die Mobiliar

Referat Handelsrichter

Simon Seebeck, lic iur. Rechtsanwalt, Teamleiter HM Komplexschaden

Welche technologischen Trends beeinflussen uns…. ?

Welche technologischen Trends beeinflussen uns ?

Cloud Computing

Digitalisierung

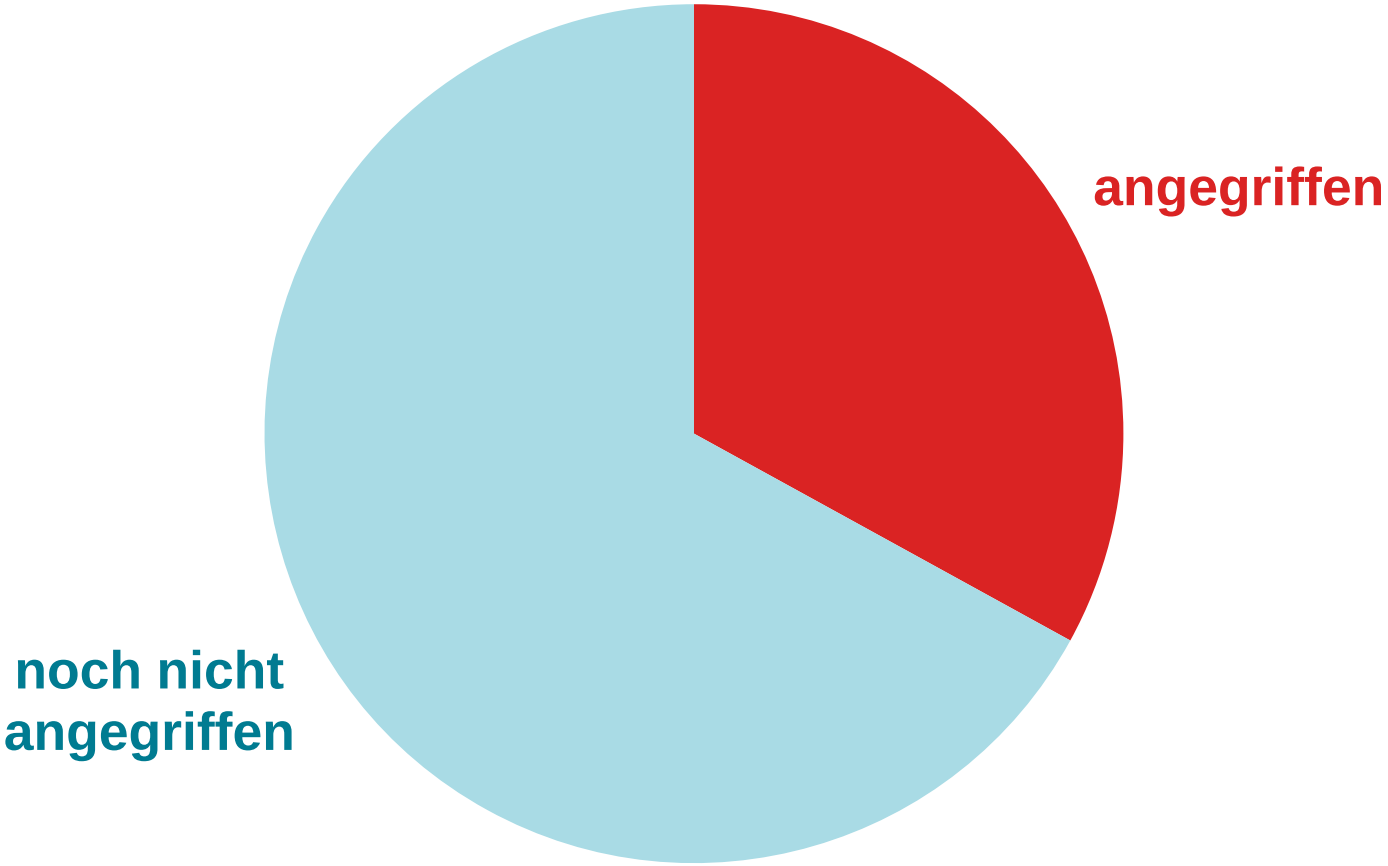
IoT

AI

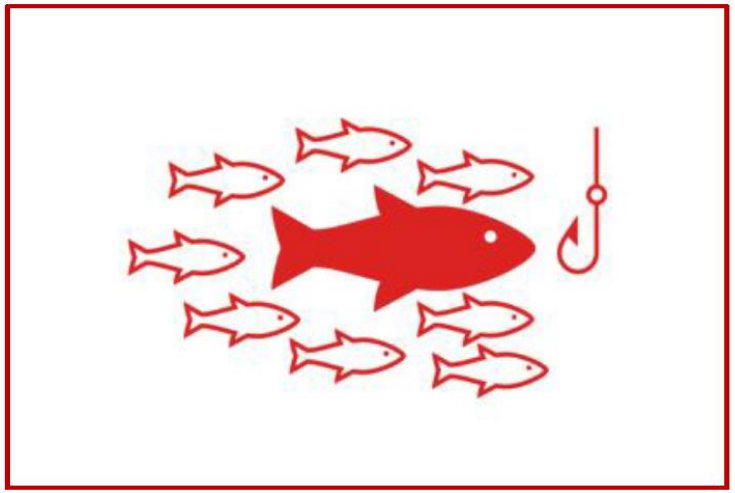
Big Data

- Alles, was digitalisiert werden kann, wird digitalisiert werden.
- Alles, was vernetzt werden kann, wird vernetzt werden.
- Alles, was automatisiert werden kann, wird automatisiert werden.
- Alles was analysiert werden kann wird analysiert.

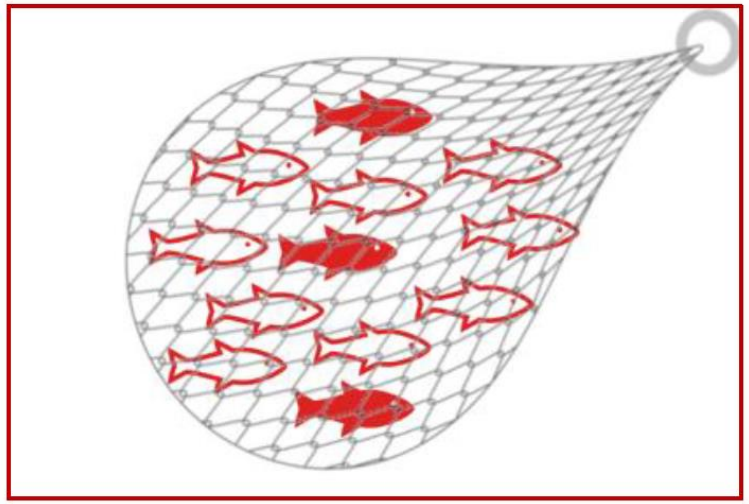
Erfolgreich angegriffene Unternehmungen



Was meinen Sie, wie denkt ein Hacker?

