DISCOVER THE SPIR.iT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

CyberSecurity: Herausforderung Home Office

Vortrag für die Techniker Krankenkasse

Tobias Rademann, M.A.

8. Dezember 2021


Merry Christmas?

Agenda

Begrüßung & Vorstellung

1. iT-Sicherheit in der Praxis
2. aktuelle Herausforderungen durch das HO
3. iT-Risiken durch das HO & sinnvolle Schutzmaßnahmen
4. Ihr effizienter Action Plan
5. Fazit

Abschlussdiskussion

Kurzprofil: R.iT GmbH

- **Ausrichtung:** iT-Unternehmensberatung
- **Fokus:** Digitale Transformation Ihres Unternehmens
  > Strategie
  > Organisation
  > Informationstechnologie

  → **Chancen** nutzen!
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte** Zentrale: Bochum
  Region Nord: Bad Schwartau
- **Zertifizierung:** BMWi-autorisiert für > iT-Sicherheit *und*
  > digitale Geschäftsprozesse
  Deutscher Excellence Preis 2021 in Bronze

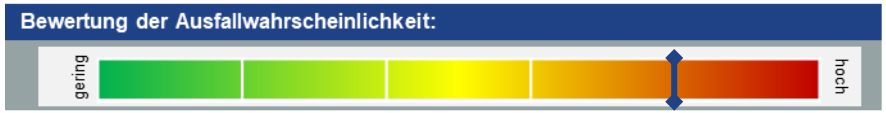
go-digital

iT-Sicherheit in der Praxis

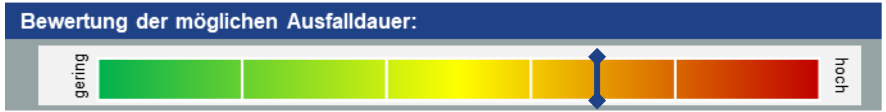
Woher wissen wir das?

Erfahrungen aus unserem RIT® iT-Risk Assessment

Risiko 1:



Risiko 2:



Risiko 3:

Risiko 4:

Risiko 5:

CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

Fall 1

- **Vorbesprechung mit dem iT-Dienstleister:**
  - Die Server laufen seit Jahren.
  - Das System ist **sicher**.
  - Die Datensicherung haben wir sogar **doppelt** ausgelegt.

- **Ergebnis der iT-Analyse:**
  - Das System war **seit dem 09.11. kompromittiert**.
  - Die zentrale Datensicherung lief **seit über sechs Wochen (!)** nicht.
  - Eine offsite-Datensicherung war **nicht vorhanden**.
  - Das Kennwort für den Zugriff auf die Datensicherung lag **im Klartext** vor.

Fall 2

24.11.: Angebotsbesprechung

- R.iT: Sollen wir uns auch Ihre **Datensicherung** anschauen?
- Kunde: Nein, die läuft problemlos. Wir haben schon zig Dateien wiederhergestellt, hier ist **definitiv kein Bedarf**.

26.11.: Anruf vom Kunden

- Kunde: Können Sie uns bei einem **iT-Sicherheitsvorfall** helfen? Wir wurden gehackt. An unsere Kunden und Lieferanten wurden zudem Schad-eMails verschickt.
- R.iT: System seit dem 09.11. kompromittiert.
  Datensicherung: Historie: **nur 1 Woche**
  Umfang: **lückenhaft**; cloud fehlte **vollständig**

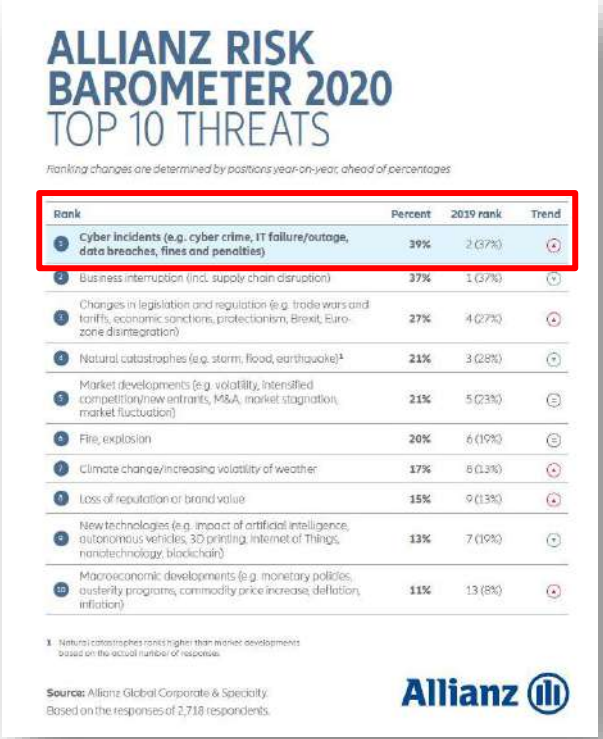
Ziel dieser Beispiele

- ~~Angst machen~~
- **Sensibilisieren**
  - →iT ist hochkomplex
  - →iT ist gewachsen (gerade jetzt nach Corona!)
  - →iT-Sicherheit = **weltweit Unternehmensrisiko Nr. 1**

➔ **handeln** Sie **proaktiv**

➔ **hinterfragen** Sie **kritisch** den **Status Quo**

➔ und sichern Sie damit die **Zukunft Ihrer Unternehmen**



ALLIANZ RISK BAROMETER 2020
TOP 10 THREATS

Ranking changes are determined by positions year-on-year, ahead of percentages

Rank		Percent	2019 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**39%**	2 (37%)	▲
2	Business interruption (incl. supply chain disruption)	37%	1 (37%)	▼
3	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Eurozone disintegration)	27%	4 (27%)	▲
4	Natural catastrophes (e.g. storm, flood, earthquake)[1]	21%	3 (28%)	▼
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	21%	5 (23%)	=
6	Fire, explosion	20%	6 (19%)	=
7	Climate change/increasing volatility of weather	17%	8 (13%)	▲
8	Loss of reputation or brand value	15%	9 (13%)	▲
9	New technologies (e.g. impact of artificial intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)	13%	7 (19%)	▼
10	Macroeconomic developments (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	11%	13 (8%)	▲

1. Natural catastrophes rank higher than market developments based on the actual number of responses.

Source: Allianz Global Corporate & Specialty.
Based on the responses of 2,718 respondents.

