CYBERSICHERHEIT, CORONA UND KOMMUNEN

BDO Consulting
30.09.2020

DAS JAHR 2020 IN ZWEI BILDERN

BDO

VORSTELLUNG

BDO Consulting GmbH

Roland Pucher, MSc.

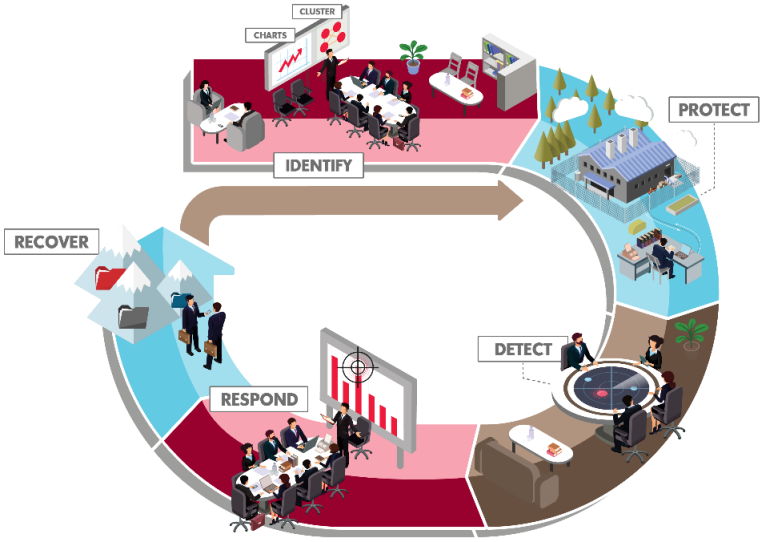
Senior Manager

M: +43 676 832626 220
E: roland.pucher@bdo.at

BDO Consulting GmbH

- IT-Advisory
- Informationssicherheit
- Datenschutz
- Data Analytics
- Digitale Forensik & eDiscovery

- Wien & Linz
- https://www.bdo.at/cyber



VORSTELLUNG

BDO Consulting GmbH

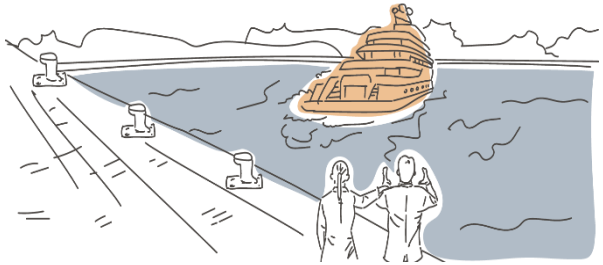
Mag. Lorenz Szabo

Manager

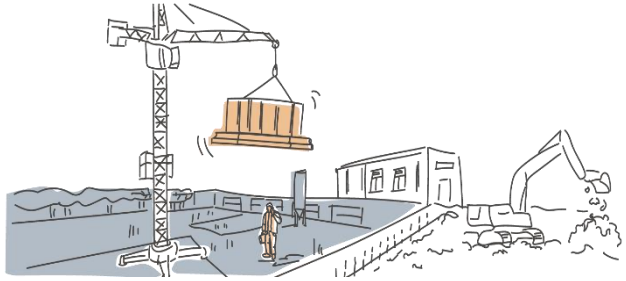
M: +43 676 832626 247
E: lorenz.szabo@bdo.at

Business Partner Management

Pre-Employment Screening



Asset Tracing Support



Risk Management

bdo.at/cybertrends

KOMMUNEN ALS PRÄFERIERTES OPFER?

Ein Waffenstillstand bei Cyber-Kriminellen wegen Corona?

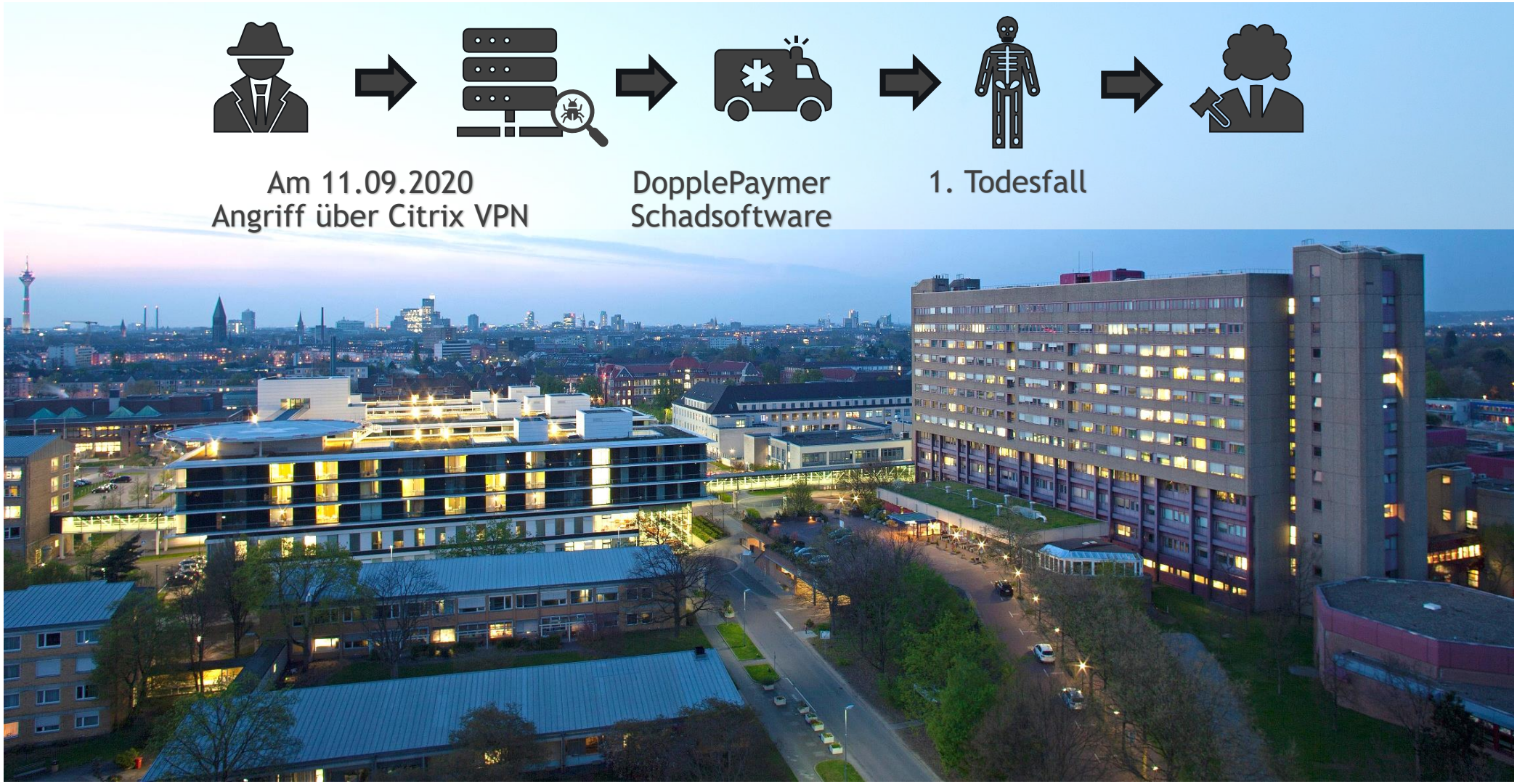
```
===

ATTENTION!!!
We have never attacked hospitals, orphanages, nursing homes, charitable
foundations, and we will not.
Commercial pharmaceutical organizations are not eligible for this list;
they are the only ones who benefit from the current pandemic.
If an attack mistakenly occurs on one of the foregoing organizations,
we will provide the decryptor for free, apologize and help fix the
vulnerabilities.

=== CL0P^_- LEAKS
```

