CYBER SECURITY

Aktuelle Bedrohungen und Quick Wins

16.11.2022

Mario NEUBAUER
BDO Austria

BDO

VORSTELLUNG

BDO Consulting / Cyber Security

Mario
Neubauer
Manager

+43 664 60 375 - 4253
mario.neubauer@bdo.at

bdo.at/cyber

BEREICH: CONSULTING

Innovation, Transformation und Sicherheit brauchen die besten
Köpfe - BDO Consulting hat sie.

Wir begegnen komplexen Aufgabenstellungen mit breiten, innovativen Lösungen, state-of-the-art Tools und umfassendem Know-how - von der ersten Analyse bis zur finalen Implementierung, national sowie international.

Denn unser Ziel ist Ihr nachhaltiger Erfolg!

Management Consulting

Cyber Security & Digital Services

Information Technology

Risk & Resilience

People & Organisation

Förderungen & Forschung

WER WIR SIND

BDO AUSTRIA

Großartiges Unternehmertum verdient besondere Aufmerksamkeit!

Nur wer zuhört und versteht, kann Sie auch umfassend betreuen. Darum ist BDO Ihr verlässlicher Wegbegleiter. Zusammen stellen wir die Weichen für Ihr Projekt und finden passende Lösungen - damit Sie sicher ins Ziel kommen.

Für Ihre Strategie setzen wir alle Hebel in Bewegung: Je nach Aufgabenstellung stellen wir das optimale Team für Sie zusammen.

Das macht uns zu BDO.
Und uns gemeinsam great.

STANDORTE

WIEN, GRAZ, LINZ, SALZBURG, KLAGENFURT, DORNBIRN, JUDENBURG, BRUCK/LEITHA, OBERWART

SERVICE-BEREICHE

AUDIT, TAX, CONSULTING, CORPORATE FINANCE, BUSINESS SERVICES & OUTSOURCING

KUND:INNEN
12.000+

MITARBEITER:INNEN
900+

PARTNER:INNEN
51

STANDORTE
9

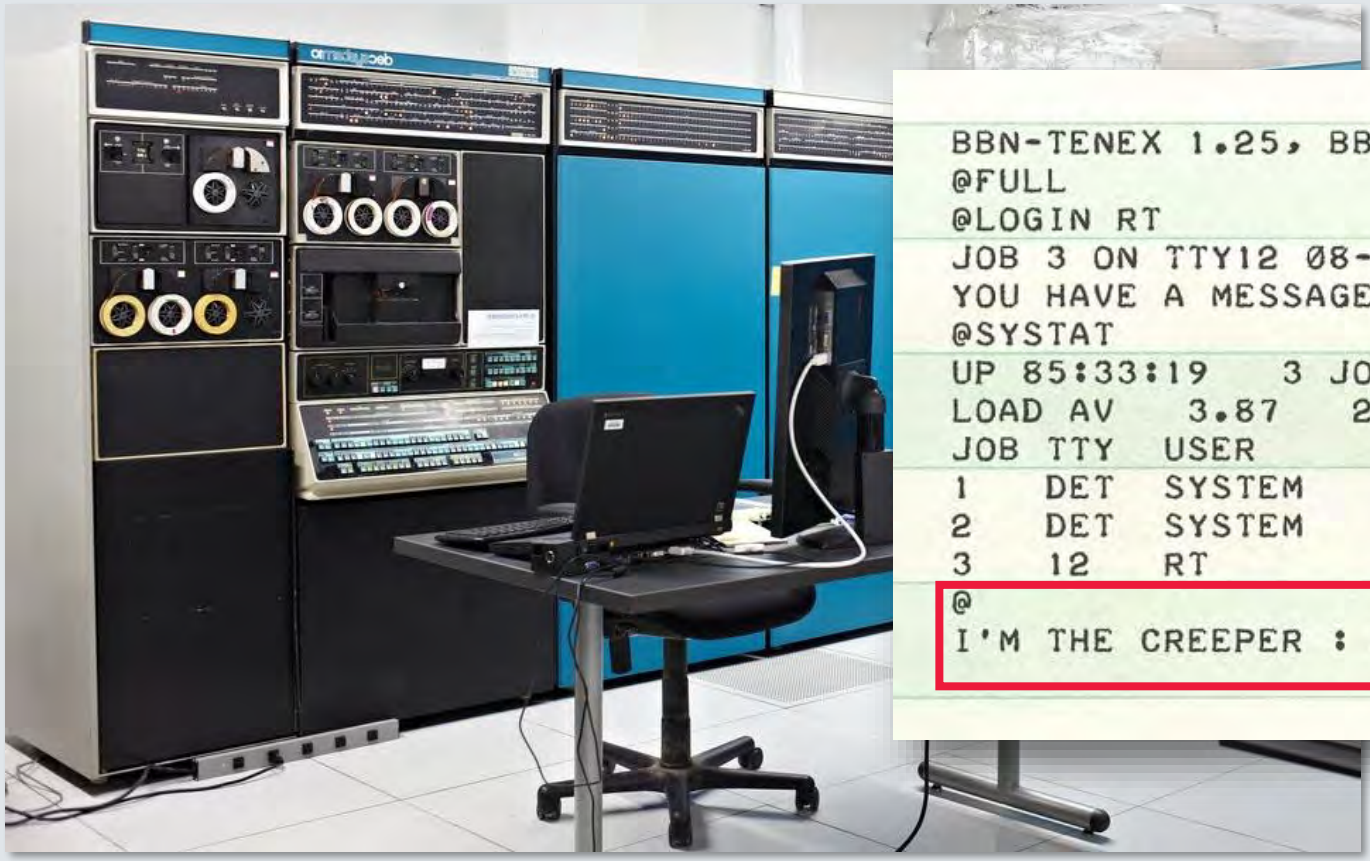
UMSATZ 2020/21
EUR 102,7 MIO.