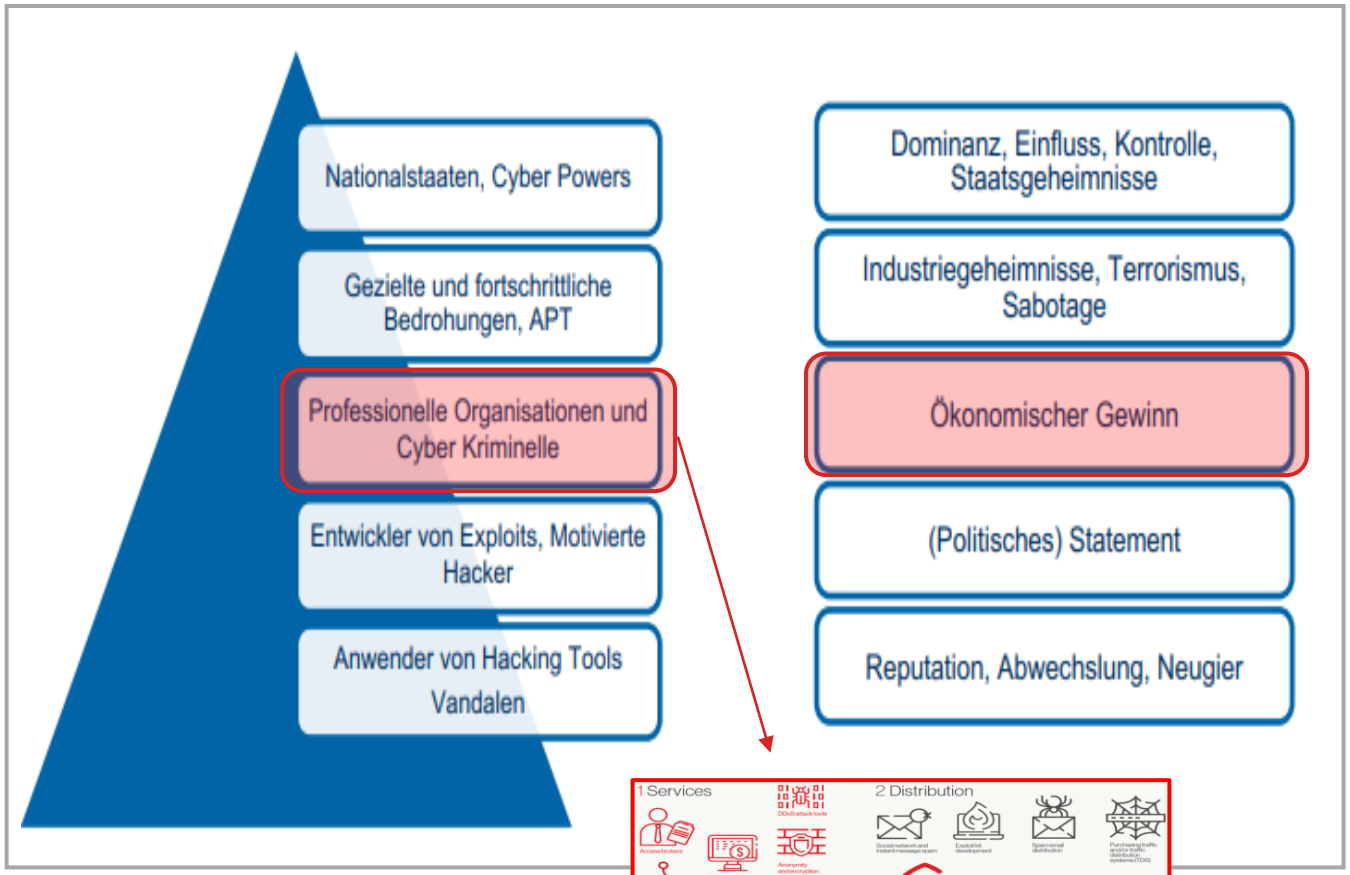


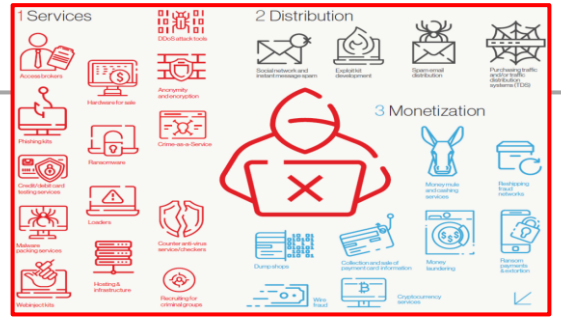
A) Ich hole mir die fetten Fische



Viele kleine Fische machen auch satt

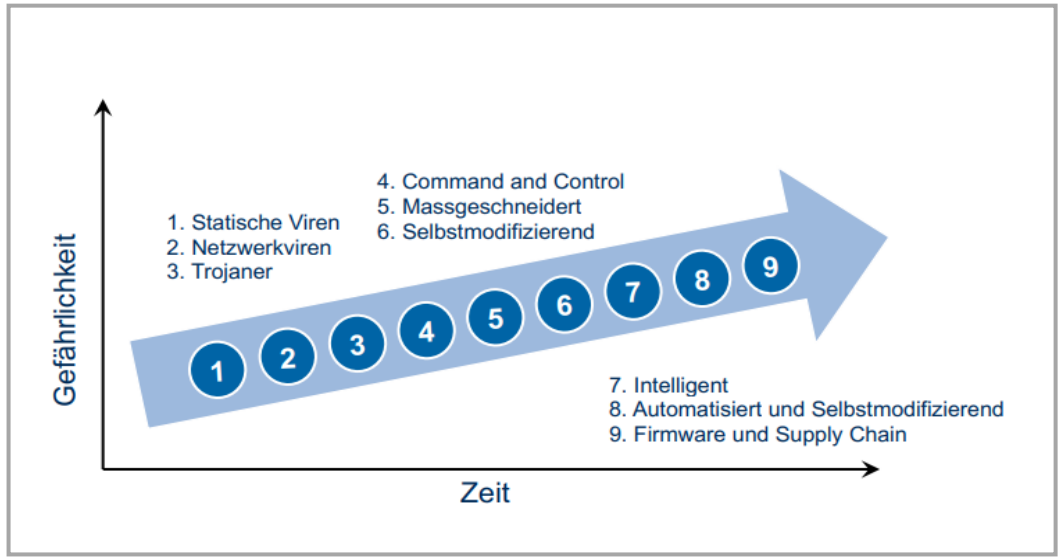
Wer greift an ?





APT = Advanced Persistent Threats

Die Entwicklung von Schadsoftware



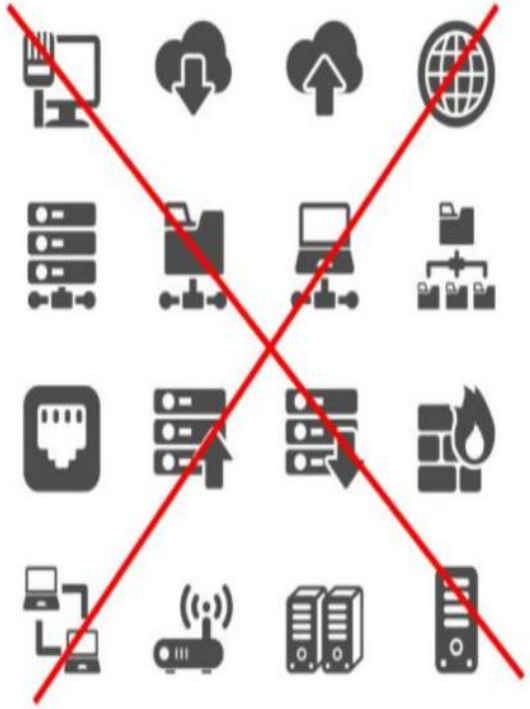
Hoher Profit – ohne Risiko!

