Live Ethical Hacking

Wie Hacker in Ihr System eindringen

Referent: Florian Muff
Hacker: Gaetano Randone
27.09.2023

BDO

Definition Computerkriminalität / Cyberkriminalität

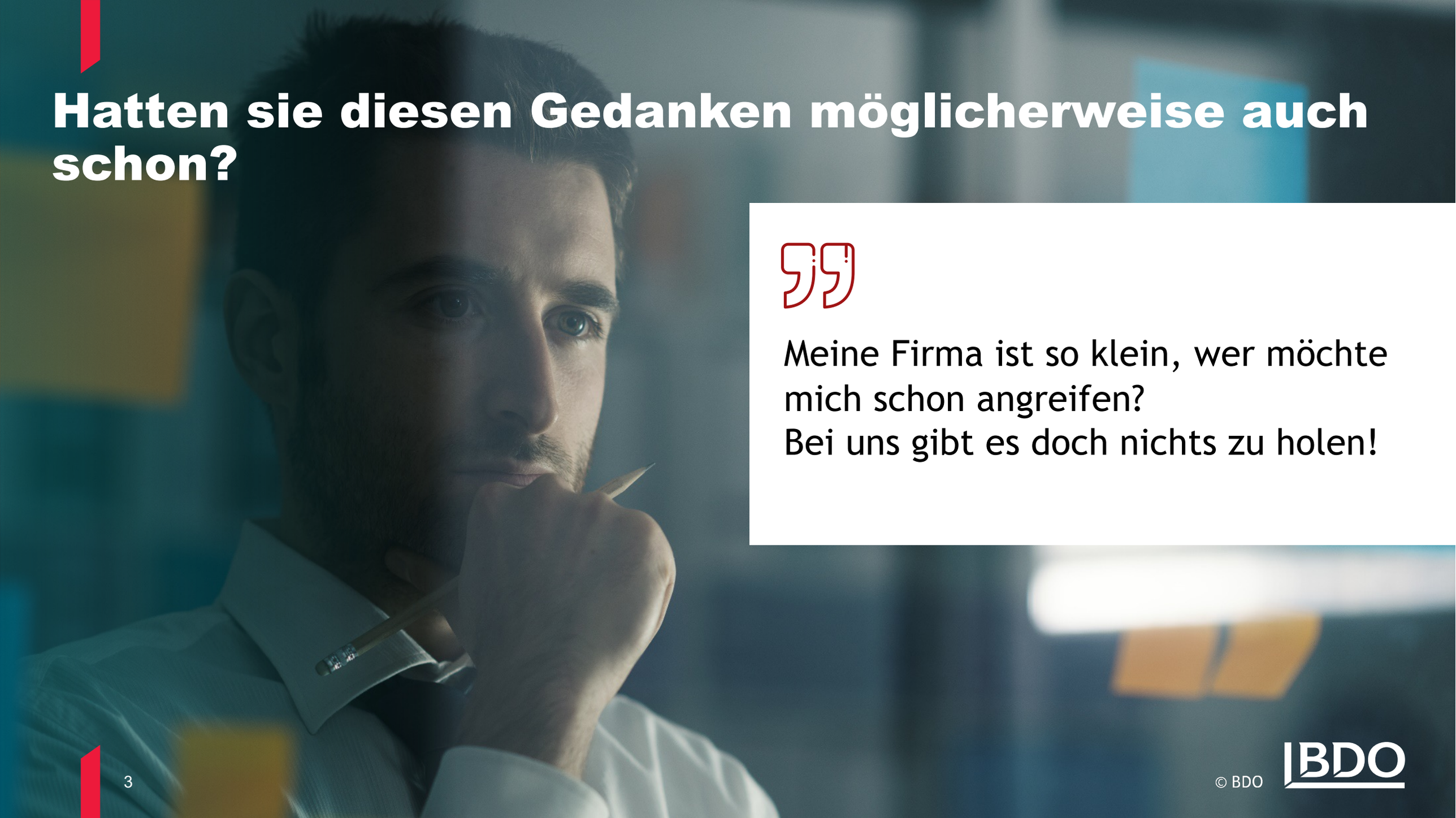
Any illegal, unethical, or unauthorized behavior relating to the automatic processing and the transmission of data

- OECD, 1986

Wikipedia:

- "Computerkriminalität (Cybercrime) umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden"
- "Internetkriminalität sind Straftaten, die auf dem Internet basieren oder mit den Techniken des Internets geschehen. "

Hatten sie diesen Gedanken möglicherweise auch schon?

