CyberSecurity: Herausforderung Home Office

Vortrag im Rahmen der Techniktagung des BDSW

Tobias Rademann, M.A.

1. September 2021

HO = drastisch steigende Cyber-Risiken

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.

23.06.2021, 14.20 Uhr

Schwachpunkt. Wer zuhause am Notebook arbeitet, ist virtuell oft angreifbar

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.

Agenda

1. aktuelle Herausforderungen
2. iT-Sicherheitsrisiken durch HO & sinnvolle Sicherheitsmaßnahmen
3. Ihr Action Plan
4. Fazit

Kurzprofil: R.iT GmbH

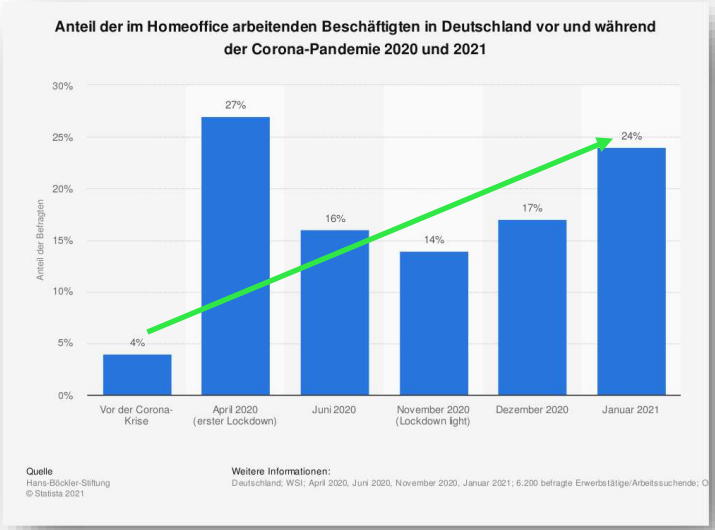
- **Fokus:** iT-Unternehmensberatung für die Digitale Transformation
- **Kernthemen:** Digitale Transformation Ihres Unternehmens
  > Strategie
  > Organisation
  > Informationstechnologie
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte** Zentrale: Bochum
  Region Nord: Bad Schwartau
- **Zertifizierung:** BMWi-autorisiert für > iT-Sicherheit *und*
  > digitale Geschäftsprozesse
  Deutscher Excellence Preis 2021 in Bronze

