



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



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:



CYBERSECURITYTM
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, Euro-zone 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%	6 (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 ranked higher than market developments based on the actual number of responses

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





aktuelle Herausforderungen

aktuelle Herausforderungen



Home Office wird
bleiben!



Home Office wird bleiben



ANTEIL DER BESCHÄFTIGTEN IM HOME-OFFICE (ANFANG 2021)

24 %

ZUSTIMMUNG ZU GESETZLICHEM ANSPRUCH AUF HOME-OFFICE

73 %

ANTEIL DER STELLENANZEIGEN MIT HOME-OFFICE-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

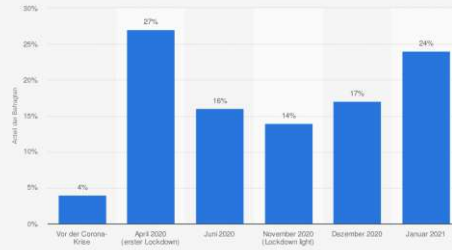


Basis: 1.782 Befragte in Deutschland, die während der Pandemie von zu Hause gearbeitet haben. Apr. 2020 bis Febr. 2021
Quelle: WSI



statista

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



Quelle:
Hartmut Bittner Stiftung
© Statista 2021

Weitere Informationen:
Deutschland; WSI; April 2020, Juni 2020, November 2020, Januar 2021; 8.200 befragte Erwerbstätige; Arbeitsmarktforschung; GfK

Perspektive von Home-Office, Telearbeit und mobilem arbeiten

HOME-OFFICE

Angaben in %
Basis: 1.500 Befragte v. 1.2020

PERSPEKTIVE VON HOME-OFFICE, TELEARBEIT UND MOBILEM ARBEITEN



- wird voraussichtlich noch ausgebaut
- wird voraussichtlich im jetzigen Umfang beibehalten
- wird voraussichtlich in geringerer Leistung beibehalten
- wird voraussichtlich wieder eingestellt
- weiß nicht

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

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

aktuelle Herausforderungen



Home Office wird
bleiben!



Home Office
erhöht **Cyber-
Risiken** drastisch



drastisch steigende Cyber-Risiken



vdI nachrichten

TECHNIK KARRIERE WIRTSCHAFT E-PAPER ABO SHOP ELIBRARY

STUDIE ZUR CYBERSICHERHEIT 15. APRIL 2021 VON REGINE BÖRSCH

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 Milliarden Schäden

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



Schwerpunkt: Wer zuhause am Notebook arbeitet, ist virtuell oft angreifbar Foto: Gerald Hainke/istockphoto.com / 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





= 'Digitale Transformation'

aktuelle Herausforderungen



Home Office wird
bleiben!