Allianz

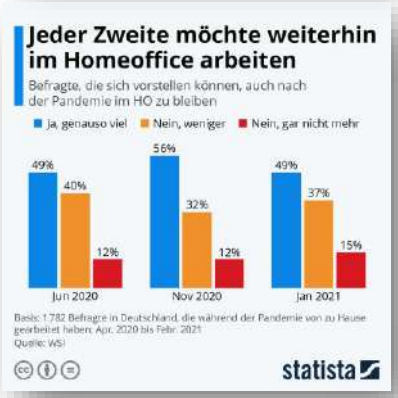
aktuelle Herausforderungen

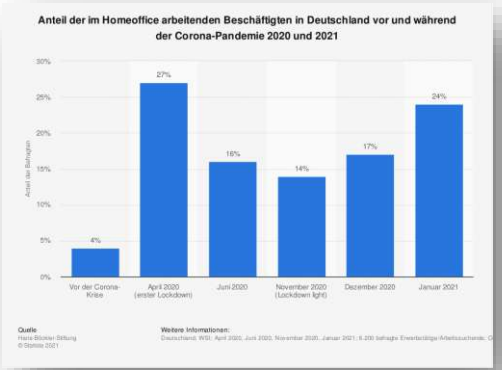
aktuelle Herausforderungen

Home Office wird bleiben!

Home Office wird bleiben

Quelle:
https://de.statista.com/themen/6093/homeoffice/





Perspektive von Home-Office, Telearbeit und mobilem arbeiten
Quelle Bundesamt für Sicherheit in der Informationstechnik

aktuelle Herausforderungen

Home Office wird bleiben!

Home Office erhöht **Cyber-Risiken** drastisch

drastisch steigende Cyber-Risiken

VDI nachrichten

E-PAPER LOGIN

TECHNIK KARRIERE WIRTSCHAFT E-PAPER ABO SHOP ELIBRARY

STUDIE ZUR CYBERSICHERHEIT 15. APR 2021 VON REGINE BÖNSCH

Homeoffice erhöht Gefahr für IT-Sicherheit drastisch

Das Verlegen der Arbeit in heimische Büros oder an Küchentische sorgt für mehr Angriffsflächen für Hacker. Diese Auswirkungen des Trends hin zum Homeoffice sind für jedes vierte kleine Unternehmen existenzbedrohend, das zeigt jetzt eine repräsentative Studie des Bundesamts für Sicherheit in der Informationstechnik.

manager magazin

Expertenschätzung

Cyberangriffe im Homeoffice verursachen Milliardenschäden

Das Homeoffice ist für Cyberkriminelle ein Geschenk, sagt das Institut der deutschen Wirtschaft. Die IT daheim sei schlechter geschützt als am Firmenstandort - durch Hackerattacken entstand daher während der Corona-Zeit ein milliardenschwerer Schaden.

23.08.2021, 14.20 Uhr

Schwachpunkt: Wer zuhause am Notebook arbeitet, ist virtuell oft angreifbar Foto: Daniel Naupold/ picture alliance / dpa

aktuelle Herausforderungen

Home Office wird bleiben!

Home Office erhöht **Cyber-Risiken** drastisch

(Folgen von) Corona: **mehr mit weniger**

durch Corona: mehr mit weniger

Auswirkungen von Corona → iT-Sicherheit

- **strategische Ebene:** Fokus auf Arbeitsfähigkeit, ~~nicht auf iT-Sicherheit~~
- **operative Ebene:** weniger Personal verfügbar für iT-Sicherheit
  komplexere Prozesse *(bspw. durch verteiltes Arbeiten)*
- **finanzielle Ebene:** weniger Geld verfügbar
- **menschliche Ebene:** Verunsicherung, Isolation

→ iT-Sicherheitsmaßnahmen stagnieren / fallen bei steigenden Anforderungen und Risiken

aktuelle Herausforderungen

Home Office wird bleiben!

Home Office erhöht **Cyber-Risiken** drastisch

(Folgen von) Corona: **mehr mit weniger**

Flexibilität: Kernanforderung der Digitalen Transformation

Flexibilität

Leistungsfähigkeit moderner **iT** entwickelt sich **exponentiell**

diese exponentielle Leistungssteigerung in der iT schafft ganz **neue Werkzeuge**

diese Werkzeuge schaffen ganz **neue** Möglichkeiten für **Prozess- und Produktinnovationen**

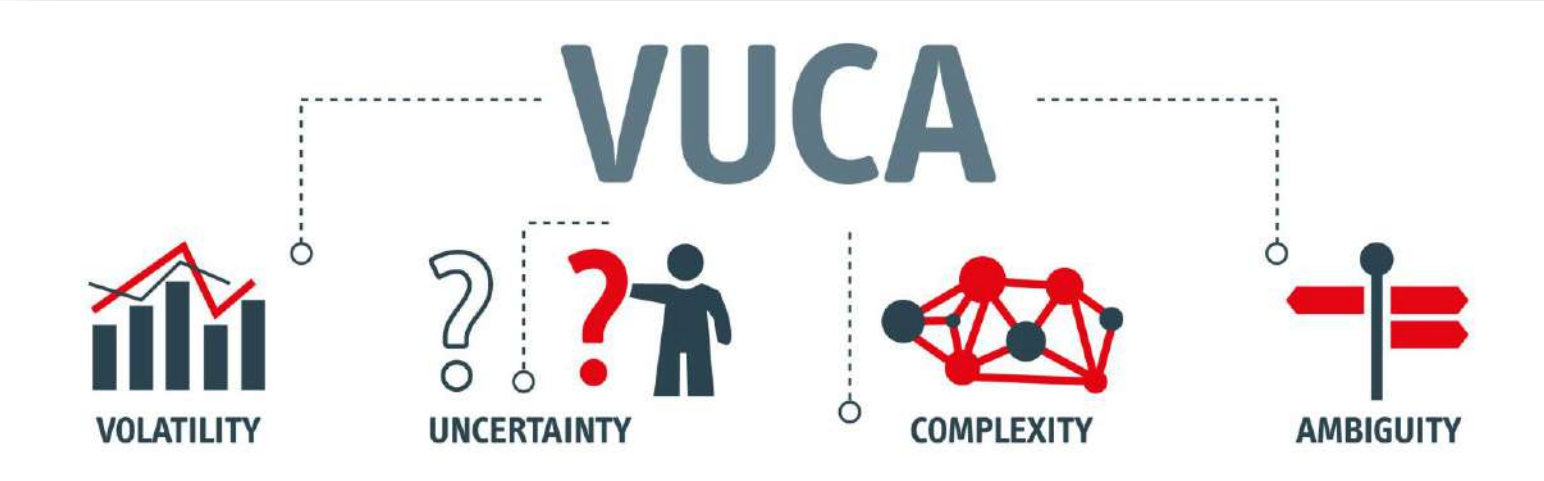
diese Prozess- und Produktinnovationen schaffen ganz **neue Märkte und Geschäftsmodelle**