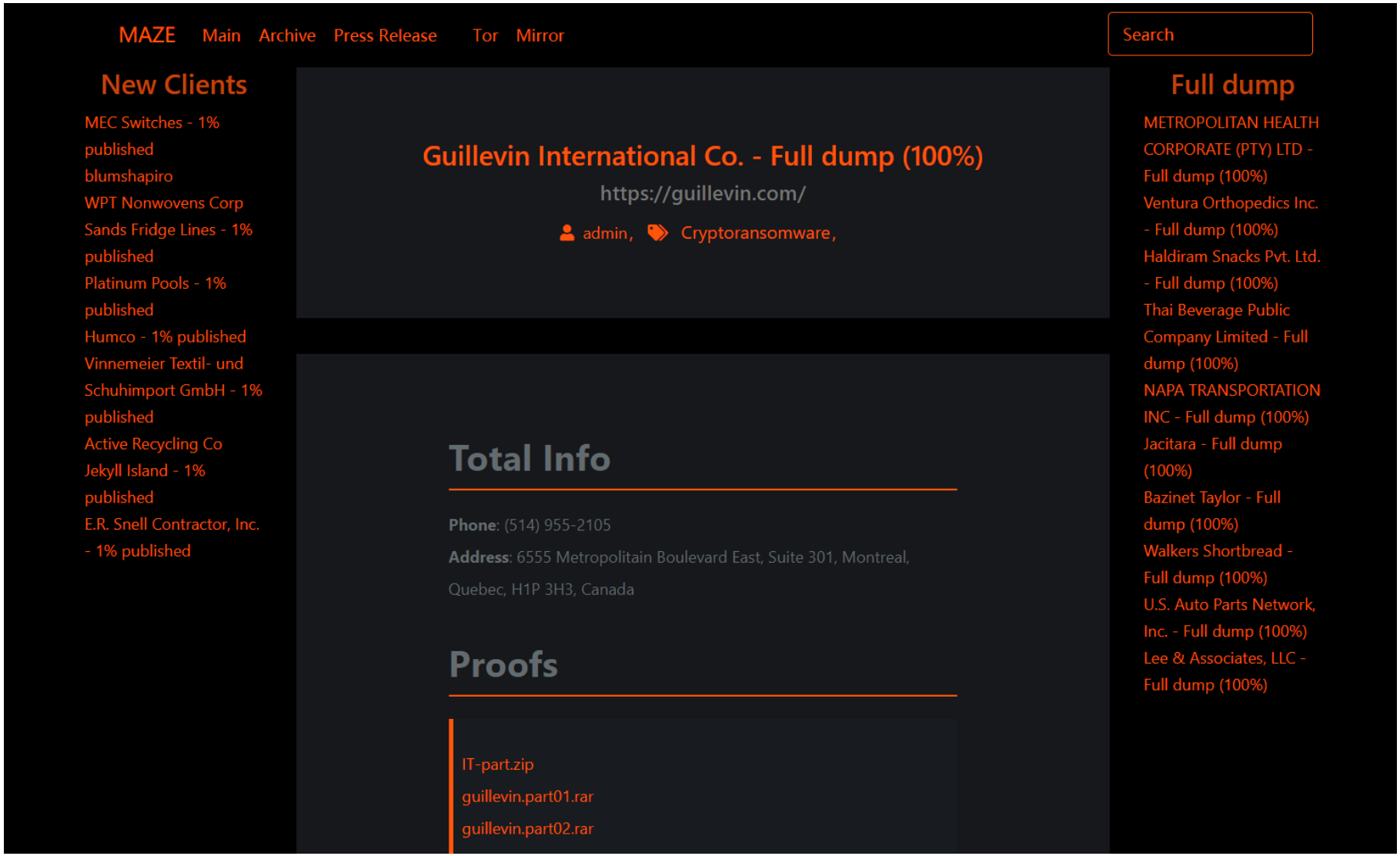
DAS „DILEMMA“ VON DÜSSELDORF

Die Suche nach den Schuldigen…



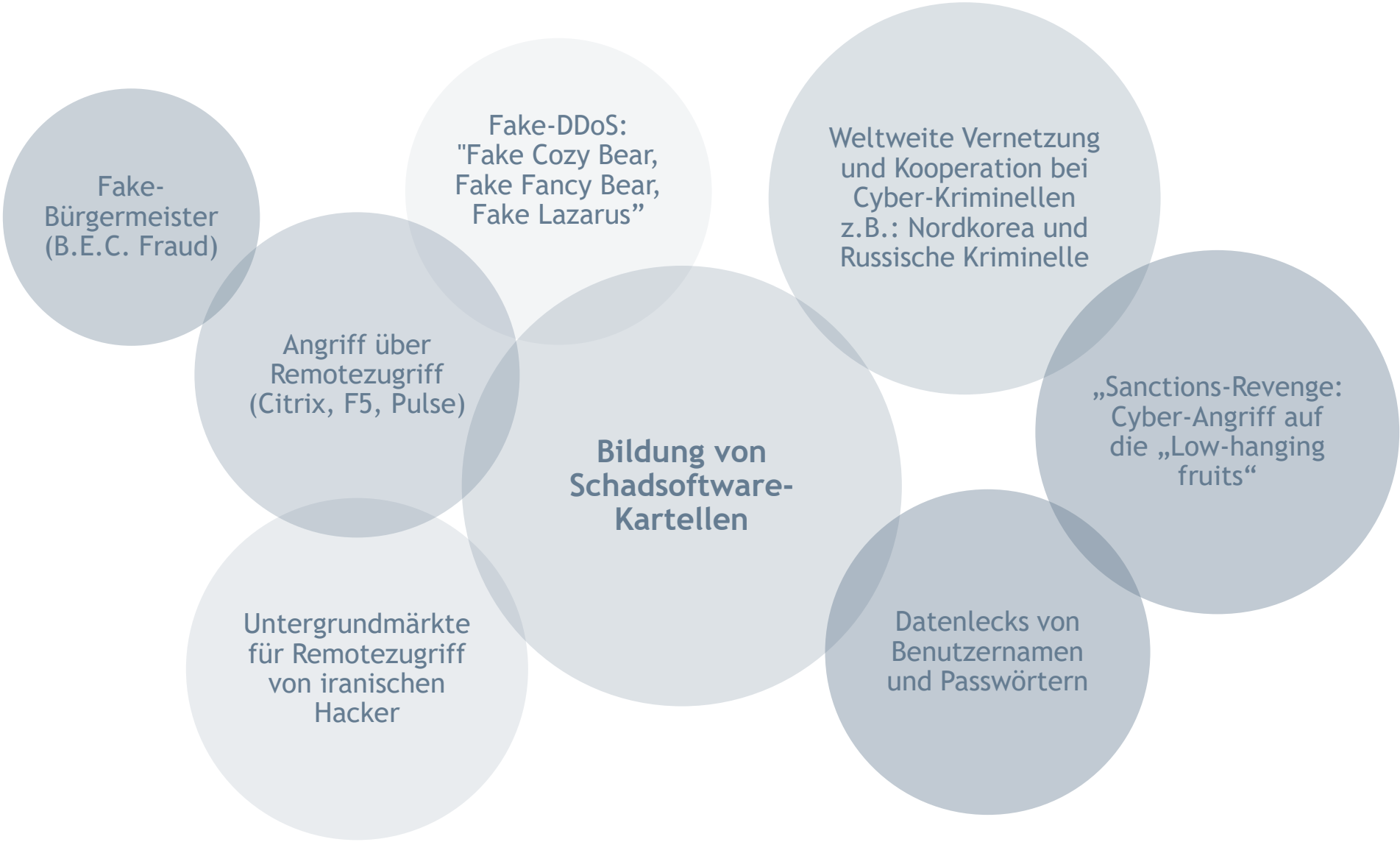