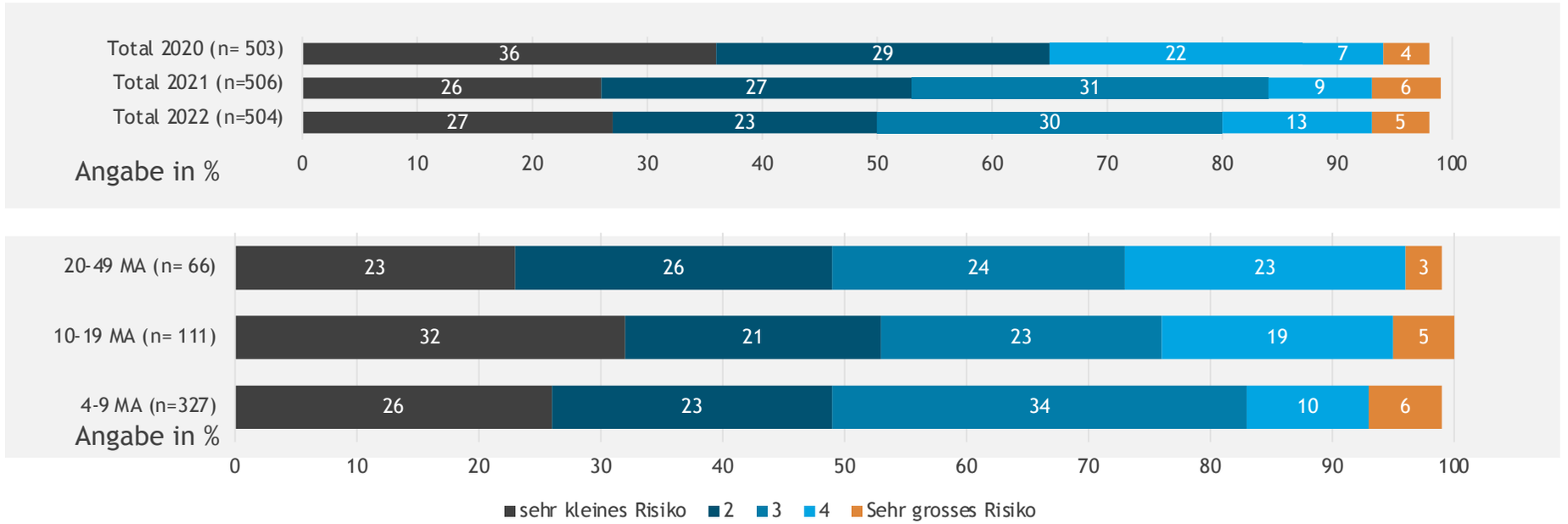


> Meine Firma ist so klein, wer möchte mich schon angreifen?
> Bei uns gibt es doch nichts zu holen!

© BDO

Dann sind Sie laut einer Studie der GFS-Zürich nicht allein

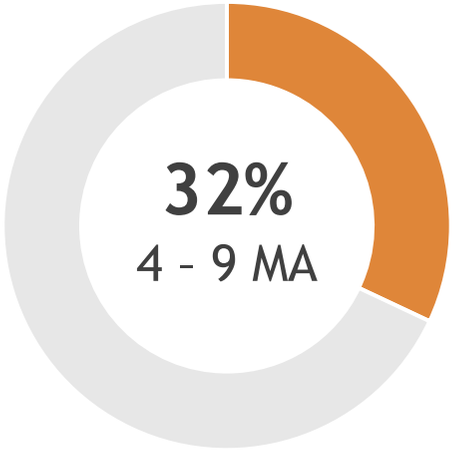
Als wie hoch schätzen Sie das Risiko ein, dass Ihr Unternehmen innerhalb der nächsten zwei bis drei Jahre von einem Cyberangriff betroffen sein wird, der Ihr Geschäft für mindestens einen Tag lang ausser Kraft setzt?

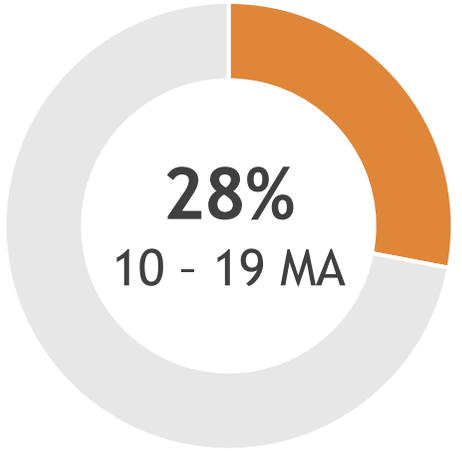


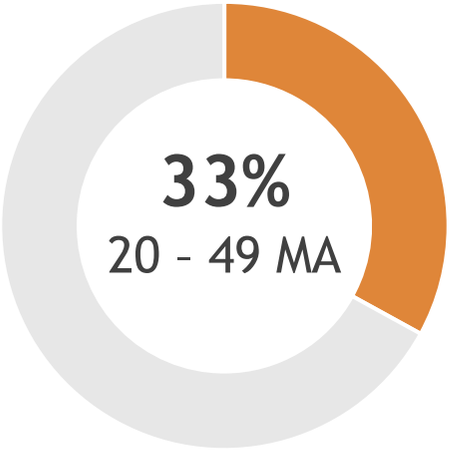
Quelle: gfs-zürich, «Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU» (2022)


But are you $ure?

But are you $ure?







55’000

Schweizer KMU wurden 2021 Opfer eines Cyberangriffs, rechnet man die Angaben auf die Grundgesamtheit hoch

Quelle: gfs-zürich, «Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU» (2022)

Top 5 Angriffstypen auf Schweizer KMU

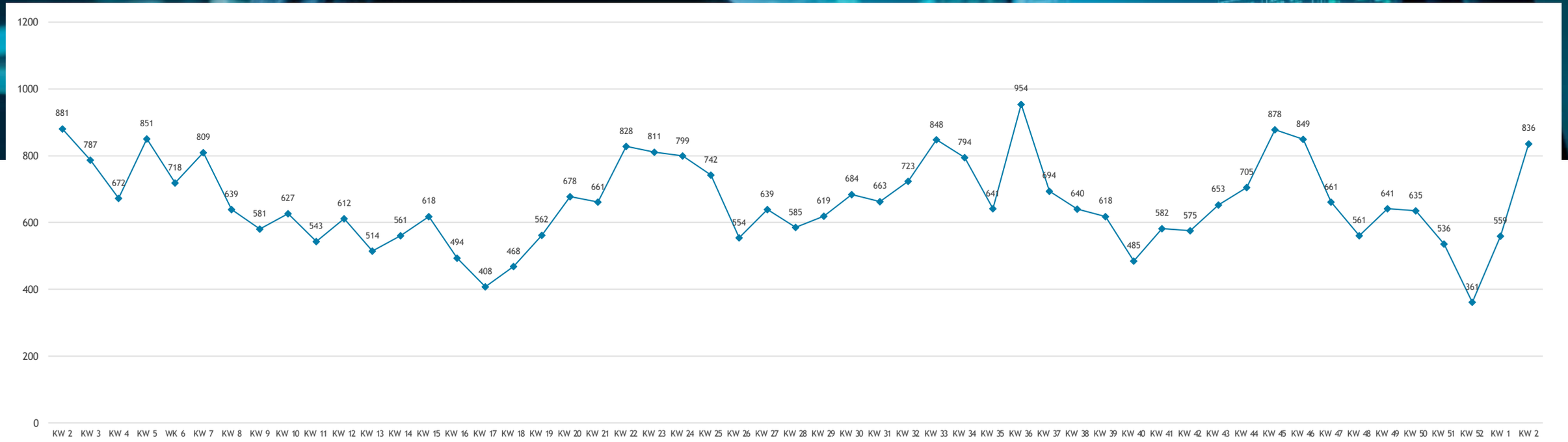
20%	Malware/Schadsoftware
11%	Phishing/ Identitätsdiebstahl
7%	Datendiebstahl/-Verlust
6%	DDoS
5%	Erpressung