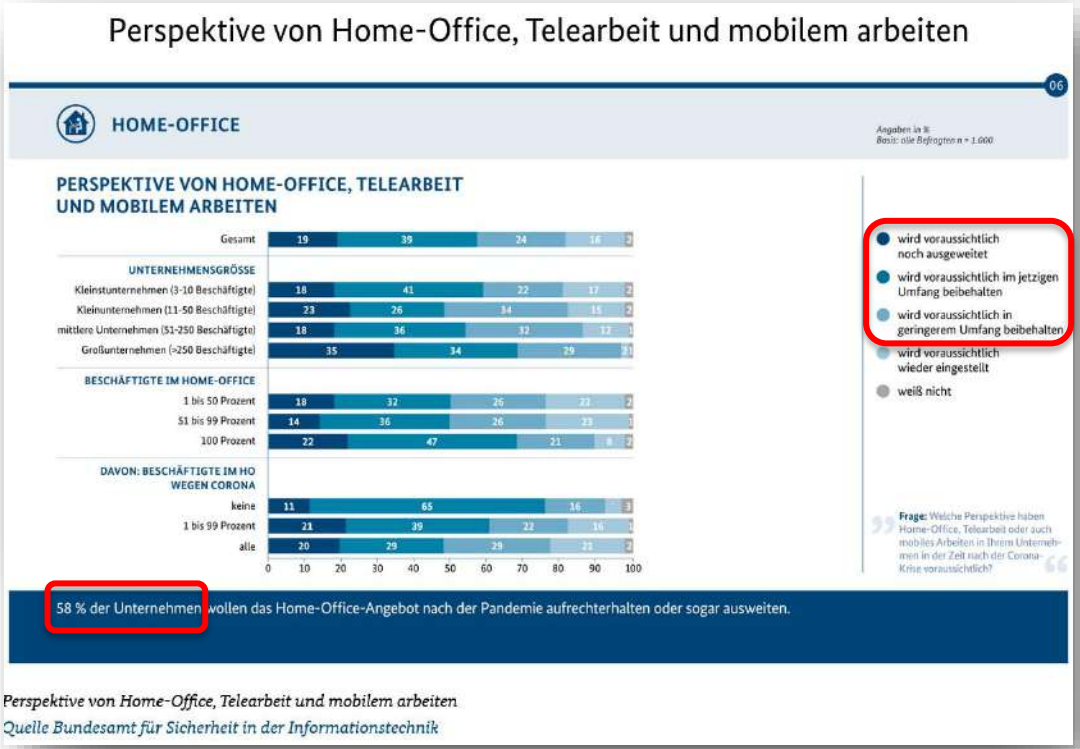
aktuelle Herausforderungen

aktuelle Herausforderungen

Home Office wird bleiben!

Home Office wird bleiben





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

Home Office wird bleiben

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

aktuelle Herausforderungen

Home Office wird bleiben!

Flexibilität: Kernanforderung der Digitalen Transformation

Flexibilität

= 'Digitale Transformation'

Flexibilität

= 'Digitale Transformation'

➔ Corona als wertvolles Beispiel für massive **Veränderungsprozesse** und deren **Konsequenzen**

aktuelle Herausforderungen

Home Office wird bleiben!

Flexibilität: Kernanforderung der Digitalen Transformation