	Ransomware	Kokain Schmuggel in 1992
Revenue/Unit	$140,000/attack	$60,000/kilo
Operating Costs/Unit	$2,500/attack*	$5,000/kilo
Profit Margin	98%	91%
Arrests/Unit	.0008**	.50
Deaths/Unit	0	.25
Barriers to Entry	None	Very High

Webinar Donald Ortmann, bitkom akademie 22.11.2022

Wo wird angegriffen ?

85 Prozent aller erfolgreichen Angriffe – erfolgen über den Menschen und nicht über die Maschine



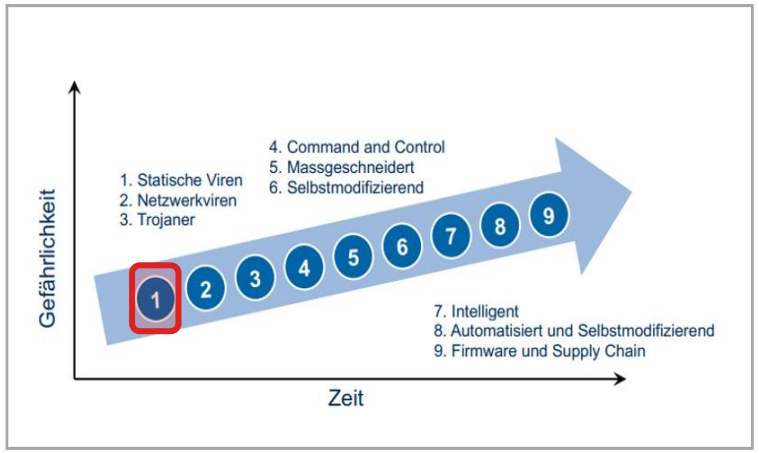
Quelle: Webinar Cyber-Samurai

Wie wird angegriffen - Creeper - der erste Computer Virus

1971

Erster Computer Virus von
Bob Thomas

Verursachte eine Drucker-
Fehlermeldung



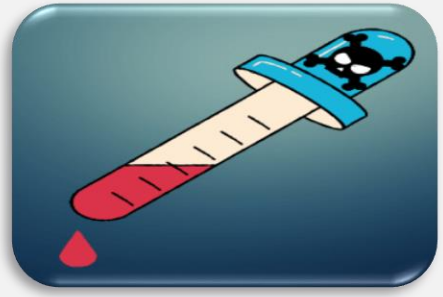
Emotet

2014

Bankentrojaner

Fokus: Bankdaten

2017



"Dropper"

Waffenplattform für Cyberkriminelle

2019

Spion

u.a. Kopieren von Zugangsdaten u Sammeln Mailadressen

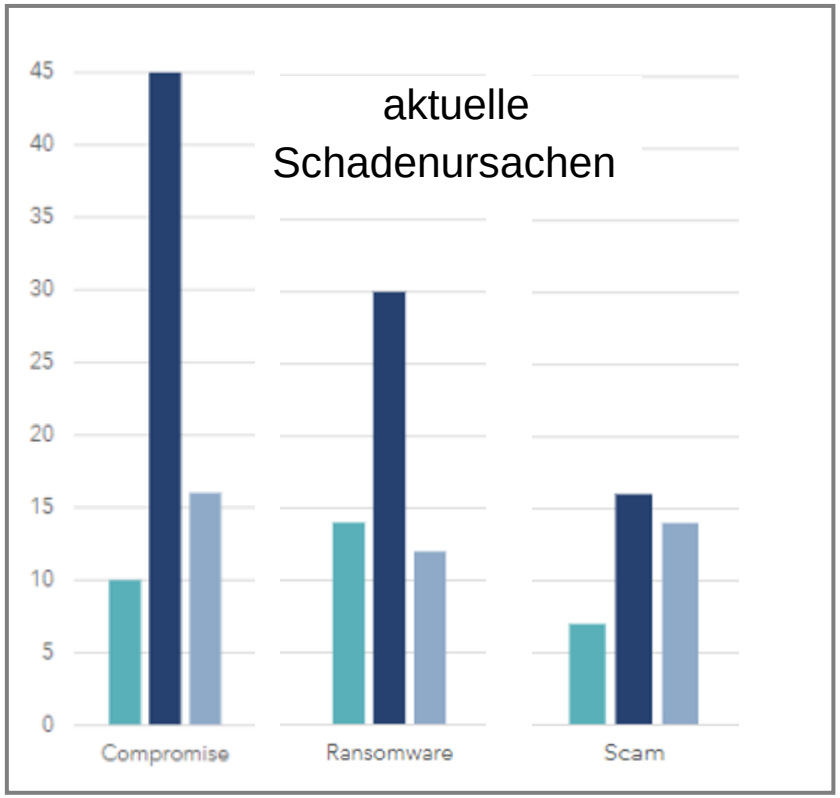
2020

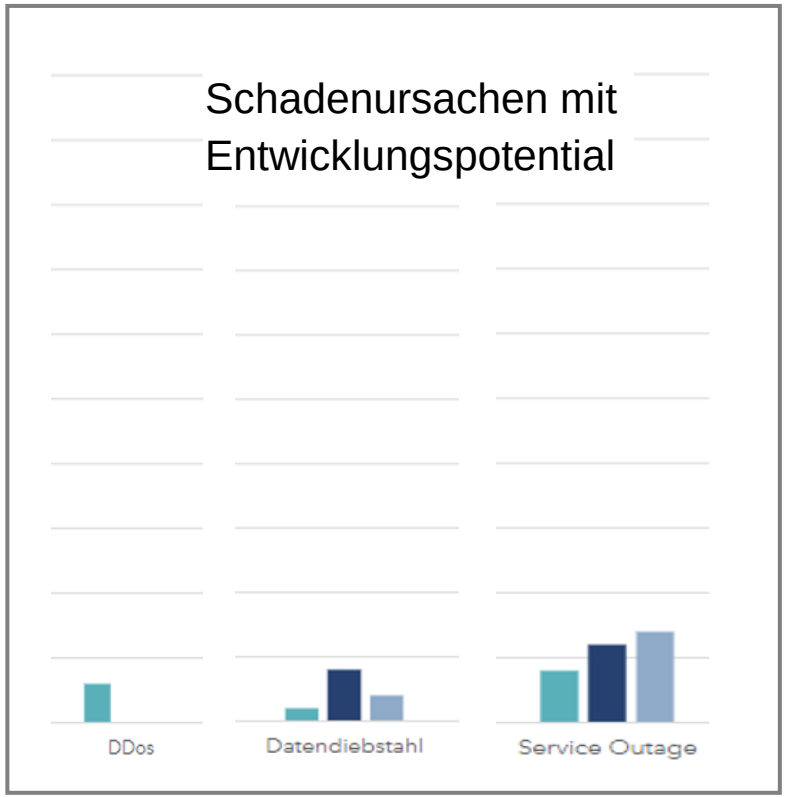
Er weiss, mit wem du sprichst….