- Umsatzverlust
- Reputationsverlust
- Verlust von Kundendaten

Quelle: gfs-zürich, «Auswirkungen der Corona-Krise auf die Digitalisierung und Cybersicherheit in Schweizer KMU» (2022)

Snapshot: Schweiz

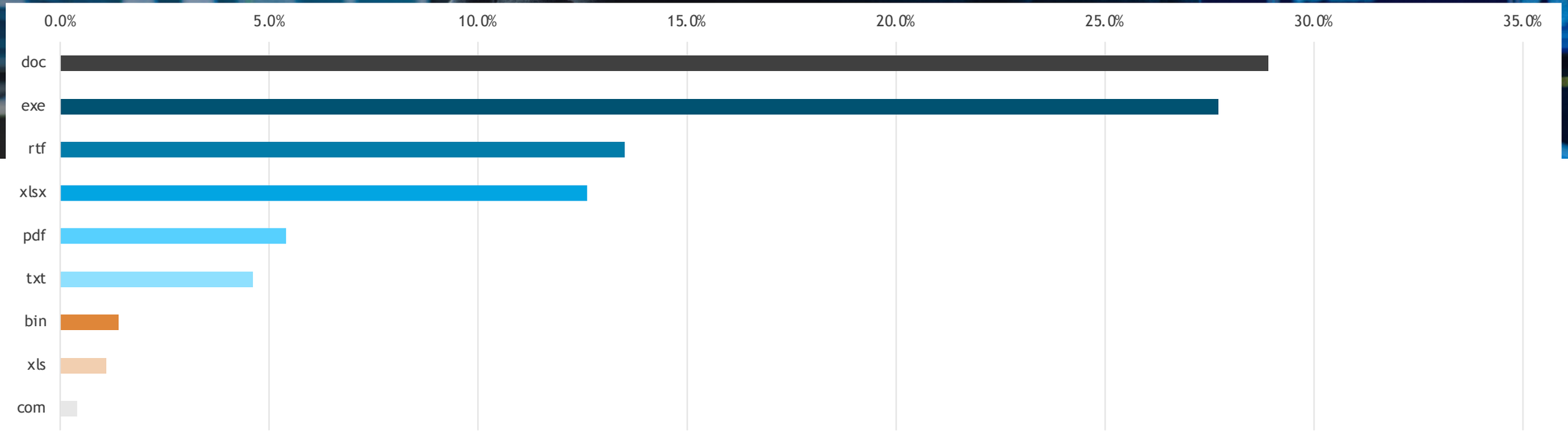
35‘037 Eingegangene Meldungen
beim nationalen Zentrum für Cybersicherheit (Januar 2022 – Januar 2023)



 Quelle: NCSC

Snapshot: Schweiz

.doc ist der häufigste Dateityp
bei der Verbreitung von Malware (2020)