ANKÜNDIGUNGSSEITEN IM „DARK-WEB“

Beispiele: Clop & Maze



TRENDS 2020 AND BEYOND

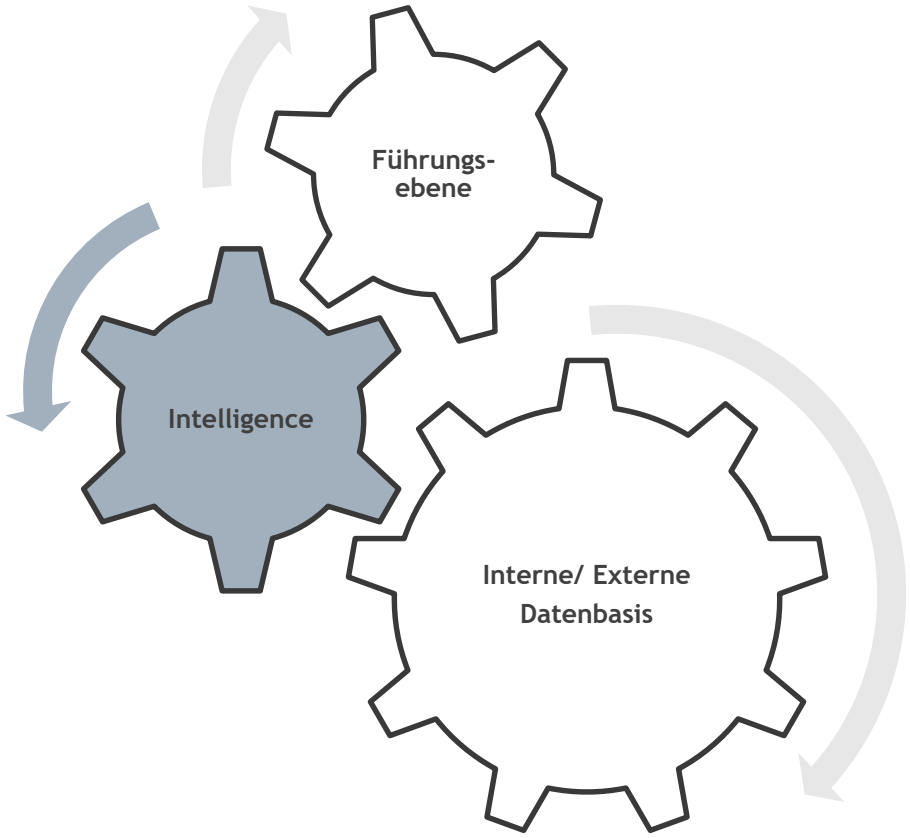
Was planen Angreifer – Was ist besonders begehrt?