(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

aktuelle Herausforderungen

Home Office wird bleiben!

Flexibilität: Kernanforderung der Digitalen Transformation

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

Home Office erhöht **Cyber-Risiken** drastisch

drastisch steigende Cyber-Risiken

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.

23.06.2021, 14.20 Uhr

Schwachpunkt. Wer zuhause am Notebook arbeitet, ist virtuell oft angreifbar

VDI nachrichten

E-PAPER-LOGIN

TECHNIK KARRIERE WIRTSCHAFT E-PAPER ABO SHOP ELIBRARY

STUDIE ZUR CYBERSICHERHEIT 15. APR 2021 VON REGINE BÖNSCH

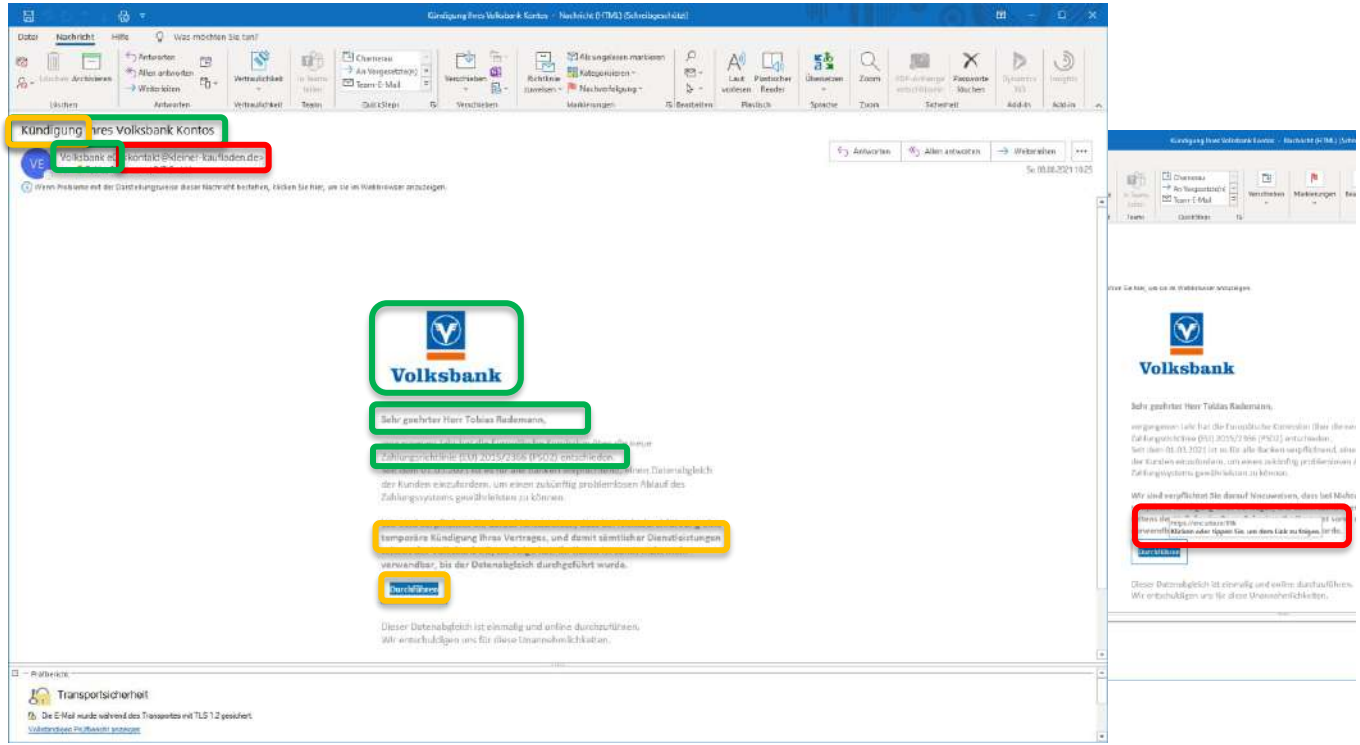
Homeoffice erhöht Gefahr für IT-Sicherheit drastisch

