



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

CyberSecurity: Herausforderung Home Office

Vortrag im Rahmen der Techniktagung des BDSW
Tobias Rademann, M.A.

1. September 2021



HO = drastisch steigende Cyber-Risiken



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



go-digital



aktuelle Herausforderungen

aktuelle Herausforderungen



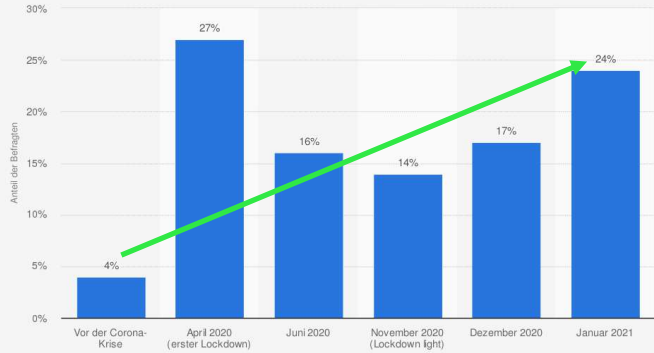
Home Office wird
bleiben!



Home Office wird bleiben



Anteil der im Homeoffice arbeitenden Beschäftigten in Deutschland vor und während der Corona-Pandemie 2020 und 2021



Quelle: Hans-Böckler-Stiftung © Statista 2021
Weitere Informationen: Deutschland, WSI; April 2020, Juni 2020, November 2020, Januar 2021; 6.200 befragte Erwerbstätige/Arbeitssuchende; © Statista 2021

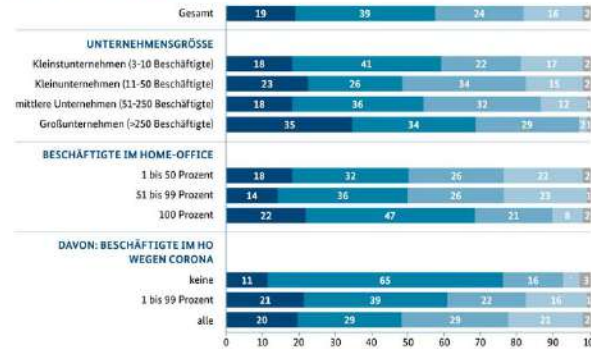
Perspektive von Home-Office, Telearbeit und mobilem arbeiten



HOME-OFFICE

Angaben in %
Basis: alle Befragten n = 1.000

PERSPEKTIVE VON HOME-OFFICE, TELEARBEIT UND MOBILEM ARBEITEN



- wird voraussichtlich noch ausgeweitet
- wird voraussichtlich im jetzigen Umfang beibehalten
- wird voraussichtlich in geringerem Umfang beibehalten
- wird voraussichtlich wieder eingestellt
- weiß nicht

Frage: Welche Perspektive haben Home-Office, Telearbeit oder auch mobiles Arbeiten in Ihrem Unternehmen in der Zeit nach der Corona-Krise voraussichtlich?

58 % der Unternehmen wollen das Home-Office-Angebot nach der Pandemie aufrechterhalten oder sogar ausweiten.

Perspektive von Home-Office, Telearbeit und mobilem arbeiten

Quelle Bundesamt für Sicherheit in der Informationstechnik



Home Office wird bleiben



ANTEIL DER BESCHÄFTIGTEN IM HOMEOFFICE (ANFANG 2021)

24 %

ZUSTIMMUNG ZU GESETZLICHEM ANSPRUCH AUF HOMEOFFICE

73 %

ANTEIL DER STELLENANZEIGEN MIT HOMEOFFICE-ANGEBOT

1,5 %

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

Jeder Zweite möchte weiterhin im Homeoffice arbeiten

Befragte, die sich vorstellen können, auch nach der Pandemie im HO zu bleiben

■ Ja, genauso viel ■ Nein, weniger ■ Nein, gar nicht mehr



Basis: 1.782 Befragte in Deutschland, die während der Pandemie von zu Hause gearbeitet haben; Apr. 2020 bis Febr. 2021

Quelle: WSI



statista

aktuelle Herausforderungen



Home Office wird
bleiben!