… schaffen ganz **neue Arbeits- und Lebensbedingungen**

… schaffen ganz **neue Anforderungen** und erfordern ganz **neue Fähigkeiten**

= 'Digitale Transformation'

Flexibilität



= 'Digitale Transformation'

aktuelle Herausforderungen

Home Office wird bleiben!

Home Office erhöht **Cyber-Risiken** drastisch

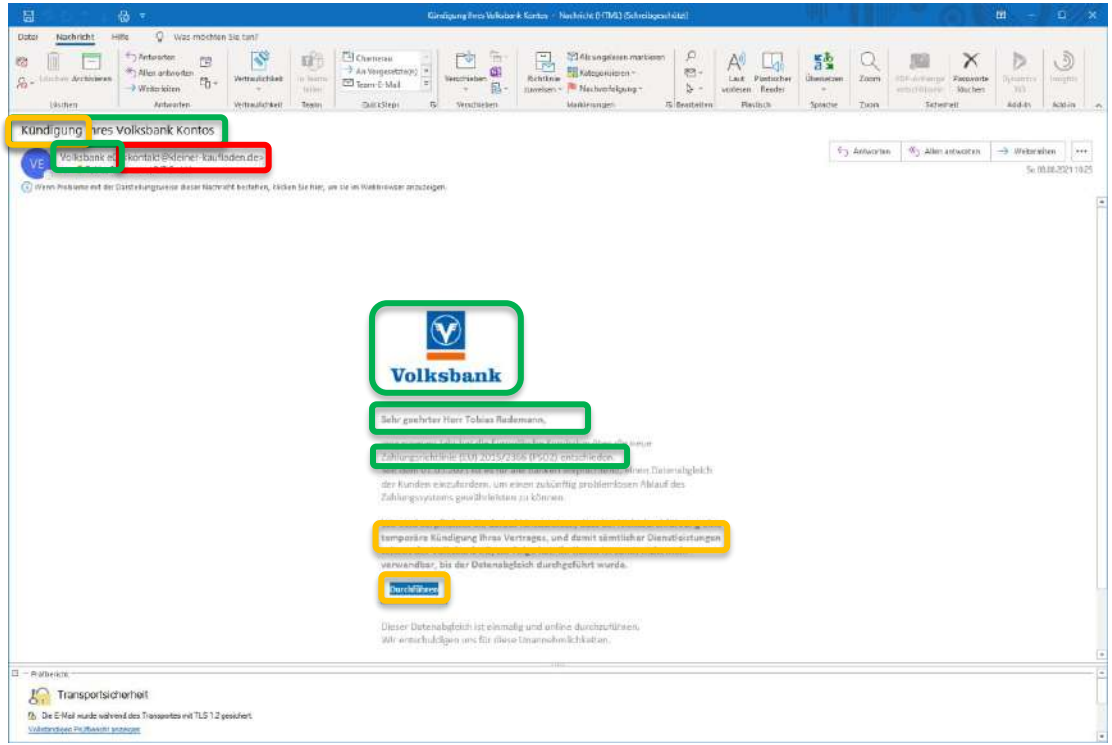
(Folgen von) Corona: **mehr mit weniger**

