflichtversicherung:
- Schutz bei Ansprüchen Dritter in Zusammenhang mit Cyber-Schäden
- Einschluss immaterieller Schäden
- Abwehrkosten bei behördlichen Datenschutzverfahren
- Kosten der Wahrnehmung der rechtlichen Interessen bei Einleitung eines Strafverfahrens
- Freistellung externer Dienstleister (z.B. Auftragsverarbeiter)
- Vertragsstrafen an E-Payment Service Provider
- Vertragsstrafen wegen der Verletzung von Geheimhaltungsverpflichtungen

Cyber-Betriebsunterbrechung:
- On-Premises Hard- und Software
- Verfügungen der Datenschutzbehörde
- Cloud Ausfall
- Wechselwirkungsschäden
- Mehrkosten

Soforthilfe im Notfall!

Bausteine einer Cyberversicherung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Mögliche Assistanceleistungen

- Krisenhotline*)
- Krisenplan
- Online-Cyber-Training für MA
- Überprüfung der IT-Sicherheit

*) Wird grundsätzlich von jedem Cyber-VR angeboten!

Cyberversicherung: Die wesentlichsten Ausschlüsse

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Vorsatz oder wissentliche Pflichtverletzung
- Krieg
- Störung oder Ausfall der öffentlichen oder privaten technischen Infrastruktur
- Hoheitliche Eingriffe
- Naturkatastrophen
- Kernenergie, Radioaktivität, biologische und chemische Ursachen
- Sachschäden
- Personenschäden
- Produktrückruf
- Produkt- und Dienstleistungshaftpflicht

Was zeichnet eine gute Cyberversicherung aus?

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Umfassender Versicherungsschutz für Schadenersatzforderungen
- Umfassender Versicherungsschutz für Eigenschäden (inkl. BU)
- Einschluss Vertragsstrafen
- Rechtsschutz bei Strafverfahren
- Weltweiter Versicherungsschutz ohne Einschränkungen für die USA und Kanada
- Unbegrenzte Rückwärtsdeckung
- Entsprechende Nachhaftung
- Qualität des Krisendienstleisters mit 24/7 Hotline
- Kompetenz des VR bzw. dessen Schadensabteilung

Was zeichnet eine gute Cyberversicherung aus?

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Keine versteckten bzw. nicht exakt definierten Obliegenheiten

§ 6 VersVG

- Primäre Obliegenheiten
- Sekundäre Obliegenheiten

Beispiele für primäre Obliegenheiten

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Der Versicherungsnehmer hat angemessene Schutzmechanismen ***nach dem Stand der Technik*** zu verwenden (insbesondere für Kennworteinstellungen, Systemkonfigurationen und Firewalls sowie das Aufspielen neuer Software).

- Auf Änderungen des ***Standes der Technik*** hat der Versicherungsnehmer in angemessener Zeit durch erforderliche Maßnahmen zu reagieren…