„INTELLIGENCE“ MIT MEHRWERT

Von Daten zu Wissen zu kritischen Entscheidungsgrundlagen

Transparent und nachvollziehbar



- Ziele/-vision
- Stakeholder-Analyse in Bezug auf Informationsbedarf
- Datenbeschaffung und -Bewertung
- Analyse und Ableitungen treffen → Information erzeugen
- Risikoanalyse & Kosten-/Nutzen-Analyse „Priorisierung“
- Entscheidungsgrundlage („zweckorientiertes Wissen“) formulieren
- Umsetzung der Entscheidung & Nachverfolgung

Recherchiert, validiert und verifiziert

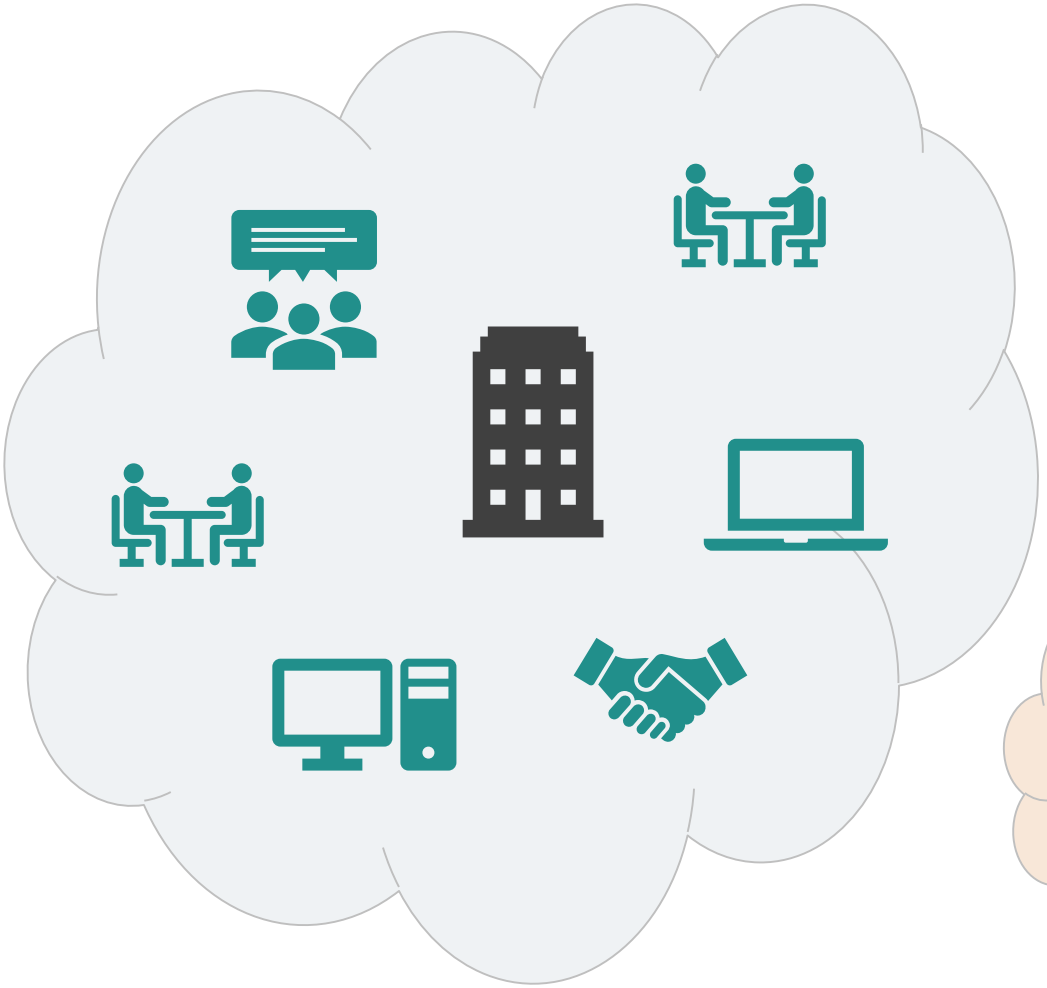
HERAUSFORDERUNGEN

Cyber Security in der Pandemie

DAS UNTERNEHMEN VOR COVID-19

Cyber Security in der Pandemie

Unternehmensintern

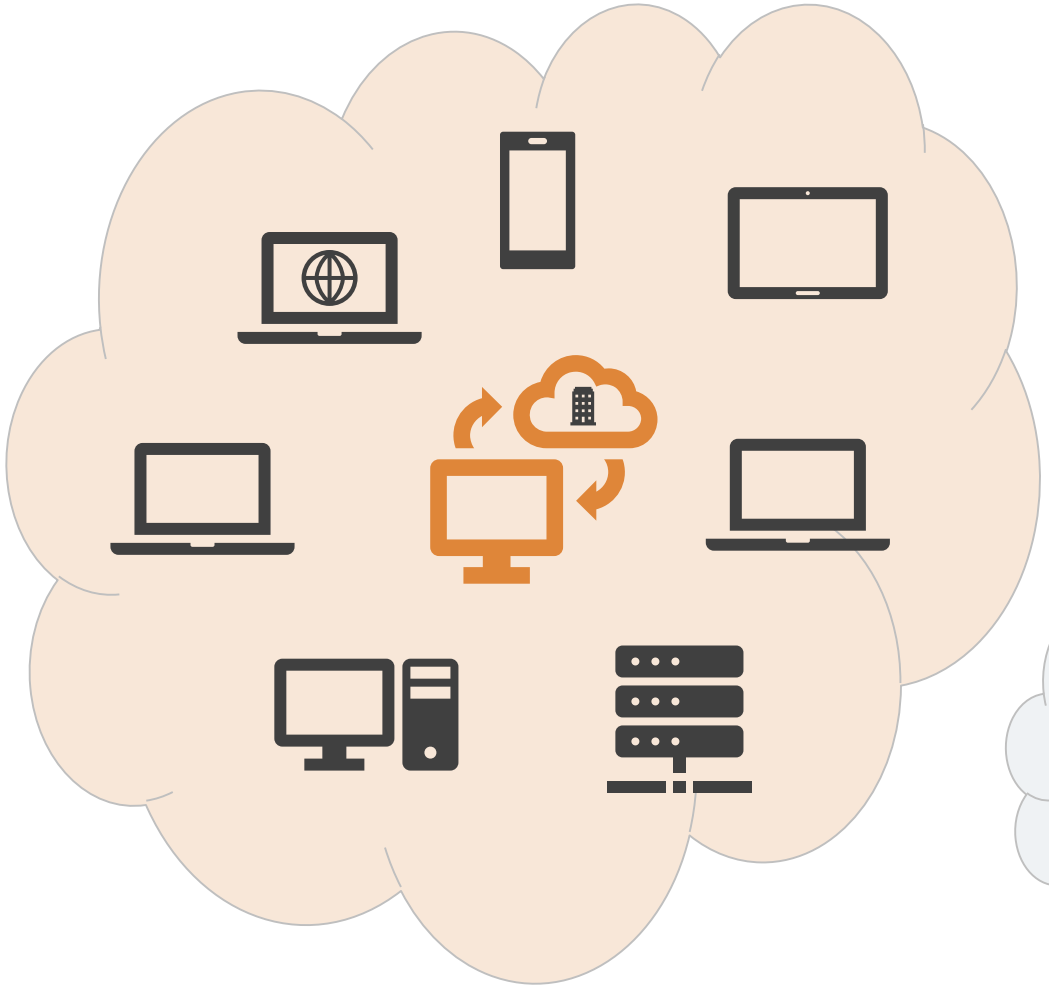


- Viele Mitarbeiter im internen Netzwerk
- Wenig Mitarbeiter extern
- Begrenzte Anzahl an Kanälen in das Unternehmensnetzwerk hinein
- Externe Zugänge:
  - Website, zum Teil von externen Dienstleistern gehostet
  - Webmail
  - Restriktives VPN

Remote

DAS UNTERNEHMEN NACH COVID-19

Cyber Security in der Pandemie



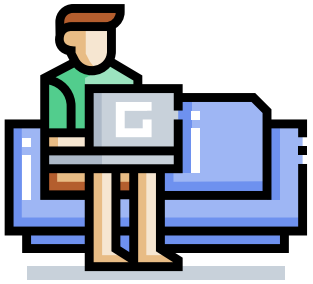
- Weniger Mitarbeiter direkt im Unternehmen
- Viele Mitarbeiter extern mit Zugängen zum internen Netzwerk
- Externe Zugänge:
  - Webmail für alle Mitarbeiter
  - Remote-Desktop-Verbindungen für alle Mitarbeiter
  - VPN oder ähnliches (z.B. Citrix) für alle Mitarbeiter
  - FTP-Server oder andere Lösungen für den Datenaustausch
- Mehrere Wege in das Unternehmensnetzwerk
  - Erhöhtes Risiko im Home-Office durch Phishing bzw. unbefugten Zugriff

Unternehmensintern

AUSWIRKUNGEN DER KRISE

Cyber Security in der Pandemie