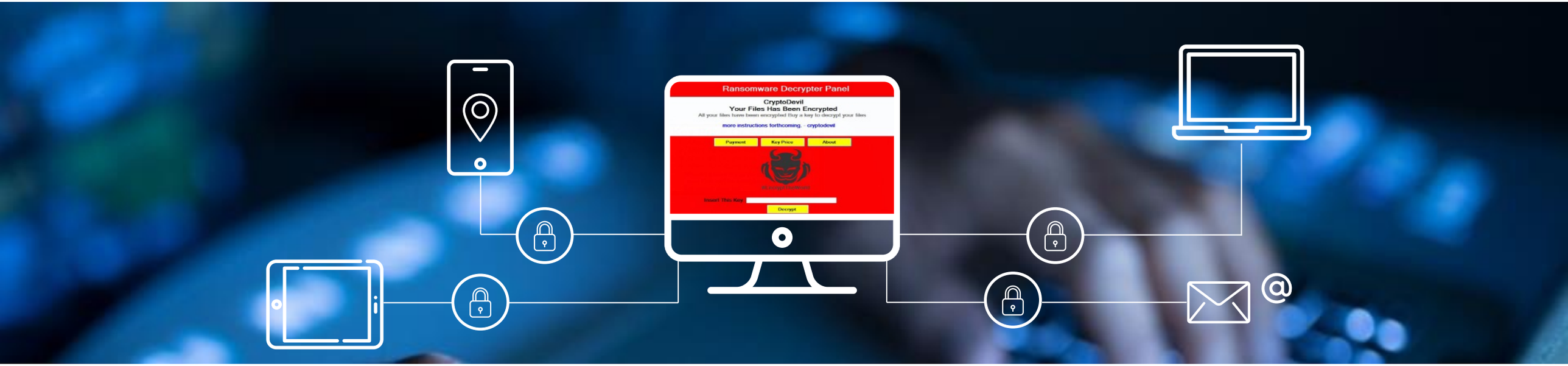


Quelle: Check Point, Computerworld

Beispiel eines Hacks in der Baubranche im Jahr 2021

Beispiel eines Hacks in der Baubranche im Jahr 2021

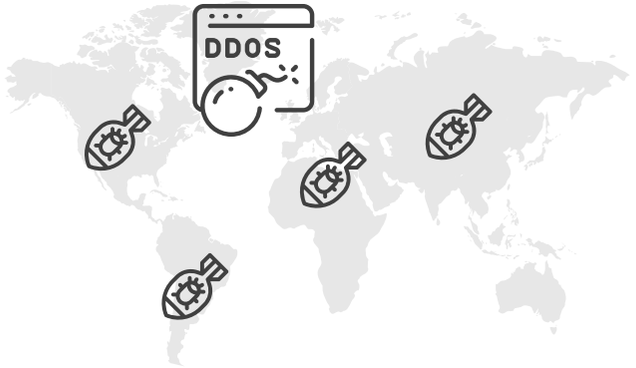
- **Security Breach in Serverinfrastrukturen**
- **Wichtige Betriebsdaten wurden von den Kriminellen verschlüsselt**
- **Erpresser stellen Lösegeldforderungen, um die Daten wieder zu entschlüsseln**
- **Grosses Risiko von Identitätsdiebstahl**



Wie läuft beispielsweise eine DDoS-Attacke ab?

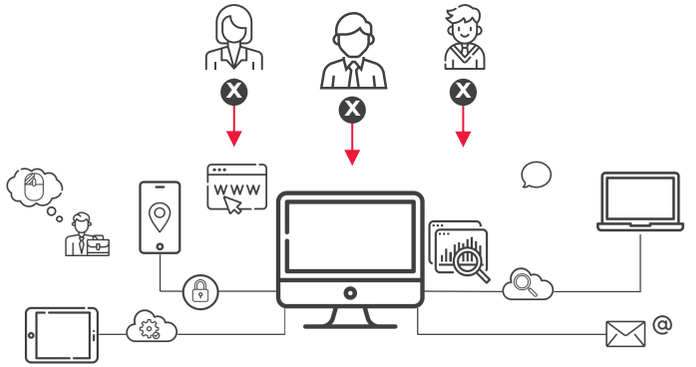
Schritt 1

Der Kriminelle beauftragt einen DDoS Attack Service und bezahlt via Online-Zahlungsservices oder mit Kryptowährungen



Schritt 2

Der DDoS Service attackiert über seine eigene Infrastruktur das Ziel. DDoS Services geben an legal zu sein, sind es aber nicht!



Schritt 3

Der DDoS Angriff überlastet das Ziel-Netzwerk und macht die Dienste für reguläre Nutzer unbrauchbar

- Klau von Kreditkartendaten
- Klau von Kundendaten
- DDoS Attacke
- Reputational Damage
- Identitätsdiebstahl der Kunden
- Umsatzverlust

© BDO

Hacking in der globalen Perspektive

30’000

Webseiten werden pro Tag gehackt

64%

Aller Unternehmen weltweit haben schon einen Cyber-angriff erlebt

150%

Zunahme von Ransomware Attacken im Vergleich zum Vorjahr

39 Sek.

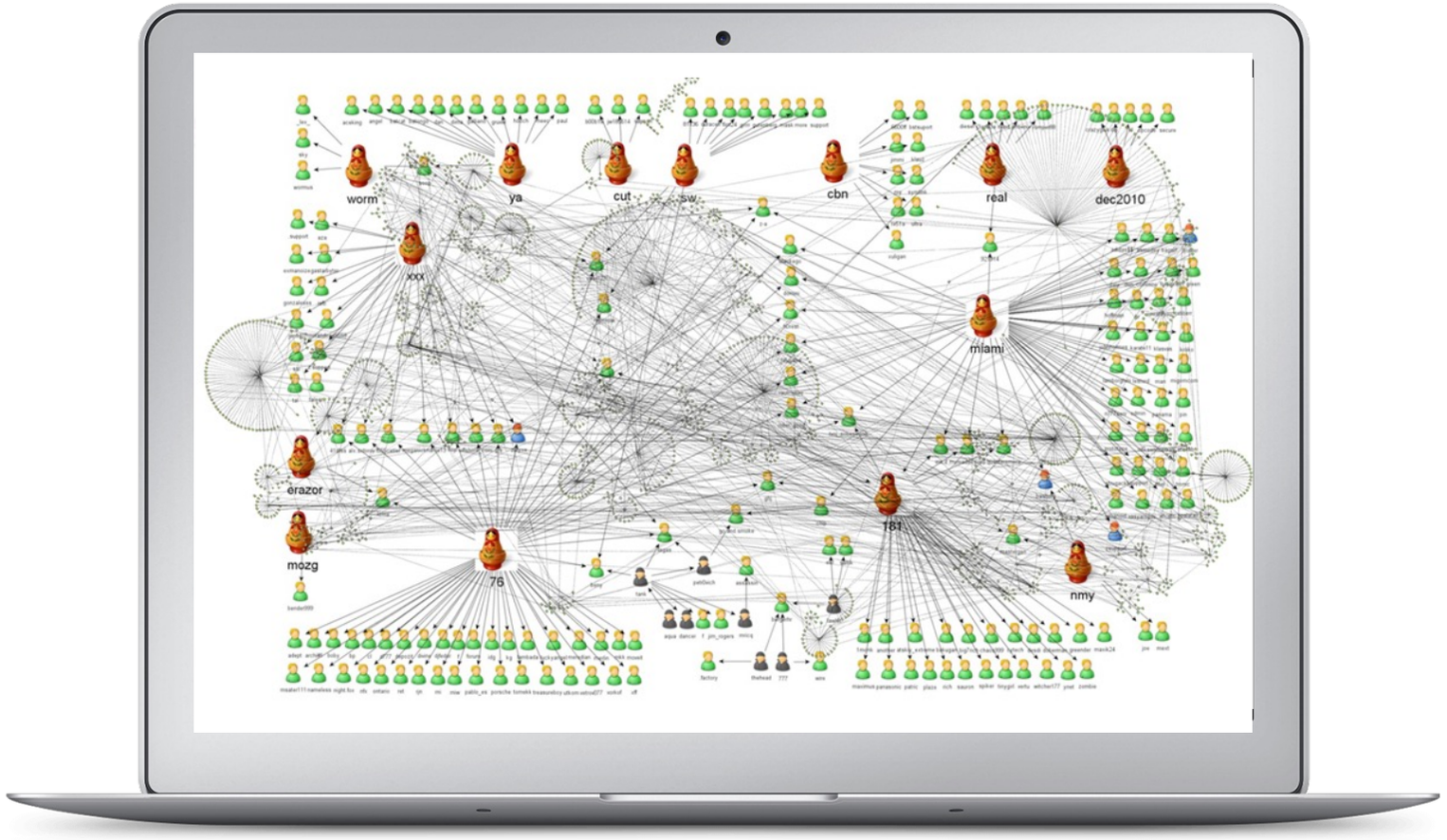
Ist der durchschnitt-liche Zeitraum in dem eine neue Online Attacke stattfindet