Home Office
erhöht **Cyber-
Risiken** drastisch



(Folgen von)
Corona:
mehr mit weniger

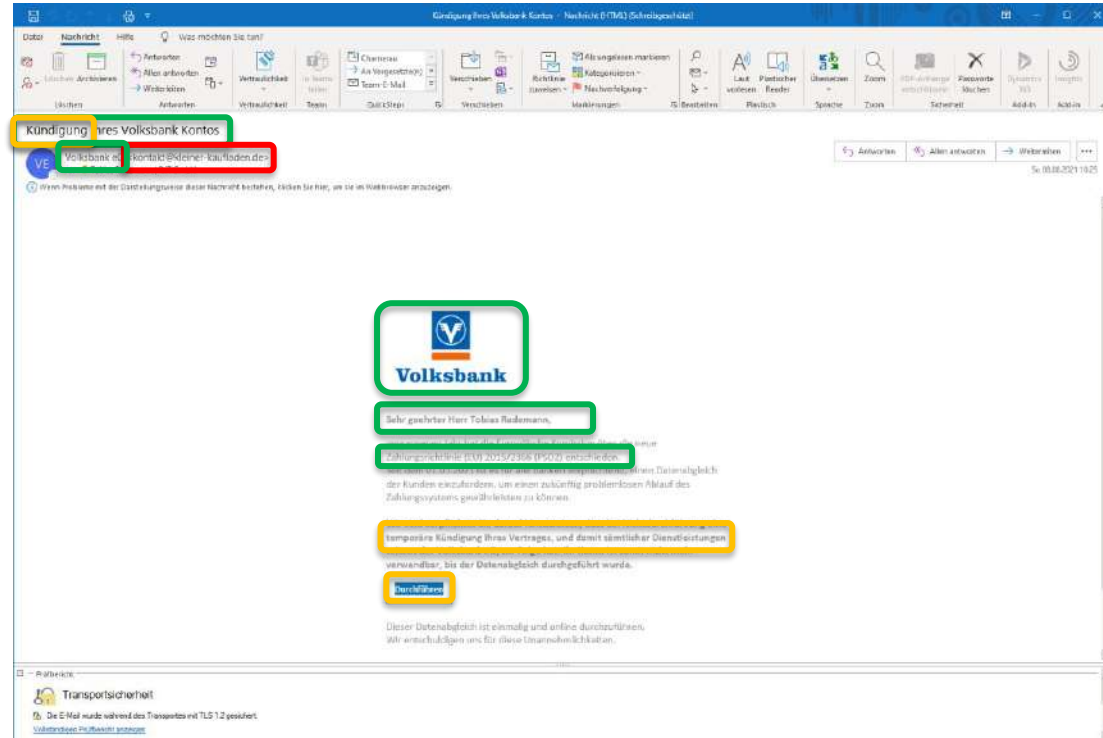


Flexibilität:
Kernanforderung
der Digitalen
Transformation

iT-Sicherheitsrisiken durch HO & sinnvolle Schutzmaßnahmen

aktuelle Risiken

■ Phishing Mails



aktuelle Risiken & Schutzmaßnahmen

- **Phishing Mails**

Schutzmaßnahmen



SENSIBILISIERUNG VON
MITARBEITER*INNEN



ANTI-SPAM
GATEWAY



REGELMÄßIGE
UPDATES



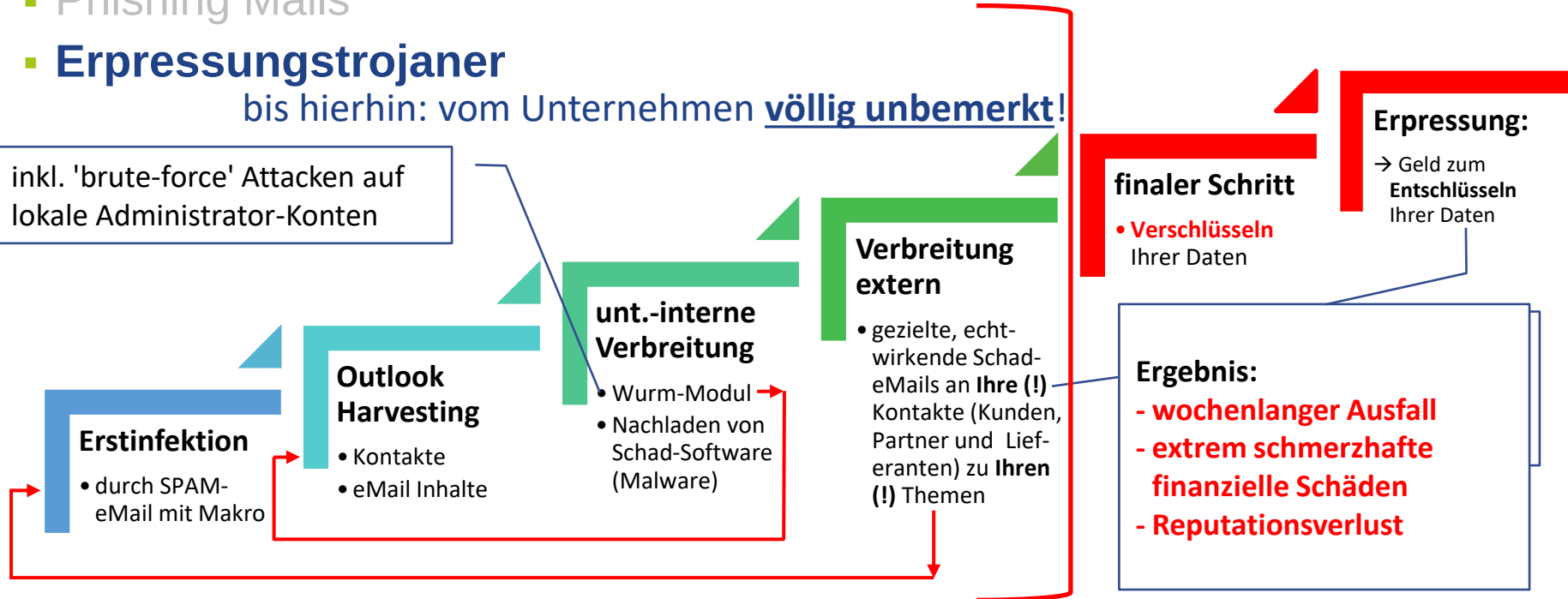
MULTI-FAKTOR-
AUTHENTIFIZIERUNG

aktuelle Risiken

- Phishing Mails
- **Erpressungstrojaner**

bis hierhin: vom Unternehmen völlig unbemerkt!