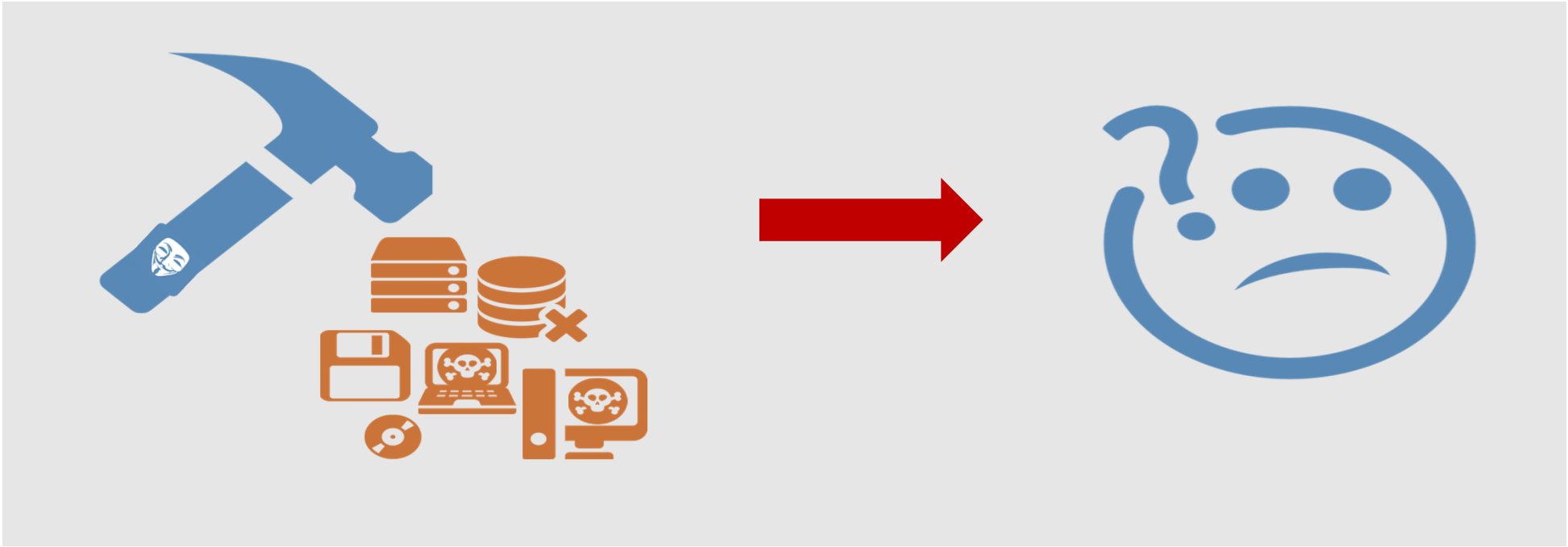
Beispiele für primäre Obliegenheiten

- 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

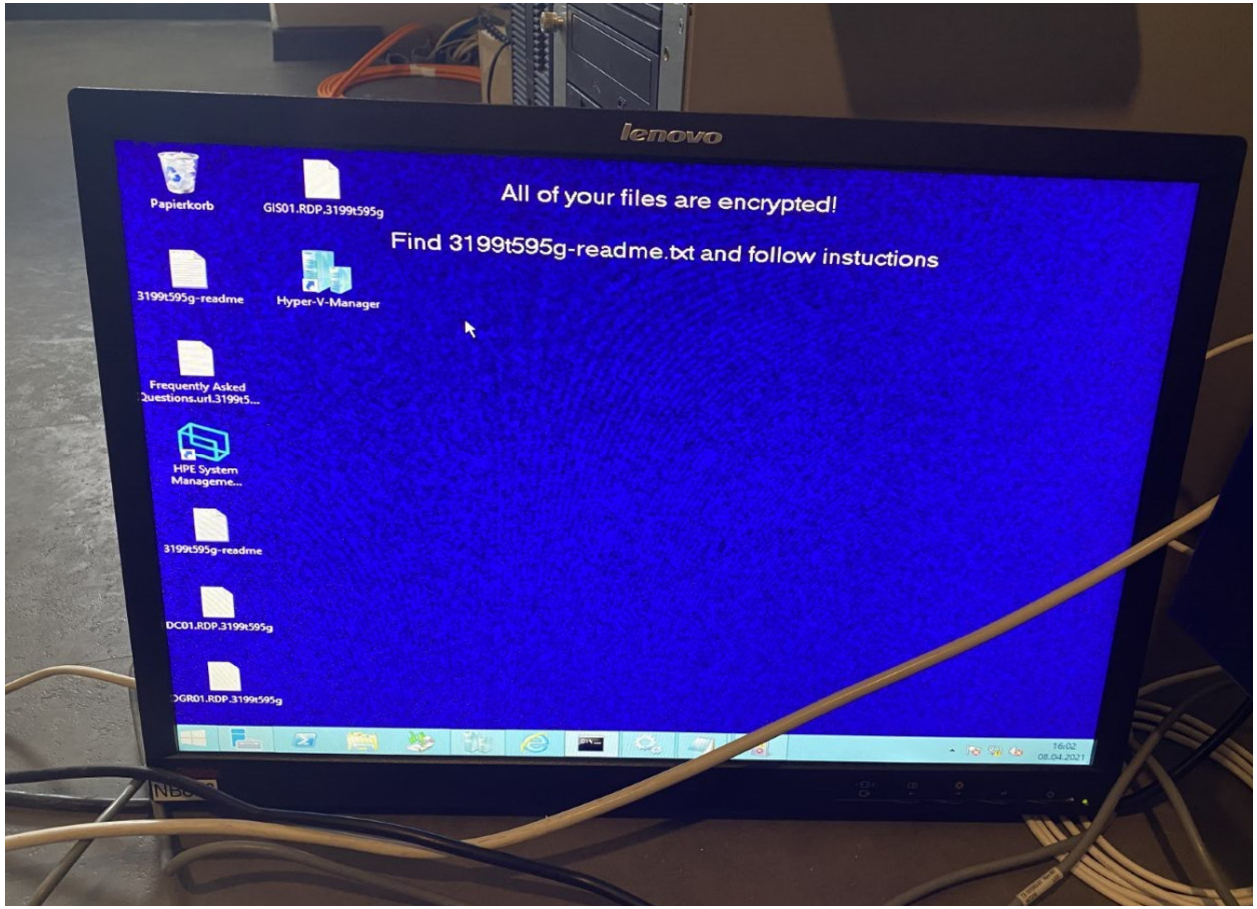
Stellen Sie sich vor, Sie kommen Montagmorgen ins Büro, und nichts geht mehr...