- Höhere Abhängigkeit von IT-Infrastruktur
- Höherer Schaden bei Ausfällen
- Größere Angriffsfläche (Remote-Dienste)



- Weniger Kontrolle (Homeoffice)
- Weniger Struktur im Arbeitsalltag
- Beeinträchtigter Informationsfluss im Unternehmen

CYBER-SECURITY - MENSCH, PROZESSE UND TECHNOLOGIE!

Cyber Security in der Pandemie

Prozesse & Organisation

- Governance
- Management Systeme
- Richtlinien und Policies
- Lieferanten & Partnermanagement
- Compliance & Auditierung

Mensch

- Cyber-Hygiene
- Training & Awareness
- Fähigkeiten und Qualifikation

Technologie

- IT-Systeme & IT-Architektur
- Applikationslandkarte
- Antivirus, Firewall …
- Zugriffsschutz

HERAUSFORDERUNGEN HOME HOFFICE

Cyber Security in der Pandemie

- **Neue Risiken insb. durch Arbeit im Home-Office**
  - Mitarbeiter und Endgeräte außerhalb des Unternehmens (Netzwerks)
  - Kollaboration Tools
  - Phishing & Credential Fraud
  - Schadsoftware
  - Remote-Zugriffsmöglichkeiten bieten zusätzliche Angriffsfläche

- **Organisatorische und technische Maßnahmen** für die Arbeit im Home-Office müssen erst umgesetzt werden, z.B.
  - Richtlinien
  - Schulung der Mitarbeiter
  - Reaktion auf Vorfälle (Incident Response)

ZAHLEN, DATEN, FAKTEN

Cyber Security in der Pandemie

Bedrohungen in Zeiten von Corona

18 Millionen

täglich identifizierte Malware- und Phishing-E-Mails im Zusammenhang mit COVID-19 bei Google Mail

240 Millionen

täglich identifizierte Spam-Mails im Zusammenhang mit COVID-19 bei Google Mail

> 800.000

täglich von Kaspersky identifizierte RDP Bruteforce Angriffe in Nachbarländern (Spitzenwerte)