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



aktuelle Risiken

- Phishing Mails
- 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: 84TWtMwd4HqZa9nukG5zeDfAlQad57piKBadcPF2tGj8xePSk52mySSLNcYasAgaD.Jod5MBjIAoK4Ko4SkUR7TBGf2X

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

INSTRUCTIONS | **CHAT SUPPORT** | **ABOUT US**

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
`84TWtMwd4HqZa9nukG5zeDfAlQad57piKBadcPF2tGj8xePSk52mySSLNcYasAgaD.Jod5MBjIAoK4Ko4SkUR7TBGf2X`
3. Wait for **10** confirmations by blockchain
4. Reload current page after, and get a link to download General-Decryptor

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

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 & Schutzmaßnahmen

- Phishing Mails
- **Erpressungstrojaner**

Schutzmaßnahmen



OFFLINE (!)
DATENSICHERUNG



REGELMÄßIGE
UPDATES



SENSIBILISIERUNG VON
MITARBEITER*INNEN



MULTI-FAKTOR-
AUTHENTIFIZIERUNG



SICHERE PASSWORTE



MOBILE DEVICE
MANAGEMENT

aktuelle Risiken

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

bis hierhin: vom Unternehmen
völlig unbemerkt!

Erstinfektion

- durch SPAM-eMail mit Makro

Outlook Harvesting

- Kontakte
- eMail Inhalte

unt.-interne Verbreitung

- Wurm-Modul
- Nachladen von Schad-Software (Malware)

Verbreitung extern

- gezielte, echt-wirkende Schad-eMails an **Ihre (!)** Kontakte (Kunden, Partnern und Lieferanten) zu **Ihren (!)** Themen

neu: finaler Schritt 1a

- **Kopieren** Ihrer Daten

finaler Schritt 1b

- **Verschlüsseln** Ihrer Daten

Erpressung:

- Geld zum **Entschlüsseln** Ihrer Daten
- Geld zum **nicht-Veröffentlichen** Ihrer Daten

Ergebnis:

- **S.O.**
- **Veröffentlichung sensibler Informationen**
- **Strafen**

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

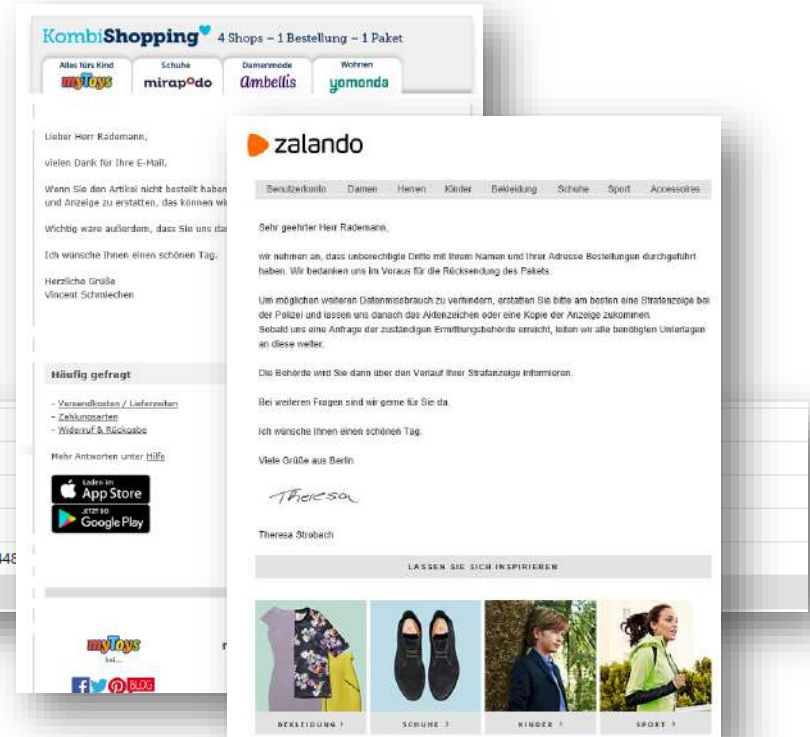


MULTI-FAKTOR-
AUTHENTIFIZIERUNG

aktuelle Risiken

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

!	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 & Schutzmaßnahmen

- 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.

