Herzlich Willkommen

Einführung Internet-Sicherheit

Freund, Feind, Mittelstand:
Augen auf vor Datenklau + Industrie-Spionage

19.01.2022,18:30 Uhr

VDI Bezirksverein Schwarzwald e.V.

Clemens Schweigler, Heinz Ziegler & Benno Vock

Dieter Carbon

Comidio GmbH & Leiter AK „Internet-Sicherheit“

dieter.carbon@trutzbox.de

Privacy made in Germany

Gestatten …

trutzbox
back to privacy

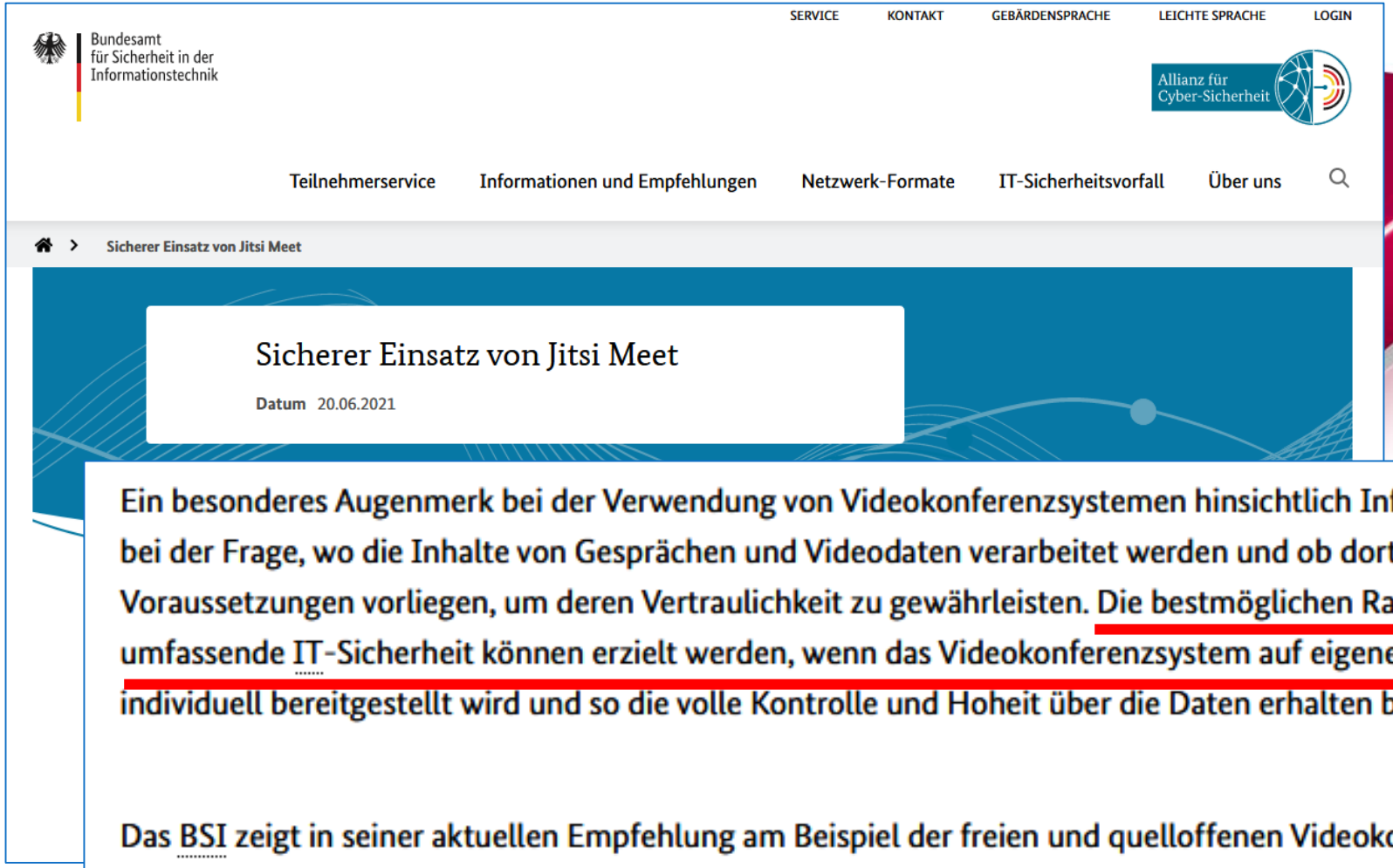
Dipl.-Ing. **Dieter Carbon**
Comidio GmbH: CSO & Partner Management

Dipl.-Ing. **Dieter Carbon**
Leiter Arbeitskreis Internet-Sicherheit

dieter.carbon@trutzbox.de

Privacy made in Germany

Der Werbeblock …



30 mm

Ein besonderes Augenmerk bei der Verwendung von Videokonferenzsystemen hinsichtlich Informationssicherheit liegt bei der Frage, wo die Inhalte von Gesprächen und Videodaten verarbeitet werden und ob dort die erforderlichen Voraussetzungen vorliegen, um deren Vertraulichkeit zu gewährleisten. Die bestmöglichen Rahmenbedingungen für umfassende IT-Sicherheit können erzielt werden, wenn das Videokonferenzsystem auf eigenen Systemen betrieben oder individuell bereitgestellt wird und so die volle Kontrolle und Hoheit über die Daten erhalten bleibt.

Das BSI zeigt in seiner aktuellen Empfehlung am Beispiel der freien und quelloffenen Videokonferenzsoftware Jitsi Meet auf, wie ein selbstverwaltetes Videokonferenzsystem konfiguriert sowie betrieben werden kann und welche Aspekte der IT-Sicherheit beachtet werden sollten. Das Papier richtet sich an IT-Verantwortliche im Unternehmen.

Der Werbeblock …

Rheingau-Bezirksverein e.V.
AKIS Arbeitskreis Internet-Sicherheit

Veranstaltungen 2021

18:00 - 18:55 SmallTalk
19:00 - 21:00 Vortrag & Dis

Die Veranstaltungen finden ONLINE über den Jitsi-Server des Rheingau-BV statt.
Der Einwahl-Link lautet: https://conference.vdi-rheingau.de/akis

Mi 03.02.2021	AKIS-39	**(Be-)Treffen uns Autonome Waffen-Systeme?**
	Dr. Reinhard Grünwald, Büro für Technikfolgen-Abschätzung be Deutschen Bundestag, Berlin	
Mi 03.03.2021	AKIS-40	**Die Verengung der journalistischen Welt - Warum unabhängiger Journalismus so stark gefährdet ist.**
	Peter Welchering, Medienbüro Welchering (für u.a. Deutschlandradio, ZDF, verschiedene ARD-Sender, FAZ), Stuttg	
Mi 05.05.2021	AKIS-41	**Smartphone-"Alternativen"? - Android LineageOS für besseren Datenschutz**
	Prof. Dr-Ing. Rainer Keller, Fakultät Informationstechnik, Studiengangleitung - Angewandte Informatik, Hochschule Essli	
Mi 02.06.2021	AKIS-42	**"S"in IoT steht für Sicherheit? ... ein Demo-Hack**
	Frank Ewert, Sicherheitsberater, Vorstand SICHERES NETZ HILFT Freiburg	
Mi 07.07.2021	AKIS-43	**IT-Sicherheit von Maschinellem Lernen?**
	Dr. Sven Herpig, Stiftung Neue Verantwortung e. V., Berlin	
Mi 01.09.2021	AKIS-44	**Privatsphäre kontra Sicherheit?**
	Linus Neumann, Sicherheitsberater und Sprecher des CCC Chao Computer Clubs, Berlin	
~~Mi 06.10.2021~~ Mi 13.10.2021	AKIS-45	**Hoch-Risiko Cybercrime - wenn Hacker einen Energieversorger angreifen**
	Michael Georgi, Bereichsleiter IT, Technische Werke Ludwigsha am Rhein AG	
Mi 03.11.2021	AKIS-46	**"Ich habe nichts zu verbergen"**
	Hermann Sauer, Geschäftsführer Comidio GmbH, Eltville	
Mi 01.12.2021	AKIS-47	**So nutzen Cyberkriminelle Ihre Daten**
	Ralf Benzmüller, Executive Speaker G DATA SecurityLabs, Bochu	

John Tracker + Dieter Carbon
Leitung Arbeitskreis Internet-Sicherheit

Die Veranstaltungen bilden abgeschlossene Einheite
Teilnahmevoraussetzung ist Interesse.

Die Kosten für die Arbeitskreisveranstaltungen trägt
Rheingau-Bezirksverein; Mitglieder und Gäste sind z
Veranstaltungen herzlich willkommen.

dieter.carbon@trutzbox.de 0176 10209513

https://www.vdi.de/ueber-uns/vor-ort/bezirksvereine/rheingau-bezirksverein-ev/veranstaltungen

Mi 03.02.2021	AKIS-39	**(Be-)Treffen uns Autonome Waffen-Systeme?**
	Dr. Reinhard Grünwald, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin	
Mi 03.03.2021	AKIS-40	**Die Verengung der journalistischen Welt - Warum unabhängiger Journalismus so stark gefährdet ist.**
	Peter Welchering, Medienbüro Welchering (für u.a. Deutschlandradio, ZDF, verschiedene ARD-Sender, FAZ), Stuttgart	
Mi 05.05.2021	AKIS-41	**Smartphone-"Alternativen"? - Android LineageOS für besseren Datenschutz**
	Prof. Dr-Ing. Rainer Keller, Fakultät Informationstechnik, Studiengangleitung - Angewandte Informatik, Hochschule Esslingen	
Mi 02.06.2021	AKIS-42	**"S"in IoT steht für Sicherheit? ... ein Demo-Hack**
	Frank Ewert, Sicherheitsberater, Vorstand SICHERES NETZ HILFT e.V., Freiburg	
Mi 07.07.2021	AKIS-43	**IT-Sicherheit von Maschinellem Lernen?**
	Dr. Sven Herpig, Stiftung Neue Verantwortung e. V., Berlin	
Mi 01.09.2021	AKIS-44	**Privatsphäre kontra Sicherheit?**
	Linus Neumann, Sicherheitsberater und Sprecher des CCC Chaos Computer Clubs, Berlin	
~~Mi 06.10.2021~~ Mi 13.10.2021	AKIS-45	**Hoch-Risiko Cybercrime - wenn Hacker einen Energieversorger angreifen**
	Michael Georgi, Bereichsleiter IT, Technische Werke Ludwigshafen am Rhein AG	
Mi 03.11.2021	AKIS-46	**"Ich habe nichts zu verbergen"**
	Hermann Sauer, Geschäftsführer Comidio GmbH, Eltville	
Mi 01.12.2021	AKIS-47	**So nutzen Cyberkriminelle Ihre Daten**
	Ralf Benzmüller, Executive Speaker G DATA SecurityLabs, Bochum	

Der Werbeblock …

Online-Vortrags-Angebot: AKIS Aufklärung & Kommunikation zur Internet-Sicherheit

Im Rahmen des **Arbeitskreis Internet-Sicherheit** des VDI Rheingau-Bezirksverein (BV) biete ich (außerhalb des Rheingau-BV) Online-Vorträge und -Workshops gemäß DSGVO auf BV-eigenem Jitsi-Server an:
einen Einführungs-Vortrag (A) und Themen-Vorträge und -Workshops (B - H) jeweils im Format:

- Vortrag / Workshop — 60 - 90 Minuten / 90 - 120 Minuten
- Diskussion — 30 - 60 Minuten
- Teilnahme-Reihenfolge — A als erster; B - H unabhängig
- Teilnahme-Voraussetzung — keine (außer Interesse); Vortrag vor Workshop
- Teilnehmende-Beitrag — i.d.R. kostenfrei, bestimmt durch Organisator (VDI-Bezirksverein, Institution, Unternehmen)
- Gruppengröße — max. 40 Teilnehmende

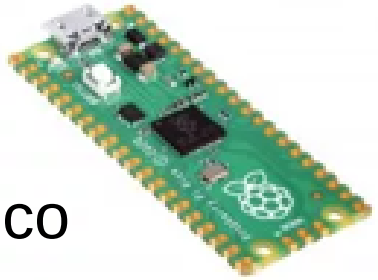
Zu den Themen (B - H) gibt es jeweils einen Vortrag (zur Einordnung) und einen Workshop (zur Umsetzung) mit Übungs- und Anwendungs-Beispielen.

	A ttention Einführung Internet-Sicherheit	**B rowsing** Surfen & Internet of Things	**C yphering** E-Mail & Verschlüsselung	**D istance Meetings** WebMeetings & Videokonferenzen	**E mergency** Risk Analysis & Contingency Planning	**H ome** Smart Home & Home Automation
	Präambel: Agenda & Vorstellung, Werbeblock, Buddha, Zielsetzungs-Puzzle, Gefährdungs-Übersicht, Empfehlungen, Umfrage / Abstimmung, Sprachgebrauch, Problem + Lösung mit 3 Strichen, Nachlese					
Vortrag	• Definitionen IT & Sicherheit • IT-Schutzziele • Aktive und passive Gefährdung • Schadsoftware verstehen • Metadaten • Schutzmaßnahmen	• Struktur Surfen • Passive Gefährdung beim Surfen • Tracker auf Webseiten • Real Time Bidding • Big Player, OCEAN • Einführung IoT	• QR, Hash • Verschlüsselung, PGP • TLS, Zertifikate • E-Mail, Gefährdung • Digitale Signaturen • Crypto Atlas, Quellen TKÜ • Software Arten, Open Source	• Passive Gefährdung bei WebMeetings • WebMeeting Vergleiche • Metadaten • Datenschutz Anforderungen • Antwort-Memo	• Notfall-Definition • Notfall-Planung • Digitaler Nachlass • Vorgehensweise anhand BSI-Standard 200-4 Business Continuity Management	• Randbedingungen • Gefährdungen • Definitionen • Beteiligte • Anforderungen • Aussichten
Workshop		• Surfen mit verschiedenen Browsern • Website-Analyse • Tracker-Verfolgung • Browser-Priorisierung durch Nutzwert-Analyse	• QR- und Hash-Codes erstellen • Zertifikate analysieren • Thunderbird installieren • Verschlüsselte E-Mails austauschen • Libre Office vorstellen	• Nutzung offener Jitsi-Meetings • Jitsi-Meet installieren • Aufsetzen und Durchführen eigener Jitsi-Meetings • Webmeeting-Priorisierung durch Nutzwert-Analyse	• Aufsetzen individueller Notfallpläne • Wiederherstellungskonzepte • Wiederanlaufkonzepte • Notfall-Wiki	• Gefährdungen • Smart Home - Smart Hack • IT-Sicherheit in vernetzten Gebäuden • "PI400" • Tool-Priorisierung durch Nutzwert-Analyse
	Ressourcen-Wiki: Empfehlungen — Literatur; Referenz-, Video-, Podcast-, Newsletter-Links; Checkliste; Termine; Glossar; Tools, Nutzwert-Analyse, Mindmaps					

dieter.carbon@trutzbox.de

Privacy made in Germany

Der Werbeblock …



Online-Workshops: Programmieren mit dem Raspberry Pi Pico

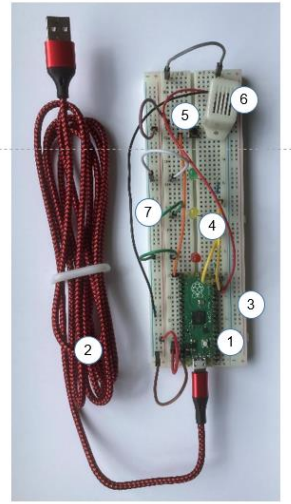
VDI Bezirks-Verein organisiert:

bv-rheingau@vdi.de

Im Teilnahmebeitrag von 20 € enthalten:

1. Raspberry Pi Pico, RP2040 Mikrocontroller
2. Micro-USB Kabel (Verbindung zum PC)
3. Steckbrett mit 830 Kontakten
4. 3 LEDs mit Vorwiderständen
5. Taster
6. Summer
7. 10 Verbindungskabel

und die Versandkosten.



ZUKUNFTS PILOTEN

VDInis-Club Koblenz

Bei weiteren Fragen könnt ihr uns gerne eine E-Mail an: vdini.zukunftspiloten@vdi-koblenz.de schreiben.

Wir freuen uns schon jetzt auf euch und euer reges Interesse an diesem wirklich tollen Angebot der VDInis und Zukunftspiloten Koblenz.

Herzliche Grüße aus Koblenz von euren 2 Clubleiterinnen **Karin Peiter** und **Beate Schumacher** sowie unserem Workshopleiter **Dieter Carbon**

VDI Mittelrheinischer Bezirksverein

bietet 2 Online-Workshops:

Programmier-Projekte in Theorie und Praxis **EVA-1** & **EVA-2**

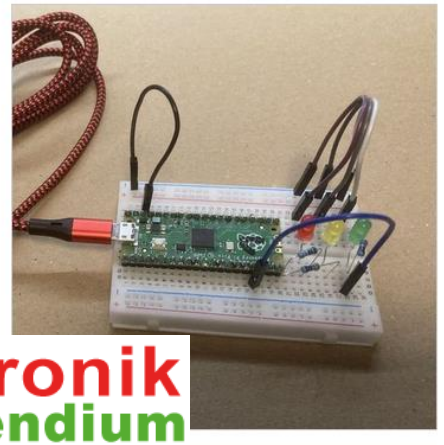
mit dem **Raspberry Pi Pico**

für 10- bis 14-Jährige mit Einstieg ohne Programmierkenntnisse

„Einzel-Personen“:

Workshops

https://www.elektronik-kompendium.de/service/events/



Elektronik Kompendium

Picobello 1

Für Einsteiger **ohne** Vorkenntnisse.

- Einführung in die Bedienung und Programmierung mit der Thonny Python IDE
- Einführung in die grundlegenden MicroPython-Befehle
- Experimente mit den Onboard-Komponenten auf dem Pico (ohne externe Bauteile)
- Experimente zur Ansteuerung von Leuchtdioden und Tastern

Picobello 2

Für Einsteiger **mit** Vorkenntnissen.
Für Teilnehmer von Picobello 1.