Flexibilität: Kernanforderung der Digitalen Transformation

iT-Sicherheitsrisiken durch HO & sinnvolle Schutzmaßnahmen

aktuelle Risiken

- **Phishing Mails**



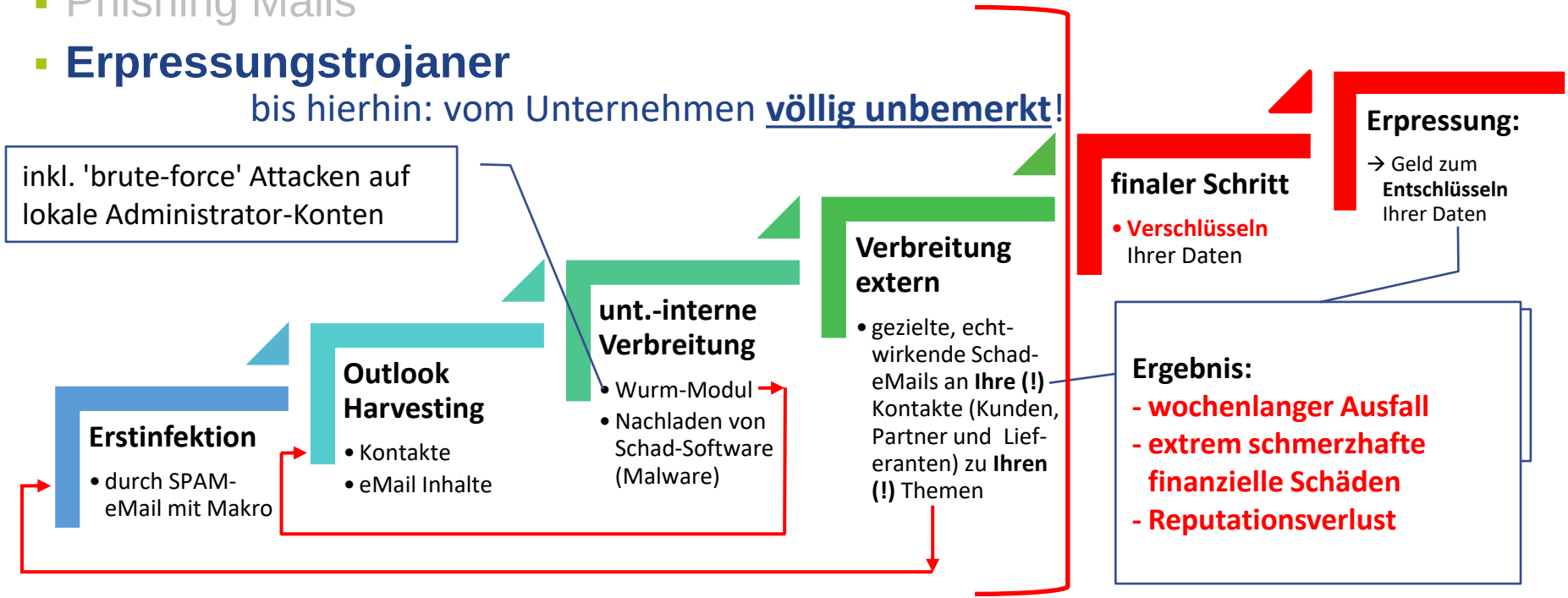
aktuelle Risiken & Schutzmaßnahmen

- **Phishing Mails**

aktuelle Risiken

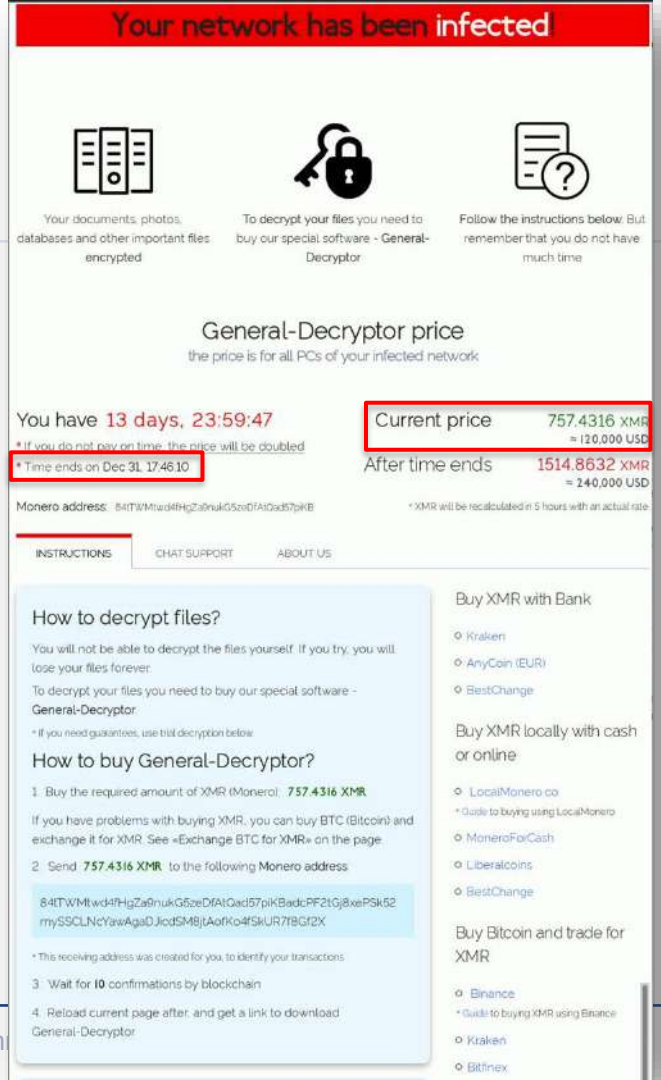
- Phishing Mails
- **Erpressungstrojaner**

bis hierhin: vom Unternehmen **völlig unbemerkt**!