10.18%

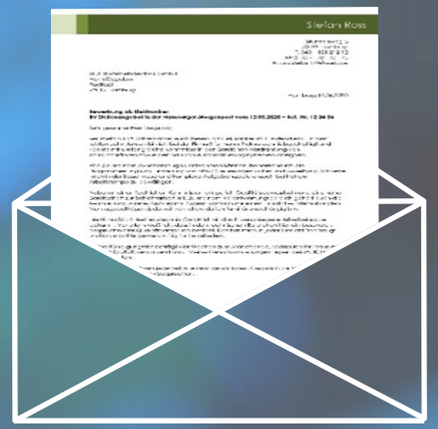
Aller Internet-nutzer wurden im Jahr 2020 Opfer einer Malware-Attacke (Kaspersky)

Wer sind die Hacker? Es gibt verschiedene Typen

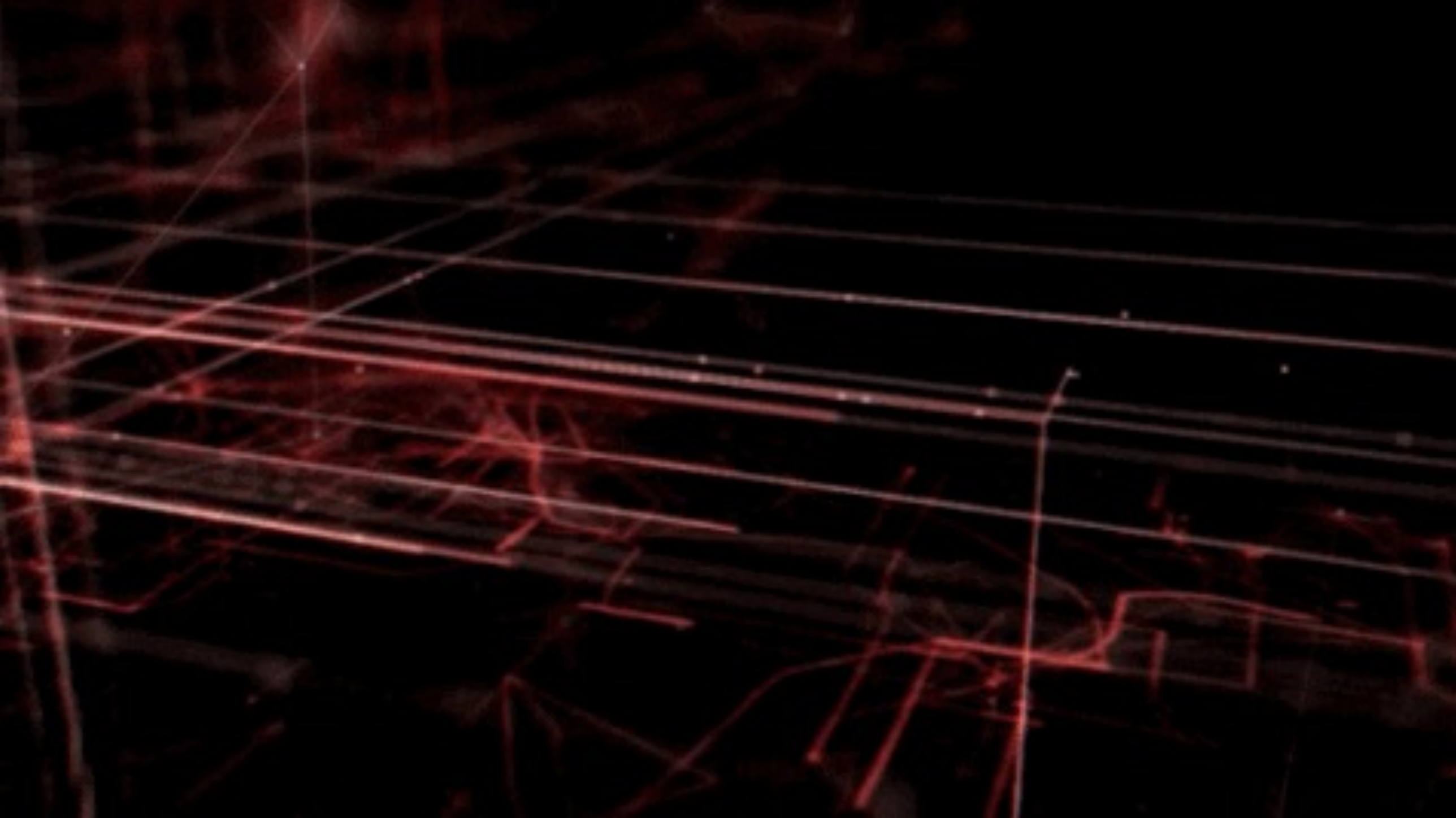
Hacker Gruppen – informelle Organisationen