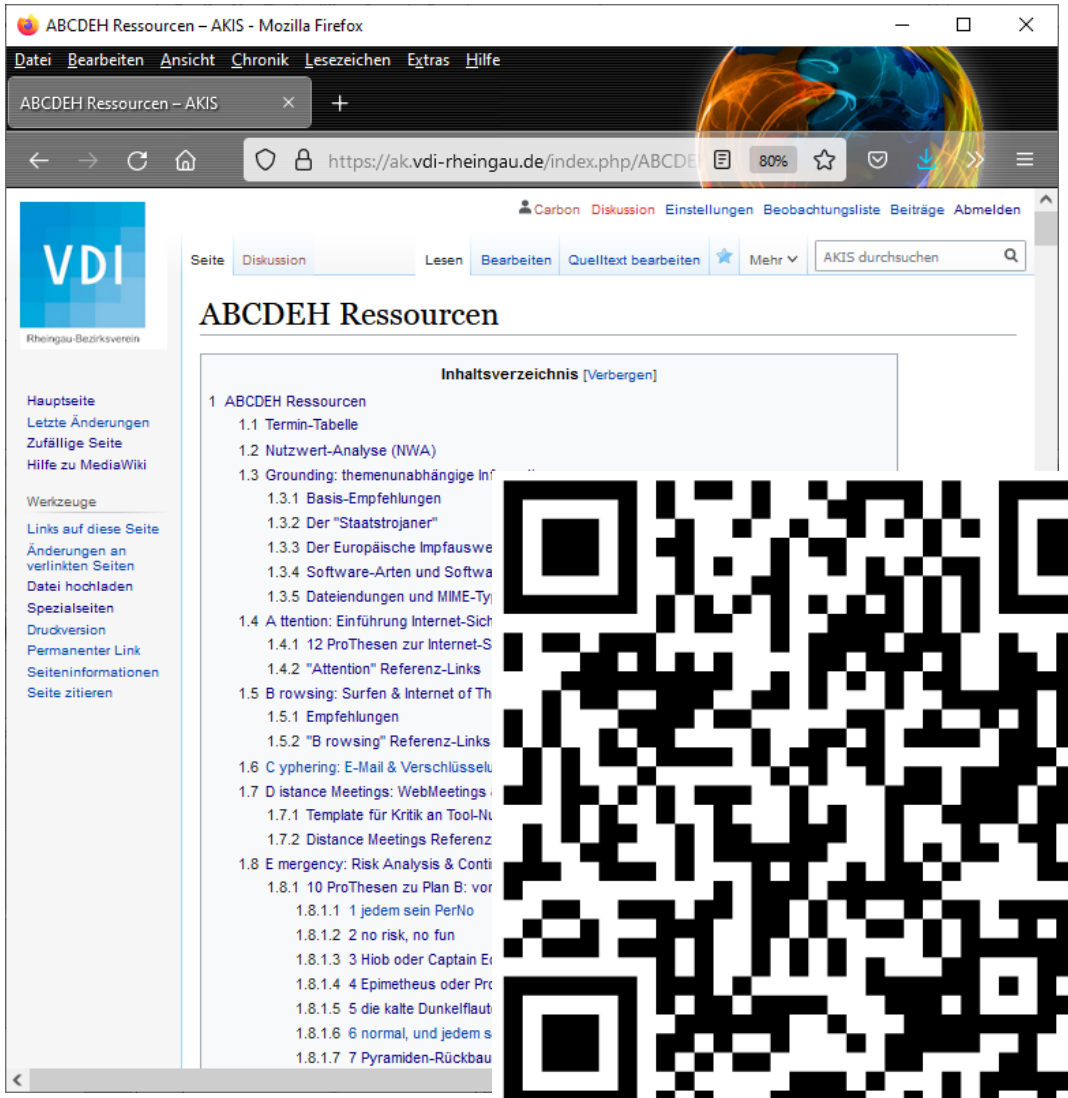
- Konkrete Programmier-Anwendungen mit mehreren Leuchtdioden, Tastern und Temperatursensor
- Ampelsteuerung
- Temperatur-Logger
- Würfel
- Reaktionsspiel

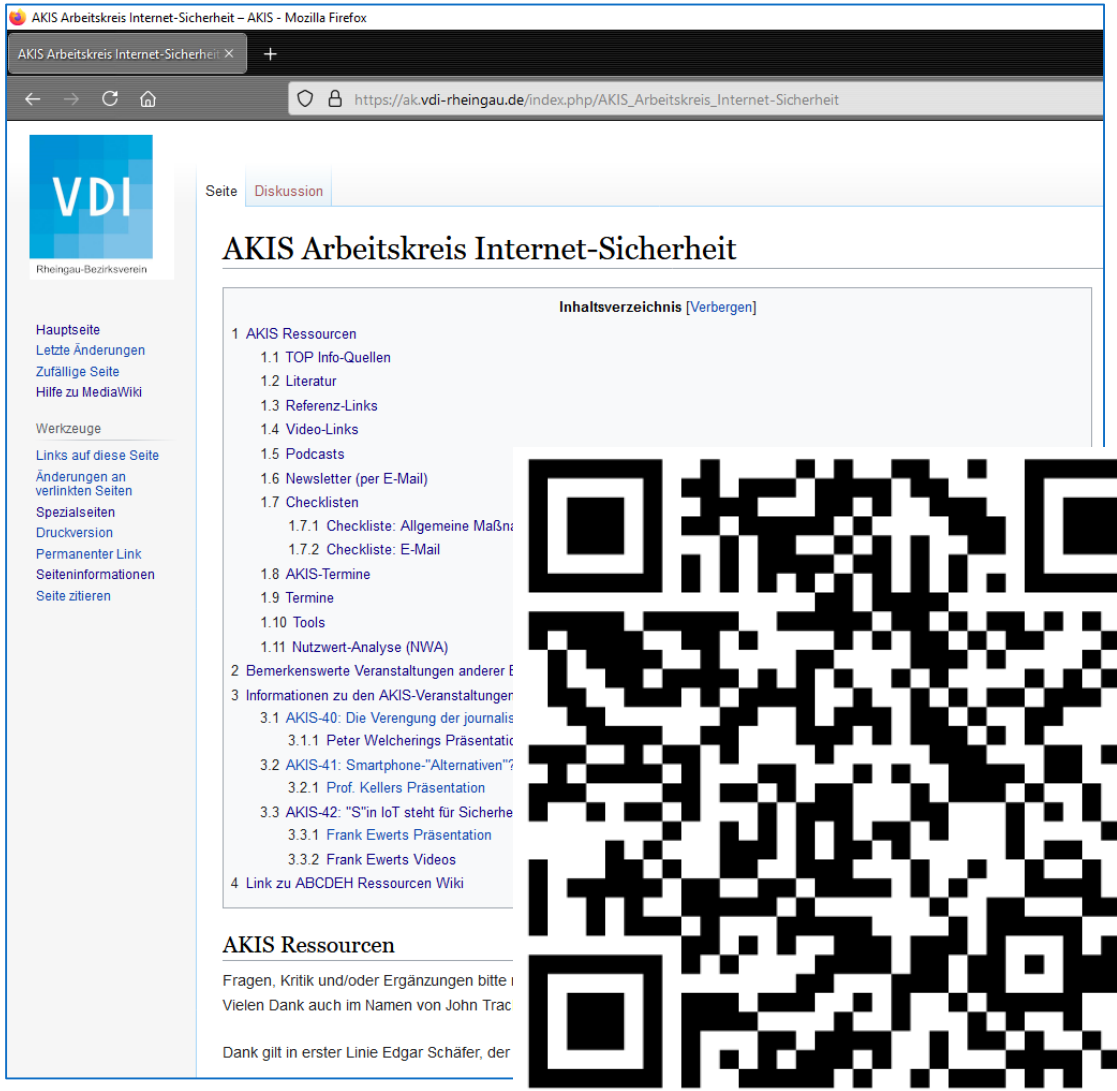
Privacy made in Germany

Die Wikis

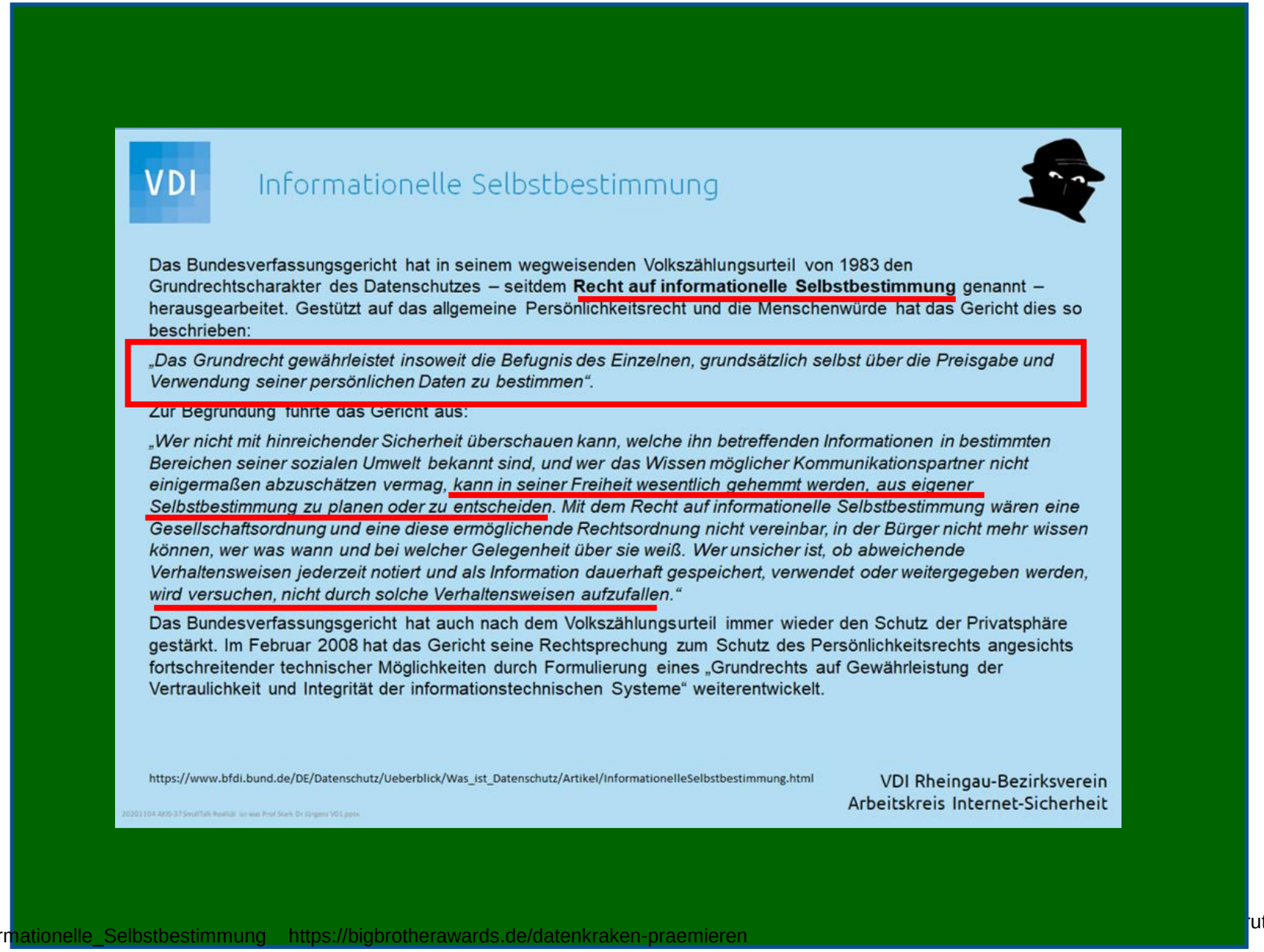
https://ak.vdi-rheingau.de/index.php/ABCDEH_Ressourcen

https://ak.vdi-rheingau.de/index.php/AKIS_Arbeitskreis_Internet-Sicherheit





Informationelle Selbstbestimmung



Informationelle Selbstbestimmung

Das Bundesverfassungsgericht hat in seinem wegweisenden Volkszählungsurteil von 1983 den Grundrechtscharakter des Datenschutzes – seitdem **Recht auf informationelle Selbstbestimmung** genannt – herausgearbeitet. Gestützt auf das allgemeine Persönlichkeitsrecht und die Menschenwürde hat das Gericht dies so beschrieben:

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.

Zur Begründung führte das Gericht aus:

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“

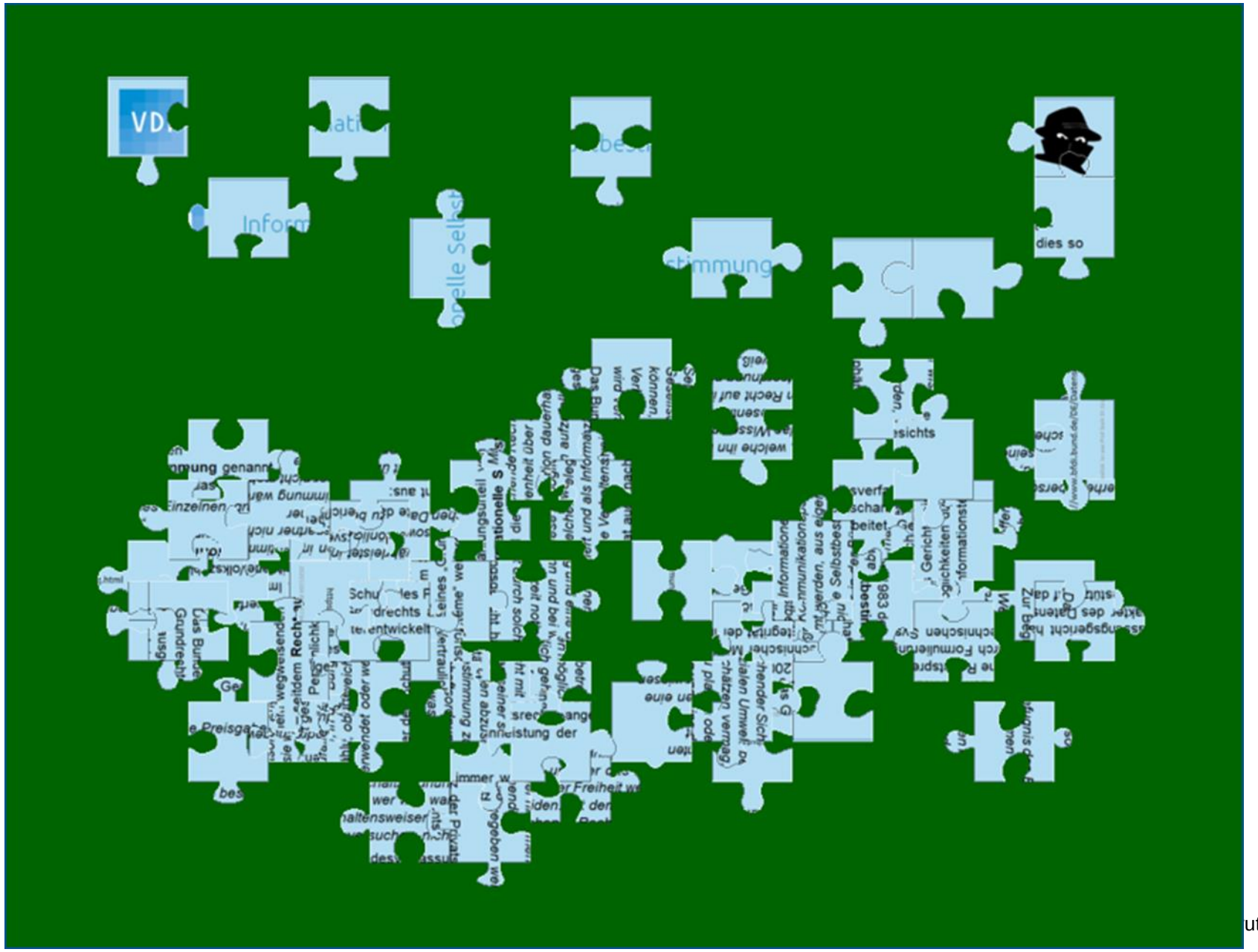
Das Bundesverfassungsgericht hat auch nach dem Volkszählungsurteil immer wieder den Schutz der Privatsphäre gestärkt. Im Februar 2008 hat das Gericht seine Rechtsprechung zum Schutz des Persönlichkeitsrechts angesichts fortschreitender technischer Möglichkeiten durch Formulierung eines „Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität der informationstechnischen Systeme“ weiterentwickelt.

https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/InformationelleSelbstbestimmung.html

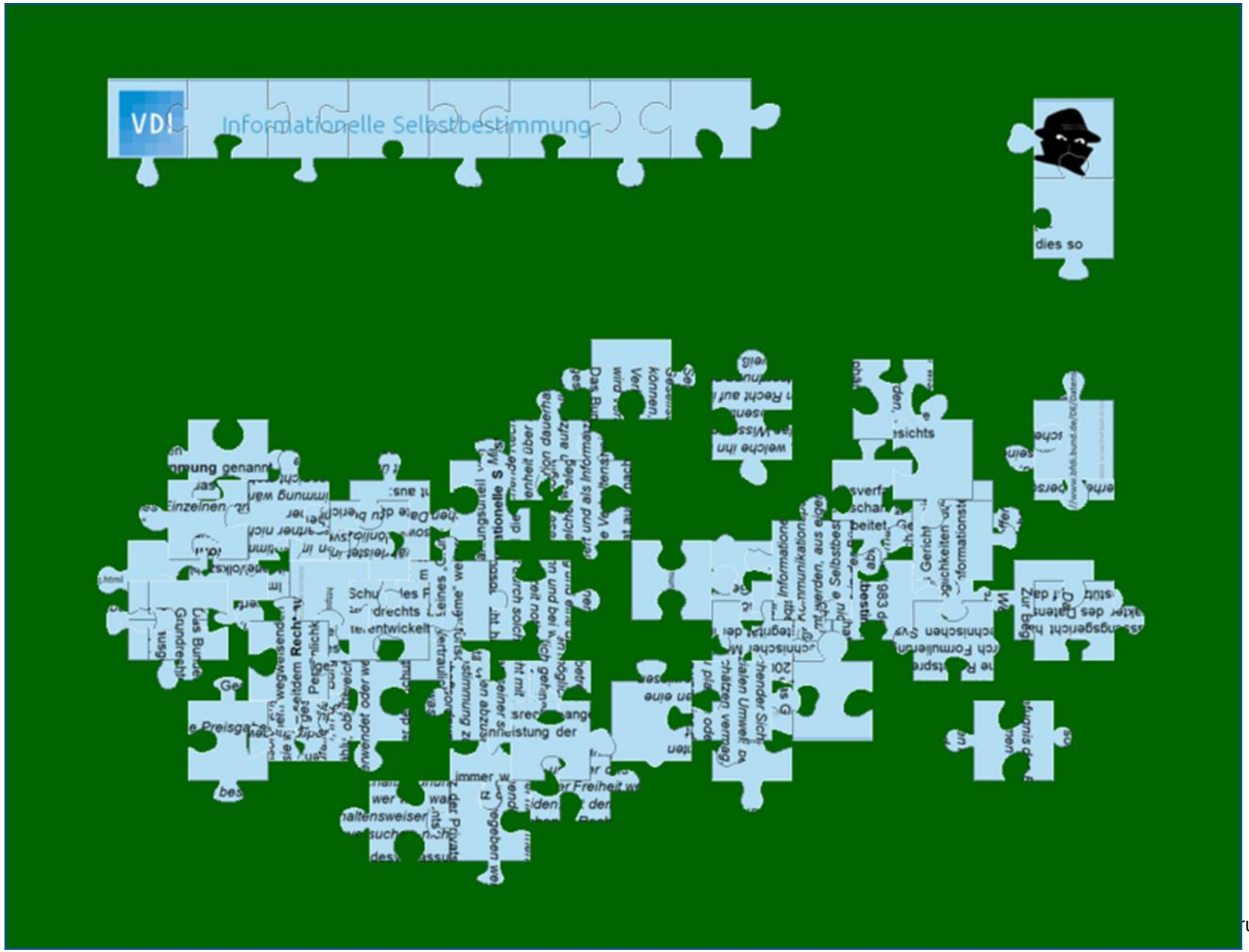
VDI Rheingau-Bezirksverein
Arbeitskreis Internet-Sicherheit

https://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung https://bigbrotherawards.de/datenkraken-praemieren

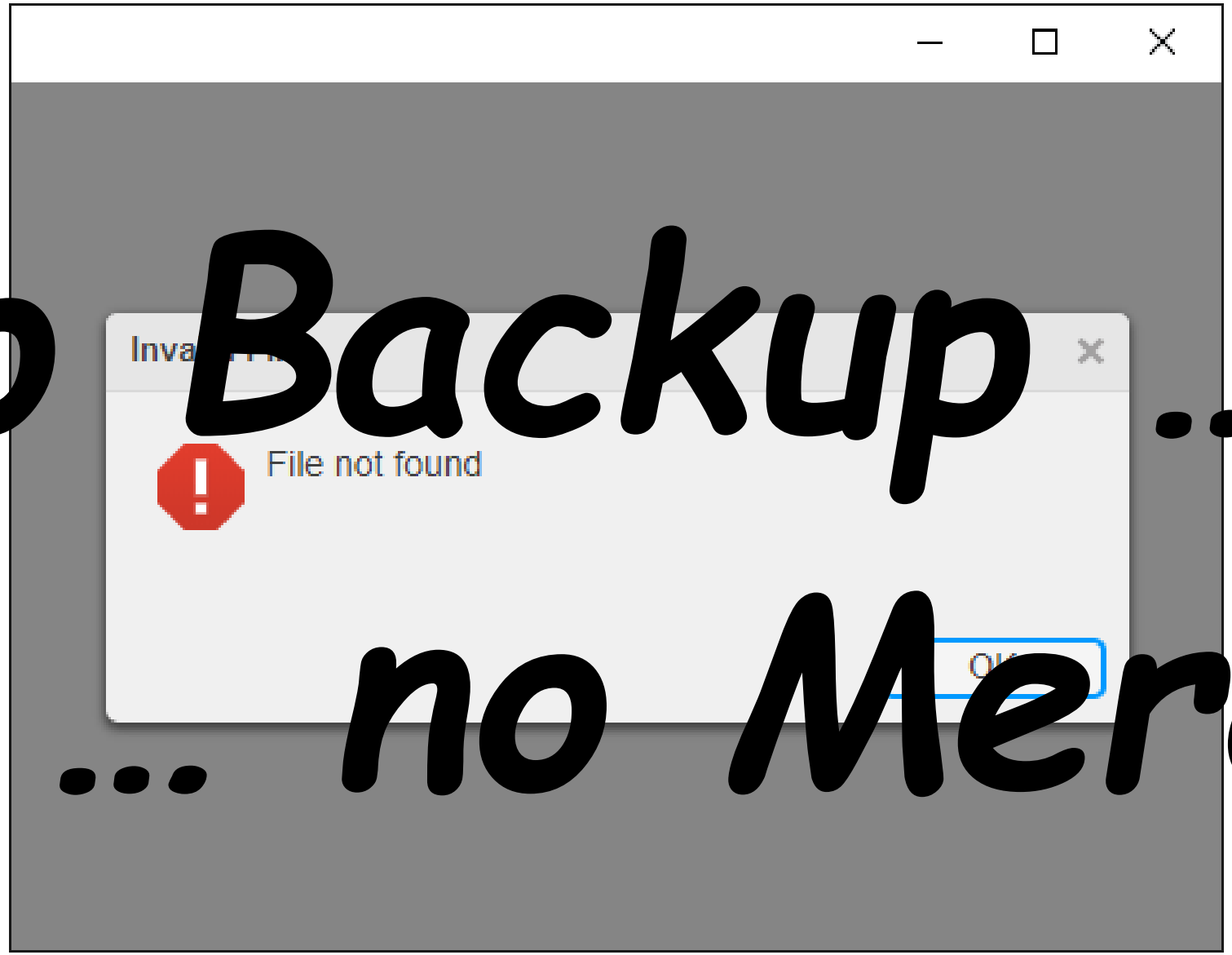
Machen Sie sich ein Bild …



Machen Sie sich ein Bild …



Schon gehabt?