Zugang zu Adressbücher und Mailprogrammen

Die Schadenfälle von heute sind nicht die Schadenfälle von morgen.

Zahlen 2022 - Schadenfälle aus dem Segment KMU/U

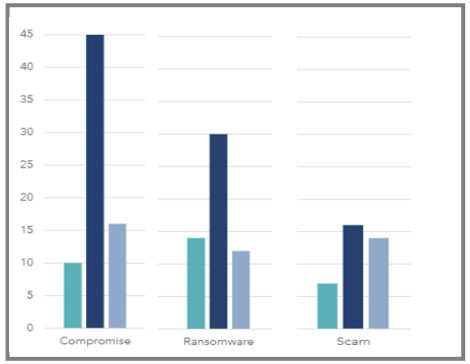




"Compromise"

Kommentar:
Die grössten Schadenkategorien sind: Schwachstellen (Compromise), Ransomware und Betrug (Scam). Zusätzlich waren Cloud-Dienstleister (Service Outage) vermehrt Ursache für Betriebsunterbrüche bei unseren VN.

Ein Krypto-Trojaner verschlüsselt die Daten ("*Ransomware*")



- Nach einer Phishing Mail installiert sich eine Verschlüsselungssoftware auf dem Rechner unseres Versicherungsnehmers (Zahnarzt).

- Der Zahnarzt hatte keinen Zugriff mehr auf seine Daten (Patienten-, Buchhaltungsdaten, Röntgenaufnahmen, etc.)
  – Offene Rechnungen von ca. CHF 100’000
  – Noch nicht verrechnete Arbeiten von ca. CHF 140’000
  – Keine Agenda
  – Die medizinischen Geräte konnte nicht mehr bedient werden

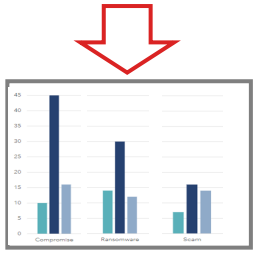
- Die Praxis war 3 Tage geschlossen.

- Der IT Partner des VN`s setzte alle Rechner neu auf. Die Daten konnten über ein Backup neu eingespielt werden.

Was ist zu tun?

- Reinigung der Rechner / Netzwerke
- Einspielen des Back Up
- Wiederherstellung von Daten

Ransomware Doppelangriff und 3 Erpressungen



SECURITY INSIDER

Ransomware und Daten-Exfiltration – eine gefährliche Kombination

Angriff

Daten werden gestohlen

Zugang zum Netzwerk wird im Darknet verkauft

Daten werden verschlüsselt

Erpressung

- Analyse Netzwerk
- Sammelt Passwörter
- 8 - 12 Monate im Netzwerk unterwegs
- Stört die Datensicherung (Backup)
- Kronjuwelen werden gefunden

Androhung:

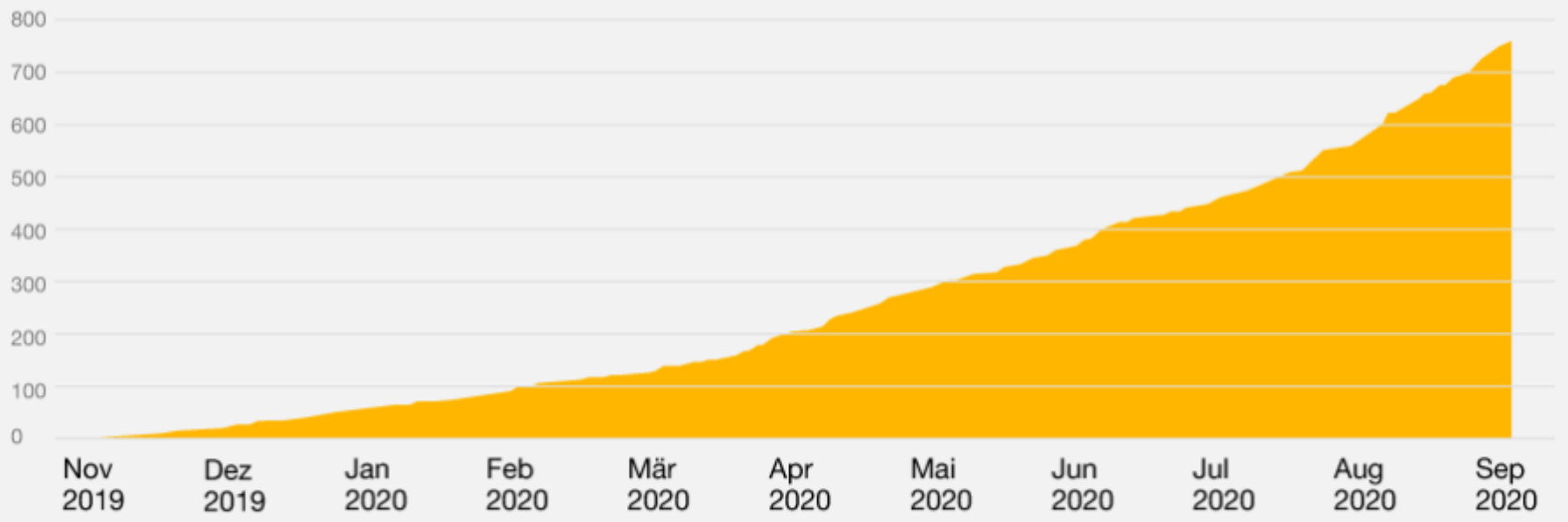
1 - Veröffentlichung (Daten Leak)

2 - Verlust der Daten

Erpressung Dritter

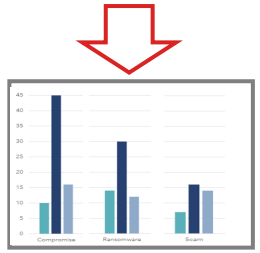
3

Anzahl der Ransomware Date Leaks



Quelle: PwC White Paper „Responding to the growing threat of human-operated ransomware attacks"

Beispiele: Doppelangriff und Daten-Exfiltration



CYBER-ATTACKE

Publiziert 4. Oktober 2021, 14:17

Hacker stellt Kundendaten von Zurich Versicherung online

Der Schweizer Versicherungsriese ist gehackt worden. Die Daten stehen im Darknet für den Download zur Verfügung. Passwörter oder Bankdaten sind laut Zurich Versicherung aber keine gestohlen worden.

NACH CYBERANGRIFF

Continental informiert von Datenraub betroffene Mitarbeiter

August 2022 / LockBit 3.0

TREUHANDBÜRO ERPRESST

Publiziert 9. November 2021, 20:56

Hacker stellen Schweizer Steuererklärungen ins Internet

Vertrauliche Daten von Privatpersonen und Firmen landeten im Internet. Hunderte Firmen sind von Cyberkriminalität betroffen.