Flexibilität:
Kernanforderung
der Digitalen
Transformation



Flexibilität



Leistungsfähigkeit
moderner **iT**
entwickelt sich
exponentiell

diese exponentielle
Leistungssteigerung
in der iT schafft ganz
neue Werkzeuge

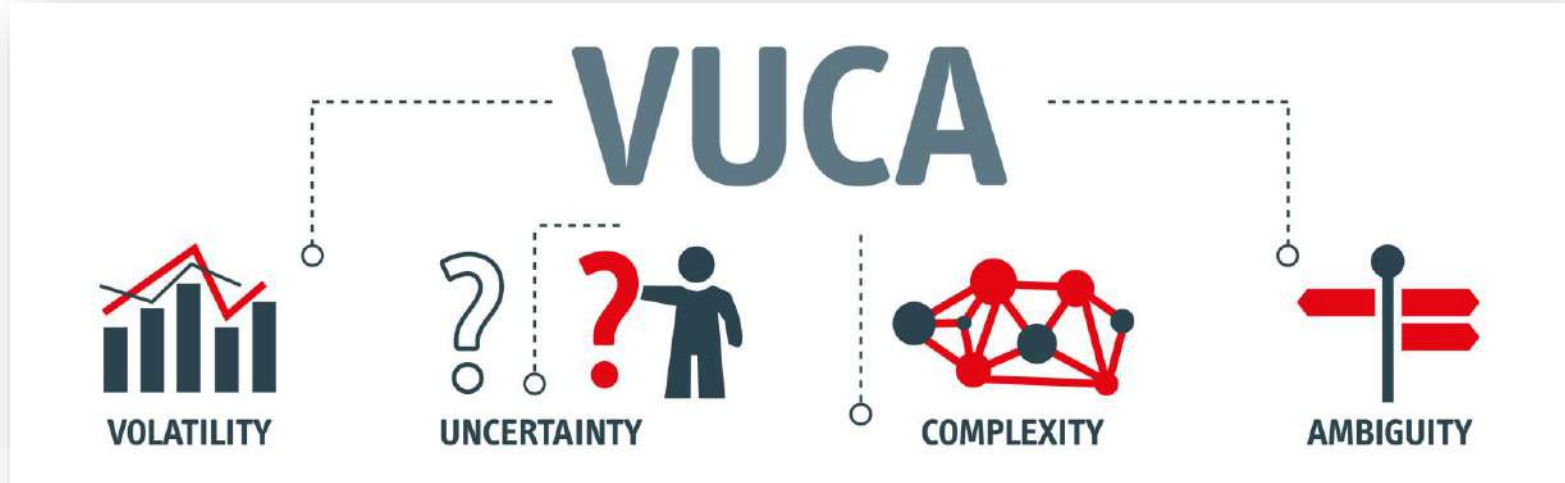
diese Werkzeuge
schaffen ganz **neue**
Möglichkeiten für
Prozess- und
Produktinnovationen

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

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

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

= 'Digitale Transformation'



= '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



iT-Sicherheitsrisiken durch HO & sinnvolle Sicherheitsmaßnahmen

aktuelle Risiken



■ Phishing Mails

The screenshot shows a phishing email from 'Volksbank' with the subject 'Kündigung Ihres Volksbank Kontos'. The email body contains the following text:

Kündigung Ihres Volksbank Kontos

Volkbank ist Ihr Kontakt-Partner für alle Bankdienstleistungen. Wir sind verpflichtet Sie darauf hinzuweisen, dass Sie Ihre Bankdienstleistungen nur über die Volksbank App oder das Internetbanking nutzen können.

Sehr geehrter Herr Tobias Rademacher,

Zahlungsschritte für 2022/23 sind erforderlich.

Um den reibungslosen Ablauf der Datenübergabe zu gewährleisten, ist es erforderlich, dass Sie die Datenübergabe bestätigen. Dies ist notwendig, um einen zukünftig problemlosen Ablauf des Zahlungssystems gewährleisten zu können.

temporäre Kündigung Ihres Vertrages, und damit sämtlicher Dienstleistungen

verbindlich, bis der Datenaustausch durchgeführt wurde.

Durchführung

Dieser Datenaustausch ist einmalig und online durchzuführen. Wir entschuldigen uns für diese Unannehmlichkeiten.