No Backup ...

... no Merci!

dieter.carbon@trutzbox.de

Privacy made in Germany

Backup und StandBy

Raspberry Pi 400 DE Kit

com

net

com

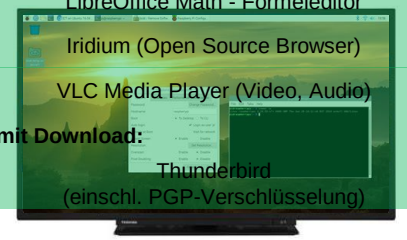
net

Standardmäßig:

LibreOffice Writer - Textverarbeitung	kompatibel mit. Microsoft Word
LibreOffice Calc - Tabellenkalkulation	kompatibel mit. Microsoft Excel
LibreOffice Impress - Präsentationen	kompatibel mit. Microsoft Powerpoint
LibreOffice Draw - Zeichnungen	
LibreOffice Base - Datenbanken	
LibreOffice Math - Formeleditor	
Iridium (Open Source Browser)	
VLC Media Player (Video, Audio)	

mit Download:

Thunderbird
(einschl. PGP-Verschlüsselung)



Media Player (Video, Audio)

(Mail Client; wie Microsoft Outlook)

1 oder 2 Fernseher mit HDMI-Anschluss

aktuell
max. 1 Woche

data

apps

Raspberry Pi 400

BackUp

Zeitnah
regelmäßig
off-line
off-site
3 times
different HW

Historie
alle 3-6 Monate

Privacy made in Germany

Empfehlungen

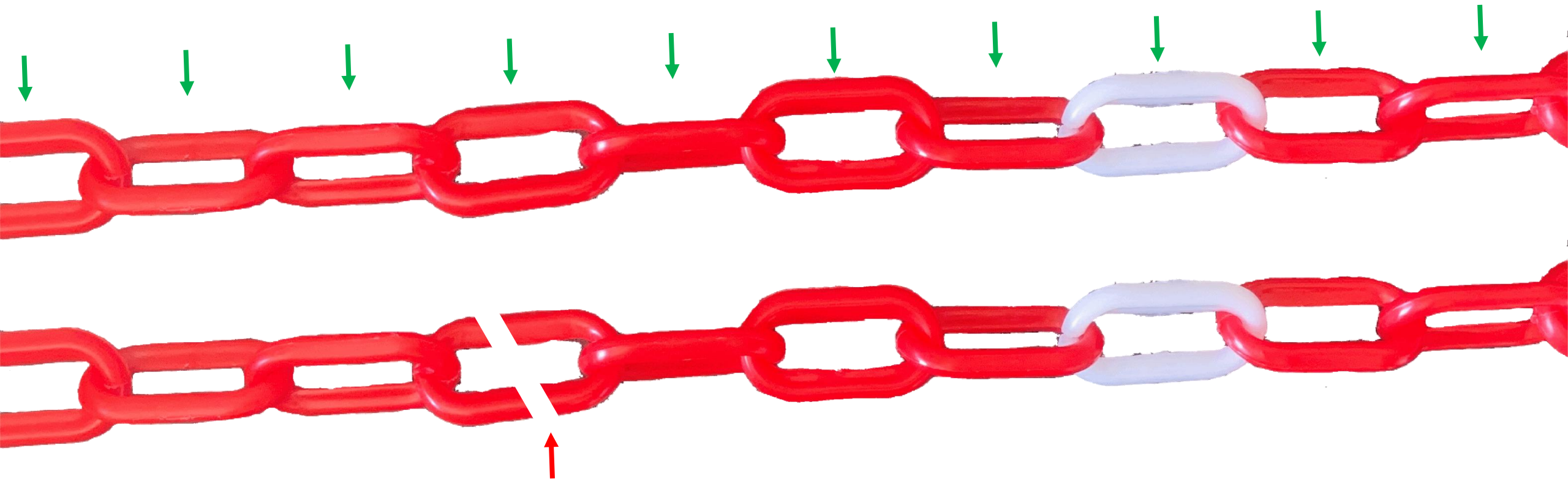
1. Backup machen! (off-line, off-site)
2. Traue ich dem Anbieter?
3. Traue ich der Technik des Anbieters?
4. Updates einspielen
5. Notfall-Planung

dieter.carbon@trutzbox.de

Verteidiger Dilemma

Verteidiger

… muss alle „Stellen“ schließen



Angreifer

… braucht nur 1 „Stelle“ öffnen (oder finden)

dieter.carbon@trutzbox.de

Nachlese

Cybermobbing nimmt „bedrohliche Dynamik“ auf

Die Zahl der Opfer von Mobbing ist laut Studie in Deutschland seit 2018 um 8,3 % gestiegen, bei Cybermobbing sogar um 25 %. Etwa 5 Mio. der Erwachsenen bis 65 Jahre (11,5 %) sind betroffen. Insgesamt waren in Deutschland 32,6 % der Befragten schon einmal Opfer von Mobbingattacken gewesen (Österreich: 36,1 %, Schweiz: 38,7 %). Hochgerechnet entspreche dies bundesweit rund 17 Mio. Menschen.

Cybermobbing belastet vor allem Frauen und junge Menschen.

VDI - n
26. M. 2021

Die Zahl der Opfer von Mobbing ist laut Studie in Deutschland seit 2018 um 8,3 % gestiegen, bei Cybermobbing sogar um 25 %. Etwa 5 Mio. der Erwachsenen bis 65 Jahre (11,5 %) sind betroffen. Insgesamt waren in Deutschland 32,6 % der Befragten schon einmal Opfer von Mobbingattacken gewesen (Österreich: 36,1 %, Schweiz: 38,7 %). Hochgerechnet entspreche dies bundesweit rund 17 Mio. Menschen.

„Es bleibt kaum ein gesellschaftliches Subsystem verschont, Mobbing und Cybermobbing finden statt in Schulen, in der Ausbildung, am Arbeitsplatz, im Freundeskreis und in der Nachbarschaft“, heißt es in der Studie. Die Folgen schlagen sich bei den Opfern teilweise existenziell auf Körper, Psyche und Persönlichkeit nieder und haben oft traumatische Auswirkungen.

Durch daraus entstehende Produktionsausfallkosten im Krankheitsfall entsteht der deutschen Wirtschaft nach Berechnungen des Bündnisses gegen Cybermobbing ein direkter Schaden von mindestens 8 Mrd. €. Die gesamten Kosten dürften aber um ein Vielfaches höher liegen, wenn man etwa Versetzungen, verminderte Arbeitsleistung, Kompetenzverlust, Frühverrentungen, Personalsuche und Einarbeitung neuer Mitarbeiter dazuzähle. „Von daher ist es umso erstaunlicher, wie zögerlich Unternehmen sind, auf diese reale finanzielle Belastung durch Mobbing und Cybermobbing mit entsprechenden Maßnahmen zu reagieren“, heißt es.

ws

Eigene Recherche

dieter.carbon@trutzbox.de

Privacy made in Germany

Nachlese

ICT 19.11.2021

Wie die kopflosen Hühner

mf | Die „technische Störun
über die hier Kunden im Me
Markt in München-Pasing ir
miert werden, ist Folge eine
schweren Hackerangriffs. A
Montag vergangener Woche
musste die Elektronikkette
allen europäischen Ländern
insgesamt rund 3.100 Kasse
vom Netz nehmen. Am Freit
waren EC-Kartenzahlungen
wieder möglich, Kreditkarte
noch nicht. Rechnungen aus
cken ging ebenfalls nicht. D
Online-Shops waren hingeg
nicht betroffen, aber Online
Bestellungen konnten nicht
den Filialen abgeholt werde
Twitter-Nutzer „Haby" garni
sein Bild vom Media Markt
Leipzig-Paunsdorf mit dem
satz „ihr seid der größte Sat
den". So sind nun einmal är
che Kunden.

Gar nicht auszudenken,
diese Kunden erfahren wür
dass online im Shop hinter
ten Bankverbindung und K
tendaten womöglich im Be

Wurden darüber hinaus Kundendaten mit sensiblen Zahlungsinformationen gestohlen? Diese öffentlich zu machen, sind übliche Drohgebärden, um die Lösegeldzahlung gegebenenfalls zu beschleunigen.

Fragen über Fragen, die aktuell auf Twitter die Runde machen. Dazu eben viele Bilder und besagte Screenshots der Erpressermails. Die Pressestellen schweigen, bestätigen nur, dass es sich um einen Cyberangriff handele und man die zuständige Behörde informiert habe. Und dann der Satz, mit dem dpa einen Firmensprecher zitiert: „Für die Kunden bestehe derzeit kein Handlungsbedarf." Was soll das genau heißen? Wie sollen Kunden das interpretieren, wenn sie in einer Filiale keine Dienste wie Gutscheineinlösung nutzen können?

Der Cyberangriff trifft die Kommunikationsabteilung beim Retailer unvorbereitet, wie sie wohl viele Filialketten und andere Unternehmen genauso rat- und planlos treffen würde. Wer indes Spekulationen Twitter & Co. überlässt, verschärft die technische um eine kommunikative Panne. ■

Die Krisenkommunikation der Anderen

ICT 19.11.2021

Auch am Tag fünf nach dem Cyberangriff vergangene Woche Montag war auf der Webseite von Media Markt saturn nichts über die schwere Panne zu lesen. Dafür umso mehr auf Twitter & Co. Man hätte und sollte wenigstens kommunikativ vorbereitet sein.

Martin Fryba | Auch wenige Tage nach dem Cyberangriff ließ sich nicht einmal eine kurze Pressemitteilung auf der Webseite von Media Markt Saturn oder der Muttergesellschaft Ceconomy finden. Nur Plakate in einigen Filialen informieren Kunden, dass aufgrund einer „technischen Störung" viele Services nicht möglich seien (siehe Seite 4). Medien berichten davon, dass hinter dem vermuteten Ransomware-Angriff die Hackergruppe Hive stecke. Screenshots auf Twitter werden verbreitet, auf denen eine Anweisung der Hacker zu lesen ist, wie man vorgehen solle, um Datenverluste zu vermeiden. Kontaktdaten der Cyberbande sind dort zu finden: „Please contact our sales department" steht da zu lesen. Ob die Bilder echt sind, kann man nicht verifizieren.

Martin Fryba, Senior Editor und Stellvertretender Chefredakteur ICT CHANNEL

Die Lösegeldforderung soll von 240 Millionen Euro recht schnell auf 50 Millionen reduziert worden sein. Sind alle 3.100 Server und Kassensysteme von Media Markt Saturn betroffen und Anweisungen an die Filialen geschickt worden, die Kassen vom Netz zu trennen, vorerst nicht anzuschließen und Kunden gegenüber nicht das Wort Hackerangriff in den Mund zu nehmen? Wurden darüber hinaus Kundendaten mit sensiblen Zahlungsinformationen gestohlen? Diese öffentlich zu machen, sind übliche Drohgebärden, um die Lösegeldzahlung gegebenenfalls zu beschleunigen.

Fragen über Fragen, die aktuell auf Twitter die Runde machen. Dazu eben viele Bilder und besagte Screenshots der Erpressermails. Die Pressestellen schweigen, bestätigen nur, dass es sich um einen Cyberangriff handele und man die zuständige Behörde informiert habe. Und dann der Satz, mit dem dpa einen Firmensprecher zitiert: „Für die Kunden bestehe derzeit kein Handlungsbedarf." Was soll das genau heißen? Wie sollen Kunden das interpretieren, wenn sie in einer Filiale keine Dienste wie Gutscheineinlösung nutzen können?

Der Cyberangriff trifft die Kommunikationsabteilung beim Retailer unvorbereitet, wie sie wohl viele Filialketten und andere Unternehmen genauso rat- und planlos treffen würde. Wer indes Spekulationen Twitter & Co. überlässt, verschärft die technische um eine kommunikative Panne. ■

Eigene Recherche

Schwunghafter Schmuggel mit Schwind

HANDEL: Produktfälschungen entwicke… einem großen und deshalb gefährli… Wirtschaftszweig. Ein Blick hinter die Ku… Zollkontrolle in Hamburg.

VDI-n 26.11. 2…

VON WOLFGANG HEUMER

Paketausgabe des Hauptzollamtes Hamburg: Hier spielen sich regelmäßig Dramen ab, wenn Privatkunden Sendungen aus dem außereuropäischen Ausland abholen wollen, deren Begleitpapiere oder Warenbeschreibung beim Zoll Zweifel haben aufkommen lassen. Etwa 20 Personen pro Stunde können ihre Sendung nach Zahlung von Einfuhrumsatzsteuer und Einfuhrzoll mitnehmen.

Doch auf vier bis fünf von ihnen wartet eine bittere Wahrheit: Statt des im Internet scheinbar als Schnäppchen erworbenen Markenartikels steckt eine mehr oder weniger plumpe Fälschung im Paket. „Es wird mittlerweile praktisch alles kopiert oder gefälscht, was es zu kaufen gibt", sagt Abfertigungsleiterin Nicole Wiebeck.

Allein im vergangenen Jahr 2020 hat der Zoll in Deutschland gefälschte Produkte im Originalwert von 239 Mio. € aus dem Verkehr gezogen. Den Schaden haben nicht nur die Hersteller der Originalprodukte. Auch der Käufer solcher Fakes ist am Ende der Dumme.

„Im Regelfall hat er die Ware schon längst bezahlt; das Geld ist also weg", stellt die Zollamtfrau nüchtern fest. Aber wenn der Hersteller der Originalware es wünscht, wird die Fakeware auch noch beschlagnahmt und vernichtet: „Unter Umständen muss sich der Käufer zudem mit zivilrechtlichen Forderungen des Inhabers der Markenrechte auseinandersetzen", weiß Wiebeck.

Das Herrenhemd aus der jüngsten Kollektion einer Edelmarke, die elegante Damenhandtasche aus der Luxuskollektion, die Armbanduhr aus der Schweizer Manufaktur – längst geht der Handel mit gefälschten Produkten weit über den Verkauf solcher Ware auf einem Basar oder am Straßenrand einer Touristenhochburg hinaus. „Der wachsende Anteil von gefälschten und unerlaubt hergestellten Waren am Welthandel ist zutiefst besorgniserregend", stellt Christian Archambeau, Chef des Amtes der Europäischen Union für Geistiges Eigentum (EUIPO), fest.

Anhand der europäischen Zollermittlungsdaten aus dem Jahr 2019 beziffert das Amt das jährliche internationale Handelsvolumen mit gefälschten Produkten auf 411 Mrd. € – das entspricht in etwa dem Bruttoinlandsprodukt von Ländern wie Belgien oder Öster… Länder beziffern … Wächter des geis… den Gesamtwert … Fakes und R… 119 Mrd. € – etwa … ren in den europ… markt sind demna…

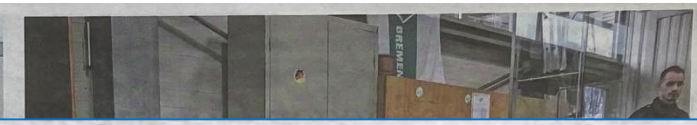
Doch es geht n… wirtschaftlichen S… auch um Verbr… Denn es werden … und Chemikalien … sche Produkte wie … großem Stil gefäls…

Manchmal hat… Produkte etwas … Bachmann, der S… in Hamburg, … „Bremsscheiben, … waren". Aber se… Fälscher mehr … der vermeintli… schwerwiegende… liegt in der Natu… technische Eign… gen nicht geprüf…

Die Fälle, dene… und ihr Team … sich meist um p… Produktpiraten. … einem Paket m… dukte finden … regelmäßig sol… hen wir von eine… Handel mit Fäl… die Zollexpertin… genmäßig die … schungen auf … Empfänger bef… sen am Wert is… tainerschifffahr… portmittel au… Markt mit gra… chend sind die … fen wie Hambu… die Hauptums…

Aber auch … greift der Zoll … kopien und Fäl… ni entdeckten … Köln gefälschte … Bluetoothkopf… mehr als 8,8 M… später beschl… am Flughafen L… re Luxusuhren … 16,2 Mio. €.

Längst schw… Schmuggler … nicht mehr n… Trenchcoat im … über den Hafe… sen den Tran… Fracht zumeist … Fahrern. Doch … Schwarzmarkt …



Nichts ist unmöglich: Bei jeder Jahrespressekonferenz präsentiert der Zoll Beispiele für gefälschte Produkte. Häufig handelt es sich um Schuhe und Kleidung, aber der Anteil technischer Produkte wie Autofelgen nimmt rapide zu. Foto: Wolfgang Heumer

Bittere Wahrheit: Bis zu 25 % aller im Hauptzollamt Hamburg kontrollierten Postpakete aus dem außereuropäischen Ausland enthalten Produktfälschungen. Zollamtfrau Nicole Wiebeck leitet die Kontrollen und lässt die Fakeware beschlagnahmen. Foto: Wolfgang Heumer

Den Pokal trugen die Beamten des Zollamtes Garching-Hochbrück im Oktober 2020 davon: In einer Postsendung aus China fanden sie die Trophäe der UEFA Champions League. Ein Fan hatte die Blechkopie der eigentlich versilberten und vergoldeten Trophäe als Souvenir für den Finalsieg der Bayern kurz zuvor für 400 € im Internet erworben – im vollen Bewusstsein, dass es eine Kopie war.