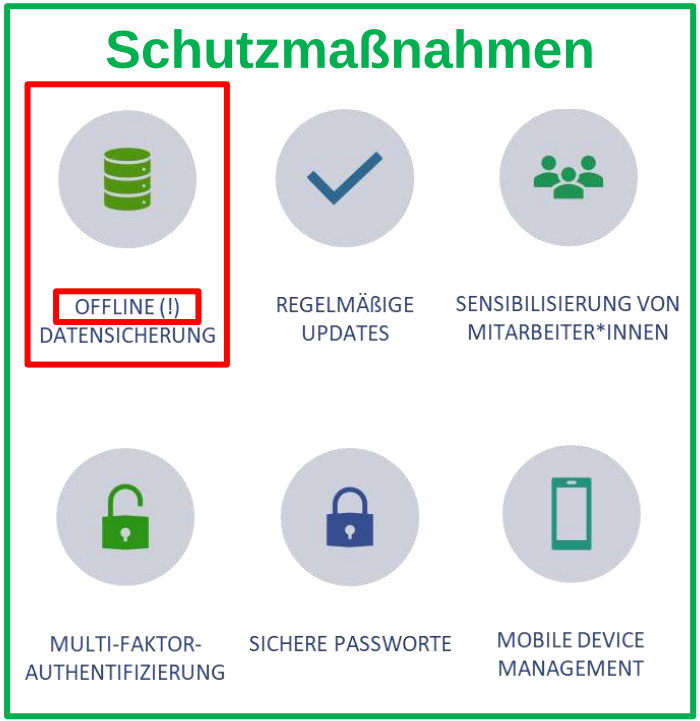
aktuelle Risiken

- Phishing Mails
- **Erpressungstrojaner**



aktuelle Risiken & Schutzmaßnahmen

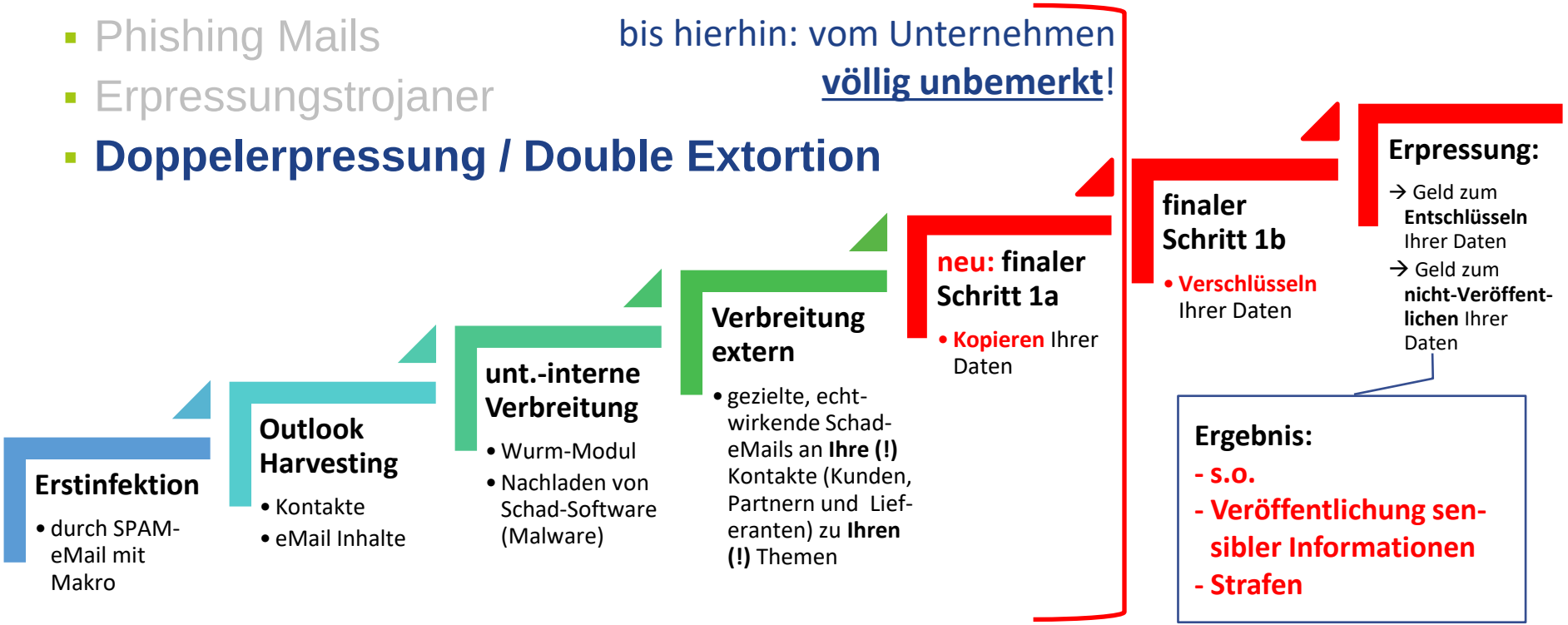
- Phishing Mails
- **Erpressungstrojaner**



aktuelle Risiken

- Phishing Mails
- Erpressungstrojaner
- **Doppelerpressung / Double Extortion**

bis hierhin: vom Unternehmen **völlig unbemerkt**!



aktuelle Risiken & Schutzmaßnahmen

- Phishing Mails
- Erpressungstrojaner
- **Doppelerpressung / Double Extortion**

Schutzmaßnahmen

DATEN-
KNAPPHEIT

DRM
(DIGITAL RIGHTS
MANAGEMENT)

+: SIEHE OBEN

aktuelle Risiken

- Phishing Mails
- Erpressungstrojaner
- Doppelerpressung / Double Extortion
- **CEO-Fraud**

aktuelle Risiken & Schutzmaßnahmen

- Phishing Mails
- Erpressungstrojaner
- Doppelerpressung / Double Extortion
- **CEO-Fraud**