The annotations highlight the following elements:

- Subject line:** 'Kündigung Ihres Volksbank Kontos' (Red box)
- Sender:** 'Volkbank ist Ihr Kontakt-Partner für alle Bankdienstleistungen' (Red box)
- Logo:** Volksbank logo (Green box)
- Text:** 'Sehr geehrter Herr Tobias Rademacher,' (Green box)
- Text:** 'Zahlungsschritte für 2022/23 sind erforderlich.' (Green box)
- Text:** 'temporäre Kündigung Ihres Vertrages, und damit sämtlicher Dienstleistungen' (Yellow box)
- Text:** 'verbindlich, bis der Datenaustausch durchgeführt wurde.' (Yellow box)
- Text:** 'Durchführung' (Yellow box)
- Text:** 'Wir sind verpflichtet Sie darauf hinzuweisen, dass Sie Ihre Bankdienstleistungen nur über die Volksbank App oder das Internetbanking nutzen können.' (Red box)
- Text:** 'Dieser Datenaustausch ist einmalig und online durchzuführen. Wir entschuldigen uns für diese Unannehmlichkeiten.' (Red box)

aktuelle Risiken & Sicherheitsmaßnahmen

- **Phishing Mails**

Schutzmaßnahmen



SENSIBILISIERUNG VON
MITARBEITER*INNEN



ANTI-SPAM
GATEWAY



REGELMÄßIGE
UPDATES



MULTI-FAKTOR-
AUTHENTIFIZIERUNG

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 Schadsoftware (Malware)