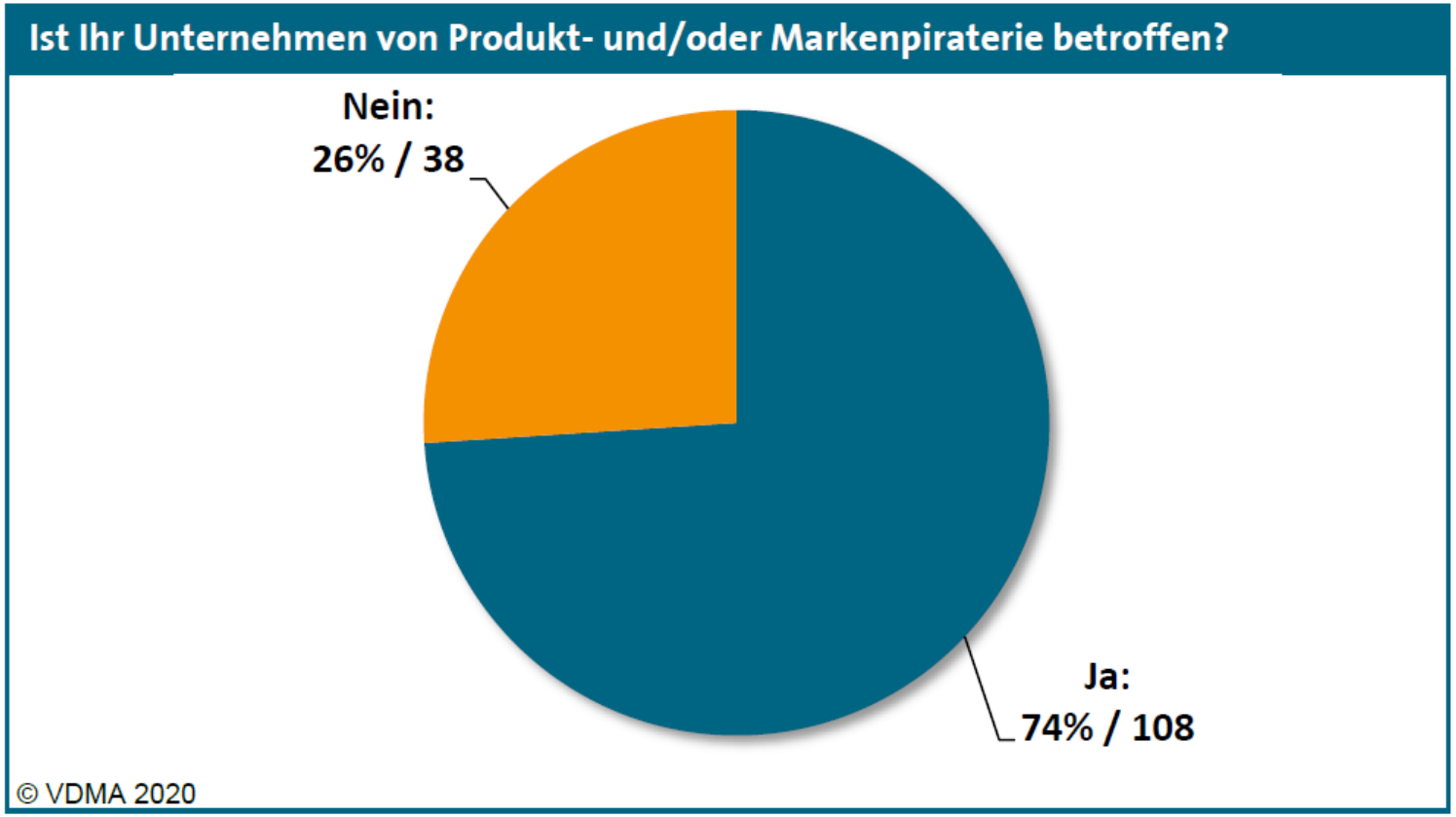
„Ihm war allerdings nicht klar, dass die Einfuhr einer Fälschung rechtlich verboten ist", erklärte Marie Müller, Sprecherin des Hauptzollamts München. Auf Antrag der UEFA brachte der Zoll den Pokal zum Schrott.

Eigene Recherche

Privacy made in Germany

Verband Deutscher Maschinen- und Anlagenbau e. V.

VDMA Studie
Produktpiraterie
2020



Anteil der von Produkt- und Markenpiraterie betroffenen Unternehmen. N=146

https://www.vdma.org/viewer/-/v2article/render/1313489

dieter.carbon@trutzbox.de

Privacy made in Germany

Verband Deutscher Maschinen- und Anlagenbau e. V.

„Die wichtigsten Ergebnisse der VDMA Studie Produktpiraterie 2020 im Überblick:

• 74 Prozent der Unternehmen im Maschinen- und Anlagenbau sind von Produktpiraterie betroffen (2018: 71 Prozent). Bei Unternehmen mit mehr als 500 Mitarbeitern beträgt die Quote sogar rund 90 Prozent. Damit erreicht die Bedrohung durch Produkt- und Markenpiraterie ein neues Allzeithoch.

• Im Vergleich zu den letzten Studien zeigt sich bei der wahrgenommenen Bedrohung eine deutliche Trendwende: Nach einem stetigen Rückgang sprechen sich mit einer Zunahme um rund 40 Prozent nunmehr 52 Prozent der Befragten für eine Zunahme des Bedrohungsniveaus aus.

• Der geschätzte Schaden im Umsatzjahr 2019 betrug 7,6 Milliarden Euro und erhöht sich damit im Vergleich zur Studie von 2018 um 300 Millionen Euro. Der durchschnittliche Schaden für betroffene Unternehmen betrug 4,9 Prozent des Jahresumsatzes.

• Der Umsatzverlust von 7,6 Milliarden Euro entspricht rund 35.000 Arbeitsplätzen (2018: 33.000).

• Die Volksrepublik China führt unangefochten mit 61 Prozent die Liste der Vertriebsländer von Plagiaten an. Auf Platz zwei folgt mit großem Abstand Deutschland (19 Prozent), dann Russland (12 Prozent).

• Für 72 Prozent der Unternehmen gilt der Wettbewerber als Verursacher der Plagiate. Doch auch bei Geschäftspartnern (Kunden, Zulieferer, Joint-Venture-Partner, Ersatzteilverkäufer) geben erschreckende 42 Prozent der Befragten an, dass sich unter mindestens einem von diesen einen Plagiator befindet.

• Plagiate stellen nachweisbar ein Sicherheitsrisiko dar: 36 Prozent der Unternehmen berichten von Fälschungen, die eine Gefahr für Bediener oder Anwender mit sich bringen. Erschreckende 57 Prozent der Befragten sehen bei den von ihnen entdeckten Plagiaten eine Gefahr für den sicheren Betrieb der Anlage.

• Häufigstes Plagiat bleiben in 64 Prozent der Fälle einzelne Komponenten. Dicht dahinter liegen auf Platz zwei Designplagiate mit 60 Prozent. In jeweils rund 40 Prozent der Fälle sind ganze Maschinen, Ersatzteile oder sogenannte „weiche“ Plagiate (Kataloge, Broschüren, Produktfotos) das Fälschungsziel.

• Im Plagiatsfall ist das Mittel der Wahl, die geltenden Rechte erst außergerichtlich und dann zivilrechtlich durchzusetzen. Rund die Hälfte aller betroffenen Unternehmen ergreift jedoch keinerlei Maßnahmen. Dies trifft vor allem auf kleine und mittlere Unternehmen zu, bei denen zwei von drei Unternehmen keine Maßnahmen einleiten.“

https://www.vdma.org/viewer/-/v2article/render/1313489

dieter.carbon@trutzbox.de

Privacy made in Germany

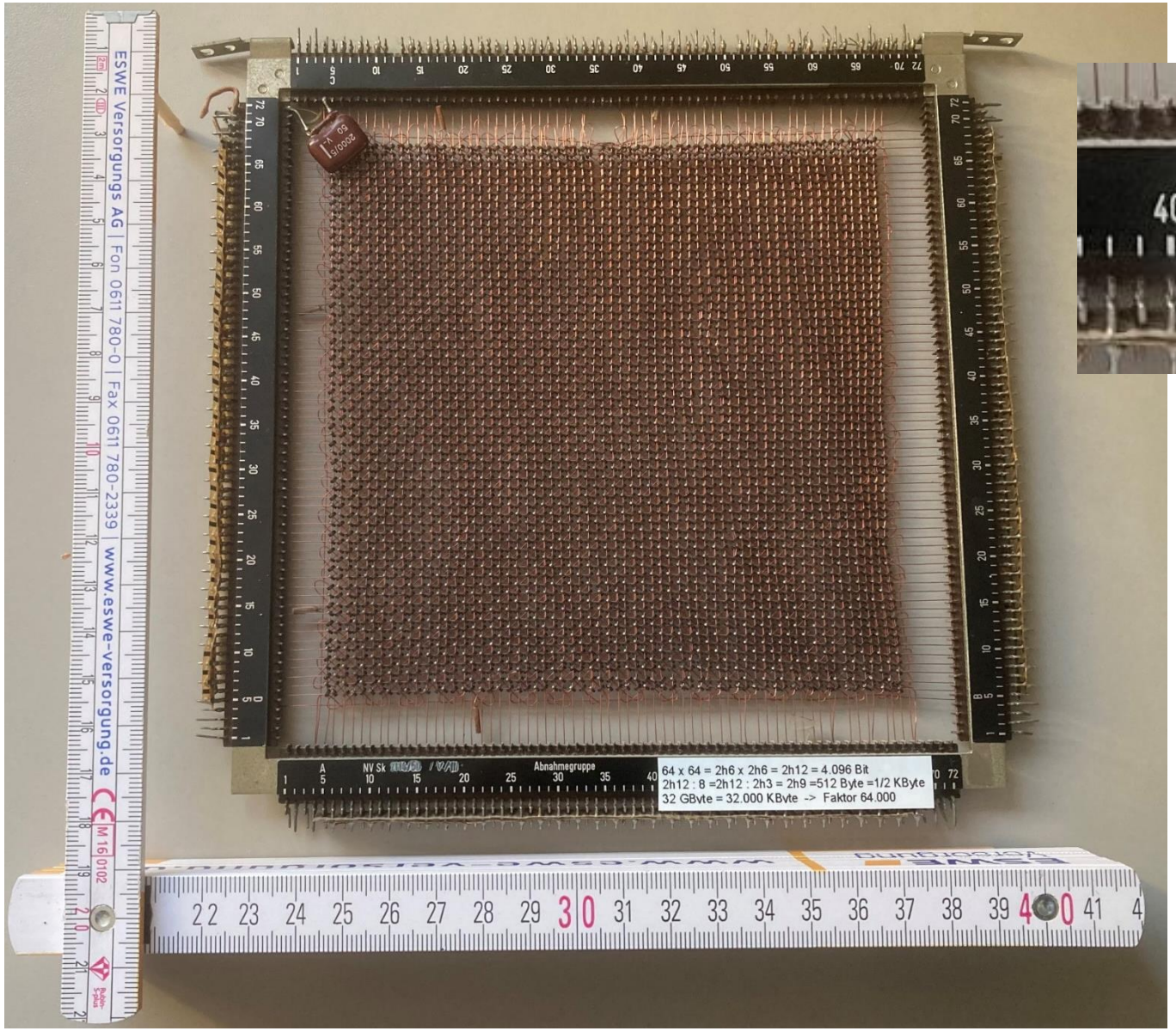
12 ProThesen zur Internet-Sicherheit: von Hörigkeit zur Mündigkeit

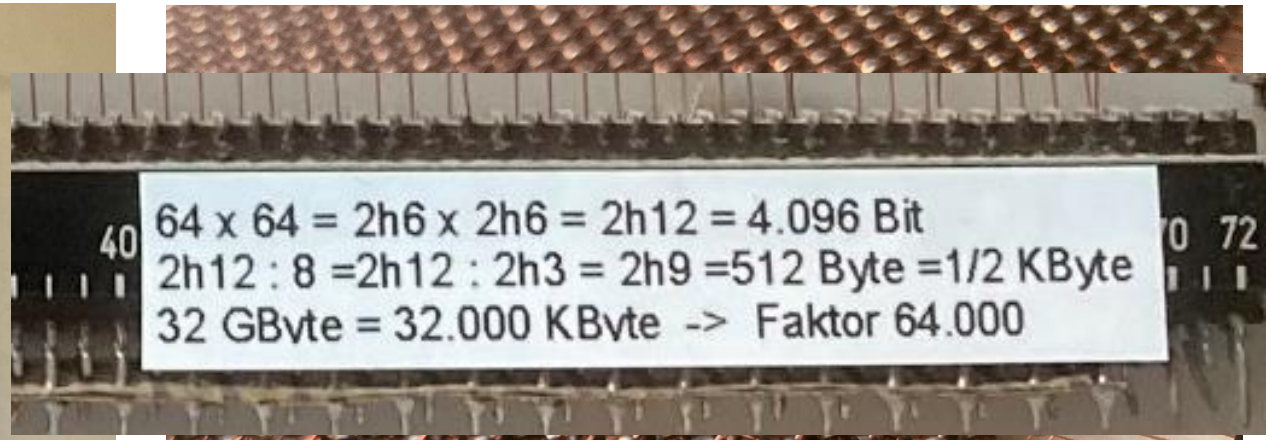
1. Digit~~al~~us first. Bedenken second
2. Wir wollen doch nur Dein Bestes
3. CIA: man schütze mich vor meinen Freunden
4. Seekabel ist Sehkabel
5. Ich bin Mittelpunkt (-> Ich bin Mittel .)
6. Bitte (k)ein Bid
7. Wer verschlüsselt, hat was zu verbergen
8. Frau Merkel skypt
9. Smart Home - alone, nur mit Strom
10. Offenes Visier; sieh, das Gute liegt so nah
11. Der Dilettant bringt was auf die Waage
12. Wer schreibt, der bleibt; Grüße von der Insel

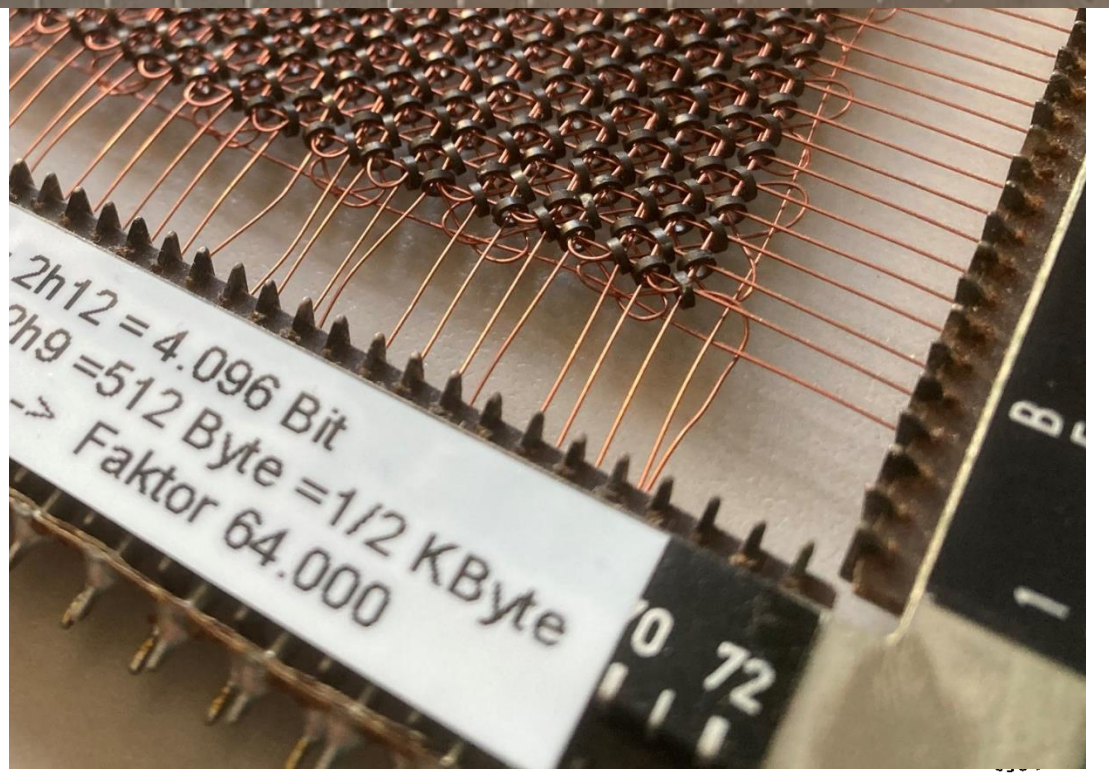
Prothese von altgriechisch πρόσθεσις *prósthesis*, ‚Anfügung', aus πρός ‚hinzu, obendrein, außerdem' und τίθημι ‚setzen, stellen, legen

https://de.wikipedia.org/wiki/Prothese

Zählen, Messen, Begreifen -> glauben, vertrauen







Krankenakten von Therapiesitzungen im Internet

Patientenakten als Waffe

Der Datenskandal in Finnland weitet sich aus

Die Folgen des Hackerangriffs auf das finnische Psychotherapiezentrum Vastaamo (F.A.Z. vom 28. Oktober 2020) ließen nicht lange auf sich warten. Die gehackte Datenbank mit zahllosen hochsensiblen Informationen ist inzwischen komplett im Internet, frei zugänglich für jeden.

Vastaamo war eine äußerst erfolgreiche finnische Firma, die Psychotherapiebehandlungen anbot und den Prozess vom Einstieg, der Therapeutenwahl bis zur Abrechnung erleichterte. Die Prominenz des Unternehmens zog knapp ein Prozent der finnischen Gesamtbevölkerung von fünfeinhalb Millionen Menschen an, um die vierzigtausend Patienten. Zu ihnen gehörten einflussreiche Männer und Frauen aus allen Teilen des Staates. Deren Krankenakten umfassen Beschreibungen der Therapiesitzungen, dazu die in Finnland wichtigen Personenkennzeichnen, Mobiltelefonnummern und Adressen. Das alles gelangte in die Hände der Hacker, die zunächst Lösegeld von Vastaamo erpressten. Da Vastaamo sich darauf nicht einließ, wurden Teile der Datenbank anfangs im Darknet veröffentlicht, danach aber wieder entfernt. Später drohten die Hacker den Einzelkunden des Therapiezentrums mittels persönlich adressierter E-Mails, deren Daten öffentlich zu machen, falls sie nicht drei- bis fünfhundert Euro in Bitcoins überweisen würden.

Die finnische Regierung und die Leitmedien des Landes appellierten an die Vernunft der Bevölkerung und baten darum, den Datendiebstahl zur Anzeige zu bringen. Im Dezember teilte die finnische Polizei mit, dass etwa 25 000 Meldungen bei ihr eingegangen seien. Die Betroffenen sprachen in den Medien über die hohen Belastungen, die ein solches Vorgehen mit sich brachte. In etlichen Behörden hatten sie gegen Gebühren ihre Rechte schützen lassen müssen: etwa die Sperrung ihrer Kreditanträge bei den Banken oder der Möglichkeit von Adressänderungen im Internet. Allein diese Sperrungen kosteten die Geschädigten pro Person etwa zweihundertfünfzig Euro. Zudem kommt die gesamte Prozedur nach zwei bis drei Jahren erneut auf sie zu, da solche Sperrungen oft nur temporär zu verhängen sind. Allerdings stellte sich in Internetdiskussionen und den finnischen Medien ein Gefühl von Zusammengehörigkeit her: Manche sprachen zum ersten Mal offen über ihre Therapieerfahrungen und verhalfen damit zu einer größeren Normalisierung des Themas. Etliche versprachen, sich die gestohlenen Daten niemals anzuschauen.

31.980 Therapieakten

In der letzten Januarwoche wurde die gesamte Datenbank im Internet frei zugänglich, wobei die Dateigröße von ursprünglich zehn Gigabyte auf unter hundert Megabyte reduziert worden war, was das Herunterladen und Weiterverbreiten enorm erleichtert. Im Netz stehen nun insgesamt 31 980 Therapieakten, geordnet nach Namen der Patienten, mit persönlichen Angaben, längeren und kürzeren Protokollen der Therapiesitzungen samt Diagnosen. Da es in Finnland keinen generalisierten Beschreibungscode für Ärzte gibt, variieren die Akten stark. Im schlimmsten Fall ist da hochsensibles Material, das für die berufliche Karriere der Betroffenen oder ihr persönliches Umfeld katastrophale Folgen haben könnte.