> 75%

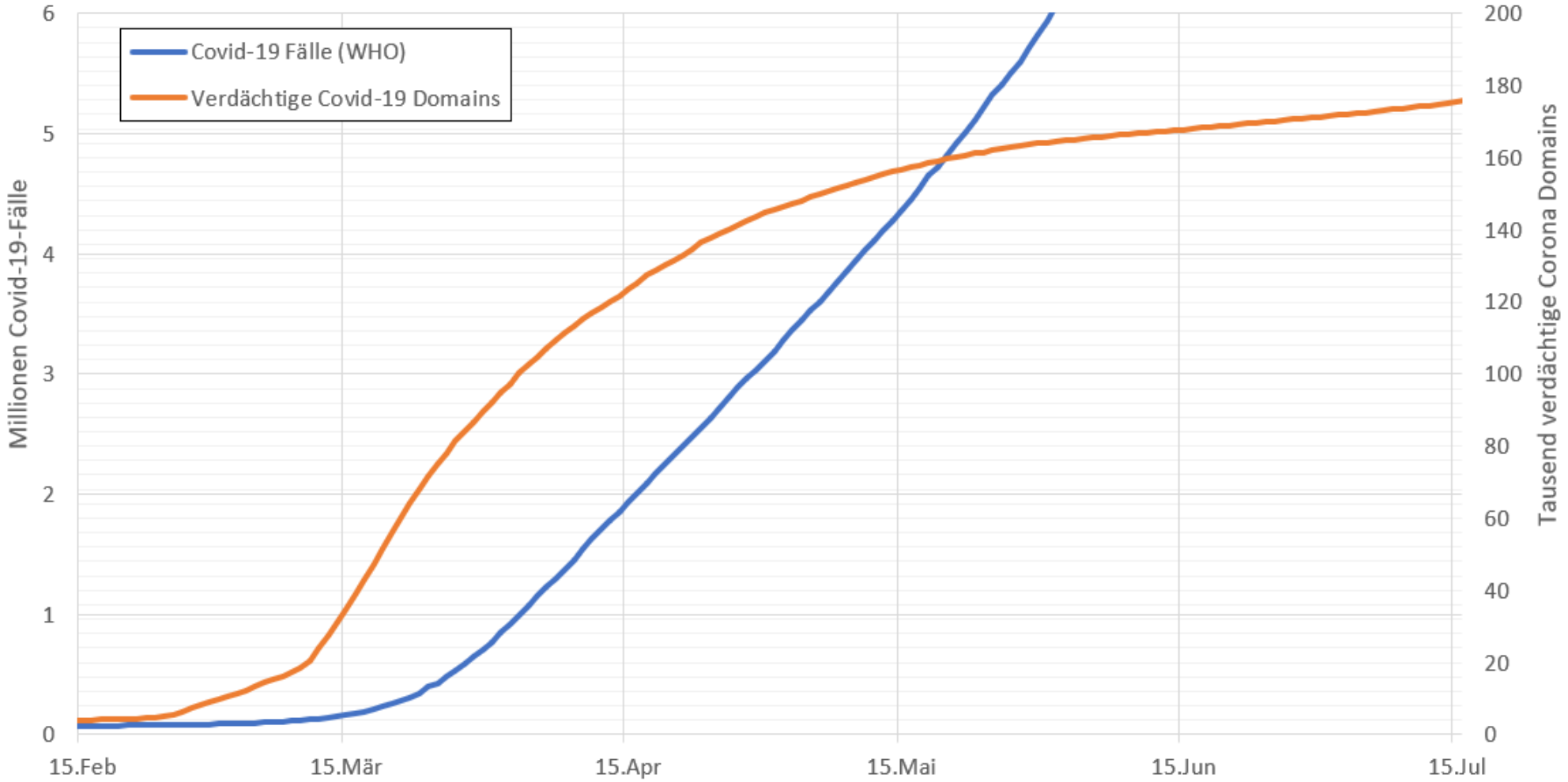
der Ransomware Angriffe im Q1 2020 verwendeten Phishing-E-Mails oder RDP als Angriffsvektor

Quellen:

https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/
https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