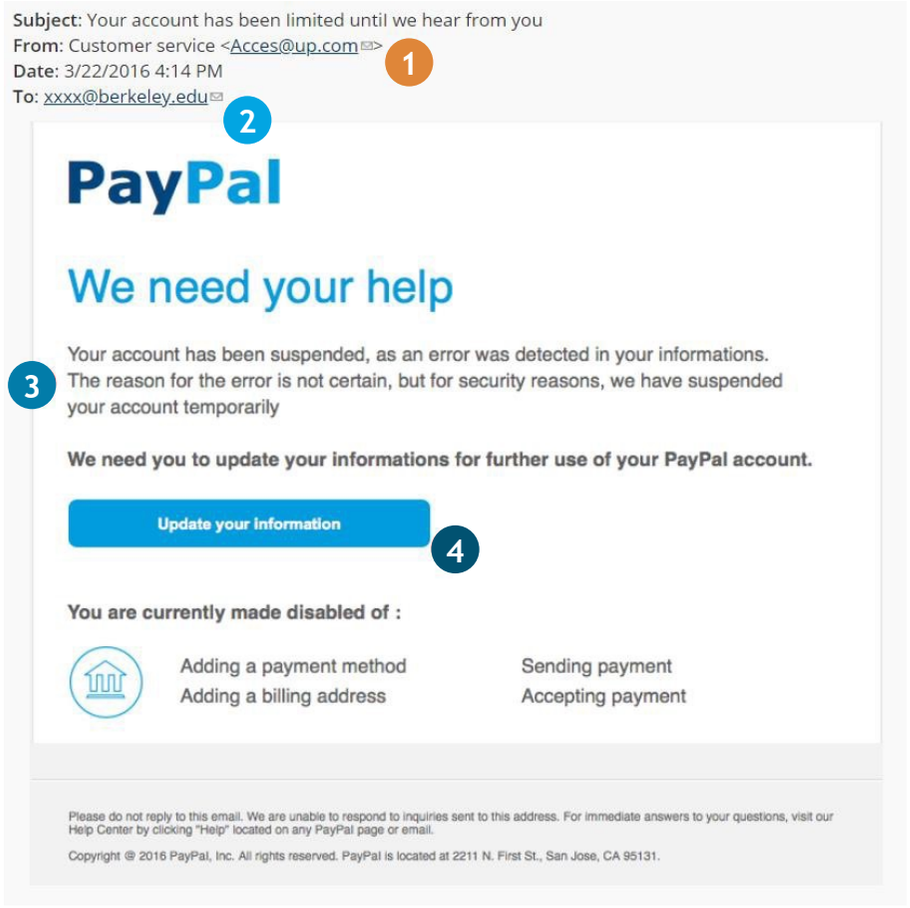
Wie kommt ein Hacker auf ihr System? Beispiel – der Bewerber



- **Anschreiben mit Bezug auf einen Offene Stelle oder Initiativbewerbung.**
- **Einseitig gedruckter Lebenslauf passend auf die Stelle oder der perfekte Kandidat bei initiativer Bewerbung.**
- **«Meine Zeugnisse und einen ausführlichen Lebenslauf habe ich in elektronischer Form beigefügt.»**



Wie erkenne ich eine Phishing-Mail?



Subject: Your account has been limited until we hear from you
From: Customer service <Acces@up.com> 1
Date: 3/22/2016 4:14 PM
To: xxxx@berkeley.edu 2

PayPal

We need your help

3 Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information 4

You are currently made disabled of :

Adding a payment method
Adding a billing address
Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright @ 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

MAILADRESSE
Ist die Absender-Mailadresse eine offizielle PayPal-Adresse? Anzeigename ≠ E-Mail-Adresse

01

WHALING
Ist der Empfängerkreis korrekt?

02

FEHLER
Gibt es Unstimmigkeiten /Rechtschreibfehler im Inhalt?

03

LINK
Auf welche Website verweist der Link?

04

Passwortsicherheit

		Nur Zahlen	Kleinbu-chstaben	Gross- und Kleinbuchstaben	Gross-, Kleinbu-chstaben und Zahlen	Alle Symbole auf der Tastatur
Beispiele		1234	ameisen	QrtM	F3P9mN	z&M@P#3
Mögliche Zeichen		10	26	52	62	95
Zeichenzahl	4	Sofort	Sofort	Sofort	Sofort	Sofort
Länge des Kennworts	5	Sofort	Sofort	Sofort	Sofort	Sofort
	6	Sofort	Sofort	Sofort	Sofort	Sofort
	7	Sofort	Sofort	2 Sekunden	7 Sekunden	31 Sekunden
	8	Sofort	Sofort	2 Minuten	7 Minuten	39 Minuten
	9	Sofort	10 Sekunden	1 Stunden	7 Stunden	2 Tage
	10	Sofort	4 Minuten	3 Tage	21 Tage	150 Tage
	11	Sofort	2 Stunden	150 Tage	3 Jahre	34 Jahre
	12	2 Sekunden	2 Tage	24 Jahre	200 Jahre	3’000 Jahre
	13	19 Sekunden	60 Tage	1’000 Jahre	12’000 Jahre	202’000 Jahre
	14	3 Minuten	4 Jahre	64’000 Jahre	750’000 Jahre	16 Mio. Jahre
	15	32 Minuten	100 Jahre	3 Mio. Jahre	46 Mio. Jahre	1 Bio. Jahre
	16	5 Stunden	3’000 Jahre	173 Mio. Jahre	3 Bio. Jahre	92 Bio. Jahre