All das könnte auf Jahrzehnte Stoff für neugierige und ambitionierte Headhunter, Journalisten, Politiker und gewöhnliche Erpresser bieten. Kaum jemand wird zugeben, er habe diese Dateien gesichtet, doch viele haben sie längst auf ihren Laptops und können sie bei Bedarf durchschnüffeln. Es gibt genügend Menschen, die sich öffentlich solidarisch geben, aber im Verborgenen ihre Neugier nicht bremsen können. Noch lässt sich nicht sagen, ob dieser Fall die Anhänger einer digitalen Gesellschaft endlich aus ihrer Naivität reißen wird.

Bezeichnend ist, dass man in Finnland nun vordringlich über eine Erleichterung der Änderung seines Personenkennzeichens diskutiert, was derzeit sehr schwierig ist. Das Hauptproblem liegt woanders. Es besteht darin, dass das Personenkennzeichen in einer digitalisierten Gesellschaft ein Mittel der Identifikation ist. Die Missbrauchsmöglichkeiten gehören zu den Abertausenden Fragen, womit sich die Avantgardisten der Digitalisierung nur sehr unwillig beschäftigen.

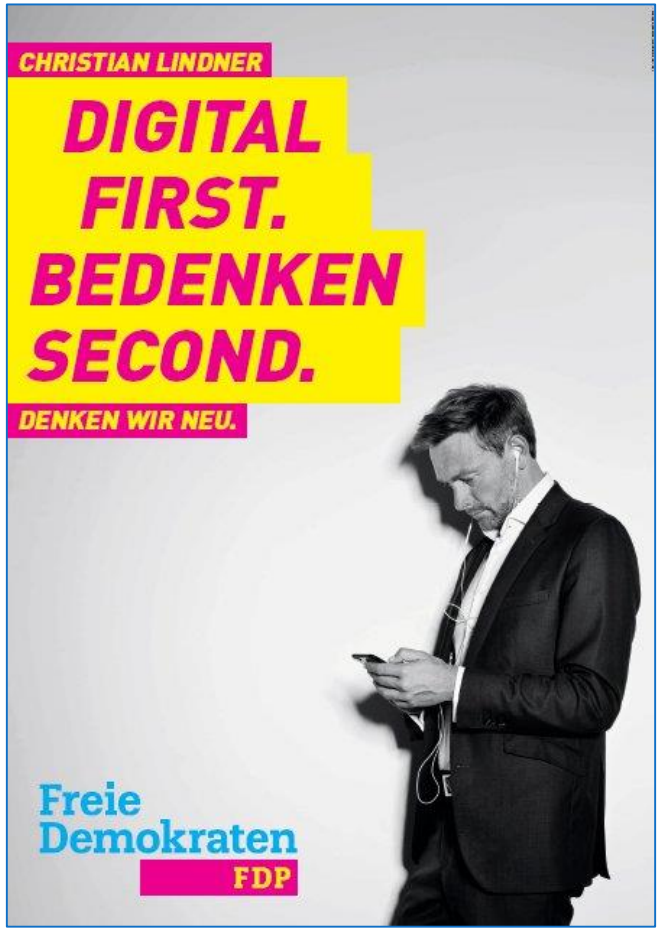
Inzwischen sind die Datenmengen so groß und mitunter derart schlecht gesichert, dass sie zu einer immer leichteren Beute für moderne Cyberkriminelle werden. Wenn Diebstähle wie in Finnland passieren, können blitzschnelle Ausbreitungswellen die Folge sein, die die staatlichen Behörden nicht mehr bremsen können. Was ursprünglich soziale Dienstleistungen erleichtern sollte, ist zur Waffe geworden, deren Einsatzmöglichkeiten wir noch gar nicht kennen. Die Täter im Fall Vastaamo laufen weiter frei herum. Die finnische Polizei hat bisher nur bekanntgegeben, sie sei in ihren Untersuchungen weitergekommen. Eine Ahnung, wer die Hacker sind, hat sie nicht. JÜRI REINVERE

FAZ vom 03.02.2021

dieter.carbon@trutzbox.de

Privacy made in Germany

Digitalisierung



Digitalus first

(Digitalisierung)

… gibt es seit wann?

… soll wie lange gefördert werden?

Prozess-Optimierung

Vernetzung

dieter.carbon@trutzbox.de

vernetzbar

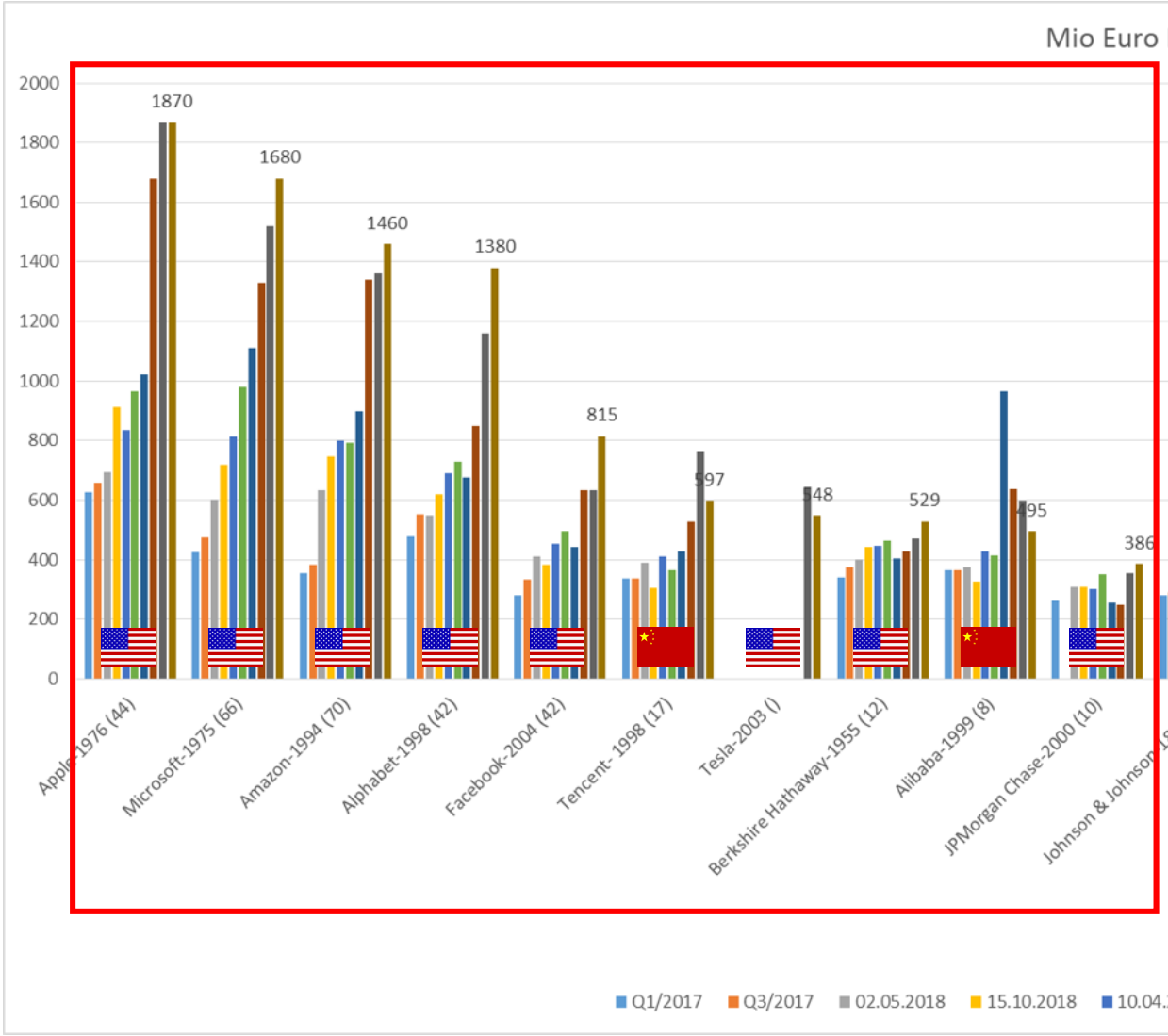
=

verletzbar

dieter.carbon@trutzbox.de

Privacy made in Germany

Wertvollste Unternehmen der Welt



seine Hauptreden 2012-14

XI JINPING

CHINA REGIEREN

seine Hauptreden 2014-17

XI JINPING

CHINA REGIEREN

II

„Steh … ave
Lass … ch u … r bauen.
In gr … s Vo
Der … hrei
Steh
Gem … che
Gem … che
Vorw

2021 100 Jahre Kommunistische Partei Chinas (8.7.)

2025 „Made in China“

2030 das wichtigste KI-Innovationszentrum der Welt

2035 meiste Patentanwendungen (weltweit)

2049 100 Jahre Volksrepublik China

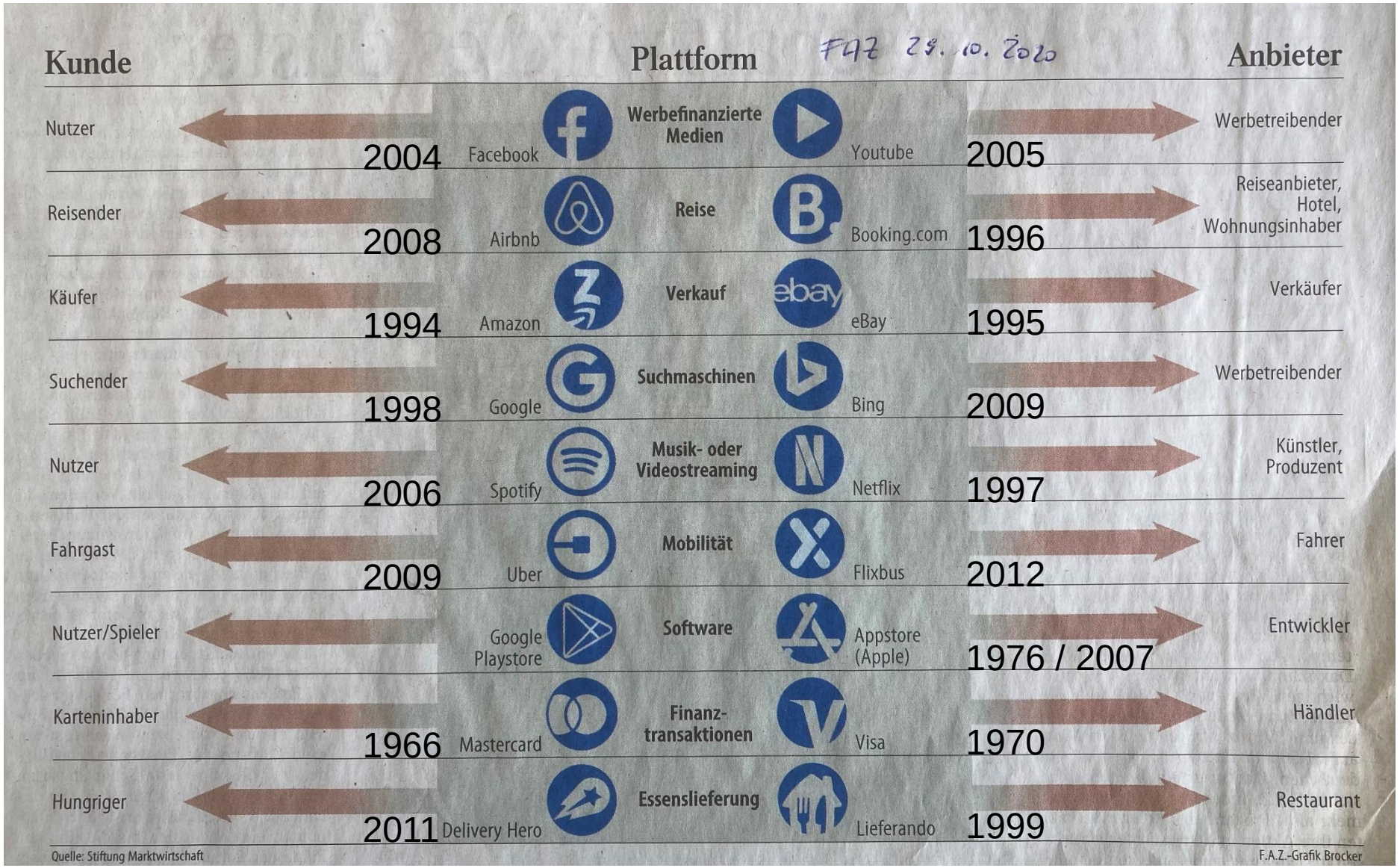
Forschungsschwerpunkte nach Xi Jinping:

Big Data, Gesichtserkennung, Robotics, KI, Quantencomputer

https://www.finanzen.net/aktien/taiwan_semiconductor_manufacturing-aktie

dieter.carbon@trutzbox.de

Plattformgeschäft



dieter.carbon@trutzbox.de

Wer interessiert sich für uns?

Berlin hat den Staatstrojaner FinFisher gekauft
https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/#spendenleiste

Software-Lücken und Hacking-Werkzeuge werden von **Geheimdiensten** und **Hackern** genutzt

FINFISHER™ Excellence in Cyber Investigation

]HackingTeam[

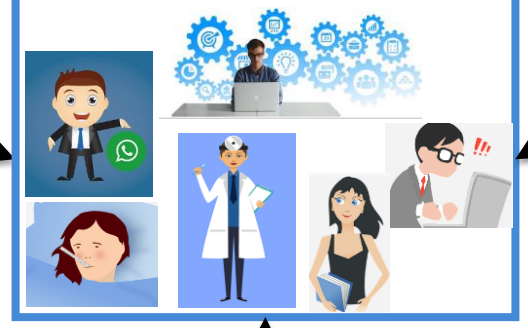
NSO GROUP

Geheimdienste und andere staatliche Institutionen

Hacker hacken auch Geheimdienste, **Staatliche Institutionen** kaufen Softwarelücken

Kriminelle Hacker (Black-Hats) suchen, nutzen und verkaufen Lücken in Software die wir alle nutzen

Wir alle



Geheimdienste haben Zugriff auf Informationen der **kommerziellen Datensammler**

Kriminelle Hacker nutzen die Daten **kommerzieller Datensammler** für ihre Angriffe (z.B. für CEO Fraud)

Kommerzielle Daten-Sammler, „Daten-Veredler“ & -Händler - Tracker-Firmen (Axciom, Oracle, Yahoo, Google, Facebook, ...)

dieter.carbon@trutzbox.de

Privacy made in Germany

Service-Kosten

SERVICE	BITCOIN (Typical price range listed along with the highest listed price)	USD (Typical price range listed along with the highest listed price)
HACKING WEB SERVER (VPS OR HOSTING)	0.034 - 0.0449, 0.47	$220 - $500, $3,000
SETTING UP KEYLOGGER	0.0263	$170
DDOS (PRICES MAY VARY)	0.0534, 0.078 - 0.39	$350, $500 - $2,500
HACKING PERSONAL COMPUTER	0.0364, 0.044 - 0.55	$280, $500 - $3,500
HACKING CELL PHONES	0.047 - 0.093	$300 - $600
EMAIL HACKING	0.078 - 0.12	$500 - $800
SOCIAL MEDIA ACCOUNT HACKING	0.0352, 0.054 - 0.11	$230, $350 - $700
CHANGE SCHOOL GRADES	0.19 - 0.58	$1,200 - $3,750
FUD RANSOMWARE + DECRYPTER	12 MO / 0.14 6 MO / 0.076 1 MO / 0.019	12 MO / $900 6 MO / $490 1 MO / $120

Prices for services on a major darknet cybercrime forum, including for "fully undetectable" ransomware, found in October 2018, reflecting exchange rates in effect at that time (Source: WatchGuard)

Allianz Risk Barometer 2021 (19.01.2021)

Top Business Risks 2021

THE MOST IMPORTANT BUSINESS RISKS IN EUROPE

1	44%		**Cyber incidents** (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)	2020: 45% (1)
2	43%		**Business interruption** (incl. supply chain disruption)	2020: 42% (2)
3	42%		**Pandemic outbreak** (e.g. health and workforce issues, restrictions on movement)	NEW
4	22%		**Changes in legislation and regulation** (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	2020: 33% (3)
5	20%		**Market developments** (e.g. volatility, intensified competition / new entrants, M&A, market stagnation, market fluctuation)	2020: 22% (4)
6	16%		**Natural catastrophes** (e.g. storm, flood, earthquake, wildfire)	2020: 19% (6)
7	15%		**Fire, explosion**	2020: 20% (5)
8	14%		**Climate change / increasing volatility of weather**	2020: 13% (9)
9	12%		**Macroeconomic developments** (e.g. monetary policies, austerity programs, commodity price increase, deflation, inflation)	2020: 13% (10)
10	10%		**New technologies** (e.g. impact of Artificial Intelligence, autonomous vehicles, 3D printing, Internet of Things, nanotechnology, blockchain)	2020: 14% (8)

Source: Allianz Global Corporate & Specialty. Figures represent how often a risk was selected as a percentage of all responses for that region. Respondents: 1,278. Figures don't add up to 100% as up to three risks could be selected. **Photos:** iStock, Adobe, Shutterstock
KEY = PURPLE risks the same as 2020 RED risks higher than 2020 GREEN risks lower than 2020 ORANGE risks not ranked in 2020

17

https://www.allianz.com/de/economic_research/publikationen/spezialthemen-fmo/2021_01_19_AllianzRiskBarometer2021.html

Passive Gefährdung

Was passiert, wenn nichts passiert?

- beim Surfen?
- beim Austausch von E-Mails?
- bei Videokonferenzen/Webmeetings?

Nutzungs-Daten und/oder Meta-Daten werden gespeichert, analysiert, strukturiert, ausgetauscht und vermarktet …

Wo? Von wem? Weiß ich davon? Sind sie korrekt? Wie korrigieren? Wie löschen? Können Sie in falsche Hände geraten? …

dieter.carbon@trutzbox.de

Schadsoftware „verstehen“

Zielsetzung Schadsoftware

1. Aufzeichnen der Tastatureingaben
2. Auslesen von Passwörtern
3. Herunterladen von Dateien auf ein Ziel-System
4. Heraufladen von Dateien von einem Ziel-Syster
5. Vorbereitungen treffen
6. Unbemerktes Ausspionieren
7. Kontrolle unbemerkt ausüben
8. Voraussetzungen (z.B. für Erpressung) scha
9. Schwache Manipulation
10. Starke Manipulation
11. Schwache Störung
12. Starke (Zer-)Störung

Verbreitung Sch

1. über Dateiar
2. über Link in
3. über Link auf einer W
4. über Wechseldatenträger

FAS 31.01.2021

IM GESPRÄCH

Unerkannt und mit äußerster Präzision

Der „Solarwinds-Hack“ lief monatelang unbemerkt über Tausende Rechner. Der Angriff gilt als ein Meisterwerk der Computerspionage – und ist vielleicht noch lange nicht zu Ende.

Von Piotr Heller

dieter.carbon@trutzbox.de

Supply Chain Attack: „Solarwinds-Hack“ (1/4)

- Ca. 250 US-Behörden und -Unternehmen (u.a. Heimatschutzministerium, Nationale Verwaltung für Nukleare Sicherheit, Cisco, Microsoft) betroffen
- Hohes Ziel: lange unbemerkt zu bleiben
- Start vermutlich September 2019
- Phase 1:
  - Erkundung Solarwinds mit Plattform „Orion“ mit ca. 30.000 Firmen- und Behörden-Kunden;
  - Orion-Updates kommen von Solarwinds;
  - Angreifer-Ziel: Updates mit Schadprogrammen versehen, um Zugang zu Solarwinds-Kunden zu erhalten.
  - Hintergrund: Updates erhalten Hersteller-Zertifikat, welches Zielsystem Bonität bestätigt.
  - Angreifer-Notwendigkeit: um Updates vor Zertifizierung zu manipulieren, muss Zugang zu Solarwinds-Systemen erfolgen.
  - Experten vermuten Zugang über schwaches Passwort.
  - Zugang besteht mindestens seit 04.09.2019.
  - Angreifer konnten Orion-Update vom Oktober manipulieren, aber ohne Schadsoftware zu verbreiten.
  - Schadcode wurde nicht im Quellcode eingefügt, sondern im Kompilierungsprozess in das Endprodukt direkt eingesetzt
  - Oktober-Update war vermutlich Testlauf;
  - Angreifer konnten feststellen, dass verfälschter Update unerkannt blieb.