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.

iT-Sicherheitsrisiken durch HO & sinnvolle Sicherheitsmaßnahmen

aktuelle Risiken

- **Phishing Mails**



aktuelle Risiken & Sicherheitsmaßnahmen

- **Phishing Mails**

aktuelle Risiken

- Phishing Mails
- **CEO-Fraud**

aktuelle Risiken & Sicherheitsmaßnahmen

- Phishing Mails
- **CEO-Fraud**

Schutzmaßnahmen

SENSIBILISIERUNG VON MITARBEITER*INNEN

MULTI-FAKTOR-AUTHENTIFIZIERUNG

aktuelle Risiken

- Phishing Mails
- CEO-Fraud
- **Erpressungstrojaner**

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

BSI (2019): "die für die Empfänger (künftig) **kaum noch** als solche zu identifizieren sind"

inkl. 'brute-force' Attacken auf eigene Administrator-Konten

Erstinfektion
- durch SPAM-eMail mit Makro

Outlook Harvesting
- Kontakte
- eMail Inhalte

Verbreitung intern
- Wurm-Modul
- Nachladen von Schad-software (Malware)

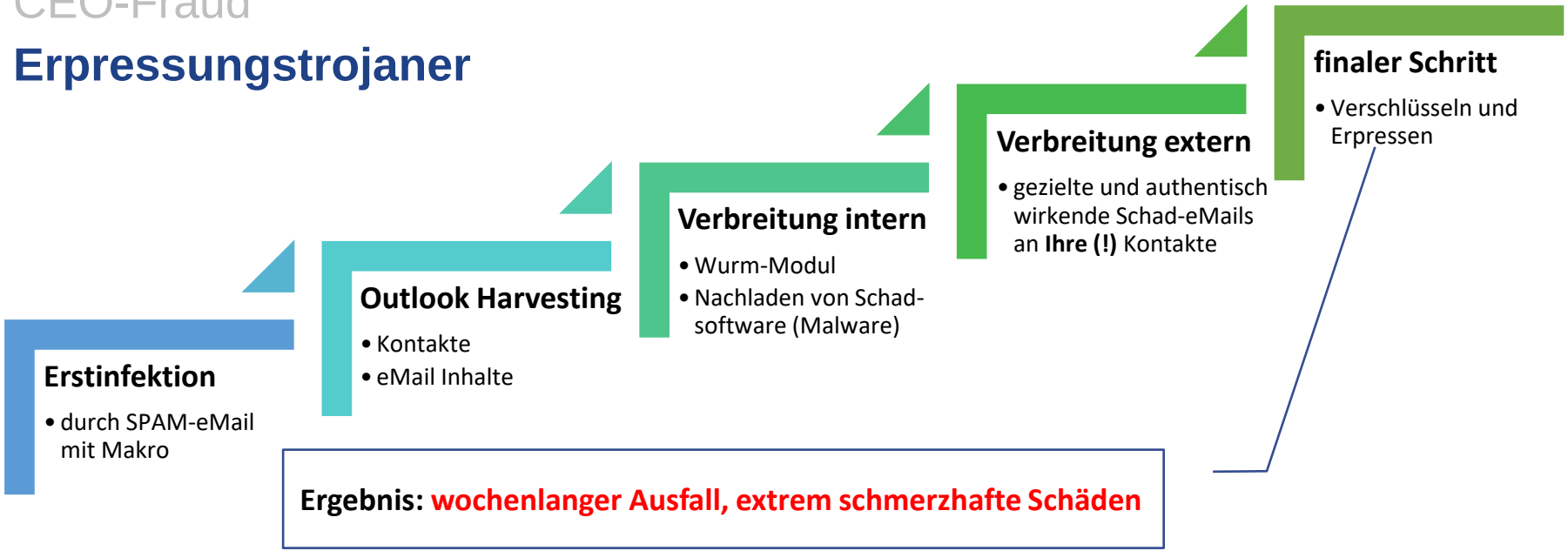
Verbreitung extern
- gezielte und authentisch wirkende Schad-eMails an **Ihre (!)** Kontakte

finaler Schritt
- Verschlüsseln und Erpressen

- Banking Trojaner (bspw. TrickBot)
- Ransomware (bspw. Ryuk)
- Auslesen von Zugangsdaten (v.a. Firefox, Outlook, Thunderbird)
- Fernzugriffe auf das System
- Suchen und Kompromittieren bzw. Löschen von Datensicherungen

aktuelle Risiken

- Phishing Mails
- CEO-Fraud
- **Erpressungstrojaner**



aktuelle Risiken

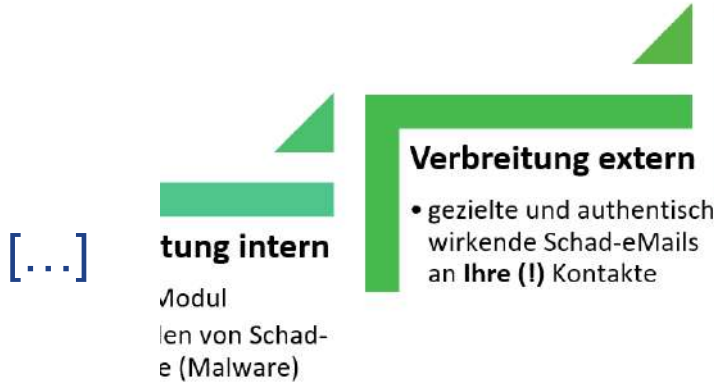
- Phishing Mails
- CEO-Fraud
- **Erpressungstrojaner**

aktuelle Risiken & Sicherheitsmaßnahmen

- Phishing Mails
- CEO-Fraud
- **Erpressungstrojaner**

aktuelle Risiken

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



➔ Sie sind **doppelt** erpressbar:
Wenn Sie nicht zahlen, dann
1. sind Ihre Daten weg
2. Ihre sensiblen Daten werden veröffentlicht
   → Imageverlust
   → Verlust vertr. Informationen
   → DSGVO-Meldung, …