Verbreitung extern

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

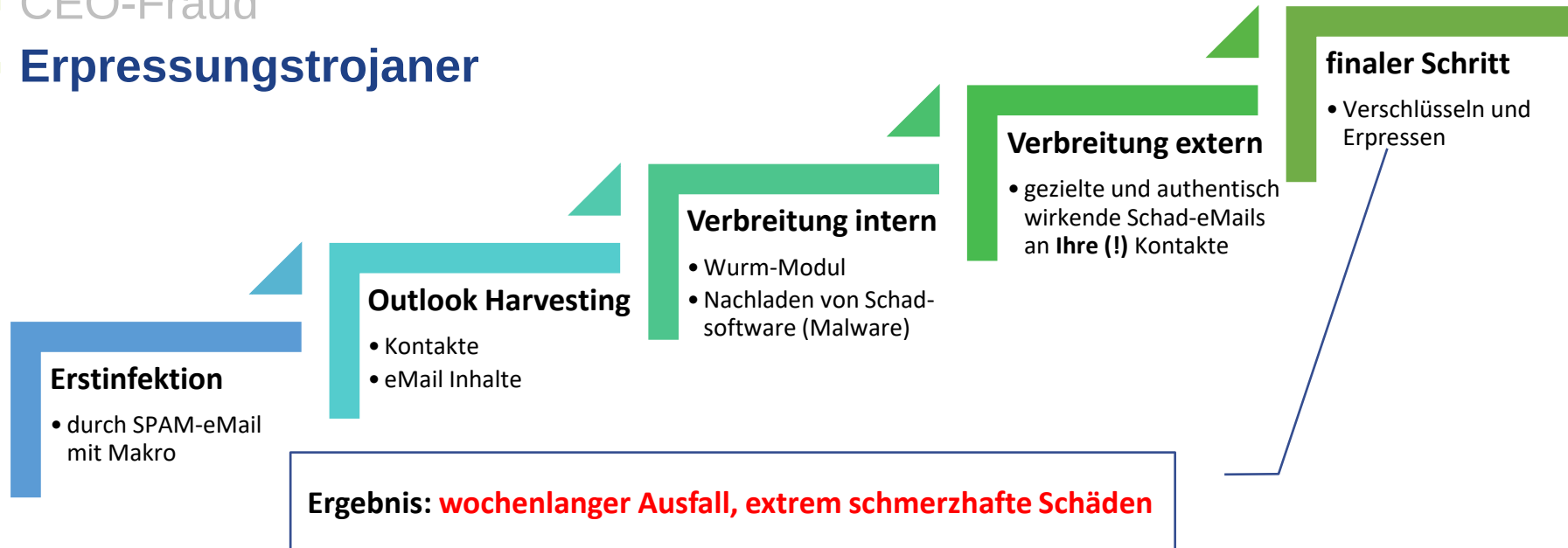
finaler Schritt

- 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

Your network has been infected



Your documents, photos, databases and other important files - encrypted



To decrypt your files you need to buy our special software - General-Decryptor



Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have **13 days, 23:59:47**

* If you do not pay on time, the price will be doubled

* Time ends on Dec 31, 17:46:10

Current price **757.4316 XMR**
≈ 120.000 USD

After time ends **1514.8632 XMR**
≈ 240.000 USD

* XMR will be recalculated in 5 hours with an actual rate

Monero address: 84TWmtvd4Hgz9nukG5eeDfAtDad57piKBadcFF2tQj8weP5k52mySSOLNcYawAgaDJcdSM8jAofKo4fSkUR7t8Gf2X

INSTRUCTIONS

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

To decrypt your files you need to buy our special software - General-Decryptor.

* If you need guarantees, use trial decryption below

How to buy General-Decryptor?

1. Buy the required amount of XMR (Monero) **757.4316 XMR**

If you have problems with buying XMR, you can buy BTC (Bitcoin) and exchange it for XMR. See «Exchange BTC for XMR» on the page.

2. Send **757.4316 XMR** to the following Monero address

84TWmtvd4Hgz9nukG5eeDfAtDad57piKBadcFF2tQj8weP5k52mySSOLNcYawAgaDJcdSM8jAofKo4fSkUR7t8Gf2X

* This receiving address was created for you, to identify your transactions

3. Wait for **10** confirmations by blockchain
4. Reload current page after, and get a link to download General-Decryptor

CHAT SUPPORT

ABOUT US

Buy XMR with Bank

- ◊ Kraken
- ◊ AnyCoin (EUR)
- ◊ BestChange

Buy XMR locally with cash or online

- ◊ LocalMonero.co
- * Guide to buying using LocalMonero
- ◊ MoneroForCash
- ◊ Liberalcoins
- ◊ BestChange

Buy Bitcoin and trade for XMR

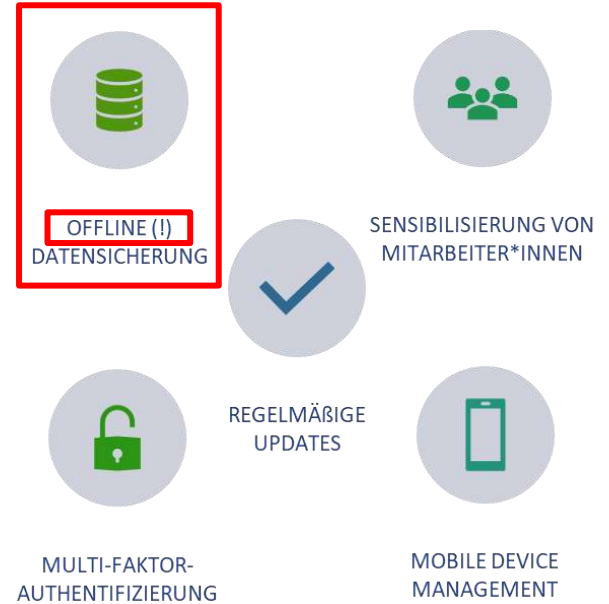
- ◊ Binance
- * Guide to buying XMR using Binance
- ◊ Kraken
- ◊ Bitfinex



aktuelle Risiken & Sicherheitsmaßnahmen

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

Schutzmaßnahmen



aktuelle Risiken

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

[...]

ung intern

Modul
len von Schad-
e (Malware)