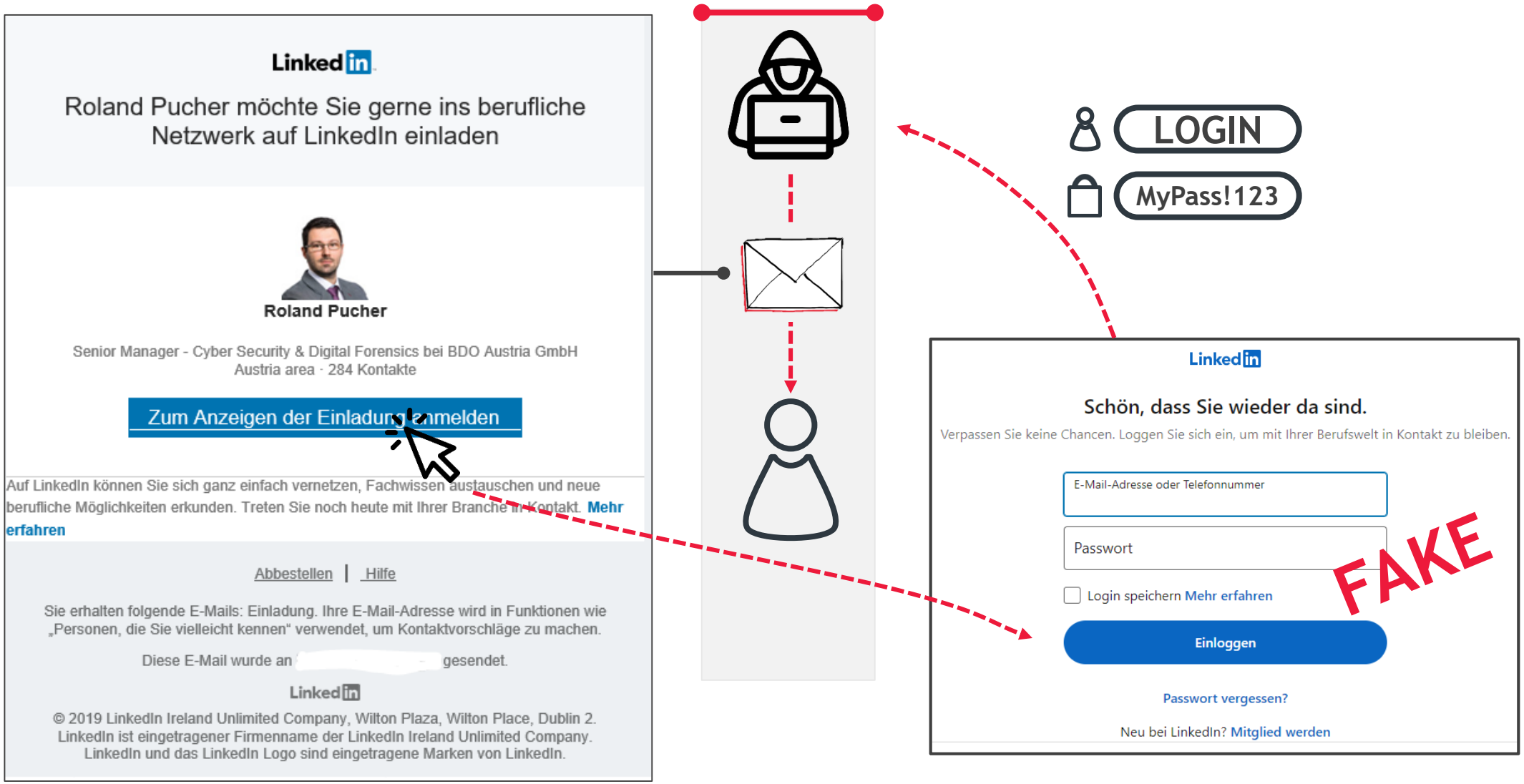
VERGLEICH: COVID-19-FÄLLE UND VERDÄCHTIGE COVID-DOMAINS

Cyber Security in der Pandemie



FAKTOR MENSCH

Phishing & Credential Fraud



FAKTOR MENSCH

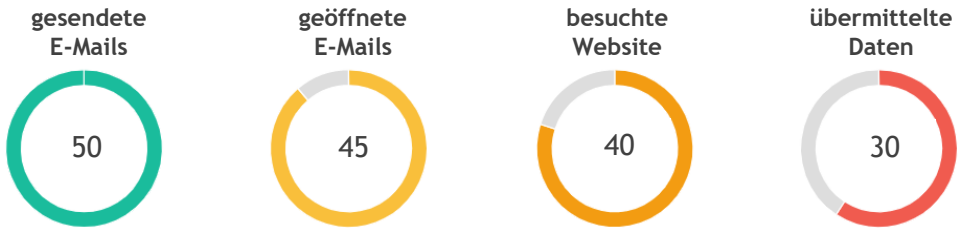
Phishing & Credential Fraud

Das Ergebnis einer Phishing-Kampagne

Ergebnisse je Szenario

Szenario 1

Zielgruppe: Standort HQ



Szenario 2

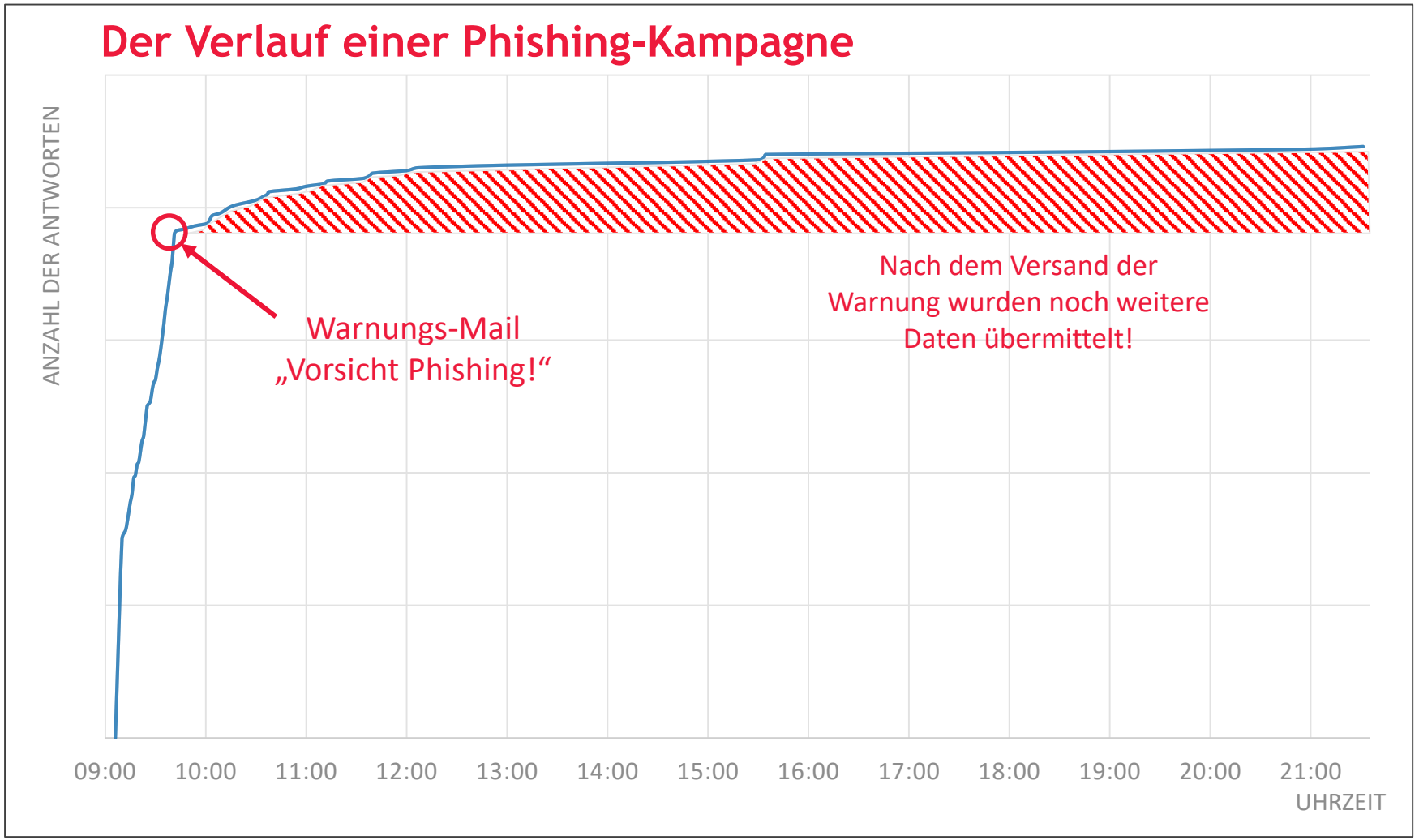
Zielgruppe : Fachliche Mitarbeiter

Szenario 3

Zielgruppe : Operative Mitarbeiter

FAKTOR MENSCH

Phishing & Credential Fraud



CYBER-ANGRIFFE IN DER KRISE

Cyber Security in der Pandemie

Faktor Technologie

- Schadsoftware (Ransomware)
- Denial of Service
- Schwachstellen in IT-Systemen

Faktor Mensch

- Social Engineering
- Phishing & Credential Fraud
- Fake-President Attack

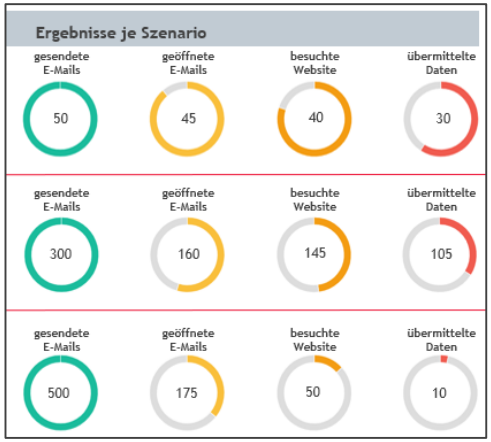
RISK ASSESSMENT

BDO Cyber Security Services

Faktor Mensch 1

Awareness Kampagne

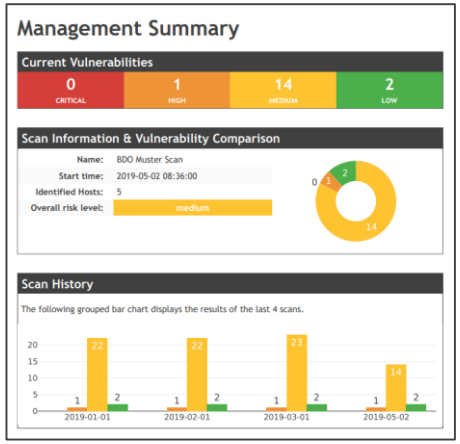
- Evaluierung der Reaktion Ihrer Mitarbeiter auf verschiedene Szenarien
- Risikofaktor Mensch wird „messbar“



Externer Perimeter 2

Vulnerability Assessment & Penetration Testing

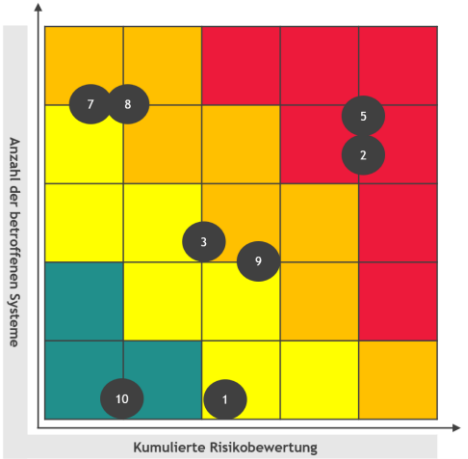
- Überprüfung aller extern (aus dem Internet) erreichbaren Systeme
- Liefert einen Überblick über Risiken und Schwachstellen der externen IT-Systeme



Interne IT-Systeme 3

Vulnerability Assessment & Penetration Testing

- Umfassende Überprüfung von IT-Systemen und Applikationen
- Zeigt Schwachstellen & Konfigurationsmängel in IT-Systemen und Applikationen



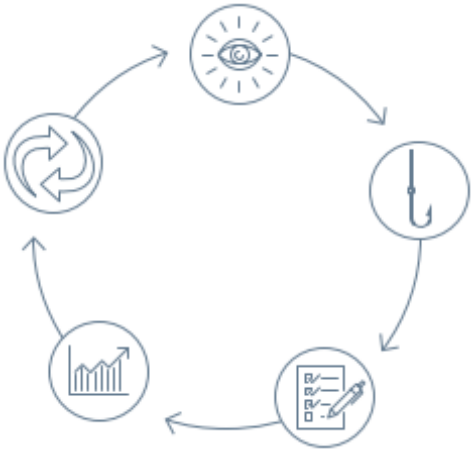
Weiterführende Maßnahmen 4

Maßnahmenumsetzung

IT-Security Assessments

Awareness & Trainings

- Individuelle Unterstützung anhand der Ergebnisse der Assessments