GRÜNDUNG
1976

Stand: Dezember 2021

WIE ALLES BEGANN - 1971

IT-Security / Cyber-Security



```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER      SUBSYS
1   DET  SYSTEM    NETSER
2   DET  SYSTEM    TIPSER
3   12   RT        EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

https://corewar.co.uk/creeper.htm

https://www.livingcomputers.org/Computer-Collection/Vintage-Computers/Mainframes/DEC-PDP-10-KI-10-(DECsystem-10).aspx

CYBER SECURITY RISIKEN

Cyber Crime und seine Auswirkungen

REPUTATIONSVERLUST

Website Defacement
Fake News
Datenlecks

DATENDIEBSTAHL

Hacking von Webseiten und IT-Netzwerken über Schwachstellen

ERPRESSUNG

Denial-of-Service Angriffe
Ransomware

AUSNUTZUNG VON RESSOURCEN

Crypto-Mining
Botnetze

SPIONAGE

Social Engineering
Phishing

BETRUG

CEO - Fraud
Fake President Angriffe

SABOTAGE

Lahmlegen des Unternehmens
Ransomware

WER SIND DIE PROFITEURE VON CYBER CRIME?

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

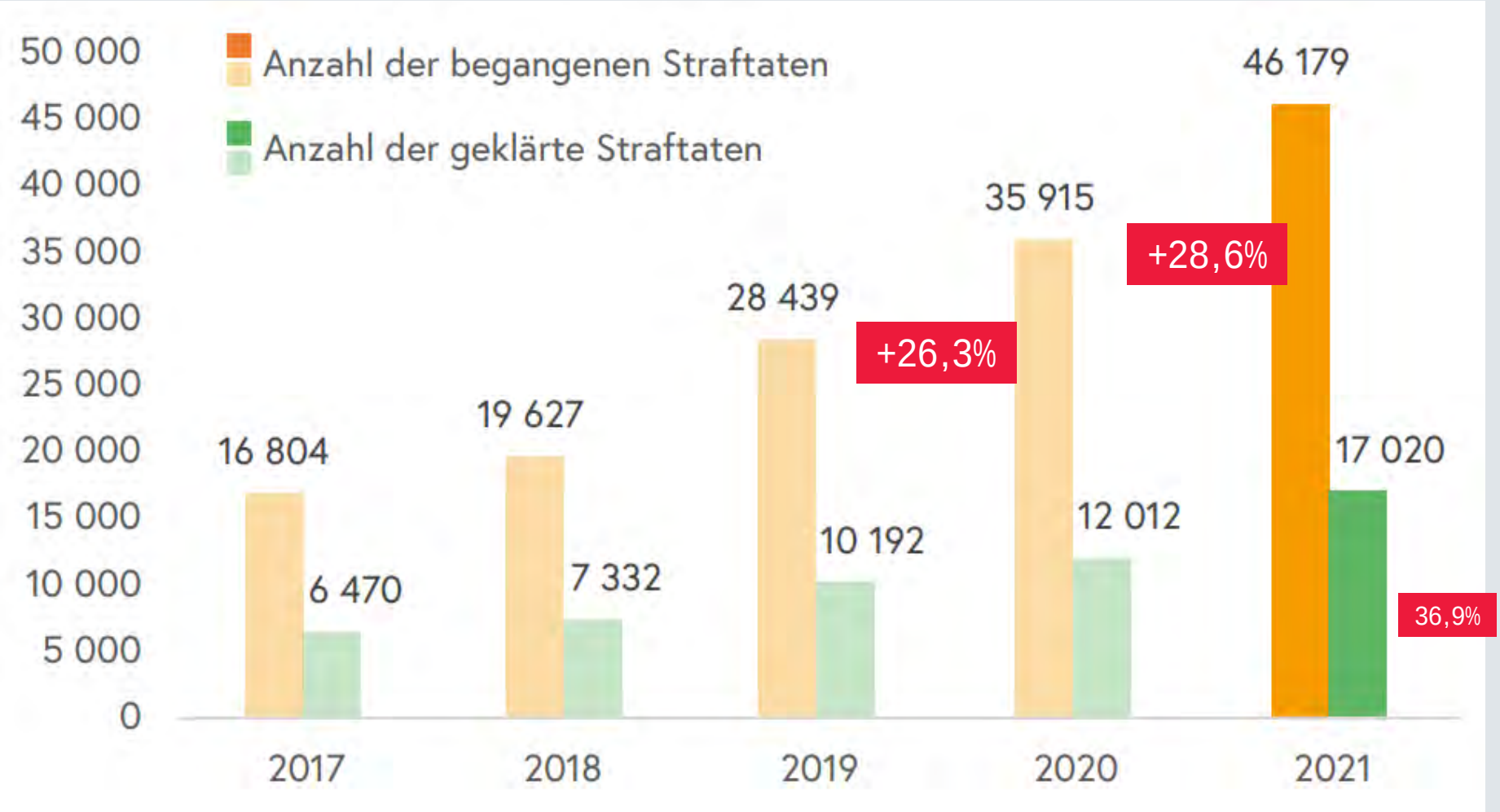
Hacker Group
REvil

https://www.interpol.int/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring
https://www.bbc.com/news/technology-59297187

AKTUELLE BEDROHUNGEN

CYBER CRIME IN ÖSTERREICH

Straftaten vs. geklärte Straftaten - Report 2021



https://bundeskriminalamt.at/306/files/2022-222_Cybercrime_Report_2021_-_V20220621_1030_webBF.pdf

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

DI Walter Stephan (CEO) aus dem Vorstand der FACC AG mit sofortiger Wirkung abberufen