FAZ vom 31.01.2021

Supply Chain Attack: „Solarwinds-Hack“ (2/4)

- Phase 2:
  - Orion-Update vom 20.02.2020 war mit Schadprogramm manipuliet.
  - Fireeye-Experten tauften diesen Update: Sunburst;
  - Ab März 2020 verteilt Solarwinds das verseuchte Update unbemerkt an 18.000 Kunden.
  - Bei mindestens 40 Firmen erfolgten manuelle Folgeaktivitäten
  - Trickreich:
    - Code-Änderungen waren derart, dass menschliche Prüfer sie übersehen konnten.
    - Zusatz-Funktionen waren im Solarwinds-Entwickler-Jargon benannt.
    - Angreifer-Code war neu, sodass bekannte Schadsoftware-Signaturen nicht griffen.
    - Sunburst wurde erst 2 Wochen nach Update aktiv mit Umgebungstest.
    - Umgebungstest prüfte, ob Sunburst in isolierter Test-Umgebung läuft (also Erkennung!?).
    - Sunburst prüft, ob Sicherheitssoftware im Einsatz; falls ja, bleibt Sunburst inaktiv.
    - Wenn Sunburst sich sicher fühlt, baut Schadsoftware Verbindung zu Angreifer-Control & Command Server auf über US-Server, da NSA nur internationale Verbindungen prüft.
    - Alle Befehle wurden als legitime Netzwerk-Kommunikation verschickt.
  - Sunburst war eine Backdoor, durch die sich die Angreifer in den infiltrierten Systemen umsahen und Änderungen vornahmen.
  - Nach Experten waren bis 04.06.2020 ausreichend viele Ziele infiltriert.
  - Die Angreifern verwischen die Spuren des Brückenkopfs indem sie die Manipulationen wieder aus den Solarwinds-Updates entfernen.

FAZ vom 31.01.2021

dieter.carbon@trutzbox.de

Privacy made in Germany

Supply Chain Attack: „Solarwinds-Hack“ (3/4)

- Phase 3:
  - Auf interessanten Netzwerken wird weitere Software nachgeladen, um tiefer in die Systeme einzudringen.
  - Zwischenziel: Verbindung zwischen Schadsoftware und Brückenkopf (Sunburst) verschleiern.
  - Selbst wenn Schafsoftware entdeckt würde, sollte Sunburst unabhängig bleiben und weitere Schadsoftware nachladen können.
  - Die Installation der Spionageprogramme erfolgte in einem Standard-Prozess des Zielrechners, welcher von sich aus ab und zu gestartet wurde.
  - Spionagesoftware wurde auf jedem Zielsystem unter anderem Namen installiert (beim Auffallen würde ein Durchsuchen auf anderen Rechnern nach gleichem Namen nichts nützen).
  - Bevor die Schadsoftware erhöhten Netzwerkbedarf hat, welcher ggf. einer Firewall auffallen würde, werden vor der Kommunikation die Firewall-Einstellungen geändert und nach der Übertragung wieder rückgängig gemacht.

Aufwand, Detail-Liebe und Ziel-Auswahl lassen staatlichen Angreifer vermuten. Tatsächliche Täterherkunft ist unklar.

Ebenfalls unklar: ob schon alle Schadsoftware-Komponenten gefunden wurden.

Supply Chain Attack: „Solarwinds-Hack“ (4/4)

BSI-Bewertung zu SolarWinds

„Als *Angriffsvektor* sind manipulierte Software-Installationsdateien oder -Updates geeignet, um verbreitete Detektionsmaßnahmen zu unterlaufen. Wenn die Angreifer in den späteren Phasen des Angriffs, wie im vorliegenden Fall, vor allem legitime Administrationswerkzeuge und gestohlene Zugangsdaten verwenden, kann der Angriff lange unentdeckt bleiben. Je nach Verbreitung der manipulierten Software können die Angreifer Zugriff auf eine hohe Zahl an Netzwerken und Systemen erlangen. Für Kundinnen und Kunden von Software-Produkten sind Supply-Chain-Angriffe nur schwierig zu erkennen. Die wichtigsten Akteure, die das Einbringen von Schadcode in Software-Produkte verhindern können, sind die Hersteller selbst. Entwicklungs- und Auslieferungssysteme bedürfen eines entsprechend hohen Sicherheitsniveaus.

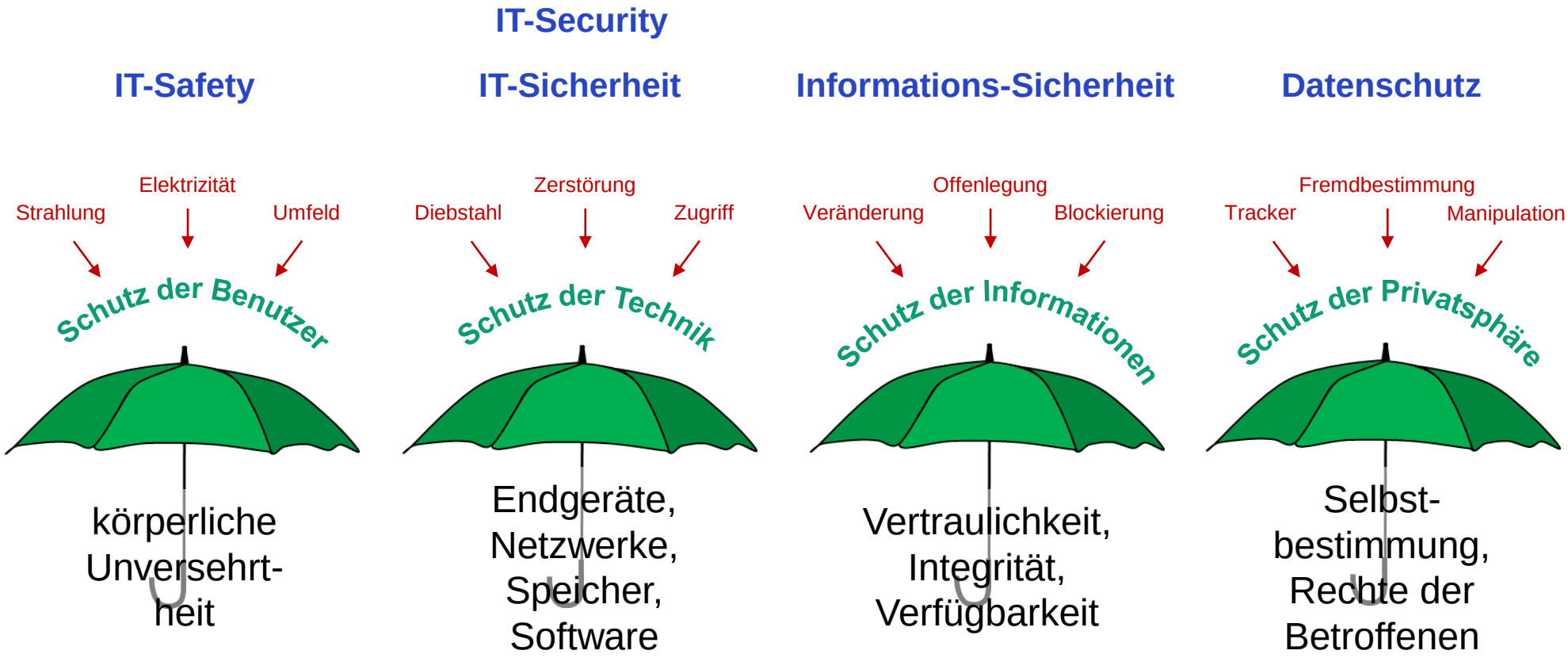
… Auch der Aufwand und die Kompetenz der Angreifer, lange unentdeckt zu bleiben, muss als technischer Meilenstein gewertet werden, der Anlass zur Sorge gibt.

… Einig sind sich die bei den Untersuchungen beteiligten Stellen darin, dass es bisher keine Anzeichen für Sabotage gegeben hat, obwohl dies in großem Umfang möglich gewesen wäre.

… Auch grundlegende Fragen wurden aufgeworfen, etwa, ob Abschreckung durch offensive Cyber-Fähigkeiten funktionieren kann und ausgebaut werden sollte.

… Eine weitere Diskussion entspann sich entlang der Frage, ob dieser massive Supply-Chain-Angriff internationale Cyber-Normen verletzt habe, und wenn nicht, ob zusätzliche Normen entwickelt werden müssten. Erst wenn solche Verhaltensregeln international etabliert sind, können Verletzungen dieser Normen politisch oder juristisch geahndet werden.“

Sprachgebrauch



dieter.carbon@trutzbox.de

Wahrheit in der IT … selbstverständlich?

Die 3 Basis-Schutzziele

• Vertraulichkeit	Confidentiality	C		
• Integrität	Integrity	I	Authentizität	Absender Inhalt
• Verfügbarkeit	Availability	A		

Wahrheit - was ist wahr?

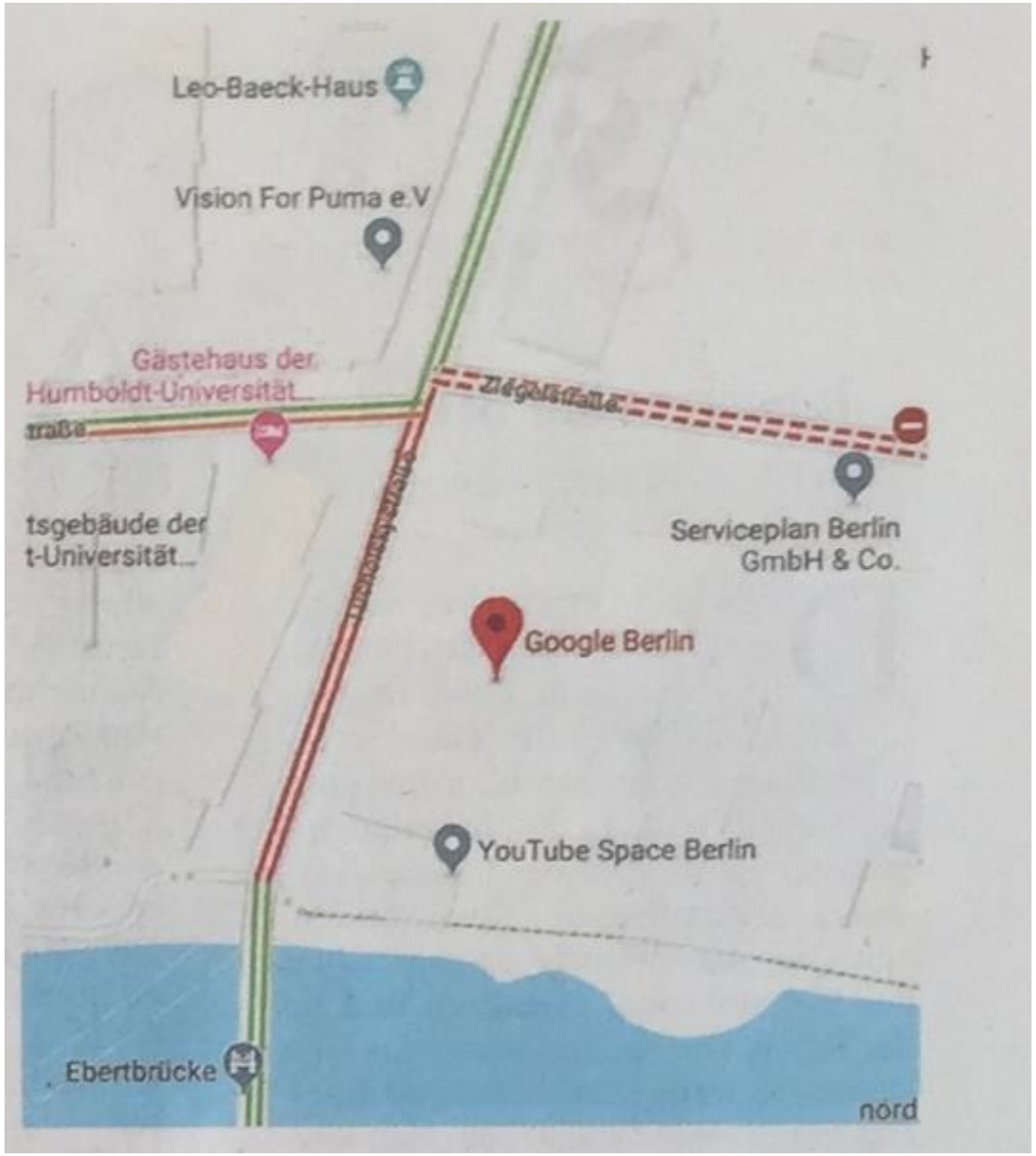
Vertrauen – wem kann ich trauen?

Verschlüsselung & Signatur

dieter.carbon@trutzbox.de

Privacy made in Germany

Wahrheit, Vertrauen



dieter.carbon@trutzbox.de

Wahrheit, Vertrauen

dieter.carbon@trutzbox.de

Wahrheit, Vertrauen

„Diese Realität gibt es nicht“

FAZ 4.2.2020

Der Berliner Künstler Simon Weckert über einen erfundenen Stau, 15 Jahre Google Maps und die Macht von Apps

Herr Weckert, Sie haben ein Video veröffentlicht, in dem zu sehen sein soll, wie man Google Maps manipulieren kann: Nutzern des Navigationsdienstes wurde auf einer Straße in Berlin ein Stau angezeigt, obwohl dort keine Autos unterwegs waren, sondern nur ein Mann mit einem Handkarren, in dem 99 Smartphones lagen. Wie kamen Sie auf die Idee?

Auf einer Demonstration am 1. Mai in Berlin ist mir aufgefallen, dass für komplett Kreuzberg ein Superstau angezeigt wurde – dabei war überhaupt kein Auto unterwegs. Das fand ich sehr interessant. Offenbar hatte Google Zugriff auf die Handydaten der Demonstranten, obwohl da mit Sicherheit kaum jemand Google Maps aktiviert hatte. Ich habe mir dann während der Hongkonger Proteste mal die Karte der Stadt angesehen. Da war es genauso.

Und das wollten Sie simulieren?

Genau. Die Frage war: wie? Man hätte natürlich einen Flashmob mit 100 Leuten organisieren können. Aber das wäre zu einfach gewesen. Mir ist außerdem aufgefallen, dass ich die Leute gar nicht brauche – sondern nur die Smartphones. Im Internet habe ich Anbieter gefunden, die Smartphones verleihen, das wird zum Beispiel bei Messen genutzt. Also habe ich mir für einen Tag 99 Smartphones ausgeliehen, in einen Handkarren geladen und bin damit durch die Stadt gefahren. Die Aktion ist schon eine Weile her, ich habe das Video jetzt veröffentlicht, weil Google Maps in dieser Woche 15 Jahre alt wird.

Hatten die Smartphones alle eine Sim-Karte?

Genau, und Google Maps war auf jedem Smartphone eingeschaltet und hat zu einer Adresse navigiert. Ich hatte das Gefühl, dass es so besser funktioniert. Wegen meiner Erfahrungen auf der Demonstration glaube ich aber, dass es auch ohne aktivierte App funktionieren würde. Das müsste man noch mal ausprobieren. Auf den Straßen in Berlin haben wir verschiedene Rhythmen getestet, mal sind wir gerannt, dann haben wir Stop-and-go simuliert. Bewegung ist immer notwendig, sonst reagiert die App nicht.

Wie schnell reagiert das System?

In Echtzeit. Bei Google Maps sieht man schon, wenn Autos an einer roten Ampel stehen. Ist viel Verkehr, färbt sich die Straße auf der Karte orange. Und Rot heißt: Stau. Dann wird anderen Autofahrern eine andere Strecke empfohlen. Um eine Straße rot zu bekommen, mussten wir mit dem Karren öfter hin und her laufen. Wir haben eine Stunde an einem Ort verbracht, bis das geklappt hat. In dem Video sieht man, wie die Straße langsam orange und irgendwann rot wird.

Was ist passiert, wenn ein Auto an Ihnen vorbeigefahren ist?

Dann wurde kein Stau mehr angezeigt, das hat das System also erkannt.

Was haben Sie noch über Google Maps gelernt?

Ich finde die physischen Auswirkungen, die so ein digitales Produkt hat, interessant. Wenn auf einer Autobahn Stau ist, werden alle Autos durch die Stadt geschickt, obwohl die städtische Infrastruktur darauf vielleicht gar nicht ausgelegt ist. Es gibt wissenschaftliche Papiere, in denen steht, dass es besser wäre, die Autos in so einem Fall in den Stau zu führen. Außerdem hat es Google Maps in den vergangenen 15 Jahren geschafft, dass jeder nur noch an diese App denkt, wenn es um Landkarten geht. Dabei gibt es Alternativen. Wieso basieren so viele andere Apps auf Google Maps, Uber zum Beispiel? Autofirmen nutzen das System sogar, um selbstfahrende Autos zu entwickeln. Ist es wirklich richtig, dass wir alle dieses eine zentrale System nutzen, oder wäre es sinnvoller, die Daten untereinander zu teilen und eigene Dienste zu entwickeln? Die könnten einen zum Beispiel zu freien Parkplätzen führen.

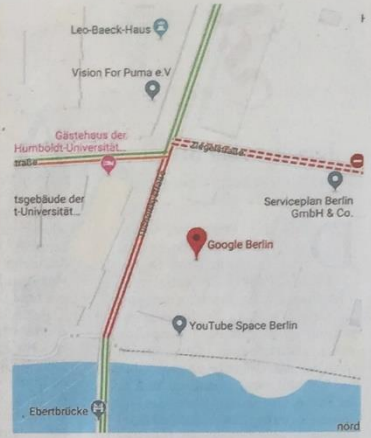
Aber Google Maps funktioniert ja gerade so gut, weil es so viele Menschen nutzen. Und ich möchte ja nicht aufgrund irgendwelcher wissenschaftlicher Papiere in einen Stau geleitet werden.

Klar, es gibt Vorteile – aber auch Nachteile. Ich bin Künstler, mich interessiert, wie Technologien unsere Gesellschaft formen. Ein berühmtes Zitat lautet: „We shape our tools, and then our tools shape us.“ Und so ist es – wir passen uns immer mehr der Technologie an, anstatt andersherum. Das zeigt meine Aktion: Wir glauben, dass diese Karten uns die Realität anzeigen, und passen unser Verhalten an diese Realität an. Dabei gibt es diese Realität nicht. Das lässt sich auf viele andere Apps übertragen: von Airbnb bis zu Tinder.

Die Fragen stellte **Sebastian Eder.**

dieter.carbon@trutzbox.de
Privacy made in Germany

Wahrheit, Vertrauen



Ein Stau ohne Autos: *Der Berliner Künstler Simon Weckert hat einen Handkarren voller Smartphones genutzt, um auf Google Maps ein Verkehrschaos zu simulieren.* Fotos Simon Weckert

„Diese Realität gibt es nicht“

FAZ 4.2.2020

Der Berliner Künstler Simon Weckert über einen erfundenen Stau, 15 Jahre Google Maps und die Macht von Apps

Herr Weckert, Sie haben ein Video veröffentlicht, in dem zu sehen sein soll, wie man Google Maps manipulieren kann: Nutzern des Navigationsdienstes wurde auf einer Straße in Berlin ein Stau angezeigt, obwohl dort keine Autos unterwegs waren, sondern nur ein Mann mit einem Handkarren, in dem 99 Smartphones lagen. Wie kamen Sie auf die Idee?

Auf einer Demonstration am 1. Mai in Berlin ist mir aufgefallen, dass für komplett Kreuzberg ein Superstau angezeigt wurde – dabei war überhaupt kein Auto unterwegs. Das fand ich sehr interessant. Offenbar hatte Google Zugriff auf die Handydaten der Demonstranten, obwohl da mit Sicherheit kaum jemand Google Maps aktiviert hatte. Ich habe mir dann während der Hongkonger Proteste mal die Karte der Stadt angesehen. Da war es genauso.