ÜBERSICHT

Cyber Security, Privacy Management & IT-Forensik

Assessment

Identifikation der Assets, Risiken & Schwachstellen

Technische Sicherheitsüberprüfungen

- Vulnerability Assessment
- Penetration Testing
- Physical Security Assessment
- Überprüfung von Sicherheitskonzepten (z.B. Firewall Review)

Informationssicherheitsmanagement

- ISO/IEC 27001 Gap Analyse
- Cyber Security Readiness Assessment

Datenschutz / DSGVO

- Datenschutz Gap Analyse
- Prüfung und Attestierung nach ISAE 3000

IT Assurance

- Prüfung der ITGCs (IT General Controls)
- Prüfung der ITACs (IT Application Controls)
- Prüfung von ausgelagerten Dienstleistungen
- Attestierung nach ISAE 3402

Consulting

Beratung in den Bereichen Cyber Security, Informationssicherheit & Datenschutz

Intelligence

- Integrity Due Diligence
- Pre-Employment Screening
- Asset-Tracing-Support
- Cyber-Intelligence Services or “Exposure Assessments”
- Threat-Intelligence Services

Datenschutz / DSGVO

- Implementierung eines Datenschutz Management Systems
- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Betroffenenrechte
- Datenschutzhandbuch und Richtlinien
- Awareness, Training & E-Learning
- Anonymisierung und Löschung personenbezogener Daten in SAP HR/HCM

Reaction

Reaktion auf Sicherheits- und Datenschutzvorfälle

IT-Forensik

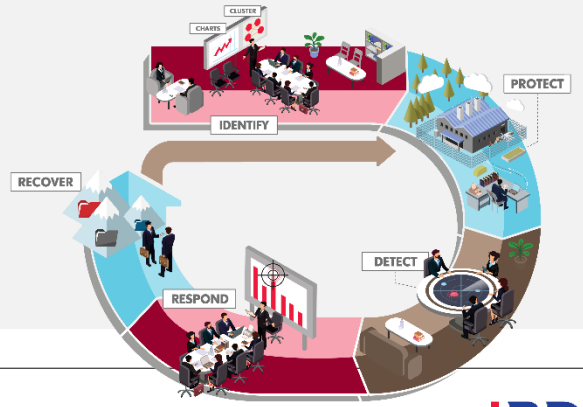
- Computerforensische Unterstützungsleistung
- eDiscovery Unterstützung
- Unterstützung beim Incident Management
- Incident Response / Malwareanalyse

Informationssicherheitsmanagement

- Unterstützung bei der Behebung von Schwachstellen und Verbesserung der IT-Infrastruktur

Datenschutz / DSGVO

- Unterstützung bei Datenschutzvorfällen




CHANGE HAPPENS, INNOVATION LEADS.
BDO