Was tun unsere Versicherungsnehmer:

- System reinigen, Backup einspielen, allenfalls verlorene Daten wiederherstellen
- Meldung gemäss Datenschutzgesetze
- Unterbruch im Betrieb

Cloud Computing

*"**Cloud Computing** beschreibt ein Modell, das bei Bedarf – meist über das Internet und geräteunabhängig – zeitnah und mit wenig Aufwand geteilte Computerressourcen als Dienstleistung, etwa in Form von Servern, Datenspeicher oder Applikationen, bereitstellt und nach Nutzung abrechnet."*

- Angriff auf Cloud Dienstleistungsanbieter A

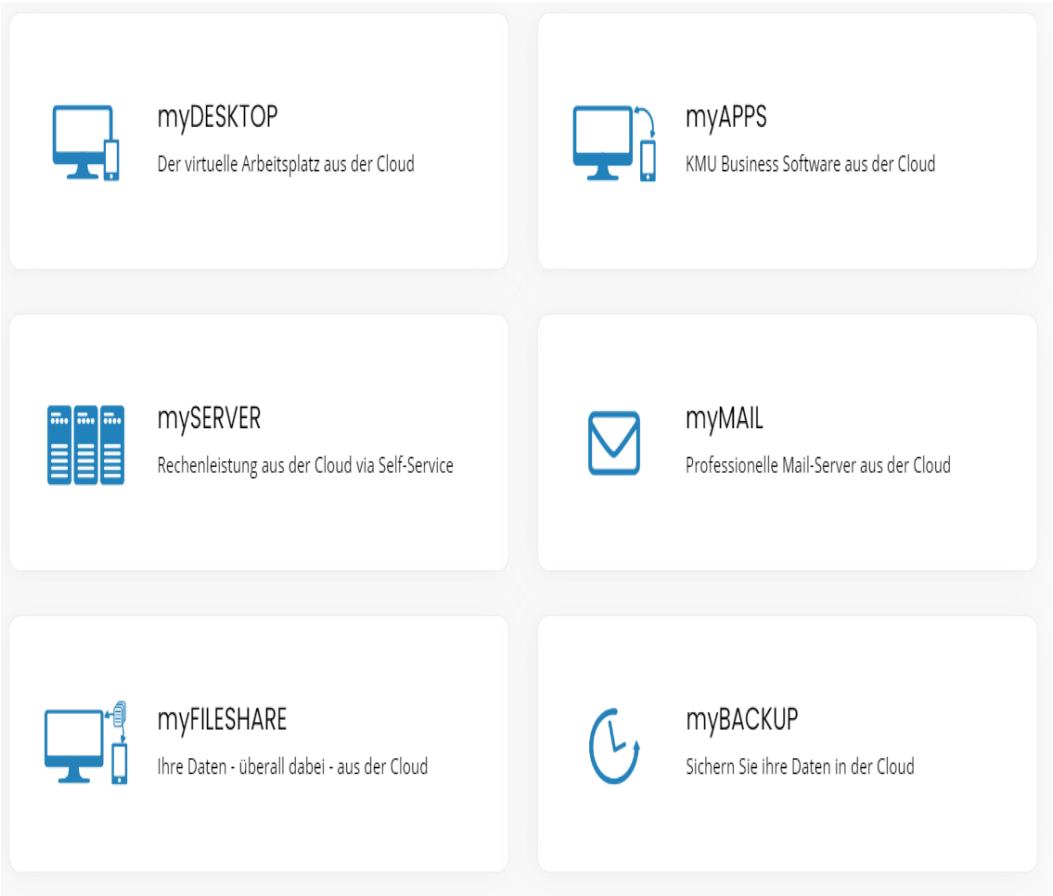
  insgesamt 5 Kunden betroffen:

- Angriff auf Cloud Dienstleistungsanbieter B

  Insgesamt 54 Kunden betroffen:

Kommentar:
Der Angriff auf einen Dienstleister betrifft in der Regel mehrere Versicherungsnehmer (Kumul).

Warum Cloud Computing nicht per Definition sicher ist:



Der Zugriff auf die Cloud erfolgt:

- Schwachstellen bei der Serversoftware,
- Konfigurationsfehler in der Cloudinfrastruktur,
- Anmeldedaten werden über gefälschte Anmeldeseiten abgegriffen und später für den Zugriff verwendet,
- Angreifern kann es gelingen, auf benachbarte Cloud Mandanten zu wechseln,
- …..

Cloud Computing

Azure-Lücke erlaubte Datenklau bei Millionen Office365-Kunden

Durch eine Fehlkonfiguration ließ sich Schadcode in Bing-Suchergebnisse einschleusen, womit Daten von Office365-Nutzern gefährdet waren. Microsoft hat reagiert.

MICROSOFT AZURE-RECHENZENTREN – ES GIBT KEINEN SICHERERE N ORT ZUM SPEICHERN IHRER DATEN

- **Schutz vor Cyber-Bedrohungen: Hohe Investitionen in IT-Sicherheit**

  Microsoft investiert **jedes Jahr 1 Milliarde US-Dollar in IT-Sicherheit**, um Ihre Daten vor Cyber-Bedrohungen zu schützen.

- **Hochqualifiziertes Experten-Team im Bereich Cyber-Security**

  Ein globales Team aus mehr als **3.500 hochqualifizierten Cyber-Security-Experten** arbeitet jeden Tag hart daran, Ihre Daten und andere Unternehmenswerte zu sichern und zu schützen.

Ein Betrug per Mail ("*Internetbetrug*")

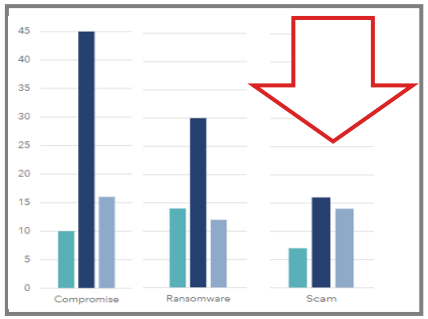
Sachverhalt

Eine Mitarbeiterin des VN (=Hotel) erhielt einen Anruf von einer Dame, die sich als Buchhalterin von Booking.com ausgab.

Sie verlangte die letzte Originalrechnung von Booking.com mit dem Hinweis, dass sie auf die Rechnung einen Rabatt gewähren würde.

Die VN-Mitarbeiterin schickte die Originalrechnung per E-Mail an die Dame. Danach erhielt sie die Rechnung mit dem Rabatt.

Der Buchhalter erkannte den Betrug, als Booking.com darauf hinwies, dass die Rechnung noch immer nicht bezahlt war.



Das Schadenbild:

- Ein Vermögensschaden

Betrug

Booking.com

Booking.com B.V.
Herengracht 597
1017 CE Amsterdam
Netherlands
VAT number: NL805734958B01
CH VAT number: CHE-415.972.701 MWST
Registered in the Netherlands No.: 31047344
https://www.booking.com

Accommodation number:	1410371
VAT number:	CHE352530324IVA
Invoice number:	1573248941
Date:	03/04/2022
Period:	01/03/2022 - 31/03/2022

INVOICE

Description	Room Sales	Commission
Reservations	CHF 90,760.35	CHF 13,614.05
7.7% VAT on CHF 13,614.05		CHF 1,048.28
Total amount due		**CHF 14,662.33**

Payment Due: April 16, 2022

Please transfer the due amount to our bank account below by the Payment Due date. Be sure to include INVOICE 1573248941 and ACCOMMODATION NUMBER 1410371 with your payment instructions.