Der Aufsichtsrat hat in seiner Sitzung vom 24. Mai 2016 Herrn DI Walter Stephan als Vorsitzenden des Vorstandes der FACC AG mit sofortiger Wirkung aus wichtigem Grund abberufen. Der Aufsichtsrat ist zum Schluss gekommen, dass Herr DI Walter Stephan seine Pflichten schwerwiegend verletzt hat, insbesondere im Zusammenhang mit dem "Fake President" Vorfall.

Hr. Robert Machtlinger wurde vorübergehend als CEO der FACC AG bestellt.

25/05/2016 | Ad-Hoc

FACC war Anfang 2016 Opfer eines "Fake President Fraud" geworden. Betrüger hatten sich gegenüber der Buchhaltung des Unternehmens als Firmenchefs ausgegeben und in mehr als 92 "streng vertraulichen" Mails die Überweisung von 54 Millionen Euro auf ausländische Konten gefordert. Die Buchhaltung kam der vermeintlichen Weisung des Vorstands nach.

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

TAUSENDE BETROFFEN

Land Kärnten nach Hackerangriff im Notbetrieb

Attacke wurde Dienstag bemerkt. Komplettes IT-System musste heruntergefahren werden. Dass Daten gestohlen worden sind, sei unwahrscheinlich, könne aber nicht ausgeschlossen werden.

Die gesamte Telefonanlage ist ausgefallen, das Mailsystem funktioniert auch nicht. Rund 3.900 Mitarbeiter und etwa 3.000 PC-Anschlüsse sind betroffen

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

06.09.2022, 21:51

Hackerangriff auf Steirer-Gemeinde – Lösegeld gefordert

Am Wochenende wurden Mitarbeiter der Stadtgemeinde Feldbach (ST) auf einen Cyber-Angriff aufmerksam. Die Hacker fordern Lösegeld in Bitcoin.

Mit einem Verschlüsselungstrojaner haben Hacker die Stadtgemeinde Feldbach angegriffen. Bis zu 10 Terabyte an Daten auf dem Verwaltungsserver könnten betroffen sein.