aktuelle Risiken & Sicherheitsmaßnahmen

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

Schutzmaßnahmen

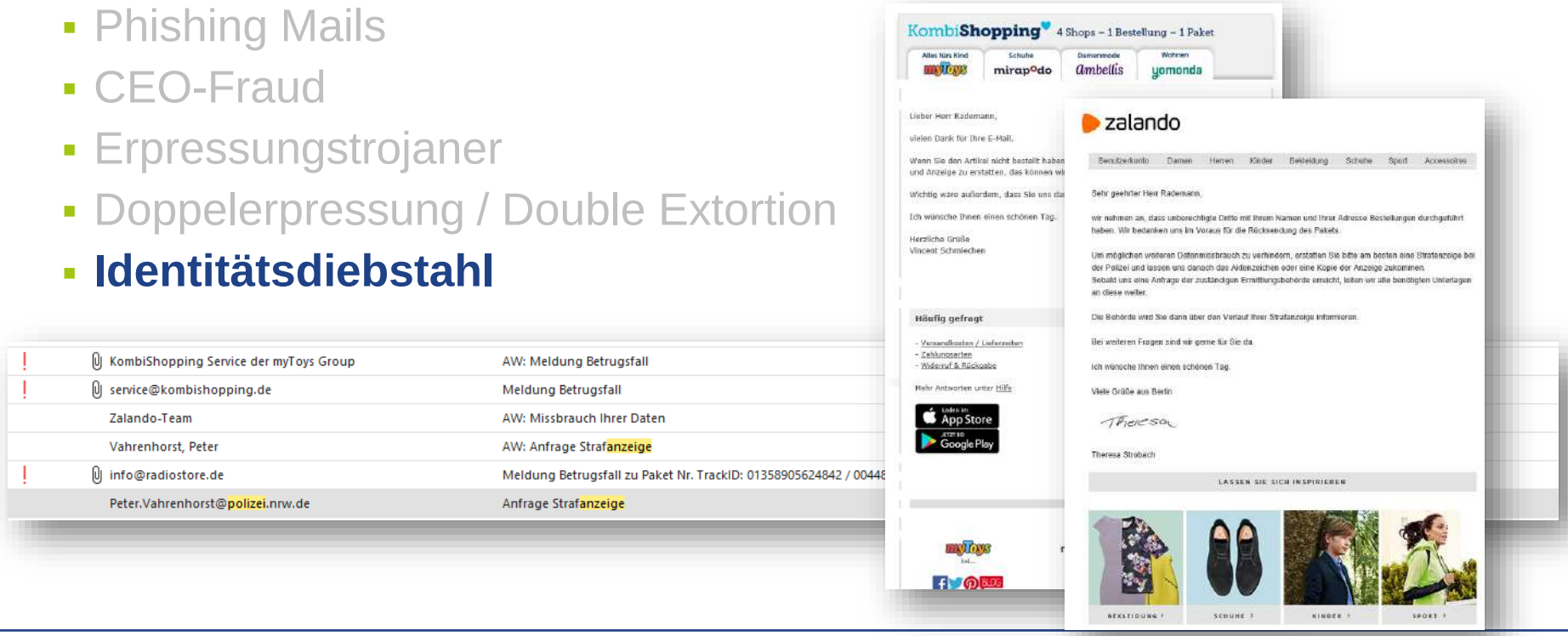
DATEN-
KNAPPHEIT

DRM
(DIGITAL RIGHTS
MANAGEMENT)