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

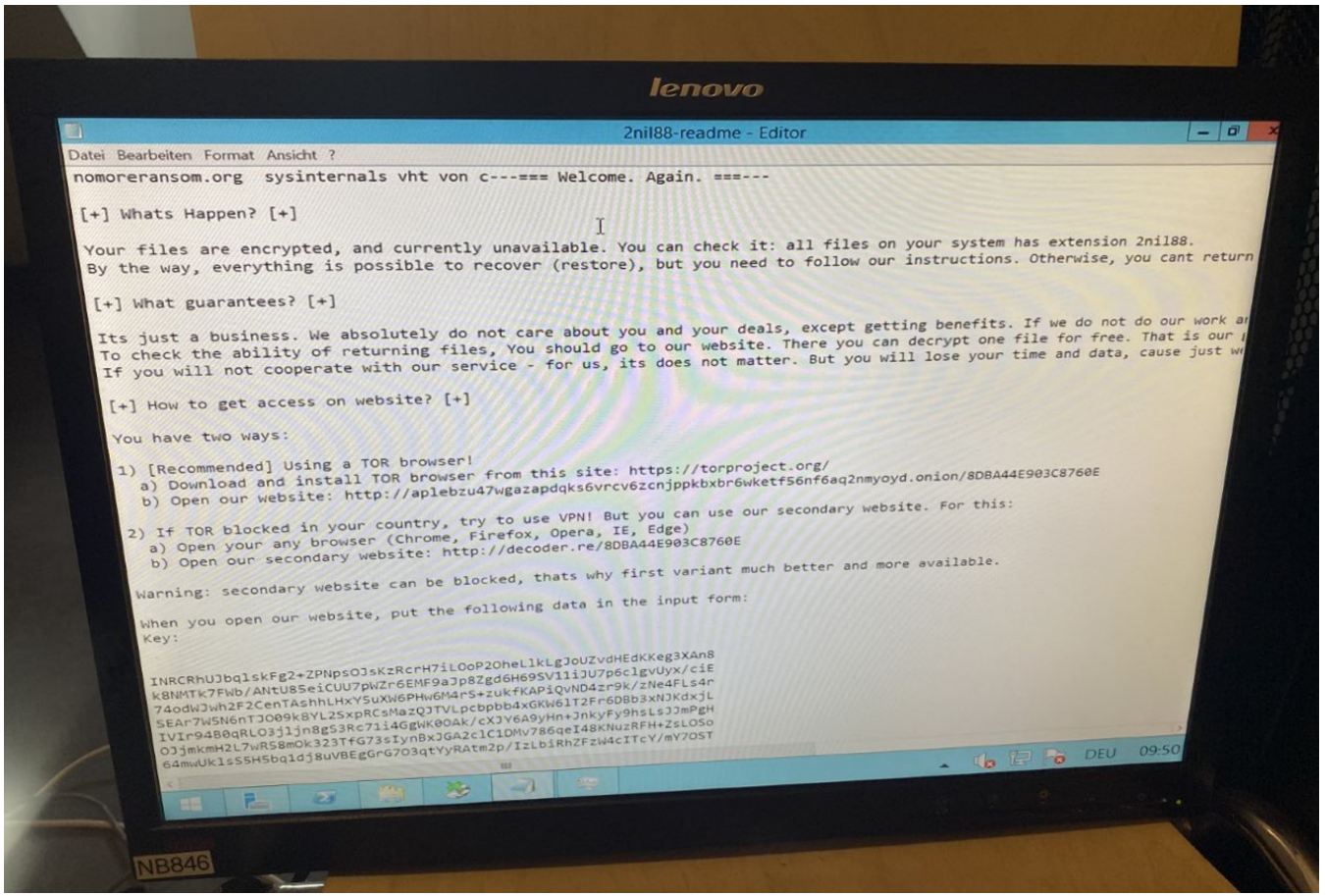


Schadensfall aus der Praxis: Entstehung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN



Schadensfall aus der Praxis: Entstehung



Schadensfall aus der Praxis: Entstehung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Eindringen in das IT-System über eine Malware
- Errechnung des Domain Admins (Tools für Passwortfindung)
- Verkauf der Zugangsdaten im Darknet
- Überwindung der Firewall (ca. 4 stündige Attacke in der Nacht, 2 TB)
- Zugang mit den gekauften Passwörtern