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

Daten gestohlen: Erpresser fordern 50 Millionen Euro von Kärntner Stadt

Hacker wollen IT-System der Stadt gehackt und Daten gestohlen haben. Laut dem Bürgermeister gäbe es derzeit keine Hinweise darauf.

Erpresser haben die Kärntner Bezirkshauptstadt Spittal an der Drau im Visier. Diese Woche war ein E-Mail eingetroffen, in dem die Absender 2.900 Bitcoins *(mehr als 50 Millionen Euro, Anmerkung)* forderten. Sie hätten nämlich das IT-System der Stadt gehackt und Daten gestohlen, bestätigte Bürgermeister Gerhard Köfer (Team Kärnten) auf APA-Anfrage einen Bericht der *Kronen Zeitung*. Bisher gebe es aber keine Hinweise, dass es wirklich einen Hackerangriff gegeben habe.

Diese Woche war ein E-Mail eingetroffen, in dem die Absender 2.900 Bitcoins (mehr als 50 Millionen Euro, Anmerkung) forderten. […] Bisher gebe es aber keine Hinweise, dass es wirklich einen Hackerangriff gegeben habe.

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

DATEN GESTOHLEN

Hacker-Angriff auch auf Weiz: „Wir hatten Glück“

Hacker haben die Verwaltung der Stadtgemeinde Feldbach lahmgelegt und fordern Lösegeld. Vor zwei Jahren war Weiz mit einer ähnlichen Cyber-Attacke konfrontiert - und kam glimpflich davon.

Nichts ist passiert. Und so kann Eggenreich mittlerweile gelassener über den Vorfall im Mai 2020 sprechen. Damals war die Stadt Weiz Opfer eines Angriffs von Hackern. Gestohlen wurden insgesamt 27 Gigabyte an Daten von einem alten Laufwerk aus dem Jahr 2018. Die Diebe drohten damit, die Beute im sogenannten Darknet, einem abgeschotteten Sammelplatz von Kriminellen im Internet, zu veröffentlichen - und sie wollten eine hohe Summe in der Kryptowährung Bitcoin.