- Ein Passwort-Manager ermöglicht es Ihnen, sich nur ein Passwort zu merken.
- Eines der Probleme bei diesem Thema ist, dass man irgendwann einem Anbieter vertrauen muss.
- https://www.passwortcheck.ch/passwortcheck/passwortcheck

2-Factor Authentication

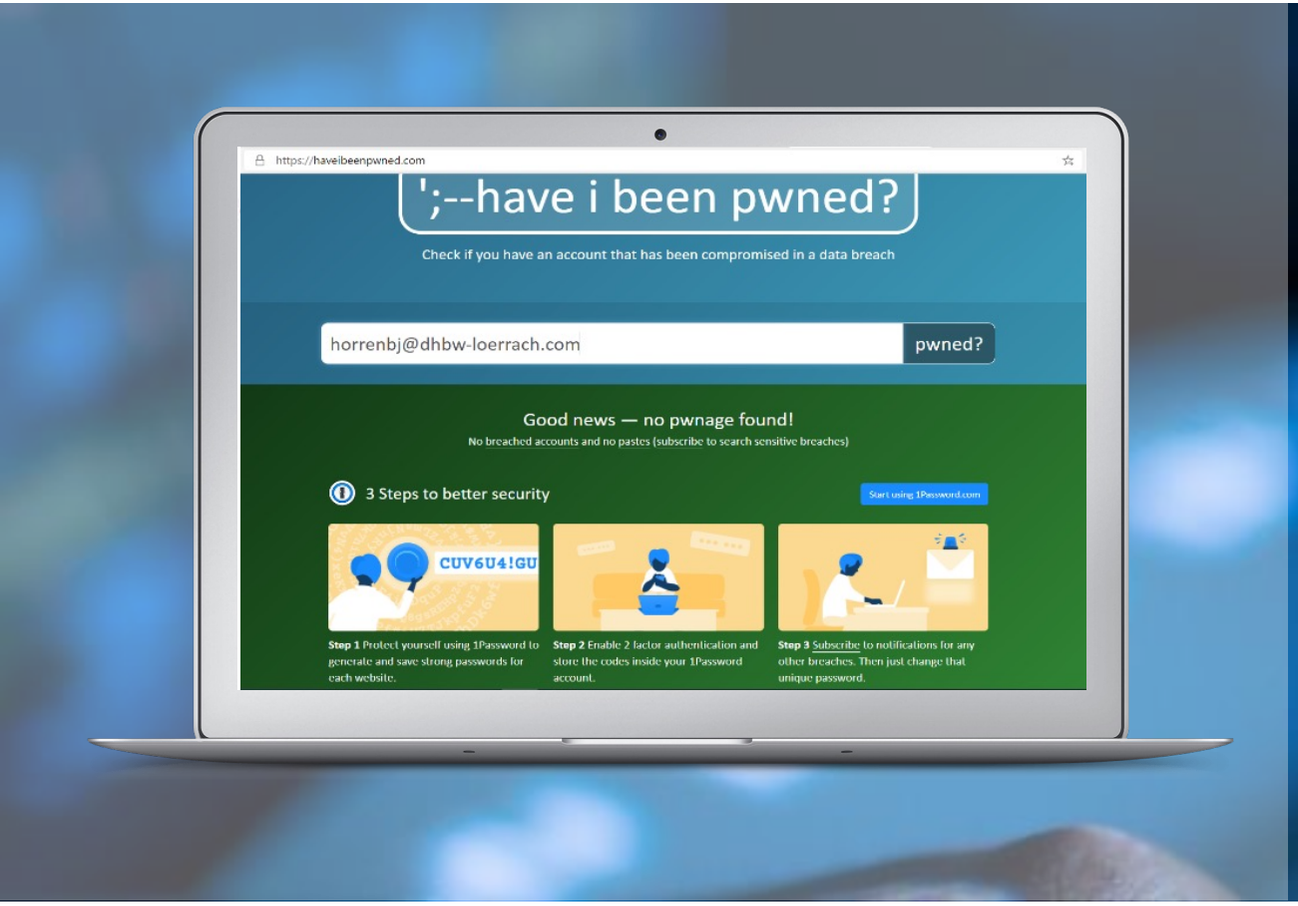
- Ermöglicht es Ihnen, böswillige Personen nicht auf Ihre Konten zugreifen zu lassen, wenn Ihre LogIn Daten ergattert werden sollten.
- Stellen Sie sich das wie die PIN-Nummer Ihrer Kreditkarte vor.
- Wie funktioniert das? In der Regel per SMS oder mit einer Authentifizierungsanwendung.