Deutsche Bank AG
Uraniastrasse 9
8001 Zurich
Switzerland
Bank Code: 87801
SWIFT: DEUTCHZZXXX
ACCOUNT: 03000384000
IBAN: CH6887801003000384000

Booking.com

Booking.com B.V.
Herengracht 597
1017 CE Amsterdam
Niederlande
Telefon: +41445111641
USt-IdNr.: NL805734958B01
MWST-Nummer (CH): CHE-415.972.701 MWST
Registriert in den Niederlanden unter Nr.: 31047344
https://www.booking.com

Accommodation number:	1410371
VAT number:	CHE352530324IVA
Invoice number:	1573248941
Date:	03/04/2022
Period:	01/03/2022 - 31/03/2022

INVOICE

Description	**Room Sales**	**Commission**
Reservations	CHF 90,760.35	CHF 13,614.05
Credit		**CHF -427.20**
7.7% VAT of 13'186.85 CHF		CHF 1'015.38
Total amount due		**CHF 14'202.23**

Payment Due: April 8, 2022

We inform you that this invoice can be paid (partially) by the amount we owe you in accordance with the (payment) clauses corresponding to our General Service Conditions. If the amount stated in the invoice exceeds the amount due, please follow the payment instructions mentioned below.

Please transfer the amount due to our account below no later than the payment due date. Make sure to include Invoice number 1573248941 and Accommodation number 1410371 on your payment instructions.

THE CURRENCY CLOUD LIMITED
BIC: TCCLGB3L
IBAN: GB14 TCCL 0414 0410 2293 57

Booking.com

Booking.com B.V.
Herengracht 597
1017 CE Amsterdam
Netherlands
VAT number: NL805734958B01
CH VAT number: CHE-415.972.701 MWST
Registered in the Netherlands No.: 31047344
https://www.booking.com

Accommodation number:	1410371
VAT number:	CHE352530324IVA
Invoice number:	1573248941
Date:	03/04/2022
Period:	01/03/2022 - 31/03/2022

INVOICE

Description	Room Sales	Commission
Reservations	CHF 90,760.35	CHF 13,614.05
7.7% VAT on CHF 13,614.05		CHF 1,048.28
Total amount due		**CHF 14,662.33**

Payment Due: April 16, 2022

Please transfer the due amount to our bank account below by the Payment Due date. Be sure to include INVOICE 1573248941 and ACCOMMODATION NUMBER 1410371 with your payment instructions.

Deutsche Bank AG
Uraniastrasse 9
8001 Zurich
Switzerland
Bank Code: 87801
SWIFT: DEUTCHZZXXX
ACCOUNT: 03000384000
IBAN: CH6887801003000384000
ACCOUNT HOLDER: Booking.com B.V.
ACCOUNT CURRENCY: CHF

Booking.com

Booking.com B.V.
Herengracht 597
1017 CE Amsterdam
Niederlande
Telefon: +41445111641
USt-IdNr.: NL805734958B01
MWST-Nummer (CH): CHE-415.972.701 MWST
Registriert in den Niederlanden unter Nr.: 31047344
https://www.booking.com

Accommodation number:	1410371
VAT number:	CHE352530324IVA
Invoice number:	1573248941
Date:	03/04/2022
Period:	01/03/2022 - 31/03/2022

INVOICE

Description	Room Sales	Commission
Reservations	CHF 90,760.35	CHF 13,614.05
Credit		**CHF -427.20**
7.7% VAT of 13'186.85 CHF		CHF 1'015.38
Total amount due		**CHF 14'202.23**

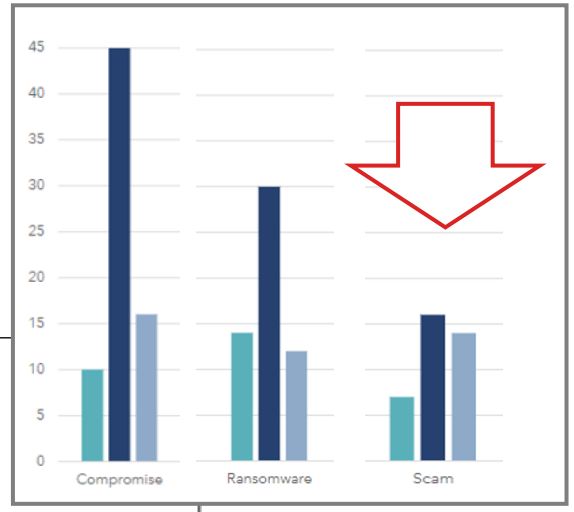
Payment Due: April 8, 2022

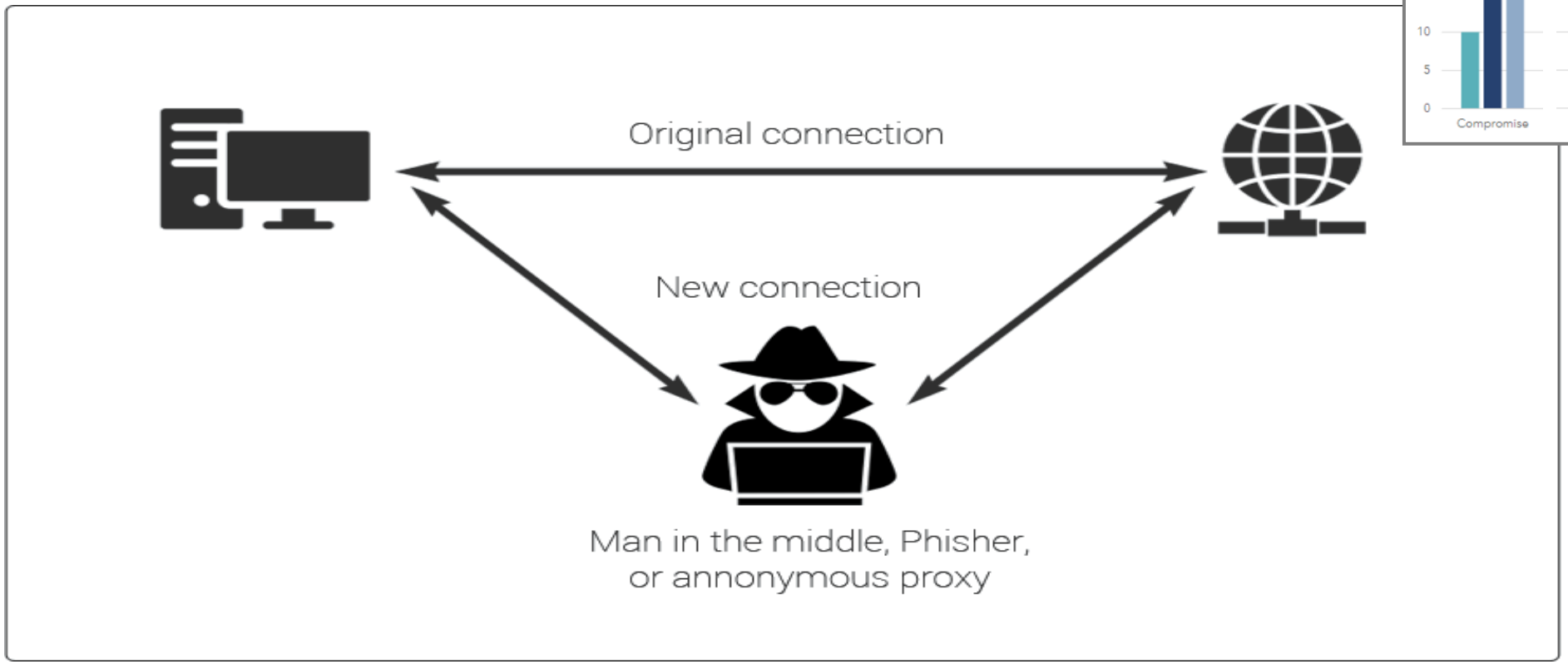
We inform you that this invoice can be paid (partially) by the amount we owe you in accordance with the (payment) clauses corresponding to our General Service Conditions. If the amount stated in the invoice exceeds the amount due, please follow the payment instructions mentioned below.