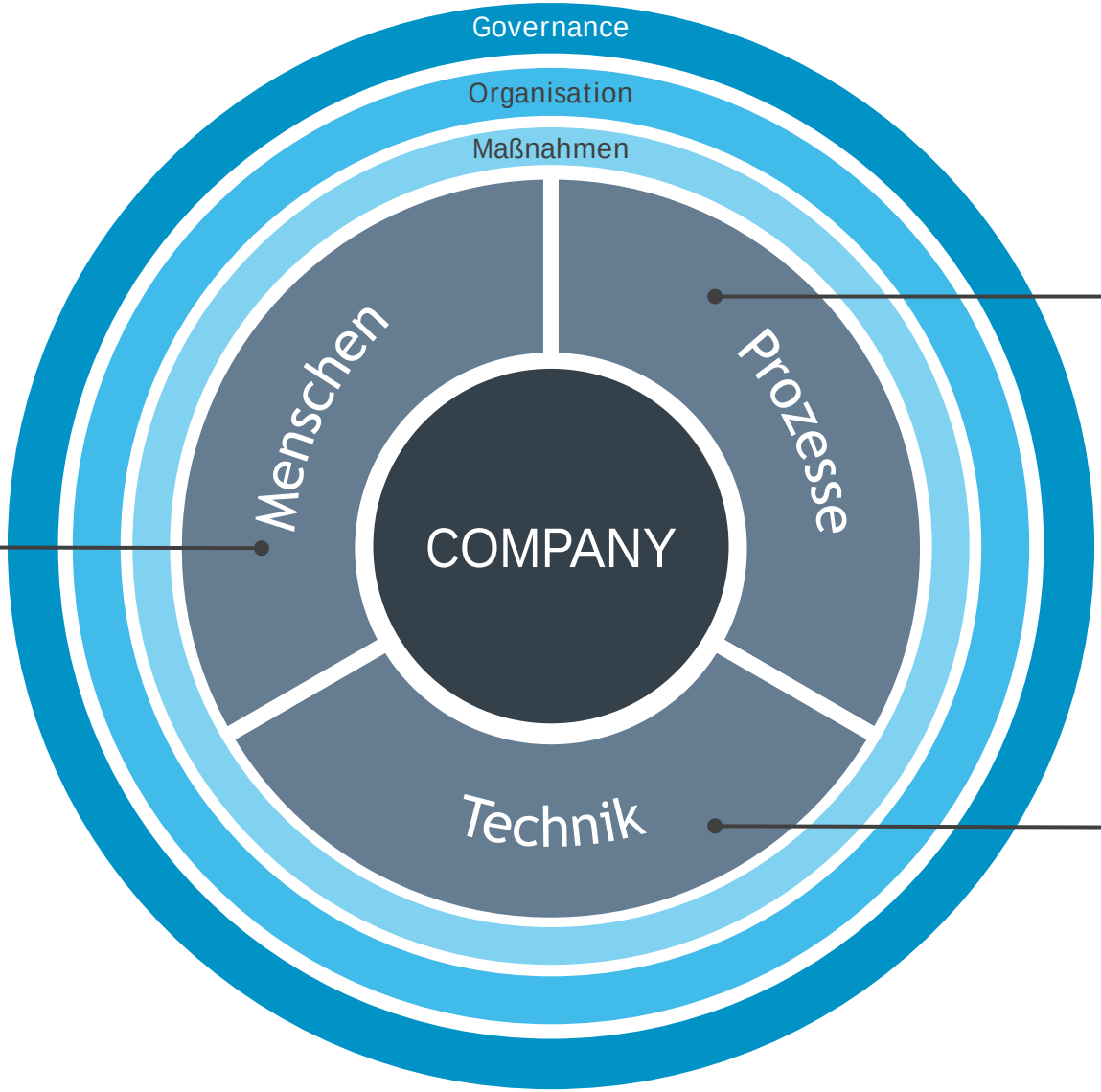
Damals war die Stadt Weiz Opfer eines Angriffs von Hackern. Gestohlen wurden insgesamt 27 Gigabyte an Daten von einem alten Laufwerk aus dem Jahr 2018.

ZIELSCHEIBE UNTERNEHMEN

Aktuelle Bedrohungen

DAS UNTERNEHMEN ALS ZIELSCHEIBE

Defense in depth



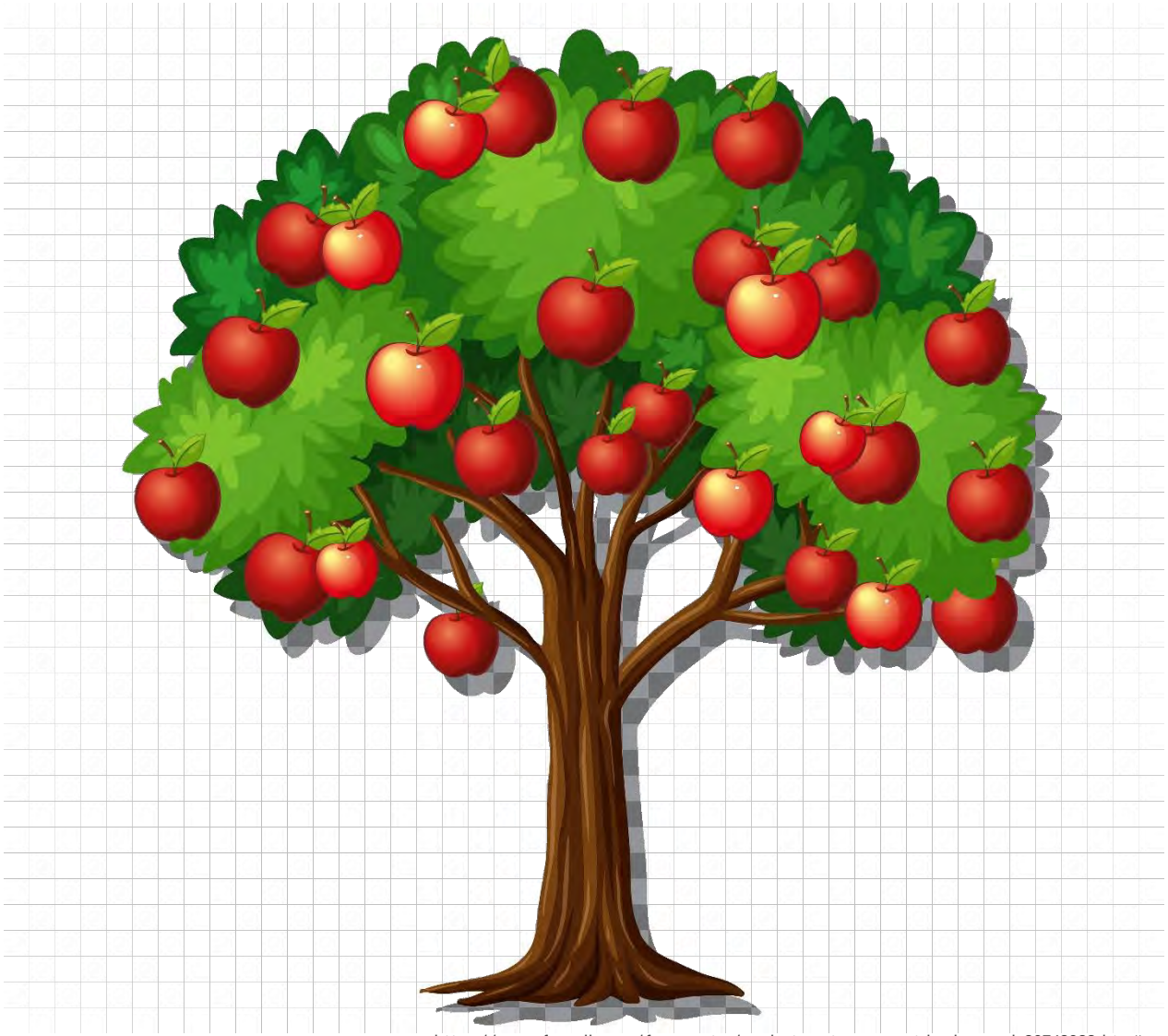
Management Systeme
Richtlinien & Policies
Partner Management
Datenschutz
Compliance & Audit

Cyber Hygiene
Training & Awareness
Fähigkeiten und Qualifikation

IT-Systeme & IT-Architektur
Applikationslandkarte
Antivirus, Firewall, VPN, ...
Zugriffs- und Zutrittsschutz

LOW HANGING FRUIT

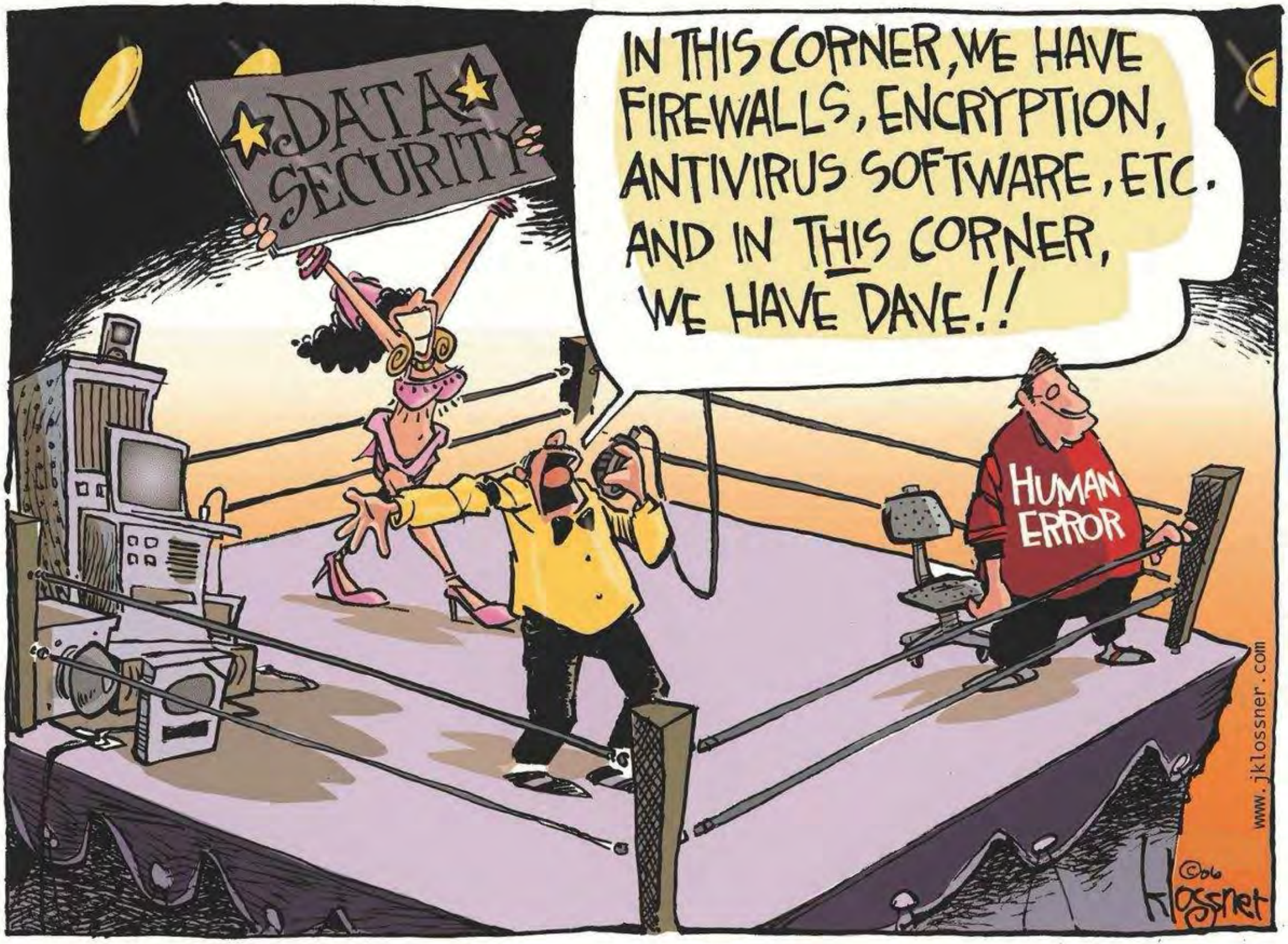
Mit wenig Aufwand zu maximalem Profit



https://www.freepik.com/free-vector/apple-tree-transparent-background_20743083.htm#query=apple%20tree&position=9&from_view=search

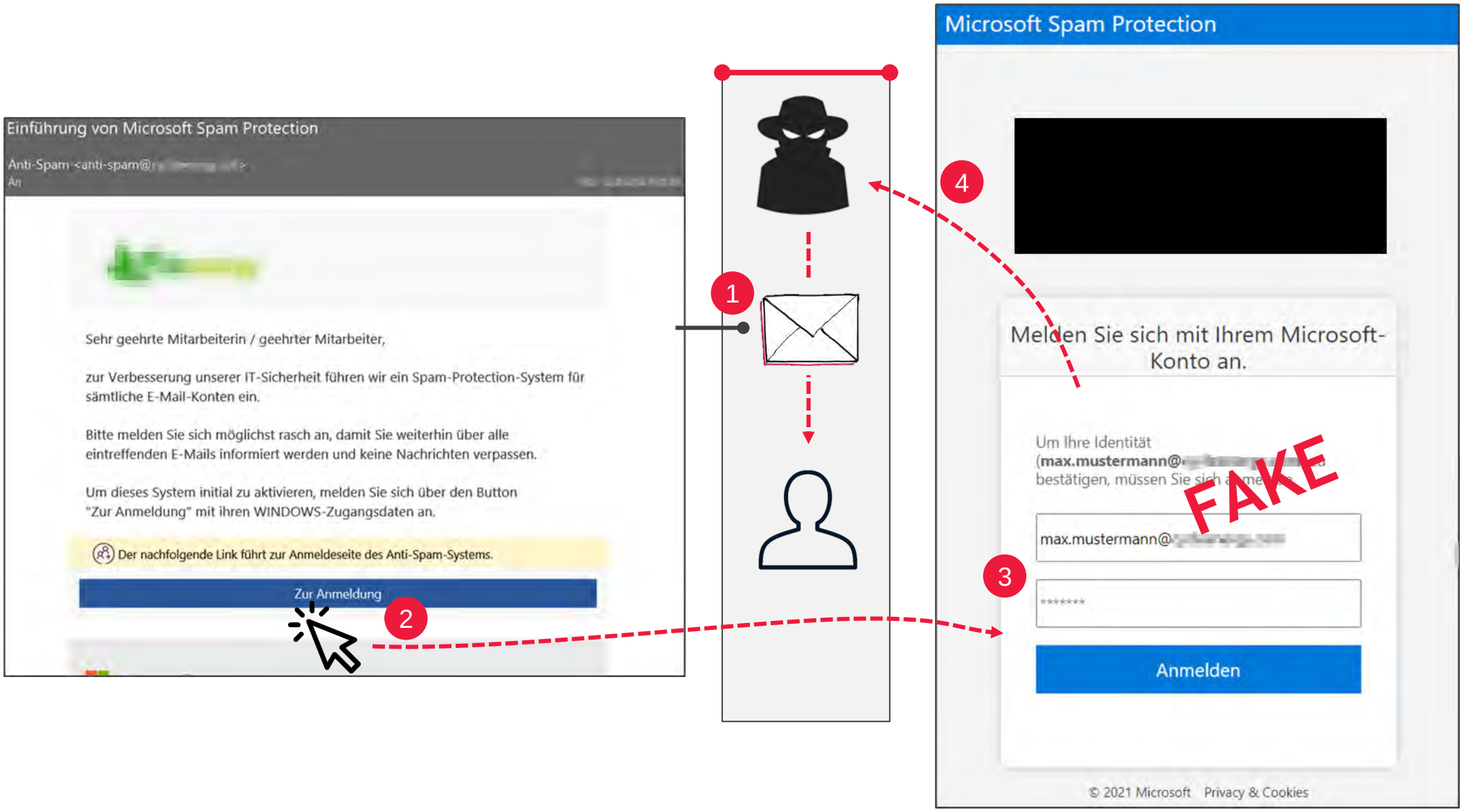
FAKTOR MENSCH

Aktuelle Bedrohungen


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06
Klossner

PHISHING - DER ANGRIFF AUF DIE MITARBEITER

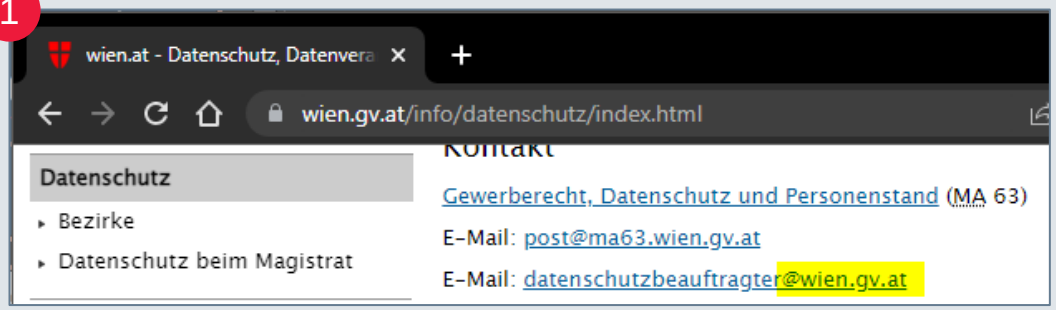
Der Faktor Mensch im Fokus der Cyber-Kriminellen



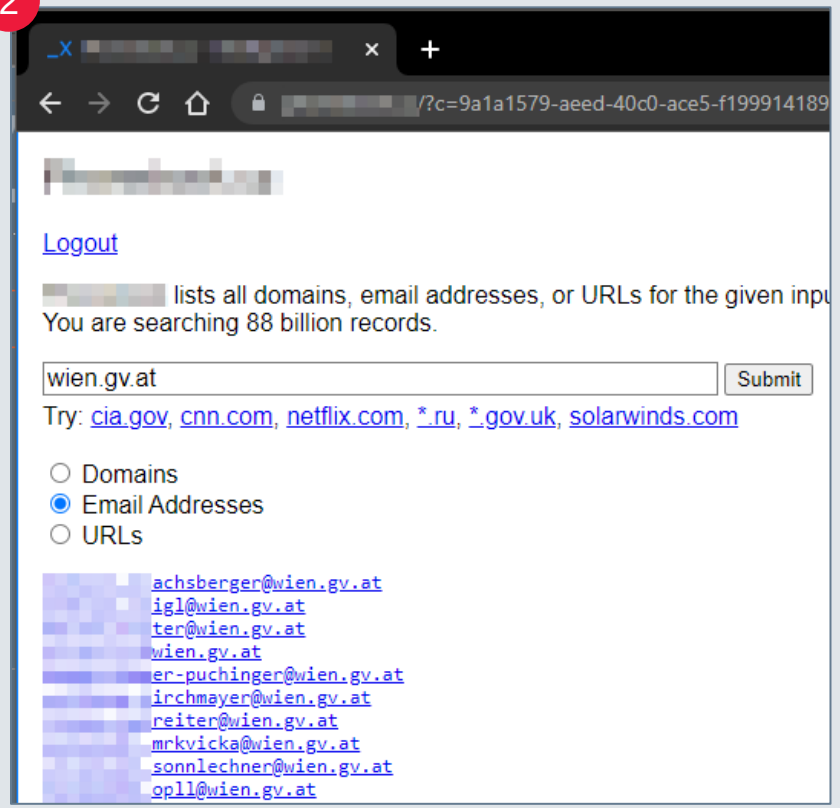
PHISHING - DER ANGRIFF AUF DIE MITARBEITER

Der Faktor Mensch im Fokus der Cyber-Kriminellen

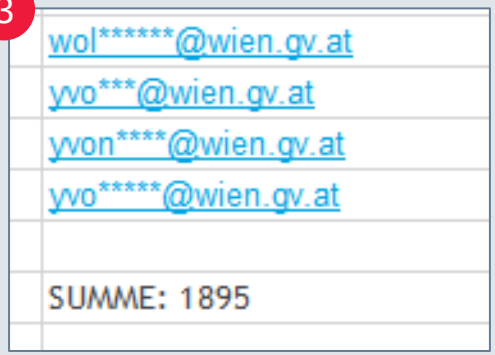
1



2



3

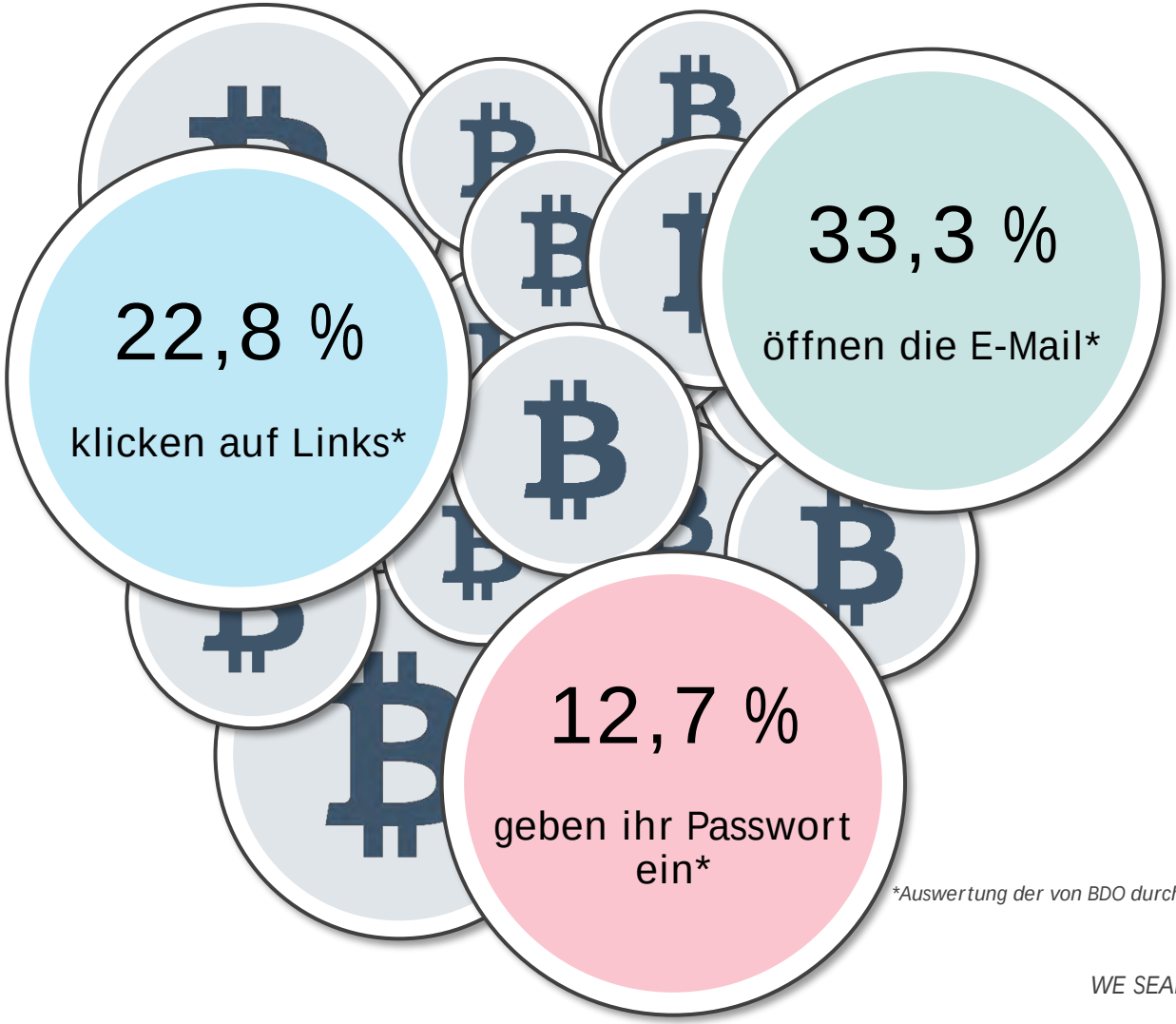


1.895 potenzielle Angriffsziele in 15 Minuten Recherche!