Verbreitung extern

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

- 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



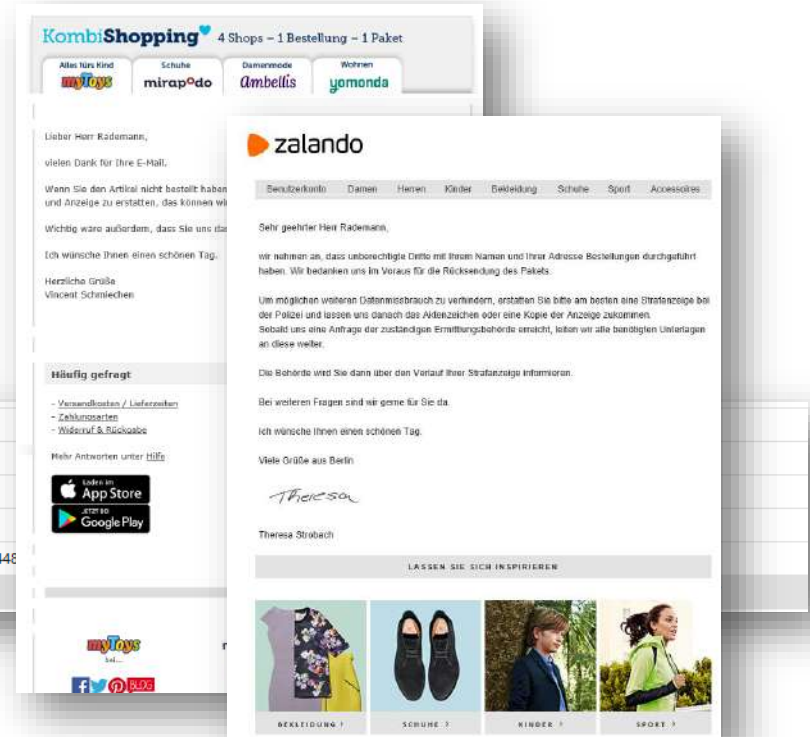
DRM
(DIGITAL RIGHTS
MANAGEMENT)

+: SIEHE OBEN

aktuelle Risiken

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

!	KombiShopping Service der myToys Group	AW: Meldung Betrugsfall
!	service@kombishopping.de	Meldung Betrugsfall
	Zalando-Team	AW: Missbrauch Ihrer Daten
	Vahrenhorst, Peter	AW: Anfrage Strafanzeige
!	info@radiostore.de	Meldung Betrugsfall zu Paket Nr. TrackID: 01358905624842 / 00448
	Peter.Vahrenhorst@polizei.nrw.de	Anfrage Strafanzeige



aktuelle Risiken & Sicherheitsmaßnahmen

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

Schutzmaßnahmen



MULTI-FAKTOR-
AUTHENTIFIZIERUNG



SENSIBILISIERUNG VON
MITARBEITER*INNEN



SICHERE PASSWORTE

aktuelle Risiken

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

heise + Sommerangebot 3 Monate 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