SCHRITT 1
Nutzername und
Passworteingabe

SCHRITT 2
Token oder
PIN Eingabe

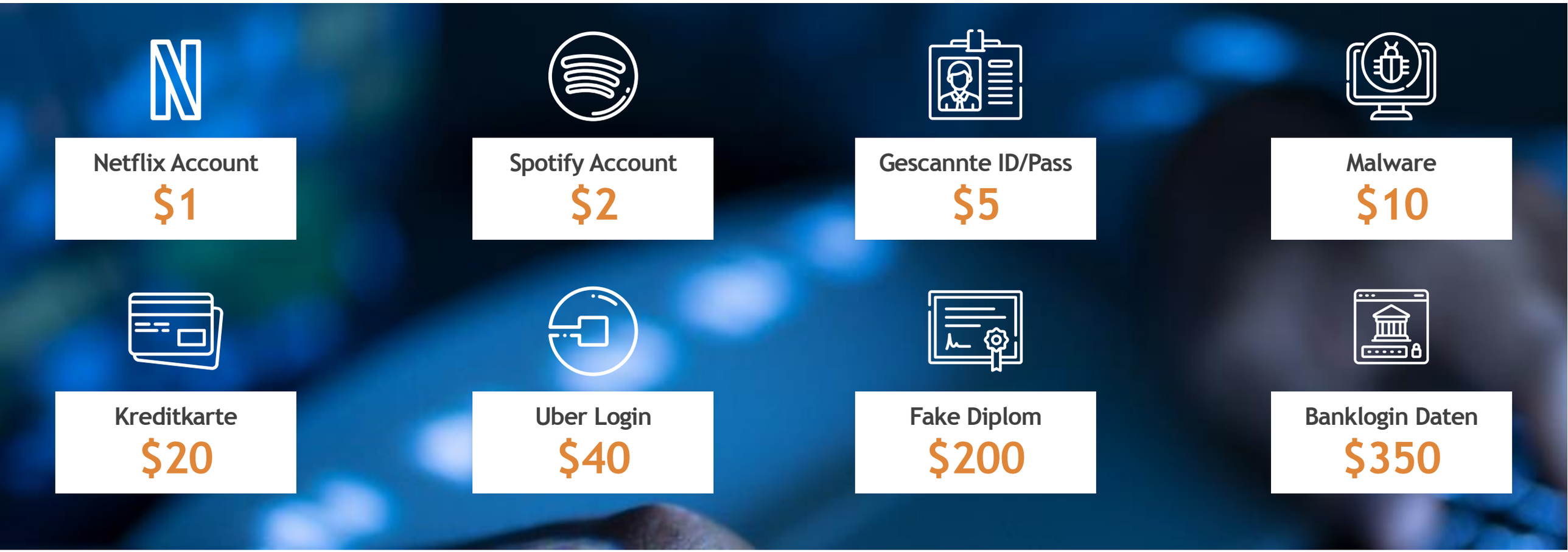
SCHRITT 3
Fingerabdruck oder weitere
biometrische Verifikation

Waren meine Daten schon in einem Datenleck?



- Auf der Website haveibeenpwned können Sie herausfinden, ob Ihre E-Mail-Adresse bereits bei einem Datendiebstahl gestohlen wurde.
- Kostenloses Abonnement - Sie werden per Email informiert, wenn Ihre Email-Adresse in einem Datendiebstahl auftaucht.

Hacking ist schwer oder teuer?



Cyber Security Grundschutzmassnahmen

NCSC Vorfall - was nun?

Multi-Faktor-Authentifizierung

- Achte auf Passwortrichtlinien
- Priorisieren Sie die Einführung von MFA
- Regelmässige Überprüfung der geltenden Regeln

Benutzeradministration

- Getrennte Konten für Admin-Aufgaben
- Überwachen Sie Aktivitäten von Admin-Konten
- Beachten Sie Passwortwechsel und ungewöhnliche Login

Cybersecurity Notfallplan

- Vorbereitung auf einen Ausfall der IT-Systeme (intern/extern)
- Notbetrieb und Wieder-herstellung Ihrer Systeme
- Durchlauf testen der Führung und Geschäftsweiterführung

Backup

- Regelmässige Erstellung von Sicherungskopien
- Bewahren Sie Backups offline an einem externen Ort auf
- Sicherungs- und Wiederherstellungstest

Software-Updates

- Software Updates regelmässig durchführen
- Wer wartet, riskiert die Sicherheit seiner Daten.
- Software Updates beheben Sicherheitslücken und Fehler

Vorsicht bei E-Mails

- Öffne keinen unbekannten Anhang
- Klicken Sie nicht auf unbekannten Links
- Vertrauliche Informationen sollten Sie niemals preisgeben.

Schlussüberlegung

Sicherheit + Produktivität = 100%

Besten Dank für Ihre Aufmerksamkeit

FRAGEN?

Florian Muff
florian.muff@bdo.ch

@BDO.Swiss

@BDO_Schweiz

BDO Schweiz

BDO SCHWEIZ

BDO AG ist eine der führenden Wirtschaftsprüfungs-, Treuhand- und Beratungsgesellschaften der Schweiz. Zu ihren Kernkompetenzen zählen Dienstleistungen in den Bereichen Wirtschaftsprüfung, Financial Services, Treuhand, Steuer- und Rechtsberatung sowie Unternehmensberatung. Mit 34 Niederlassungen verfügt BDO über das dichteste Filialnetz der Branche. Persönliche Nähe und Kompetenz gelten bei den rund 1'500 Mitarbeitenden als wichtige Voraussetzung für erfolgreiche und nachhaltige Kundenbeziehungen.
BDO AG prüft und berät Unternehmen aus Industrie- und Dienstleistungsbereichen; dazu gehören kleine und mittlere Unternehmen, börsenkotierte Firmen, Öffentliche Verwaltungen Und Non-Profit-Organisationen.

Für international ausgerichtete Kundinnen und Kunden wird die globale BDO Organisation in über 160 Ländern genutzt. BDO AG hat ihren Hauptsitz in Zürich und ist die unabhängige, rechtlich selbstständige Schweizer Mitgliedsfirma des internationalen BDO Netzwerkes mit Hauptsitz in Brüssel (B).