PHISHING - DER ANGRIFF AUF DIE MITARBEITER

Der Faktor Mensch im Fokus der Cyber-Kriminellen

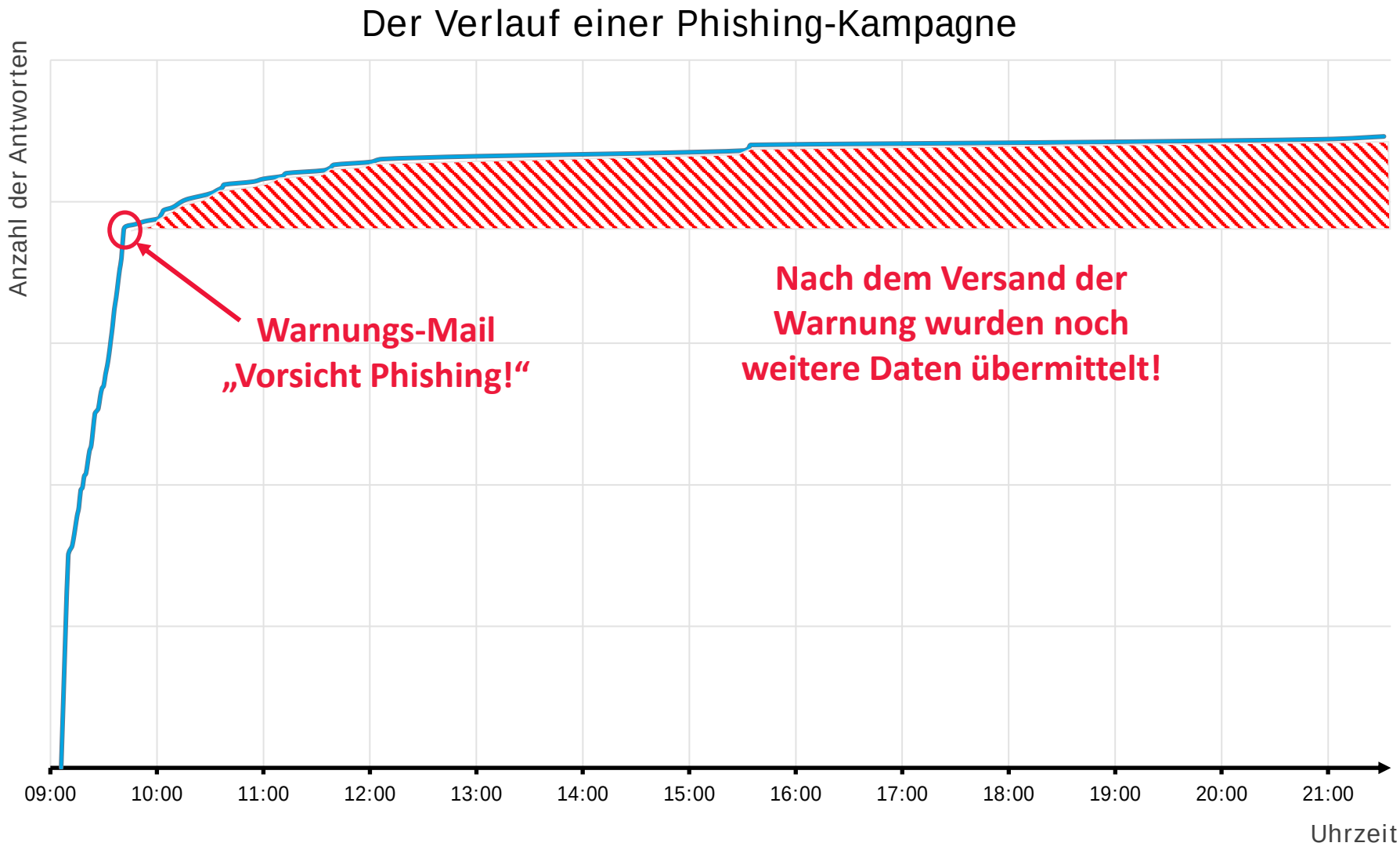
Phishing-E-Mails sind aktuelle die häufigste Angriffsart auf Unternehmen!



*Auswertung der von BDO durchgeführten Phishing-Simulationen (n=17.300 E-Mails)

BEISPIEL: PHISHING KAMPAGNE

Der Faktor Mensch im Fokus der Cyber-Kriminellen



MITARBEITER REGELMÄßIG SCHULEN!

Empfehlung - Faktor Mensch

Empfehlungen!

- Schulen Sie Ihre Mitarbeiter zu Cyber Security Themen!

  Erklären Sie dabei, wie man verdächtige E-Mails erkennt und wohin diese gemeldet werden sollen!

- Überprüfen Sie den Lernerfolg mithilfe von simulierten Phishing-Kampagnen. Dadurch machen Sie die KPI Mensch messbar!

PASSWORTHYGIENE BETREIBEN!

Empfehlung - Faktor Mensch

Empfehlungen!

- Überprüfen Sie, ob Sie von den Data Breaches betroffen sind!

  Ändern Sie Ihre Passwörter, sofern Sie von einem Data Breach betroffen sind!

- Verwenden Sie einzigartige und sichere Passwörter für jeden Dienst! -> Passwortmanager

- Verwenden Sie Mehrfaktorauthentifizierung und/oder Biometrie!

Have I been pwned?
https://haveibeenpwned.com/

HPI Identity Leak Checker
https://sec.hpi.de/ilc/

Keepass / Bitwarden
https://keepass.info/
https://bitwarden.com/

FAKTOR TECHNIK

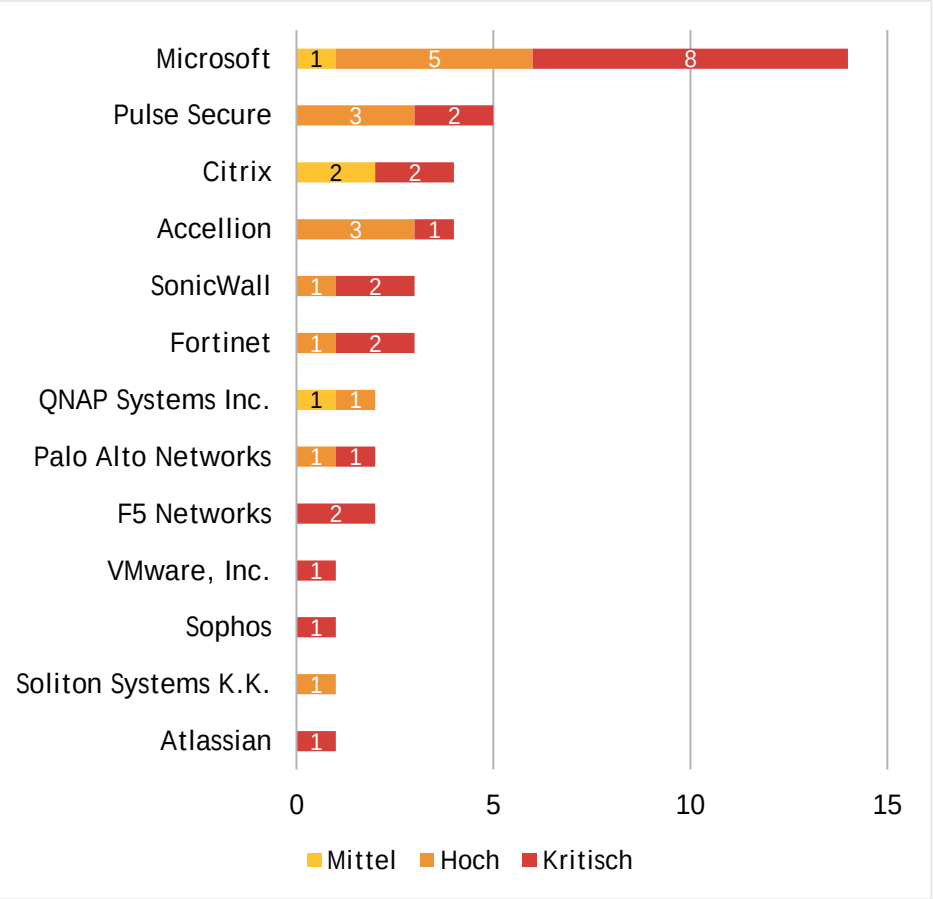
Aktuelle Bedrohungen

SCHWACHSTELLEN IN STANDARDSOFTWARE - 2021

Einfallstore für Cyberkriminelle

Kritische Sicherheitslücken haben verheerende Auswirkungen auf Unternehmen!

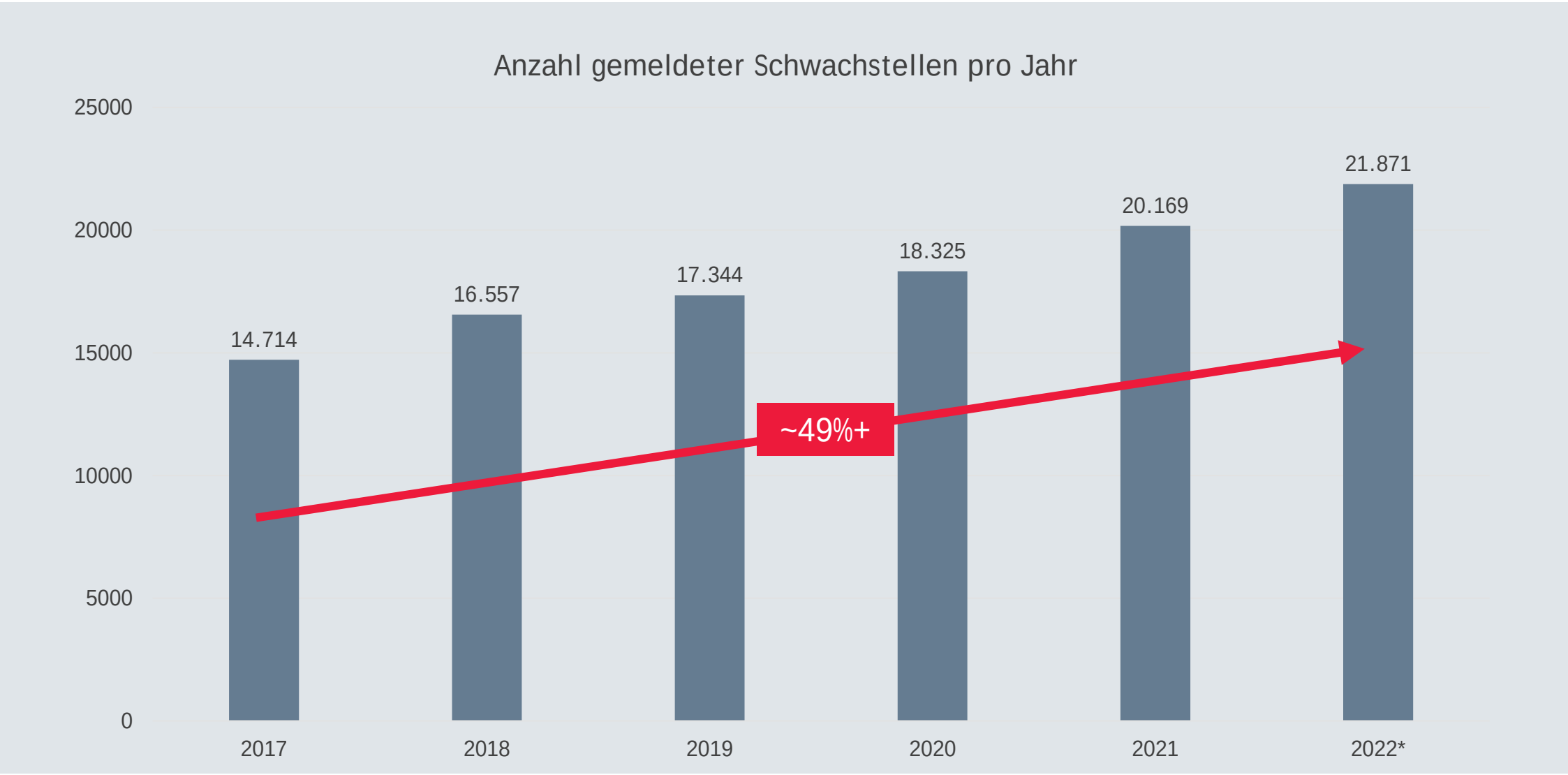