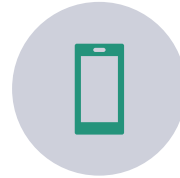
ANTI-SPAM
GATEWAY



SICHERE PASSWORTE



VPN



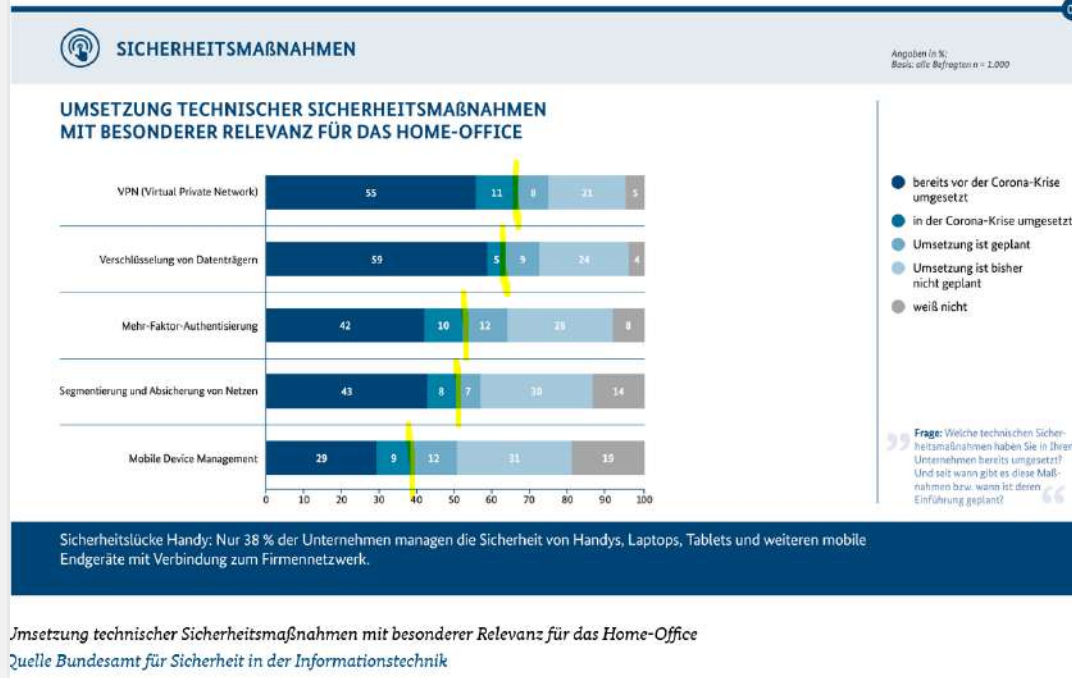
MOBILE DEVICE
MANAGEMENT



VERSCHLÜSSELUNG
VON DATENTRÄGERN

sinnvolle Sicherheitsmaßnahmen

Umsetzung technischer Sicherheitsmaßnahmen



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



IT-SICHERHEIT IM HOME-OFFICE

Wir empfehlen 5 einfache Maßnahmen:

- ✓ Virtual Private Network (VPN) einrichten
- ✓ Mehr-Faktor-Authentisierung (MFA) nutzen
- ✓ Mobile-Device-Management (MDM) einsetzen
- ✓ Regelmäßige Updates machen
- ✓ Qualifizierte Dienstleister fragen

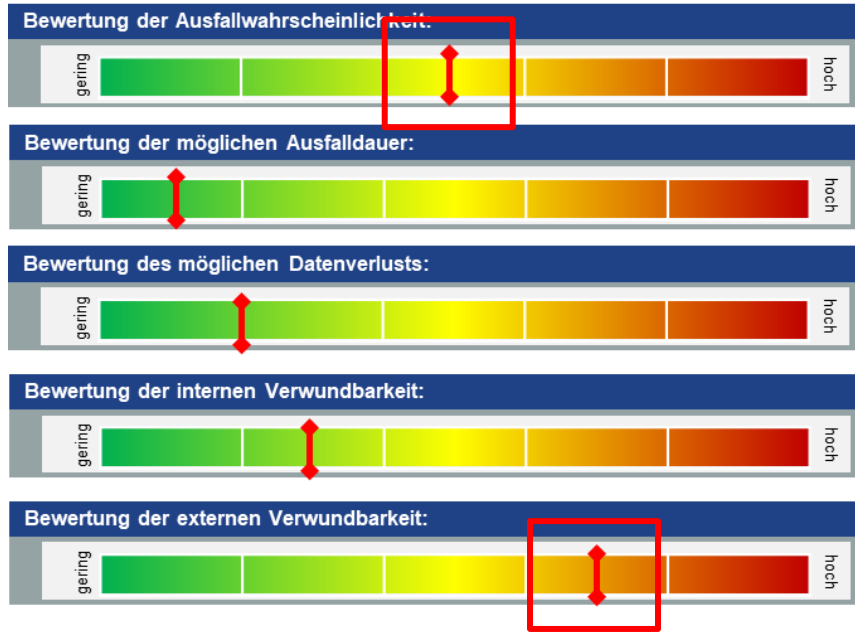
 Bundesamt für Sicherheit in der Informationstechnik

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



CYBERSECURITYTM
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

RiT® iT-Risk Assessment: Handlungsempfehl.

IT-Risk Assessment durch die RiT GmbH (September 2020)					
Handlungsempfehlungen					
Reihenfolge	empfohlene Maßnahme	Umsetzungsdetails	(Risiko-)Bereich	Priorisierung / Wichtigkeit	Priorisierung: Dringlichkeit
1	V-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 umsetzen - Administratorenkennwörter 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 abtrennen und absichern	- Server, Clients, Drucker, Telefone, Hausautomatisierung und WLANs in separate Netzwerke aufteilen - 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 ersetzen, 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 Backupnetzes 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



CYBERSECURITYTM
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>