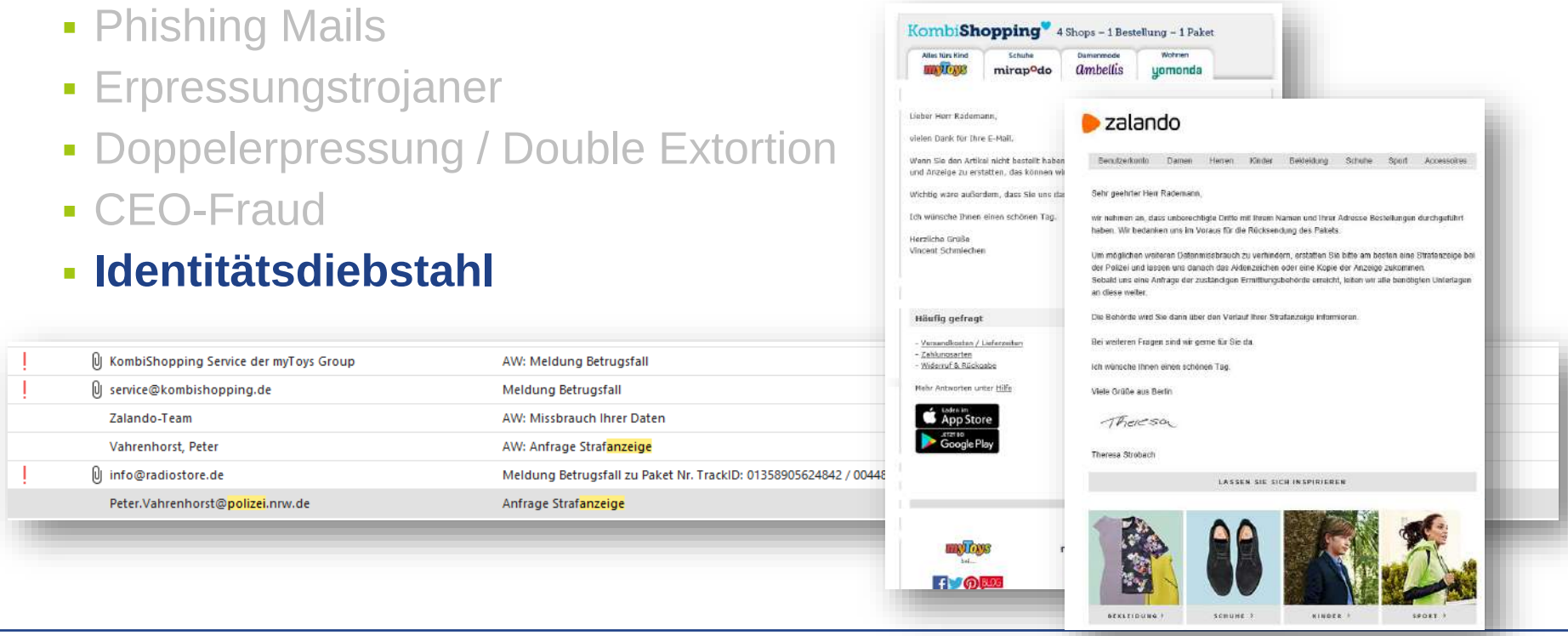
Schutzmaßnahmen

SENSIBILISIERUNG VON MITARBEITER*INNEN

MULTI-FAKTOR-AUTHENTIFIZIERUNG

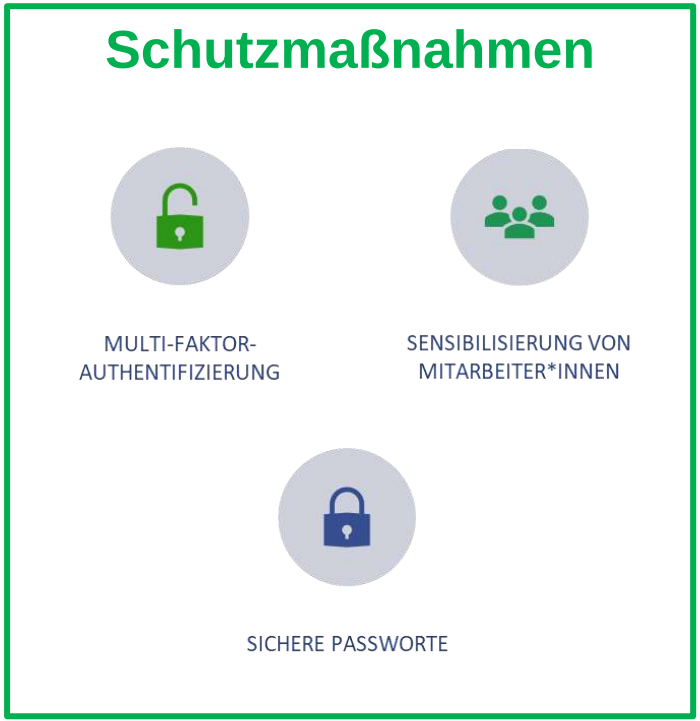
aktuelle Risiken

- Phishing Mails
- Erpressungstrojaner
- Doppelerpressung / Double Extortion
- CEO-Fraud
- **Identitätsdiebstahl**



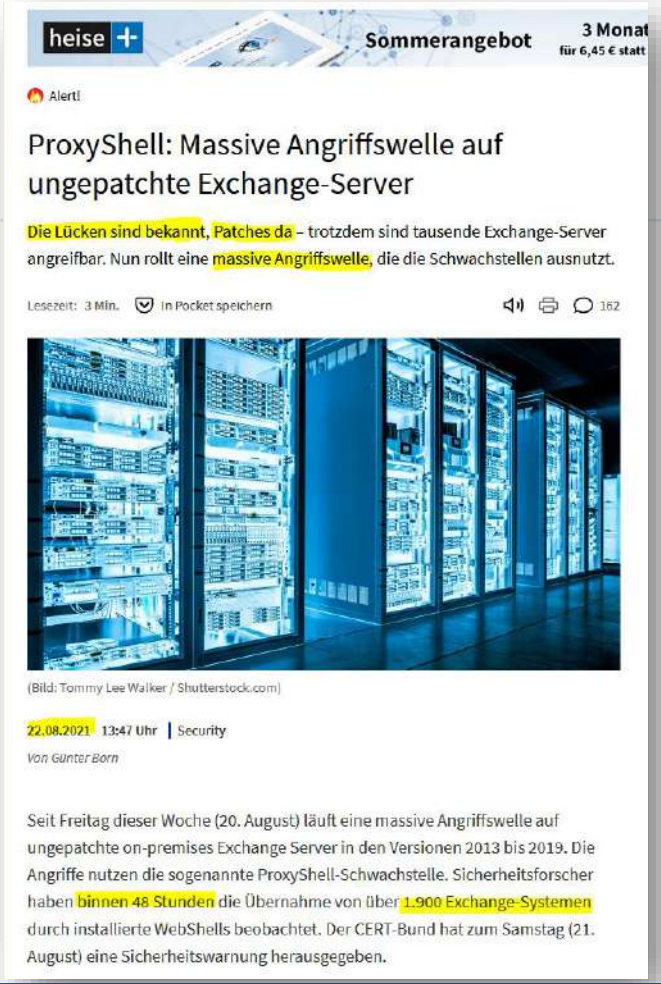
aktuelle Risiken & Schutzmaßnahmen

- Phishing Mails
- CEO-Fraud
- Erpressungstrojaner
- Doppelerpressung / Double Extortion
- **Identitätsdiebstahl**



aktuelle Risiken

- Phishing Mails
- CEO-Fraud
- Erpressungstrojaner
- Doppelerpressung / Double Extortion
- Identitätsdiebstahl
- **(Exchange-)Sicherheitslücken**



heise+ Sommerangebot 3 Monat für 6,45 € statt

Alert!

ProxyShell: Massive Angriffswelle auf ungepatchte Exchange-Server

Die Lücken sind bekannt, Patches da – trotzdem sind tausende Exchange-Server angreifbar. Nun rollt eine massive Angriffswelle, die die Schwachstellen ausnutzt.

Lesezeit: 3 Min. In Pocket speichern 162

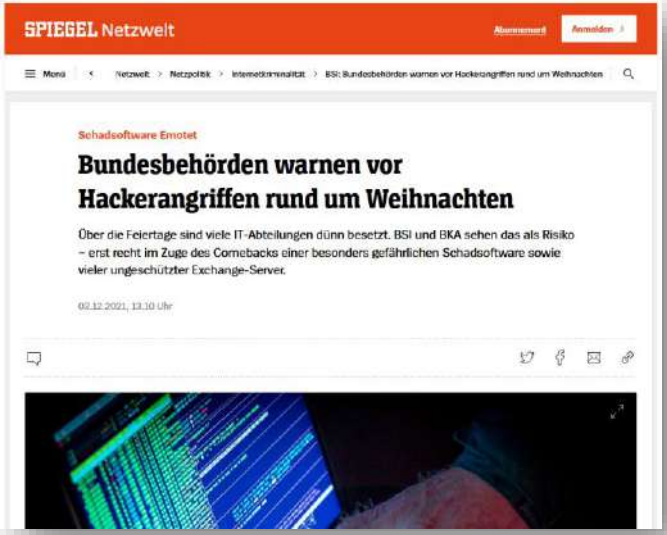
(Bild: Tommy Lee Walker / Shutterstock.com)

22.08.2021 13:47 Uhr | Security

Von Günter Born

Seit Freitag dieser Woche (20. August) läuft eine massive Angriffswelle auf ungepatchte on-premises Exchange Server in den Versionen 2013 bis 2019. Die Angriffe nutzen die sogenannte ProxyShell-Schwachstelle. Sicherheitsforscher haben binnen 48 Stunden die Übernahme von über 1.900 Exchange-Systemen durch installierte WebShells beobachtet. Der CERT-Bund hat zum Samstag (21. August) eine Sicherheitswarnung herausgegeben.