- Verschlüsselung der Backup Files und Sicherungsbänder über einen Zeitraum von ca. 5 Monaten
- Verschlüsselung der Server
- Lösegeldforderung

Spezielle Anforderungen an das Unternehmen

Fragen wenn der Plan und das Training fehlen

Was sollen wir den verärgerten Kunden sagen?

Was sagt man der Polizei und den Journalisten?

Was ist überhaupt passiert?

Wie gehen wir mit dem Shitstorm bei Facebook und Twitter um?

Wer muss jetzt was machen?

Welche Abteilungen und Prozesse sind denn betroffen?

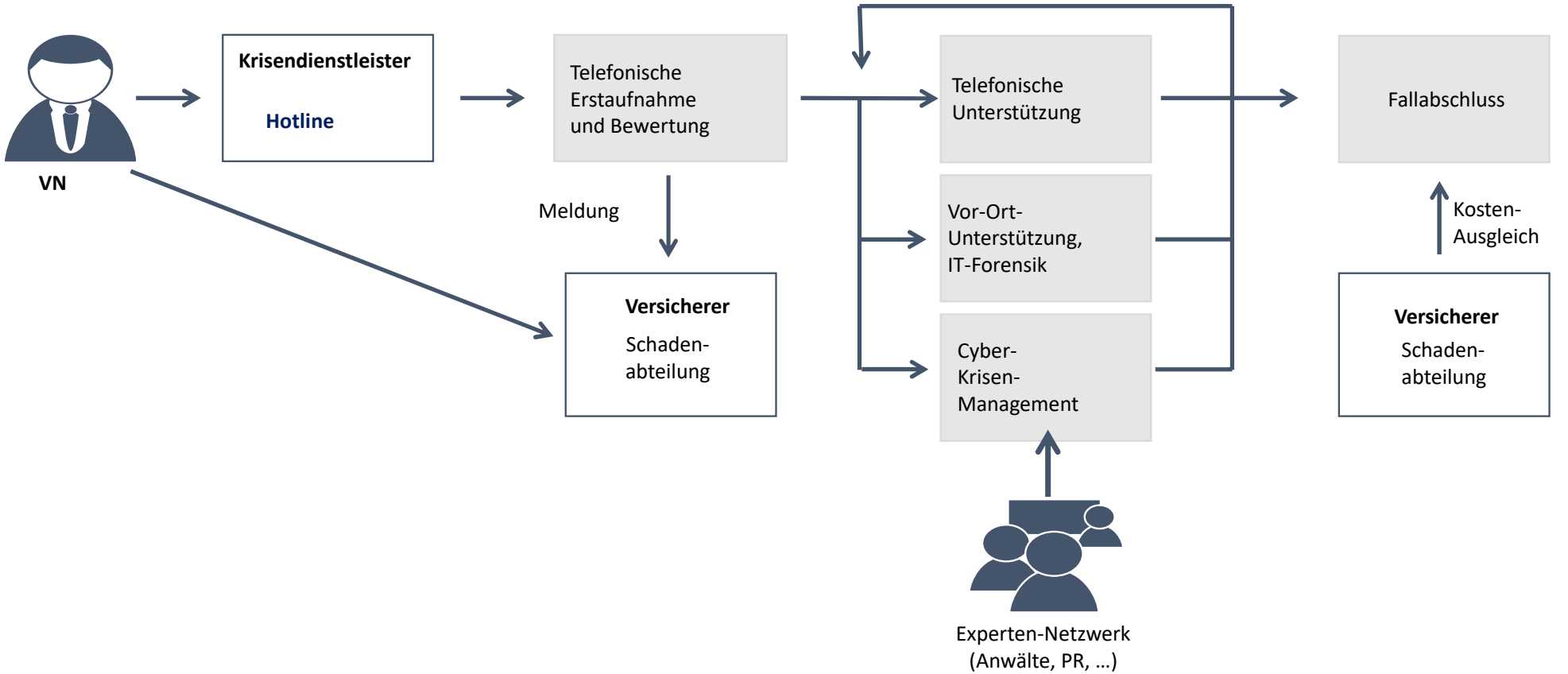
Können wir ohne Mail und Fileserver weiterarbeiten?