Merry Christmas 2021?!



BSI geht von Erpressungstrojaner-Angriffen zu Weihnachten aus

Das BSI und BKA warnen davor, dass Cyberkriminelle die ausgedünnte Personaldecke zu Weihnachten zum Einschleusen von Schadsoftware ausnutzen könnten.

Lesezeit: 2 Min. In Pocket speichern



(Bild: Michael Trause/Shutterstock.com)

02.12.2021 12:37 Uhr

Von Dirk Knop

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) warnen laut dpa für die Weihnachtsfeiertage vor einem erhöhten Cyberangriffsrisiko, insbesondere für Unternehmen und Organisationen. Gefahrenursache sei zum einen eine Welle von Spam-Nachrichten, die mit der gefährlichen Schadsoftware Emotet infiziert sind. BSI und BKA beobachteten, dass die Erpressungssoftware-Cybergangs aktuell um Mitstreiter werben.



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



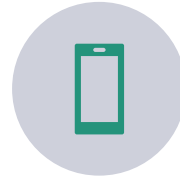
ANTI-SPAM
GATEWAY



SICHERE PASSWORTE



VPN



MOBILE DEVICE
MANAGEMENT



VERSCHLÜSSELUNG
VON DATENTRÄGERN

sinnvolle Schutzmaßnahmen

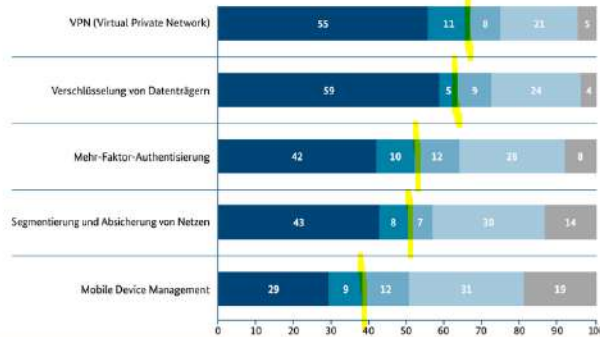
Umsetzung technischer Sicherheitsmaßnahmen



SICHERHEITSMABNAHMEN

Angaben in %;
Basis: alle Befragten n = 2.000

UMSETZUNG TECHNISCHER SICHERHEITSMABNAHMEN MIT BESONDERER RELEVANZ FÜR DAS HOME-OFFICE



- bereits vor der Corona-Krise umgesetzt
- in der Corona-Krise umgesetzt
- Umsetzung ist geplant
- Umsetzung ist bisher nicht geplant
- weiß nicht

Frage: Welche technischen Sicherheitsmaßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt? Und seit wann gibt es diese Maßnahmen bzw. wann ist deren Einführung geplant?

Sicherheitslücke Handy: Nur 38 % der Unternehmen managen die Sicherheit von Handys, Laptops, Tablets und weiteren mobile Endgeräte mit Verbindung zum Firmennetzwerk.

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



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



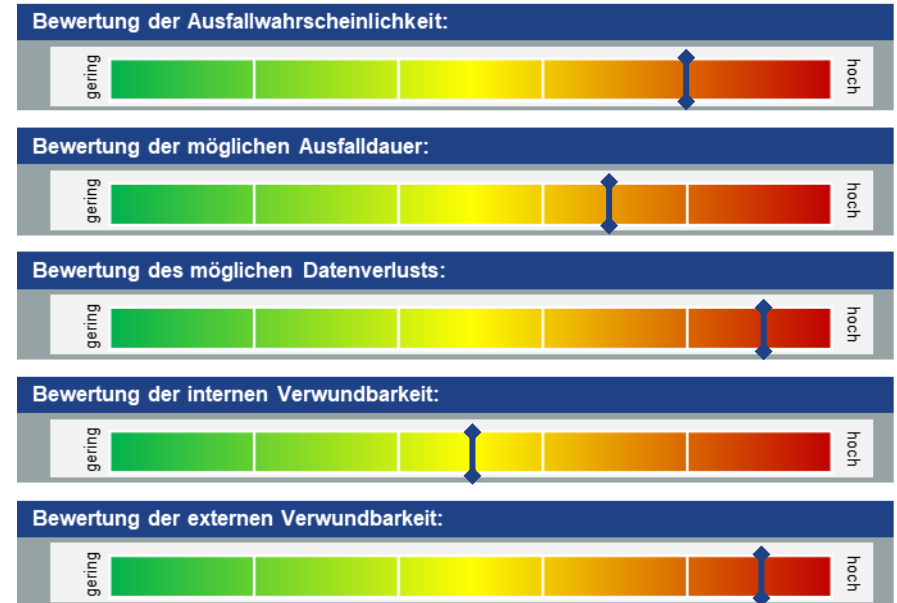
Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