2021 wurden kritische Schwachstellen in weit verbreiteter Standardsoftware (z.B. Microsoft Exchange Server, VMware ESXi etc.) von Cyberkriminellen genutzt, um Angriffe weitflächig durchzuführen.



Grafik: In 2021 identifizierte Schwachstellen in weit verbreiteter Standardsoftware

SCHWACHSTELLEN IN STANDARDSOFTWARE

Einfallstore für Cyberkriminelle



* laufendes Jahr
https://www.cvedetails.com/browse-by-date.php

STAND DER TECHNIK BEACHTEN!

Empfehlung - Faktor Technik

Empfehlungen!

- Aktuelle Sicherheitshardware und -software verwenden (z.B. Firewalls, Spam-Filter)!
- Ausführbare Inhalte (Makros) in Dateien blockieren (.pdf, .docm, .xlsm, .bat, .ps1, …)
- Einschränkung der externen Angriffsfläche (VPN, IP- / Geolocation-Filter, alte Services deaktivieren)
- Setzen Sie auf flächendeckende Zwei-Faktor-Authentifizierung

Makro Security

https://learn.microsoft.com/de-de/microsoft-365/security/intelligence/macro-malware?view=o365-worldwide

IT-SYSTEME LAUFEND AKTUELL HALTEN

Empfehlung - Faktor Technik

Empfehlungen!

- Führen Sie einen Update- und Patch-Management-Prozess ein!
- Informieren Sie sich laufend zu neuen Sicherheitslücken und Angriffen!
- Führen Sie regelmäßig (zumindest jährlich) Schwachstellenscans durch!

CERT AT
https://cert.at/

Microsoft Security Advisory
https://learn.microsoft.com/en-us/security-updates/

FAKTOR PROZESSE

Aktuelle Bedrohungen

LAUFENDE VERBESSERUNG & EXTERNE TREIBER

Prozesse unterstützen die Unternehmensentwicklung

WACHSTUM

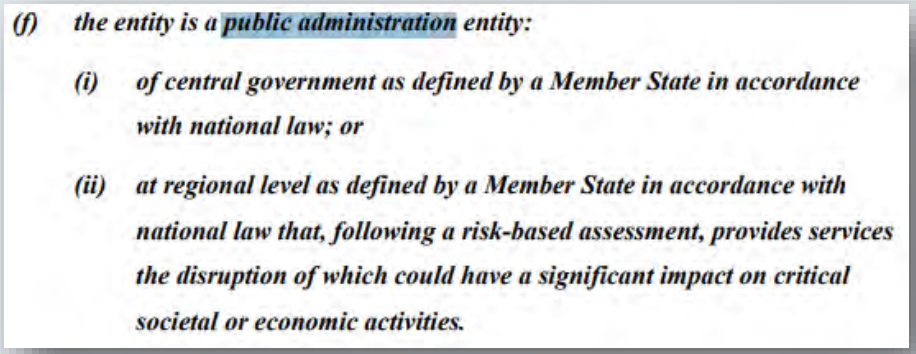
- Je größer das Unternehmen wird, umso wichtiger werden standardisierte Prozesse