Kann unsere IT-Abteilung den Fehler beheben?

Wurde die Ursache schongefunden?

Wen müssen wir verständigen?

Cyber-Versicherung: Soforthilfe in der IT-Krise



Schadensfall aus der Praxis: Wiederherstellung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

- Trennung der Netzwerkverbindung
- Kontaktaufnahme IT Forensiker
- Kontaktaufnahme Rechtsanwalt
- Verständigung Polizei und Datenschutzbehörde
- Presseaussendung
- Aufbau einer neuen Infrastruktur (Neuinstallation aller Server und Clients)
- Kontaktaufnahme mit Hackern im Darknet
- Lösegeldzahlung für Entschlüsselungssoftware
- Wiederherstellung und Wiederbeschaffung der Daten
- Inbetriebnahme der neuen Infrastruktur

Prämienbeispiel für eine Cyberversicherung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Werbeagentur

- Jahresumsatz EUR 0,5 Mio.
- Versicherungssumme: EUR 1,0 Mio.
- Selbstbehalt: EUR 1.000,-
- Jahresprämie inkl. Steuer: rund EUR 970,-

Prämienbeispiel für eine Cyberversicherung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Holzindustrie

- Jahresumsatz EUR 15,0 Mio.
- Versicherungssumme: EUR 3,0 Mio.
- Selbstbehalt: EUR 10.000,-
- Jahresprämie inkl. Steuer: rund EUR 5.500,-

Prämienbeispiel für eine Cyberversicherung

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Baugewerbe

- Jahresumsatz EUR 25,0 Mio.
- Versicherungssumme: EUR 3,0 Mio.
- Selbstbehalt: EUR 10.000,-
- Jahresprämie inkl. Steuer: rund EUR 6.300,-

Cyberversicherungen für Unternehmen:

Sinnvoll oder unnötige Kosten?

ALT+PARTNER
VERSICHERUNGSLÖSUNGEN

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?

Anton Alt

Akad. Vkfm.

E-Mail: anton.alt@alt-partner.at

Impressum:

Autor:

Anton Alt, Akad. Vkfm.

8570 Voitsberg, Wiesengasse 16

Alle Rechte vorbehalten

Auflage: November 2022

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung ohne Zustimmung des Autors ist unzulässig. Das gilt insbesondere für Fotokopien, Vervielfältigungen, Übersetzung, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Es wird darauf hingewiesen, dass alle Angaben trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen. Eine Haftung des Autors ist ausgeschlossen.

Soweit im Folgenden personenbezogene Bezeichnungen nur in der männlichen Form angeführt sind, beziehen sie sich auf Frauen oder Männer in gleicher Weise. Bei der Anwendung auf bestimmte Personen wird die jeweils geschlechtsspezifische Form verwendet.