konkrete Empfehlungen

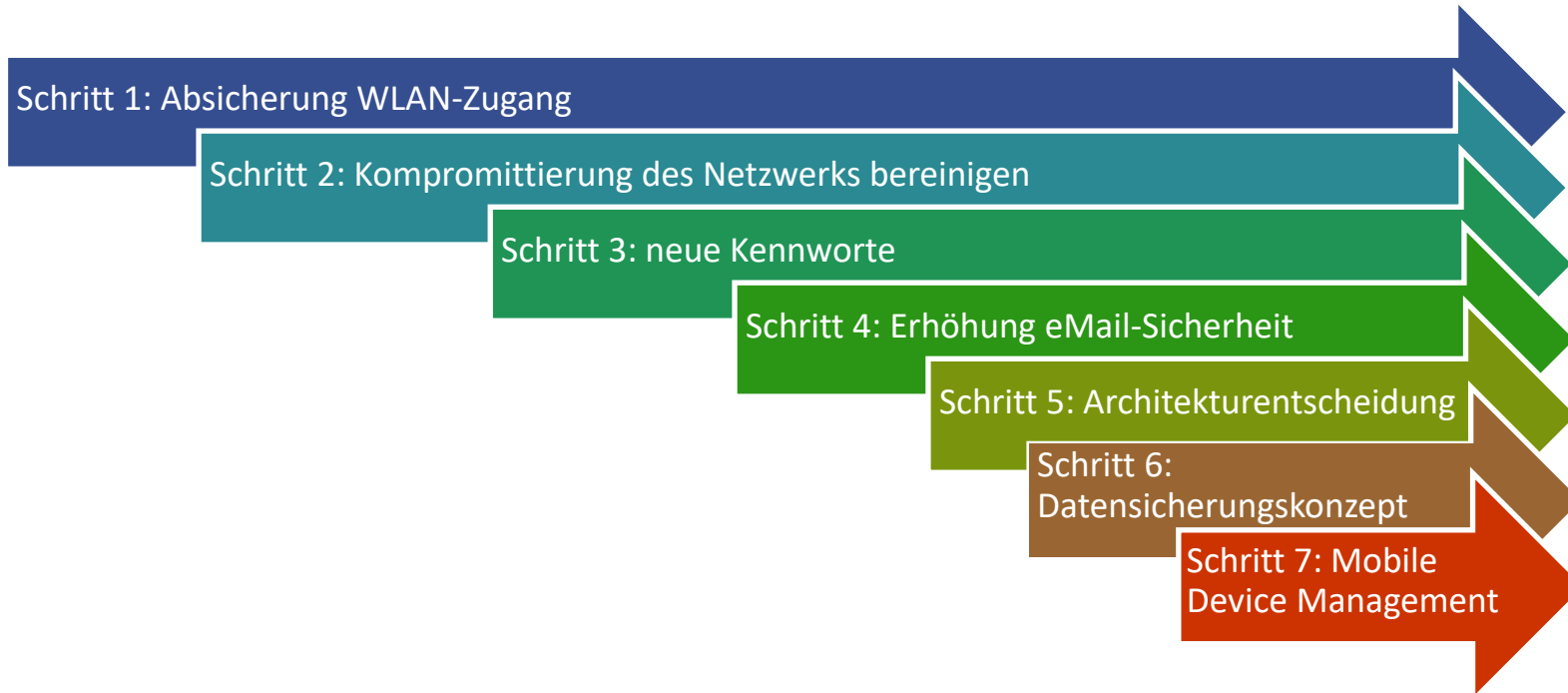
 Datensicherung	→	Veeam	https://www.veeam.com/de
 regelm. Updates	→	iT-Wartungsvertrag	
 MA-Sensibilisierung			
 sichere Passworte	→	1Password	https://1password.com/de/
	→	Überprüfung:	https://haveibeenpwned.com/
 Anti-SPAM Gateway	→	NoSpamProxy	https://www.nospamproxy.de/de/
 Firewalls	→	Sophos XG	https://www.sophos.com/de-de.aspx
 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

Ablauf:

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



priorisierte Handlungsempfehlungen (Beispiel)



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