+: SIEHE OBEN

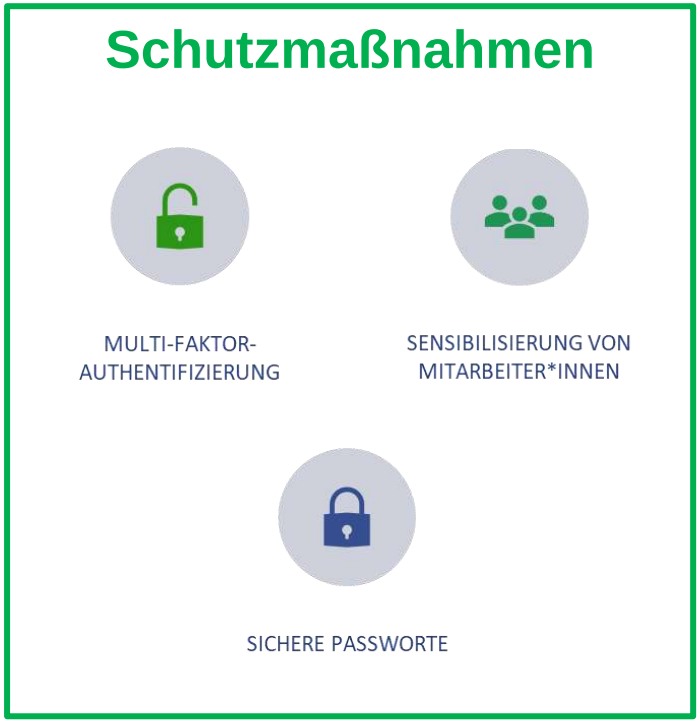
aktuelle Risiken

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



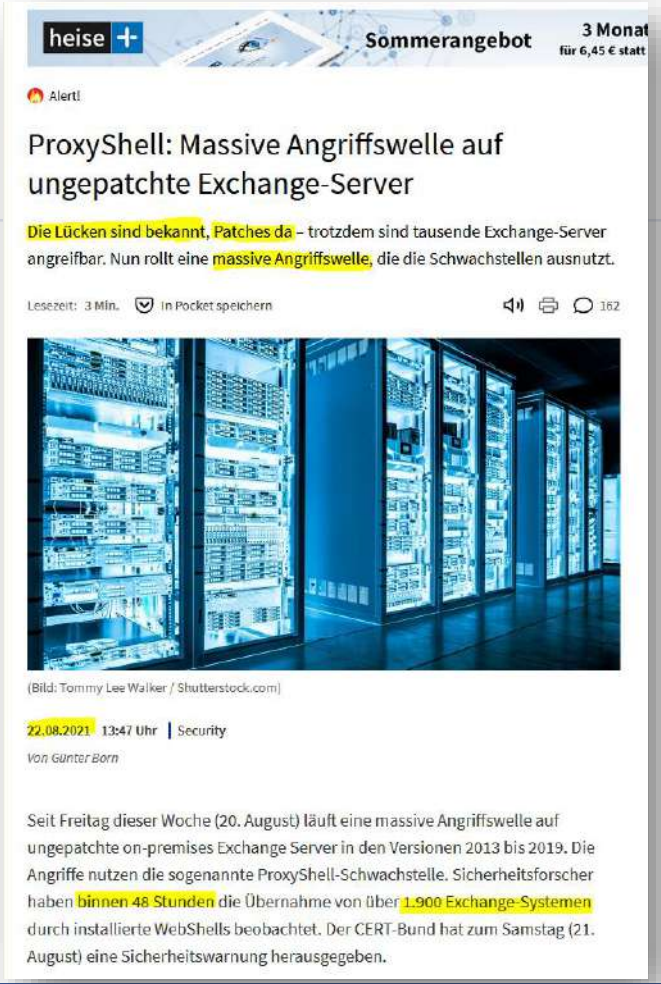
aktuelle Risiken & Sicherheitsmaßnahmen

- 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.

aktuelle Risiken & Sicherheitsmaßnahmen

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

Schutzmaßnahmen

REGELMÄßIGE
UPDATES

sinnvolle Sicherheitsmaßnahmen (Home Office)