Please transfer the amount due to our account below no later than the payment due date. Make sure to include Invoice number 1573248941 and Accommodation number 1410371 on your payment instructions.

THE CURRENCY CLOUD LIMITED
BIC: TCCLGB3L
IBAN: GB14 TCCL 0414 0410 2293 57
ACCOUNT OWNER: Booking.com B.V.
ACCOUNT CURRENCY: CHF.

Scam / Betrug





System des VN`s wurde nicht angegriffen !!

Betrug per Mail – Der Enkeltrick

Kunde meldet sich per Mail und zeigt eine neue Bankverbindung an.

Kunde mahnt Zahlungsausstand. Gibt an, keinen Bankwechsel vorgenommen und angezeigt zu haben.

Rechnung wird bezahlt

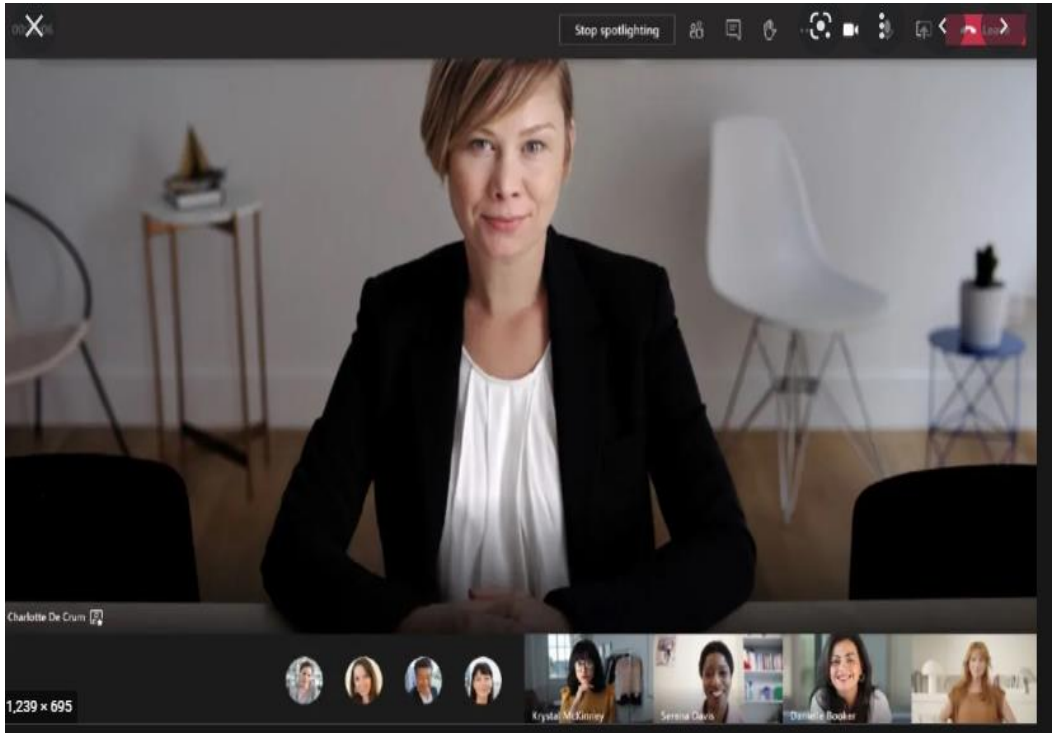
R.Mueller@Muelller.ch

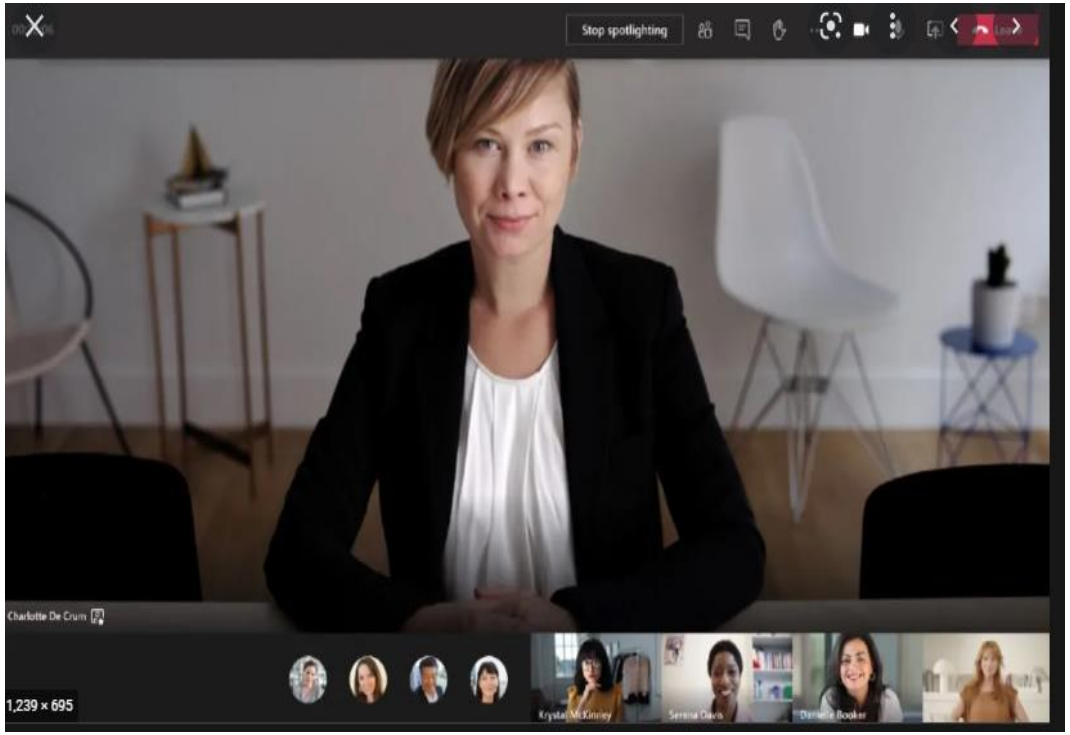
R.Mueller@Mueller.ch

Das Schadenbild:

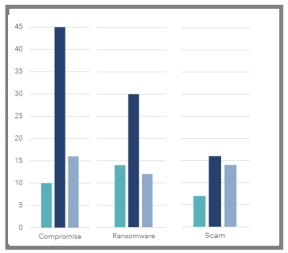
- Ein Vermögensschaden

Der Betrug von morgen.... welches ist die echte Chefin ?





Eine Schwachstelle wird ausgenutzt – MS Exchange



2021

Microsoft veröffentlicht Not-Patches für Exchange Server

SECURITY, BREACH, ATTACKE, MICROSOFT

Die vier Schwachstellen tragen die Nummern CVE-2021-26857, CVE-2021-26855, CVE-2021-26858 und CVE-2021-27065.