Merry Christmas 2021?!



aktuelle Risiken & Schutzmaßnahmen

- Phishing Mails
- CEO-Fraud
- Erpressungstrojaner
- Doppelerpressung / Double Extortion
- Identitätsdiebstahl
- **(Exchange-)Sicherheitslücken**

Schutzmaßnahmen

REGELMÄßIGE
UPDATES

sinnvolle Schutzmaßnahmen (Home Office)

OFFLINE (!)
DATENSICHERUNG
+ **HISTORIE**

SENSIBILISIERUNG VON
MITARBEITER*INNEN

REGELMÄßIGE
UPDATES

MULTI-FAKTOR-
AUTHENTIFIZIERUNG

ANTI-SPAM
GATEWAY

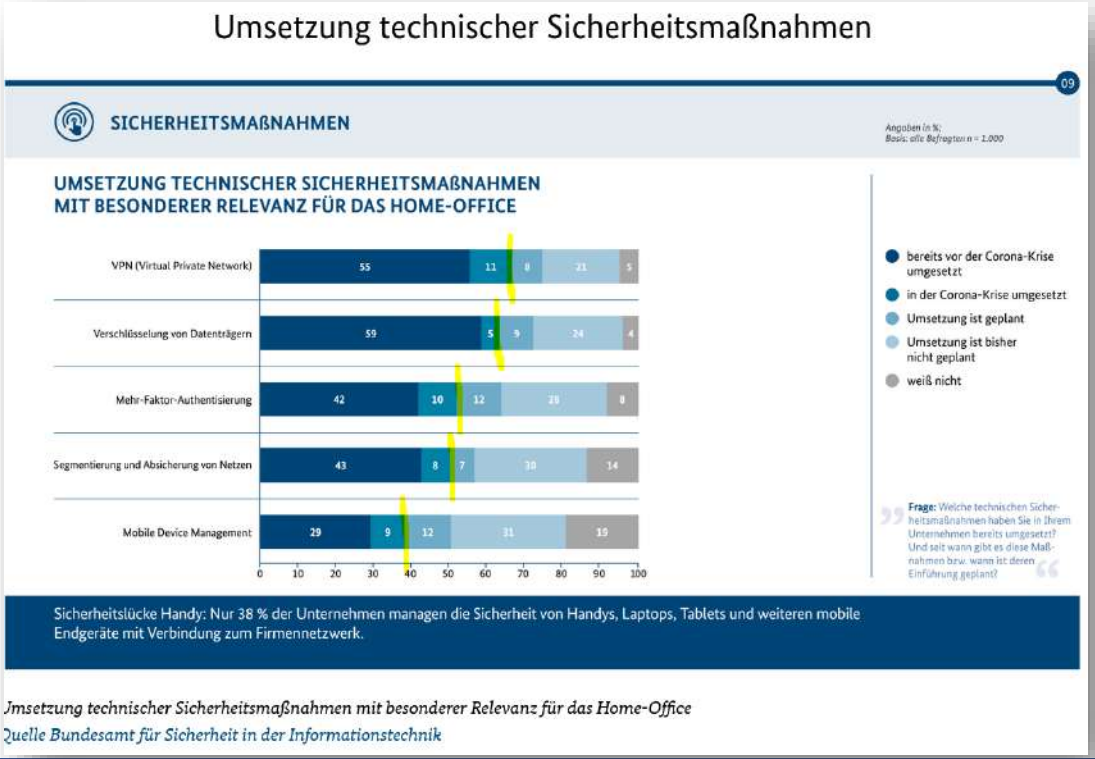
SICHERE PASSWORTE

VPN

MOBILE DEVICE
MANAGEMENT

VERSCHLÜSSELUNG
VON DATENTRÄGERN

sinnvolle Schutzmaßnahmen



Umsetzung technischer Sicherheitsmaßnahmen mit besonderer Relevanz für das Home-Office
Quelle Bundesamt für Sicherheit in der Informationstechnik

Ihr Action Plan: *sinnvolles* Vorgehen

Ihr Action Plan: sinnvolles Vorgehen

Ziel: diejenigen Maßnahmen mit dem **größten Hebel** zuerst angehen

Weg:

1.) Status Quo-**Überblick** schaffen

2.) **priorisierter** Maßnahmenkatalog

in Abstimmung auf Ihr Budget:
3.) **schrittweise & regelmäßige** Umsetzung der nächst-priorisierten Maßnahme

\+

mit einem kompetenten Partner

Die Empfehlungen des BSI

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

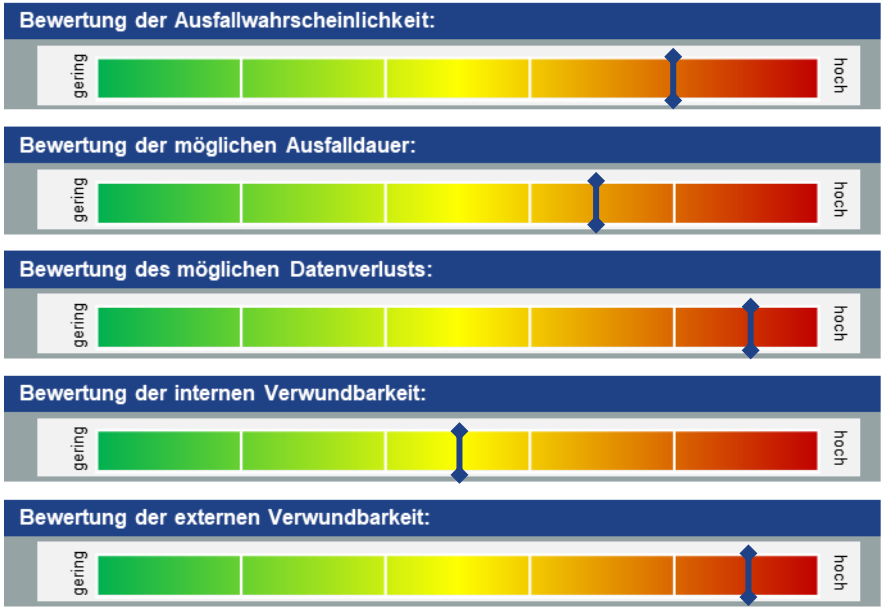
konkrete Empfehlungen

Datensicherung	→	Veeam	https://www.veeam.com/de
regelm. Updates	→	iT-Wartungsvertrag	
MA-Sensibilisierung			
sichere Passworte	→	1Password	https://1password.com/de/
	→	Überprüfung:	https://haveibeenpwned.com/
Anti-SPAM Gateway	→	NoSpamProxy	https://www.nospamproxy.de/de/
Firewalls	→	Sophos XG	https://www.sophos.com/de-de.aspx
MDM	→	Microsoft Intune	https://docs.microsoft.com/de-DE/mem/intune/
Verschlüsselung	→	Microsoft Bitlocker	
Status-Quo Analyse	→	iT-Risk Assessment	https://www.rit.de oder https://bit.ly/3BclrUz