OFFLINE (!)
DATENSICHERUNG

SENSIBILISIERUNG VON
MITARBEITER*INNEN

REGELMÄßIGE
UPDATES

MULTI-FAKTOR-
AUTHENTIFIZIERUNG

ANTI-SPAM
GATEWAY

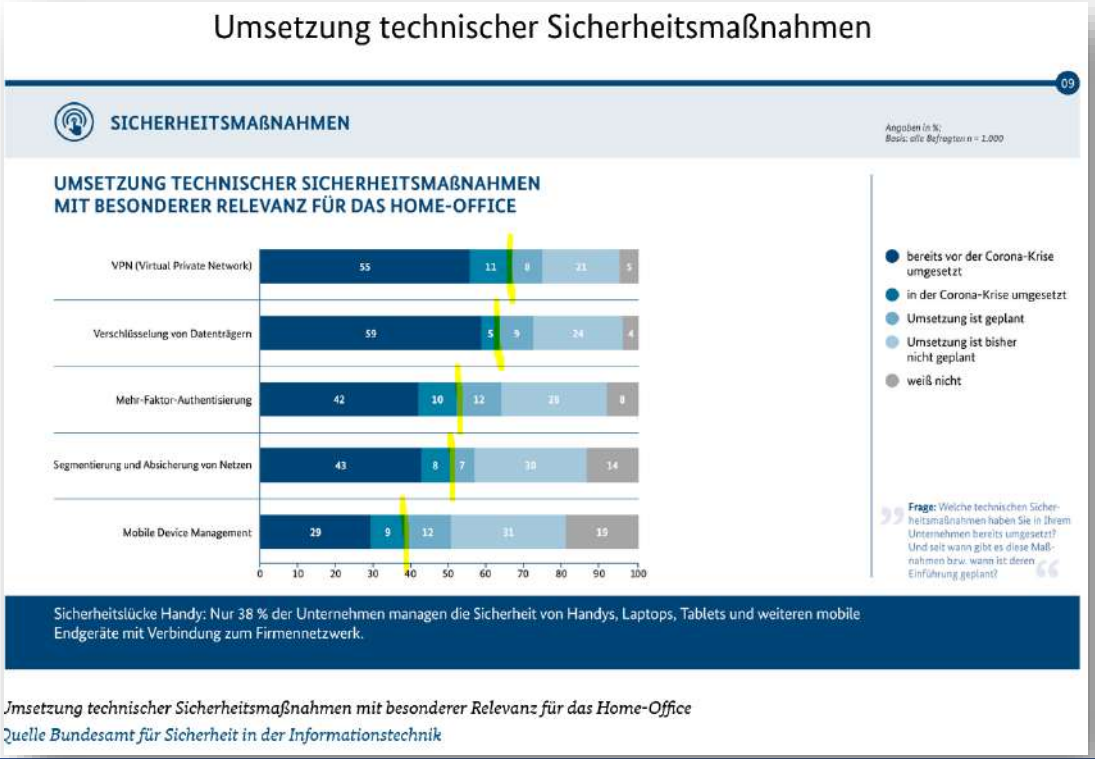
SICHERE PASSWORTE

VPN

MOBILE DEVICE
MANAGEMENT

VERSCHLÜSSELUNG
VON DATENTRÄGERN

sinnvolle Sicherheitsmaßnahmen



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

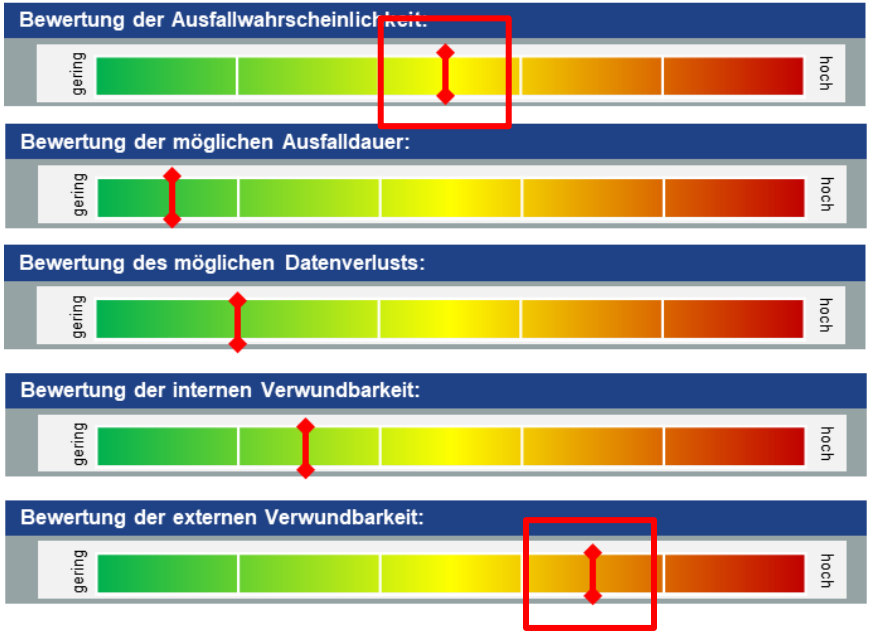
Die Empfehlungen des BSI

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 ▪ MA-Sensibilisierung	→	iT-Wartungsvertrag	
▪ 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



CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

RIT® iT-Risk Assessment: Handlungsempfehl.

iT-Risk Assessment durch die R.iT GmbH (September 2020)
Handlungsempfehlungen

Reihenfolge	empfohlene Maßnahme	Umsetzungsdetails	(Risiko-)Bereich	Priorisierung / Wichtigkeit	Priorisierung: Dringlichkeit
1	W-LAN restrukturieren	- Gäste W-Lan vom Produktivnetz trennen - Internes Netzwerk erstellen - Smartphone Netzwerk	externe Verwundbarkeit	wichtig	dringend
2	Ausfallrisiko der USVen reduzieren	- Batterien der zwei älteren USVen austauschen	Ausfallwahrscheinlichkeit	wichtig	dringend
3	Webseite rechtskonform ausgestalten	-Cookie-Banner aktualisieren	interne Verwundbarkeit	wichtig	dringend
4	Hyper-V Replikation anpassen	- Replikationszyklen von DB- und Exchange-Server verringern - fehlende Server replizieren (wenn erforderlich)	Datenverlust	wichtig	dringend
5	Internes anonymes Versenden von E-Mails unterbinden	- Versand ohne Authentifizierung deaktivieren - Drucker falls notwendig umstellen - [redacted] mit Authentifizierung umstellen - Skripte welche E-Mails versenden anpassen	externe Verwundbarkeit	wichtig	dringend
6	Kennwortrichtlinien und Kennwortänderungen	- Kennwortrichtlinie definieren und umsetzten - Administratorkennwörter verstärken - Einrichtung eines gemeinsam nutzbaren Passwortmanagement-Tools für die Administratoren für die Verwaltung generischer Kennwörter - Standard Kennwörter der IP Telefone ändern	externe Verwundbarkeit	wichtig	dringend
7	[redacted] absichern	- [redacted] Anmeldung auf AD Ebene - Standard Kennwörter ändern (Bspw [redacted] - SQL Authentifizierung abstellen / Benutzer bereinigen	Interne Verwundbarkeit	wichtig	dringend
8	Strategische Grundlagen für Notfallmanagement herstellen	- Erstellung eines Datensicherungskonzepts - Erstellung eines Notfallplan - Einführung von jährlichen Disaster Recoveries	Ausfalldauer	wichtig	nicht dringend
9	Interne Netzwerke abtrenne und absichern	- Server, Clients, Drucker, Telefone, Hausautomatisierung und WLANs in separate Netzwerke auftollen - NAC Lösung implementieren	externe Verwundbarkeit	wichtig	nicht dringend
10	Komplettes Refactoring aller Intranet-Komponenten in einer modernen und sicheren Entwicklungssprache	- ASP Skripte abschaffen und durch moderne Plattformlösung ersetzten, die keine Kennwörter und Benutzernamen enthalten - Quellcode Verwaltung einführen und mit dem IIS verknüpfen	externe Verwundbarkeit	wichtig	nicht dringend
11	Firewall-Regelwerk überarbeiten	- DNS auf die Domain Controller beschränken - Internet des Backupnetztes beschränken - SharePoint für außen unzugänglich machen	interne Verwundbarkeit	nicht wichtig	dringend
12	Geräteverschlüsselung implementieren	- Verschlüsselung aller Notebooks und Computer	Datenverlust	nicht wichtig	dringend
13	Patchmanagement für Hardwarekomponenten etablieren	- Mechanismus für regelmäßig mit Updates des Backends	Ausfallwahrscheinlichkeit	nicht wichtig	dringend

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?

offene Fragen / Diskussion

Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

THE SPIR.IT OF EXCELLENCE

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

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