Bundesamt für Sicherheit in der Informationstechnik

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

2022

Microsoft *03.10.2022, 09:21 Uhr*

Microsoft Exchange weist Zero-Day-Lücke auf

Microsoft Exchange hat zwei ungepatchte Zero-Day-Schwachstellen. Diese werden bereits aktiv ausgenutzt, warnt Redmond.

Angriff ohne Interaktion

Microsoft warnt vor kritischer Outlook-Schwachstelle

Seit April 2022 haben Angreifer aus Russland europäische Unternehmen und Organisationen über eine schwere Sicherheitslücke in Outlook attackiert, meldet Microsoft. Alle Windows-Versionen sind betroffen.

Schwachstellen

BEDROHUNGSSTUFE		
3 Hoch	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 05.04.2023	Version 1.1: Schadhafte Version der 3CX Desktop App im Umlauf
1 Niedrig	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 04.04.2023	Informationssicherheit in der Gebäudeautomation - Mangelhafte Dokumentation und Betrieb von undokumentierten Fernwartungszugängen
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 16.03.2023	Aktive Ausnutzung einer Schwachstelle in Microsoft Outlook
3 Hoch	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 08.02.2023	Version 1.2: Schwachstelle in VMware ESXi weltweit massiv ausgenutzt
2 Mittel	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 19.01.2023	Cisco VPN Geheimnisse in Klartext auslesen
3 Hoch	CYBER-SICHERHEITSWARNUNG • SICHERHEITSHINWEIS • 16.01.2023	Aktive Ausnutzung einer kritischen Sicherheitslücke in Control Web Panel

Bundesamt für Sicherheit in der Informationstechnik

20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

Ransomware-Bande Play bekennt sich zu Angriff auf NZZ und CH Media

Von Philipp Anz, 17. April 2023 um 16:13

IT INSIDE IT

Dimension der MS Exchange Lücke

Gruppe	Typische Zielregionen	Typische Sektoren	Typische Malware	Zugang zu Exploits
Hafnium	Nordamerika	ThinkTanks, NGOs, Rüstung, Kanzleien, Corona-Forschung	Mist	Vor Bekanntwerden
Tick/ BronzeButler	Ostasien, Russland	u.a. IT	Datper, Daserf, xxmm, Lilith, ShadowPad	Vor Bekanntwerden
LuckyMouse/ APT27/ EmissaryPanda	Zentralasien, Mittlerer Osten,	Behörden, intern. Organisationen	SysUpdate/ Soldier, HyperBro	Vor Bekanntwerden
Tonto Team/ Karma Panda/ Cactus Pete	Osteuropa, Asien	Regierung, IT	ShadowPad, Bisonal	Nach dem Patch
Calypso	Zentralasien, Mittlerer Osten, Südamerika, später auch Afrika, Asien, Europa	Regierungen, ungenannte Wirtschafts-sektoren	PlugX, Whitebird/ Agent.UFX	Vor Bekanntwerden
Mikroceen/ Vicious Panda	Zentralasien	Regierungen, Telkos	Mikroceen RAT	Nach dem Patch
„Winnti"-Nutzer	Ostasien	Chemie, Gesundheit, Telkos, Energie, Spiele	PlugX, Winnti v4	Vor Bekanntwerden
Websiic	Asien, Osteuropa	IT, Telko, Maschinenbau, Regierungen	Eigener Loader	Vor Bekanntwerden
DLTMiner	**weltweit**	**ungezielt**	**CryptoMiner**	**Nach dem Patch**
Unbekannte Gruppe	**u.a. Deutschland**	**großflächig**	**CobaltStrike**	**Nach dem Patch**

Mehrere Schwachstellen in MS Exchange

Bundesamt für Sicherheit in der Informationstechnik

CSW-Nr. 2021-197772-11032, Version 1.10, 17.03.2021

IT-Bedrohungslage*: 3 / Orange

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Was tun unsere Versicherungsnehmer:

- IT-Dienstleister spielen den Sicherheitspatch ein.
- Scan der Server – Suche nach dem Angriff.
- Neu Aufsetzen der Server oder wo nicht möglich, forensische Untersuchung – Suche nach Angriff.

Verletzte Lizenzrechte

Image Professionals GmbH
./.
aloha yoga gmbh

wegen unlizenzierter Vervielfältigung und öffentlicher Zugänglichmachung geschützten Bildmaterials

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit sind wir beauftragt, die rechtlichen Interessen der **Image Professionals GmbH**, Tumblingerstraße 32, 80337 München wahrzunehmen. Unsere ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Unsere Mandantschaft ist eine renommierte, international tätige Bildagentur, die ihr Repertoire weltweit vermarktet.

Anlass unserer Beauftragung ist die unerlaubte Verwendung von geschütztem Bildmaterial.

lookphotos

Loisach am Kochelsee im Winter, Oberbayern, Deutschland

Bildnummer:	70310178
Lizenzart:	Lizenzpflichtig
Fotograf:	© lookphotos / Wothe, Konrad
Aufnahmedatum:	30.12.2008
Rechte:	Exklusivrechte auf Anfrage verfügbar
Modell-Rechte:	nicht erforderlich
Eigentums-Rechte:	nicht erforderlich
Druckgröße:	ca. 43,18 × 28,79 cm bei 300dpi geeignet für Formate bis DIN A4

25. April 2023

Art. 24 des neuen Datenschutzgesetzes – in Kraft ab September 2023

Art. 24 Meldung von Verletzungen der Datensicherheit

[1] Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

[2] In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

[4] Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

"Man habe "private und persönliche vertrauliche Daten, Projekte, Gehaltslisten, Mitarbeiterinformationen und mehr" erbeutet. "

Ransomware-Bande Play bekennt sich zu Angriff auf NZZ und CH Media

IT INSIDE IT

Von Philipp Anz, 17. April 2023 um 16:13

Bei der Medienstelle von CH Media heisst es auf unsere Anfrage zum Bekennerschreiben von Play: "Wir wurden via NZZ durch das NCSC informiert, dass als Folge des Ransomware-Angriffs auch aus unserem Konzern Daten im Darknet angeboten werden. Aktuell ist uns nur ein sehr kleiner Datenabfluss bekannt, wobei die Analysearbeiten noch laufen."

Herausforderungen bei der Versicherbarkeit

Risiken sind nicht unabhängig, Kumulrisiko	Fehlen von Daten für die Modellierung für Cyber Risiken
Dynamische Veränderungen	Risikokollektive sind noch relativ klein

6 Fragen für den Heimweg für jeden Chef eines KMU

- Ist Cybersicherheit schon Chefsache ?
- Mit welchen Daten arbeiten wir - was sind unsere Kronjuwelen?
- Mit welchen Massnahmen können wir rasch die Sicherheit verbessern?

  (Passwort Qualität / 2 Faktoren Identifikation / Vier Augen Prinzip / Mitarbeitersensibilisierung)
- Wie reagieren wir, wenn wir angegriffen sind, welches sind unsere Partner ?
- Wie können wir bei einem Angriff den Betrieb weiter führen ?

Vielen Dank für Ihre Aufmerksamkeit !