RIT® iT-Risk Assessment

Ablauf:

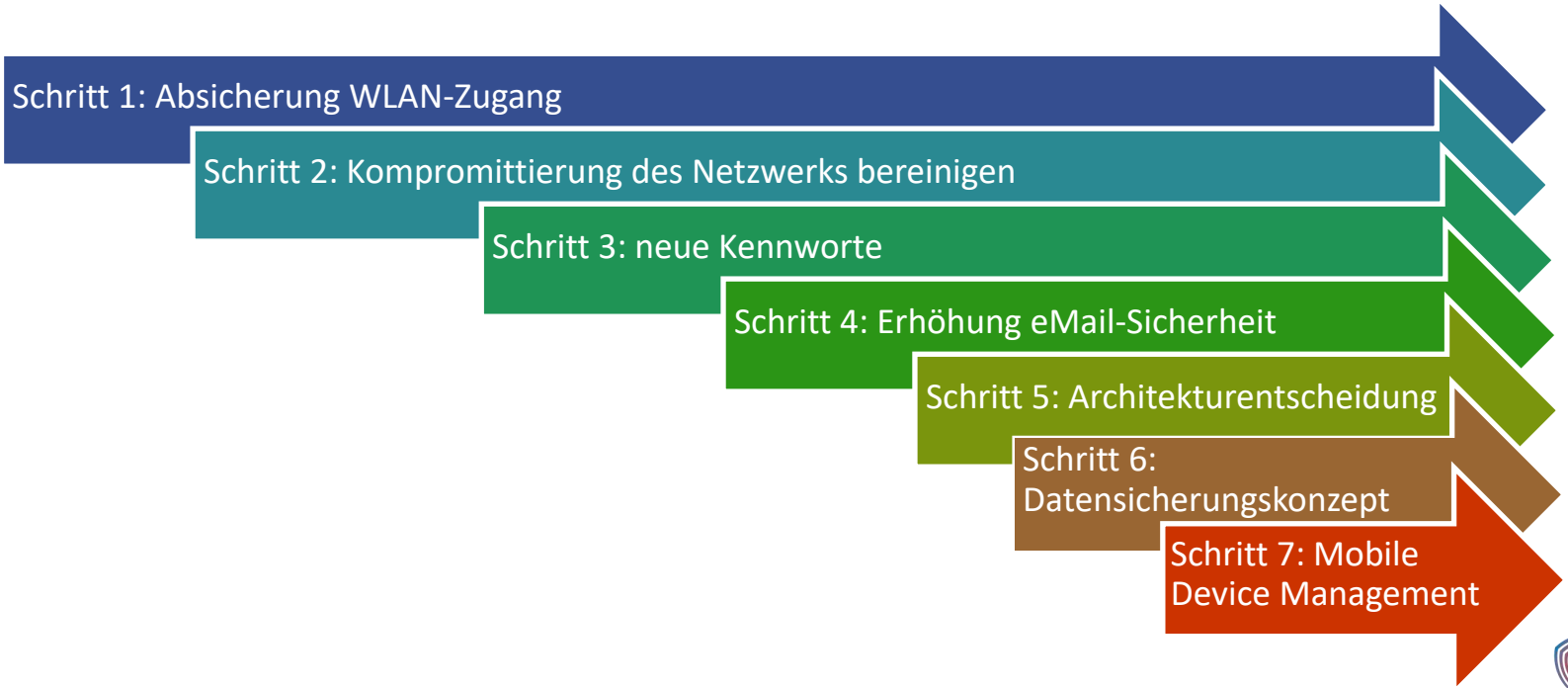
1. Erstgespräch
2. Status-Quo **Analyse**
3. **Auswertung**
4. **Bewertung**
5. **Priorisierung**: Maßnahmenkatalog



CYBERSECURITY MADE IN EUROPE™

Initiated by ECSO. Issued by eurobits e.V.

priorisierte Handlungsempfehlungen (Beispiel)



CYBERSECURITY™ MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

Fazit:
HO & iT-Sicherheit – Fluch oder Segen?

Fazit: HO & iT-Sicherheit – Fluch oder Segen?

Fazit: HO & iT-Sicherheit – Fluch oder Segen?

hilfreiche Quellen:

- **"IT-Sicherheit im Home-Office im Jahr 2020"**; Bundesamt für Sicherheit in der Informationstechnologie; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html
- **"The rise of ransomware during COVID-19 – How to adapt to the new threat environment."**; Ferbrache, David (KPMG); https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html
- **"iT-Sicherheit zu Zeiten von Corona: Erfahrungsbericht aus dem 'new normal'"**; Rademann, Tobias (R.iT); https://www.rit.de/unternehmen/downloads/vortraege
- "**100.000 Euro für Ihre Daten?**"; Air Truck Service GmbH / R.iT GmbH; https://www.rit.de/success-stories/ats-air-truck-service-gmbh-it-sicherheit

offene Fragen / Diskussion

Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

DISCOVER THE SPIR.iT OF EXCELLENCE.
SURPASS YOUR SUCCESS.

Tobias Rademann, M.A.
R.iT GmbH • www.RiT.de
Zentrale: Lise-Meitner-Allee 37, 44801 Bochum
Tel.: (0234) 43 88 00-0, Fax: -29
NL Nord: Tremskamp 5, 23611 Bad Schwartau
Tel.: (0451) 203 68-500, Fax: -499
eMail: Tobias.Rademann@RiT.de