  - Risikomanagementsystem (RMS)
  - Datenschutzmanagementsystem (DSMS)
  - Informationssicherheitsmanagementsystem (ISMS)
- Fehler einer Einzelperson können durch Prozesse abgefedert werden (z.B. 4-Augen-Prinzip)

LIEFERKETTEN

- KMUs sind häufig in die Lieferketten der großen Unternehmen (z.B. Automobilindustrie) eingebunden
- NIS2 wird noch mehr Branchen treffen (2023/2024)

EXKURS: NIS2

Prozesse unterstützen die Unternehmensentwicklung



(f) the entity is a public administration entity:

(i) of central government as defined by a Member State in accordance with national law; or

(ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

Kapitel
Governance und Risikomanagement
Umgang mit Dienstleistern, Lieferanten und Dritten
Sicherheitsarchitektur
Systemadministration
Identitäts- und Zugriffsmanagement
Systemwartung und Betrieb
Physische Sicherheit
Erkennung von Vorfällen
Bewältigung von Vorfällen
Betriebskontinuität
Krisenmanagement

NIS Verordnung:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722

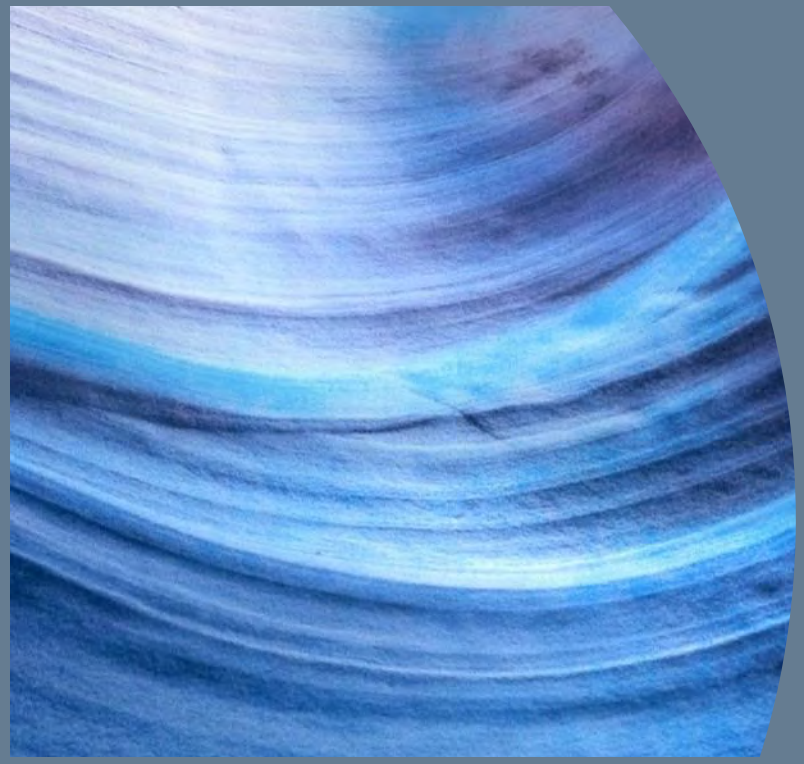
VORBEREITUNG AUF DEN ERNSTFALL

Empfehlung - Faktor Prozesse

Empfehlungen!

- Risikomanagement: Identifizieren Sie die Risiken, bewerten Sie diese und definieren Sie Maßnahmen!
- Kennen Sie Ihre schützenswerten Daten (Business Impact Analyse) und schützen Sie diese!
  - Zugriffsberechtigungen einschränken
  - Regelmäßige Backups
  - Backups vor Veränderung sichern
  - Offline Backups anlegen
- Ziehen Sie professionellen Rat hinzu!


100% SICHERHEIT EXISTIERT NICHT
RESTRISIKO VERSICHERN?



WE SEARCH FOR GREATNESS.

BDO