Und das wollten Sie simulieren?

Genau. Die Frage war: wie? Man hätte natürlich einen Flashmob mit 100 Leuten organisieren können. Aber das wäre zu einfach gewesen. Mir ist außerdem aufgefallen, dass ich die Leute gar nicht brauche – sondern nur die Smartphones. Im Internet habe ich Anbieter gefunden, die Smartphones verleihen, das wird zum Beispiel bei Messen genutzt. Also habe ich mir für einen Tag 99 Smartphones ausgeliehen, in einen Handkarren geladen und bin damit durch die Stadt gefahren. Die Aktion ist schon eine Weile her, ich habe das Video jetzt veröffentlicht, weil Google Maps in dieser Woche 15 Jahre alt wird.

Hatten die Smartphones alle eine Sim-Karte?

Genau, und Google Maps war auf jedem Smartphone eingeschaltet und hat zu einer Adresse navigiert. Ich hatte das Gefühl, dass es so besser funktioniert. Wegen meiner Erfahrungen auf der Demonstration glaube ich aber, dass es auch ohne aktivierte App funktionieren würde. Das müsste man noch mal ausprobieren. Auf den Straßen in Berlin haben wir verschiedene Rhythmen getestet, mal sind wir gerannt, dann haben wir Stop-and-go simuliert. Bewegung ist immer notwendig, sonst reagiert die App nicht.

Wie schnell reagiert das System?

In Echtzeit. Bei Google Maps sieht man schon, wenn Autos an einer roten Ampel stehen. Ist viel Verkehr, färbt sich die Straße auf der Karte orange. Und Rot heißt: Stau. Dann wird anderen Autofahrern eine andere Strecke empfohlen. Um eine Straße rot zu bekommen, mussten wir mit dem Karren öfter hin und her laufen. Wir haben eine Stunde an einem Ort verbracht, bis das geklappt hat. In dem Video sieht man, wie die Straße langsam orange und irgendwann rot wird.

Was ist passiert, wenn ein Auto an Ihnen vorbeigefahren ist?

Dann wurde kein Stau mehr angezeigt, das hat das System also erkannt.

Was haben Sie noch über Google Maps gelernt?

Ich finde die physischen Auswirkungen, die so ein digitales Produkt hat, interessant. Wenn auf einer Autobahn Stau ist, werden alle Autos durch die Stadt geschickt, obwohl die städtische Infrastruktur darauf vielleicht gar nicht ausgelegt ist. Es gibt wissenschaftliche Papiere, in denen steht, dass es besser wäre, die Autos in so einem Fall in den Stau zu führen. Außerdem hat es Google Maps in den vergangenen 15 Jahren geschafft, dass jeder nur noch an diese App denkt, wenn es um Landkarten geht. Dabei gibt es Alternativen. Wieso basieren so viele andere Apps auf Google Maps, Uber zum Beispiel? Autofirmen nutzen das System sogar, um selbstfahrende Autos zu entwickeln. Ist es wirklich richtig, dass wir alle dieses eine zentrale System nutzen, oder wäre es sinnvoller, die Daten untereinander zu teilen und eigene Dienste zu entwickeln? Die könnten einen zum Beispiel zu freien Parkplätzen führen.

Aber Google Maps funktioniert ja gerade so gut, weil es so viele Menschen nutzen. Und ich möchte ja nicht aufgrund irgendwelcher wissenschaftlicher Papiere in einen Stau geleitet werden.

Klar, es gibt Vorteile – aber auch Nachteile. Ich bin Künstler, mich interessiert, wie Technologien unsere Gesellschaft formen. Ein berühmtes Zitat lautet: „We shape our tools, and then our tools shape us.“ Und so ist es – wir passen uns immer mehr der Technologie an, anstatt andersherum. Das zeigt meine Aktion: Wir glauben, dass diese Karten uns die Realität anzeigen, und passen unser Verhalten an diese Realität an. Dabei gibt es diese Realität nicht. Das lässt sich auf viele andere Apps übertragen: von Airbnb bis zu Tinder.

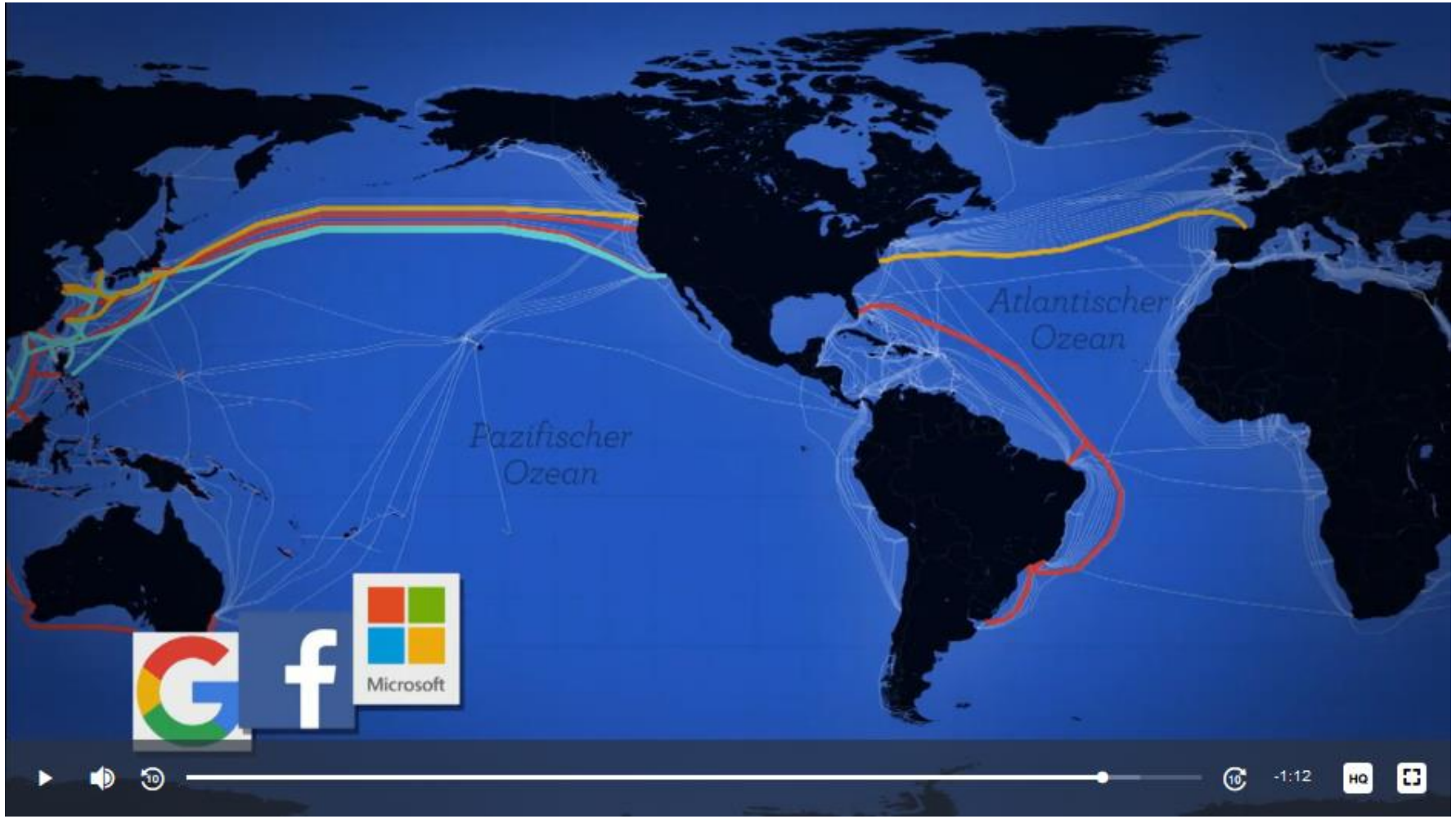
Die Fragen stellte **Sebastian Eder.**

dieter.carbon@trutzbox.de

Mit offenen Karten - Seekabel, der unsichtbare Krieg

https://www.bpb.de/mediathek/303097/seekabel-der-unsichtbare-krieg

Mit offenen Karten - Seekabel, der unsichtbare Krieg



Neuste Seekabel-Verlegungen (2017)

https://www.bpb.de/mediathek/303097/seekabel-der-unsichtbare-krieg

Mit offenen Karten - Seekabel, der unsichtbare Krieg

Die Hotelanlage wurde dem Erdboden gleichgemacht

Nach dem Vulkanausbruch bei Tonga gibt es weiterhin keine Erkenntnisse über die Zahl der Toten und Verletzten

FAZ 18.01.2022

fäh. SINGAPUR. Nach dem gigantischen Ausbruch eines Unterseevulkans in Tonga herrscht immer noch Unklarheit über das Ausmaß der Zerstörung in dem pazifischen Inselstaat. Auch über die Zahl der Toten und Verletzten in dem Land mit 105 000 Einwohnern gab es bis Montag keine Erkenntnisse. Es werden mehrere Personen vermisst, darunter eine Britin, die von dem durch die Eruption ausgelösten Tsunami mitgerissen worden war. Aufgrund eines beschädigten Unterseekabels waren die Telefon- und Internetverbindungen nach Tonga unterbrochen. Angehörige im Ausland warteten gebannt auf Nachrichten ihrer Familienmitglieder. Neuseeland und Australien schickten Militärflugzeuge, um sich ein Bild von der Lage in dem Archipel zu machen. Die beiden Nachbarländer gaben außerdem Soforthilfen von einer Million und einer halben Million Dollar frei. Hilfsorganisationen warnten vor Gesundheitsschäden für die Bevölkerung durch Asche in der Luft und verunreinigtes Trinkwasser. Die einzige Kommunikationsverbindung in den Inselstaat bestand über Satellitentelefon. Australiens Entwicklungs- und Pazifikminister Zed Seselja sprach von „ziemlich besorgniserregenden" Schilder[n] Weg erhalten die Sorge in Inseln des Ar[chipels] völlig von der [Welt] seien. „Nach [den] Informationen, die wir haben, scheint das Ausmaß der Verwüstung ziemlich groß, vor allem auf den vorgelagerten Inseln", sagte Katie Greenwood vom Internationalen Roten Kreuz der Agen[tur] Ausland. Dem Diplomaten zufolge hatte der Tsunami aber besonders das Touristengebiet an der Westküste der Hauptinsel Tongatapu getroffen. Die Besitzer des dort gelegenen Ha'atafu Beach Resort schrieben auf Facebook, dass ihre Hotelanlage vollständig dem Erdboden gleichgemacht sei. „Die gesamte westliche Küstenlinie und das Dorf Kanukupolu sind komplett zerstört" 1,2 Metern gemessen worden. Auch in Neuseeland, Japan, Alaska und Südamerika wurden Tsunamis registriert. In Peru wurden zwei Personen von den starken Wellen getötet.

Explodiert: *Vulkan im Pazifik* Foto AFP

die Eruption ausgelösten Tsunami mitgerissen worden war. Aufgrund eines beschädigten Unterseekabels waren die Telefon- und Internetverbindungen nach Tonga unterbrochen. Angehörige im Ausland warteten gebannt auf Nach-

Passive Gefährdung

beim Surfen?	beim Austausch von E-Mails?	bei Videokonferenzen/Webmeetings?

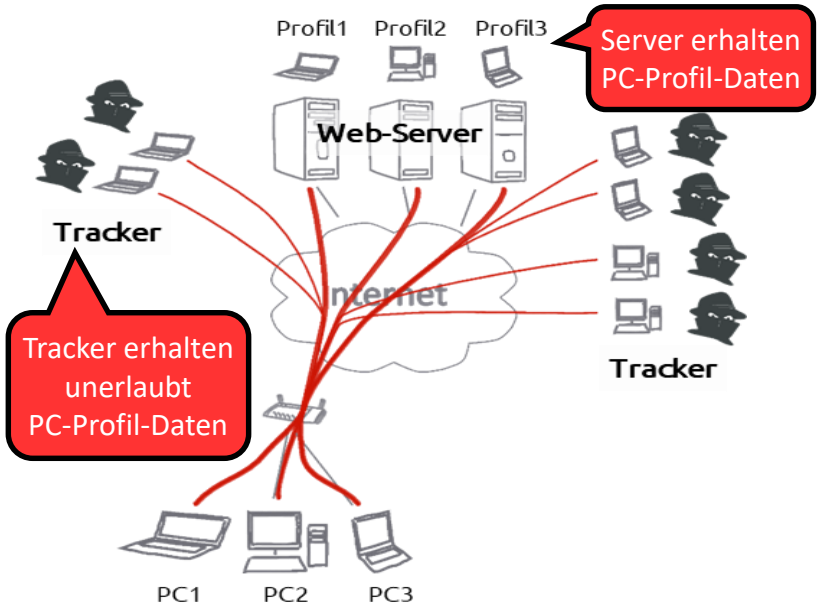
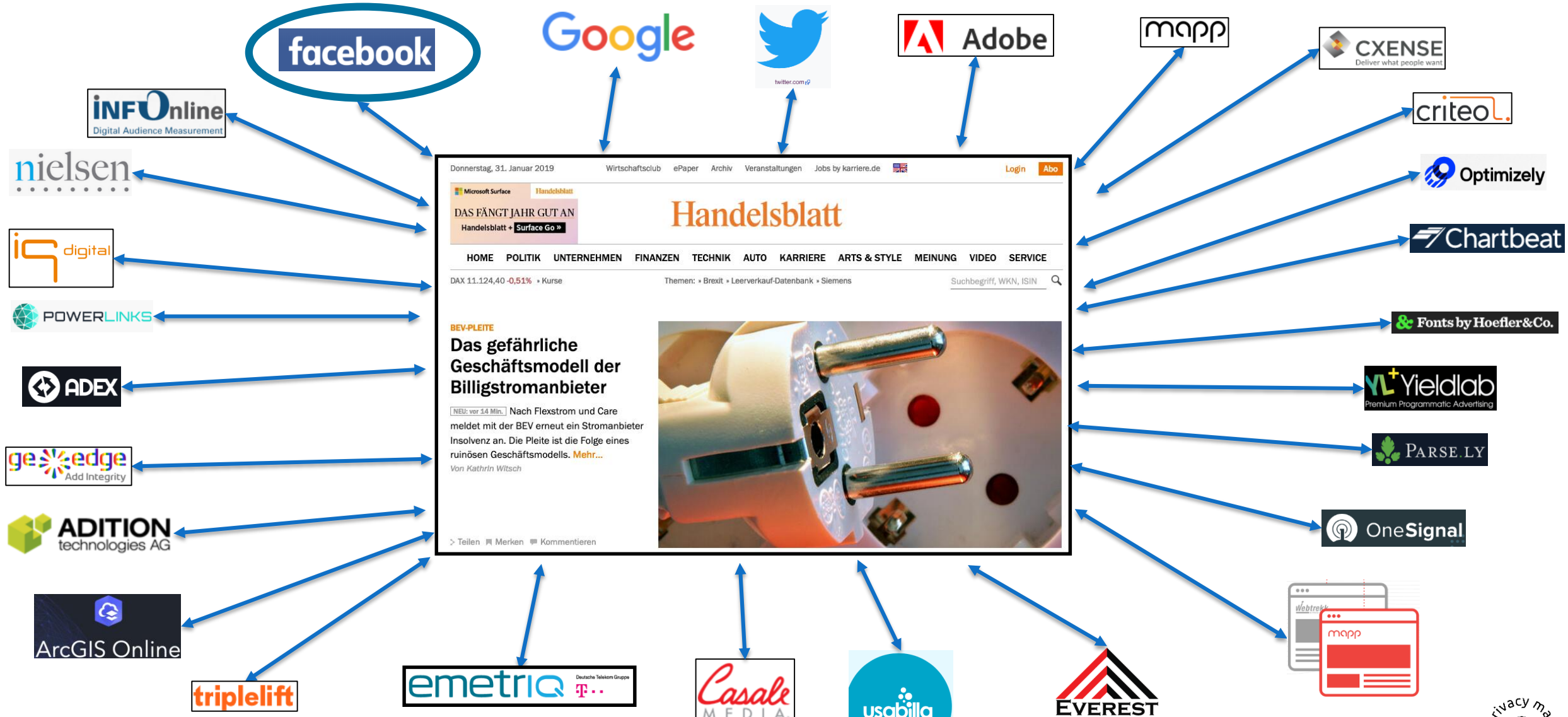


Foto: Comidio GmbH

dieter.carbon@trutzbox.de

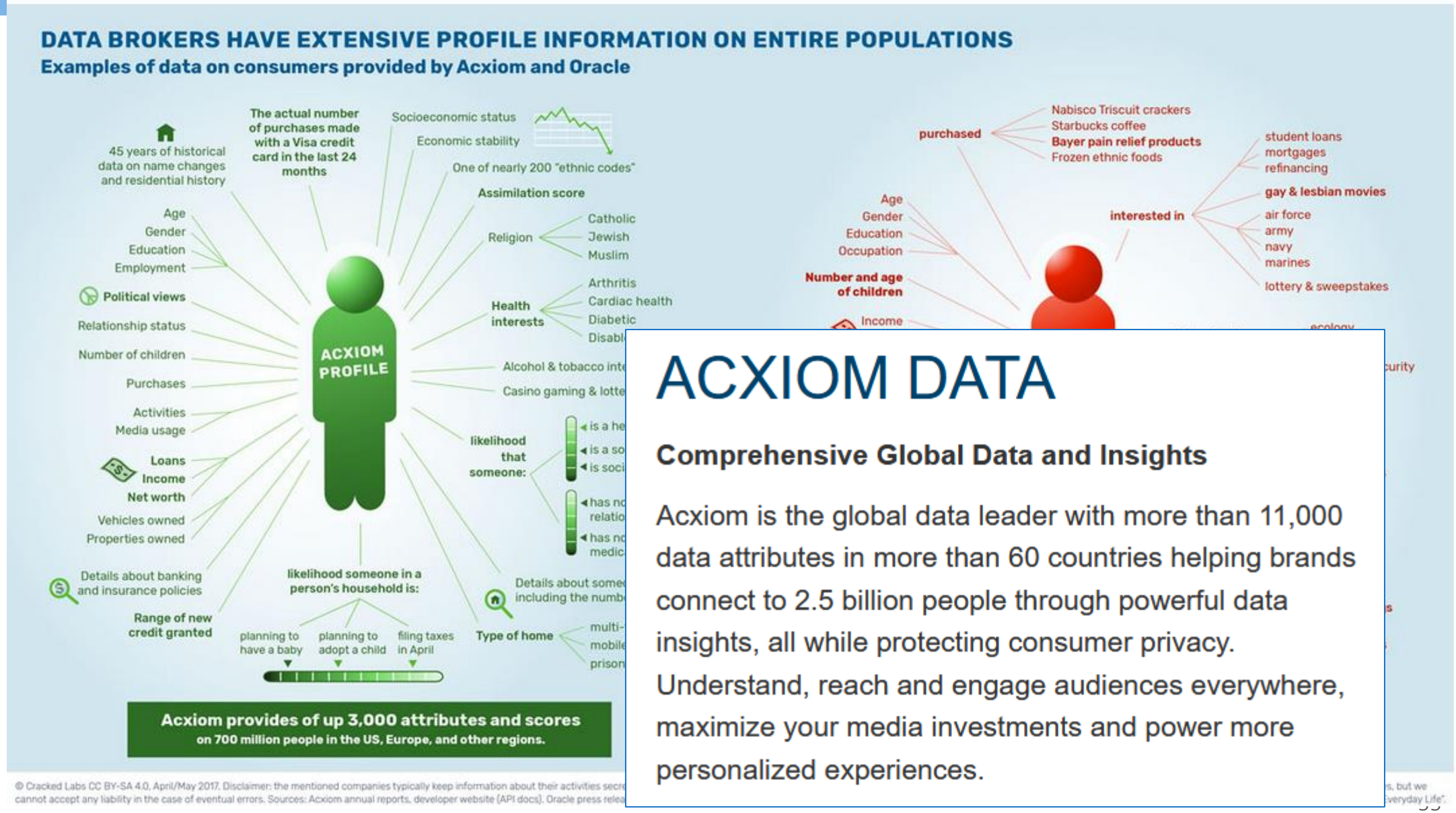
Privacy made in Germany

handelsblatt.de



abgerufen am 26.6.20, also nach Inkrafttreten der Datenschutz-Grundverordnung

Vermutlich Sammler #2 und #3



ACXIOM DATA

Comprehensive Global Data and Insights

Acxiom is the global data leader with more than 11,000 data attributes in more than 60 countries helping brands connect to 2.5 billion people through powerful data insights, all while protecting consumer privacy. Understand, reach and engage audiences everywhere, maximize your media investments and power more personalized experiences.

© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secr... cannot accept any liability in the case of eventual errors. Sources: Acxiom annual reports, developer website (API docs). Oracle press relea...

https://crackedlabs.org/en/corporate-surveillance

https://www.acxiom.com/customer-data/

dieter.carbon@trutzbox.de

Big Five

Bei den Big Five handelt es sich um ein Modell der Persönlichkeitspsychologie. Im Englischen wird es auch als OCEAN-Modell bezeichnet (nach den entsprechenden Anfangsbuchstaben).

		Faktor	schwach ausgeprägt	stark ausgeprägt
O	Openness	Offenheit für Erfahrungen	konservativ, vorsichtig	erfinderisch, neugierig
C	Conscientiousness	Gewissenhaftigkeit	unbekümmert, nachlässig	effektiv, organisiert
E	Extraversion	Extraversion	zurückhaltend, reserviert	gesellig
A	Agreeableness	Verträglichkeit	wettbewerbsorientiert, antagonistisch	kooperativ, freundlich, mitfühlend
N	Neuroticism	Neurotizismus	selbstsicher, ruhig	emotional, verletzlich

https://de.wikipedia.org/wiki/Big_Five_%28Psychologie%29

Cambridge Analytica, CEO Alexander Nix, Zugriff auf Facebook-Profile

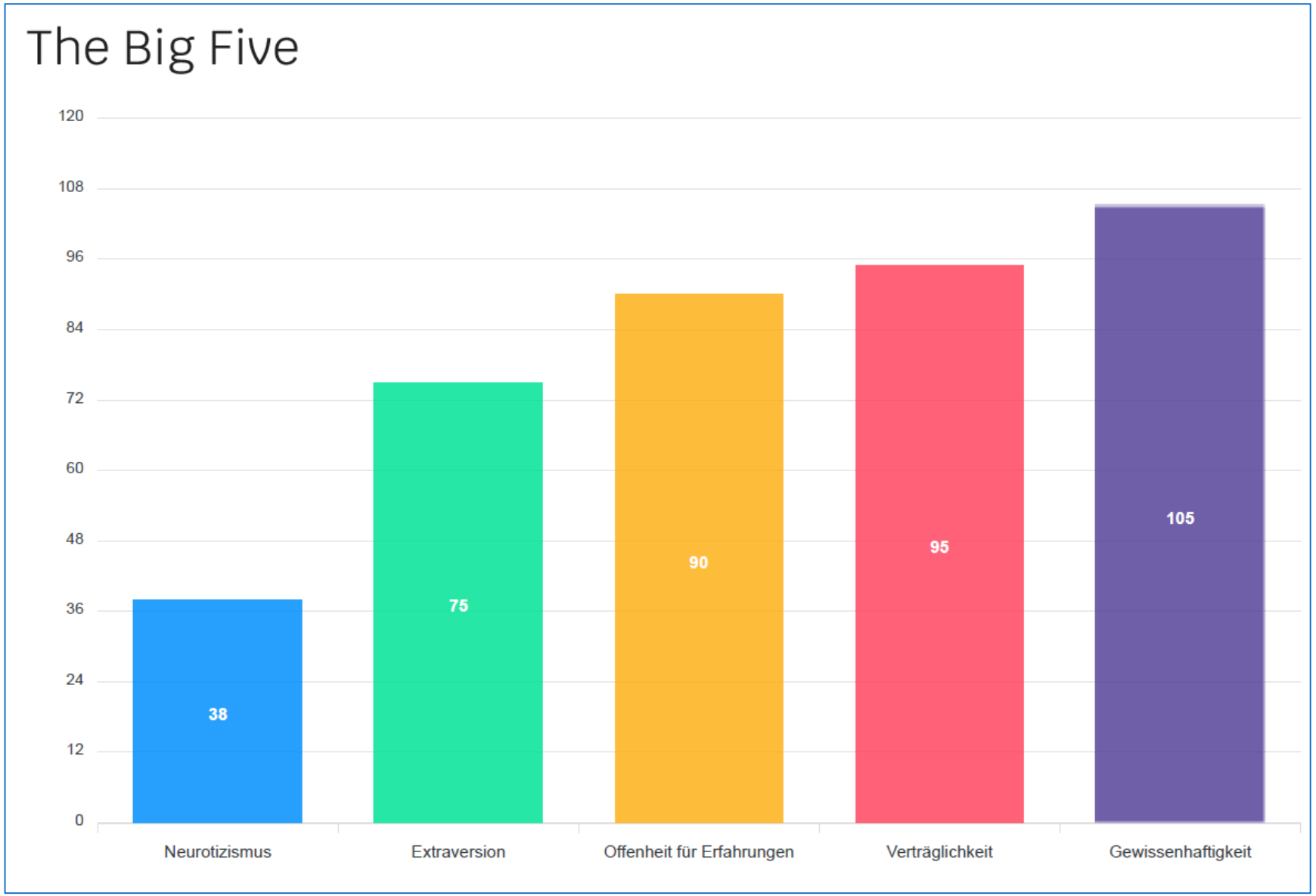
Eine andere Strategie der Identifikation von neuen Zielgruppen für das Targeting ist das Behavioural Targeting. Hierbei werden über das Internetnutzungsverhalten des Users Rückschlüsse gezogen auf bestimmte Eigenschaften wie Alter, Geschlecht, Einkommensniveau und Interessen und daraus dann Zielgruppen für die jeweiligen Kampagnen zusammengestellt.

https://onlinemarketing.de/lexikon/definition-new-audience-targeting

dieter.carbon@trutzbox.de

Privacy made in Germany

Big Five


The Big Five
120
108
96
84
72
60
48
36
24
12
0
38
75
90
95
105
Neurotizismus
Extraversion
Offenheit für Erfahrungen
Verträglichkeit
Gewissenhaftigkeit

Real Time Bidding

Werbe-fenster

Fingerprint des Webseiten-Besuchers oder App-Aufrufers wird zum Vermarkter geschickt

Ihr Profil wird mit vorangegangener „Beobachtung“ ergänzt

Onboarding-Provider

factual

ORACLE DATA CLOUD

bluekai

Datalogix

acxiom

LiveRamp an acxiom company

Ihr Profil wird auf einer Versteigerungsplattform angeboten

Dabei wird Ihr Profil weiter verbreitet

Versteigerungsplattform sucht nach besten Angeboten für Ihr Profil

Der „beste“ Anbieter bekommt den Zuschlag für die Werbefläche in Ihrem Browser/App

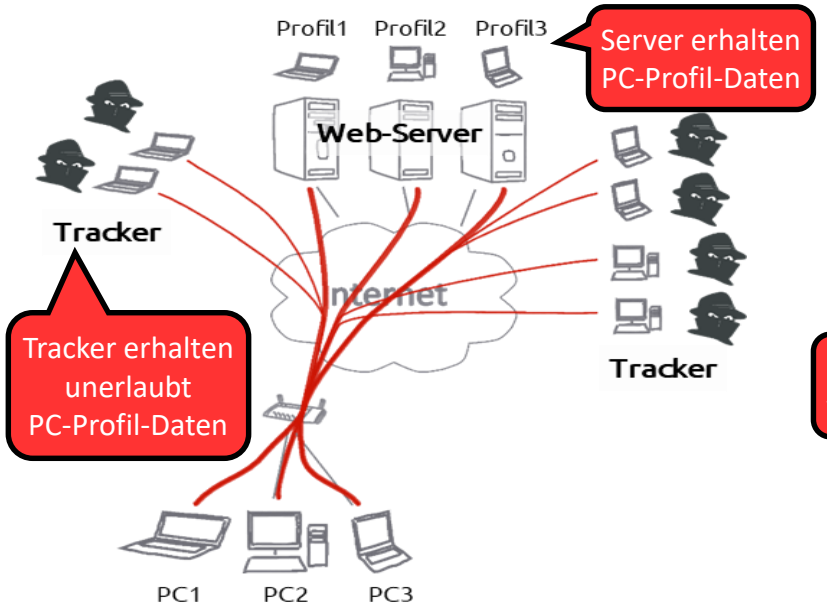
Werbefläche wird Angezeigt

100 ms

Eigene Recherche

Passive Gefährdung

beim Surfen?	beim Austausch von E-Mails?	bei Videokonferenzen/Webmeetings?



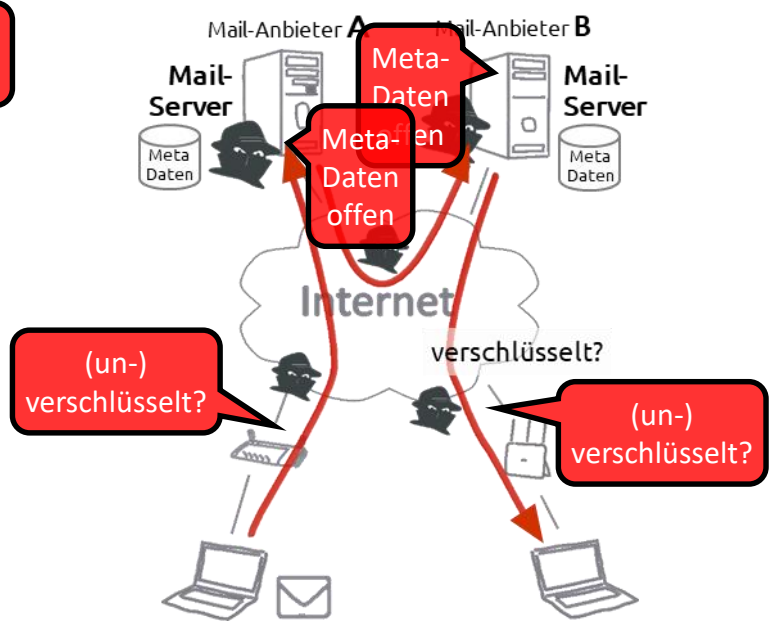
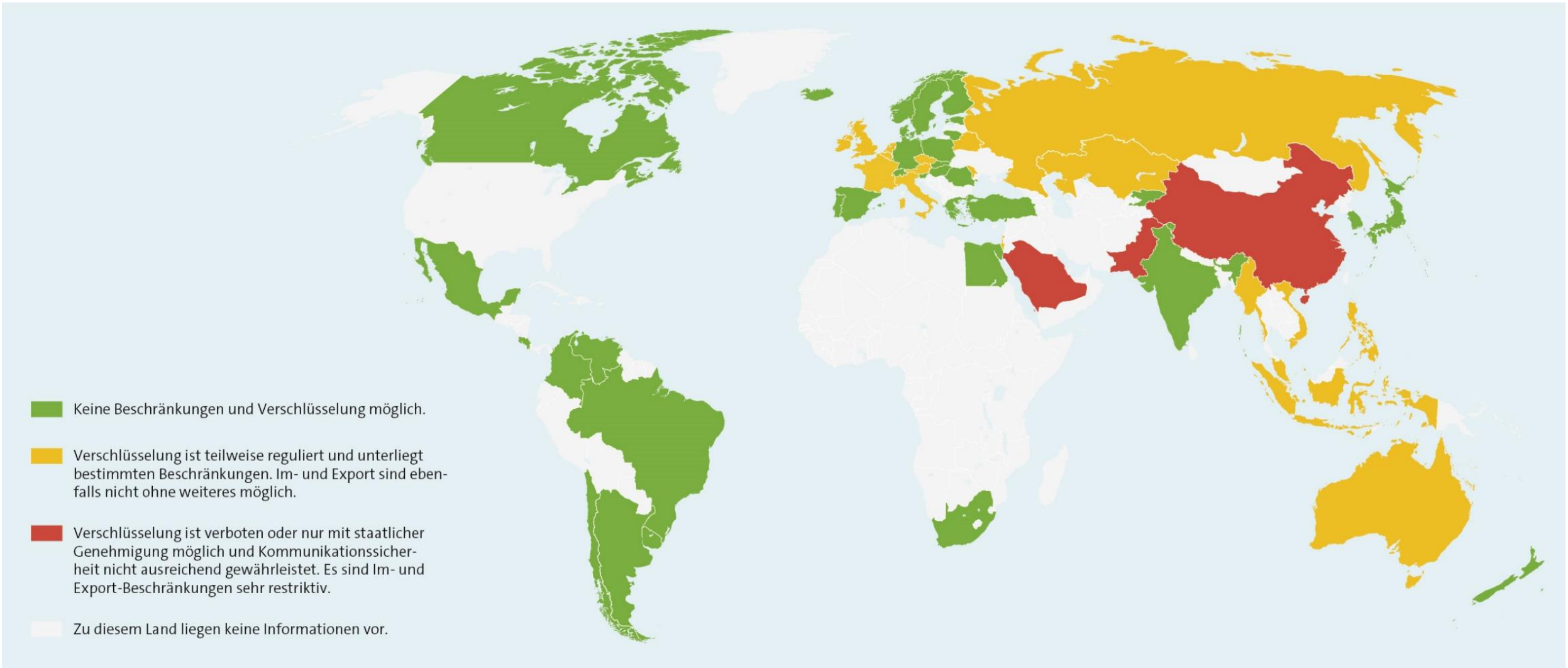


Foto: Comidio GmbH

- Ist der Absender der Absender?
- Ist der Inhalt der Inhalt?

dieter.carbon@trutzbox.de

Der Crypto-Atlas



https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Oeffentliche-Sicherheit-Wirtschaftsschutz/Crypto-Atlas-2.html

Frau Merkel … „Skypen, Telefonate, Mails … „

Warum empfiehlt Merkel eine amerikanische Software?

Fernsehansprache: „Merkel-Rede dominiert", FR-Feuilleton vom 20. März

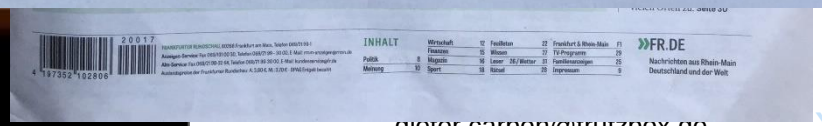
Der Fernseh-Appell unserer Bundeskanzlerin zur Pandemie war und ist meines Erachtens notwendig, sinnvoll und hilfreich angesichts des analogen Corona Virus; auch hat sie inhaltlich und im Ton die richtigen Worte gefunden. Leider kann ich dies bezüglich ihrer digitalen Empfehlungen nicht bestätigen. In ihrer zusammenfassenden Aufforderung „Wege finden, um Zuneigung und Freundschaft zu zeigen" empfiehlt sie an erster Stelle die Nutzung von Skype. Skype ist ein vermeintlich kostenloser Video Konferenz Service des amerikanischen Unternehmens Microsoft, welches Nutzungsdaten sammelt, analysiert, vermarktet und mittlerweile auch vom Innenministerium kritisch beurteilt wird. Zu Recht hat Frau Dr. Merkel vor analogen Viren gewarnt, aber bitte doch nicht mit der aktiven Empfehlung, quasi „digitale Viren" einzusetzen.

Warum macht Frau Merkel nicht auch Produktwerbung für 20 andere Videokonferenz-Tools? Warum nutzt sie nicht deutsche Lösungen? Wir, ein Team von acht Personen, haben vor fünf Jahren ein Start-Up gegründet, um uns um die digitalen Viren zu kümmern, haben jahrelang ohne Fremdmittel oder Zuschüsse geforscht und erfolgreich einen „digitalen Impfstoff" zur Durchführung von unabhängigen, sicheren und anonymen Videokonferenzen entwickelt. Nein, ich nenne nicht den Namen unseres „digitalen Medikaments", denn es geht mir nicht um Werbung, sondern um das Prinzip. Warum also empfiehlt die Kanzlerin den Einsatz eines der weltweit größten Datensammler, nämlich Microsoft?

Es gibt deutsche Lösungen, mit denen Videokonferenzen mit unbegrenzter Teilnehmerzahl in einer unbegrenzten Anzahl von Räumen gleichzeitig durchgeführt werden können. Der Hauptvorteil: ohne dass Dritte (z.B. Internet- oder Webmeeting-Anbieter) mithören, mitschreiben, mitlesen können.

Seit Jahren ist Frau Merkel verantwortungsvoll und erfolgreich für Deutschland tätig; bitte erst recht auch auf digitalem Gebiet: Videokonferenzen ja, aber keine halben Sachen. Und die Kanzlerin möge bitte auch nicht nach uns „googeln".

Dieter Carbon, Eltville



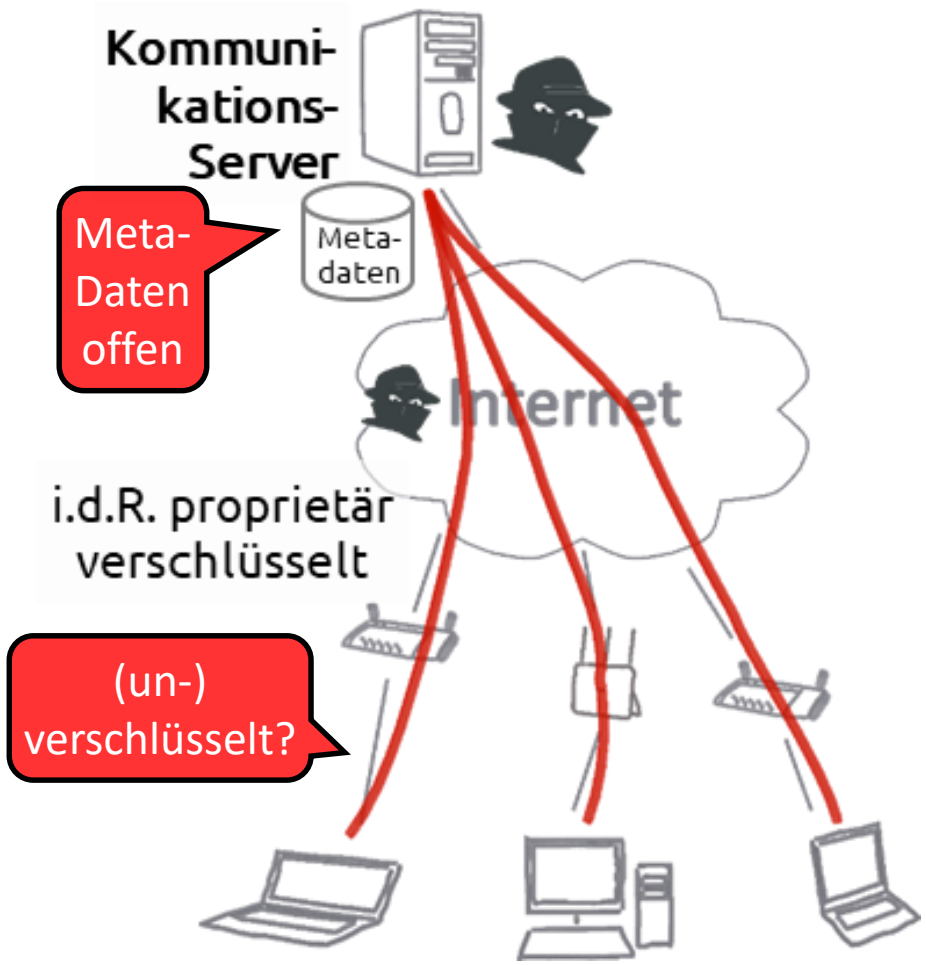
dieter.carbon@trutzbox.de

Privacy made in Germany

Passive Gefährdung … und Abhilfe

offene Metadaten und ggf. Inhaltsdaten beim Anbieter

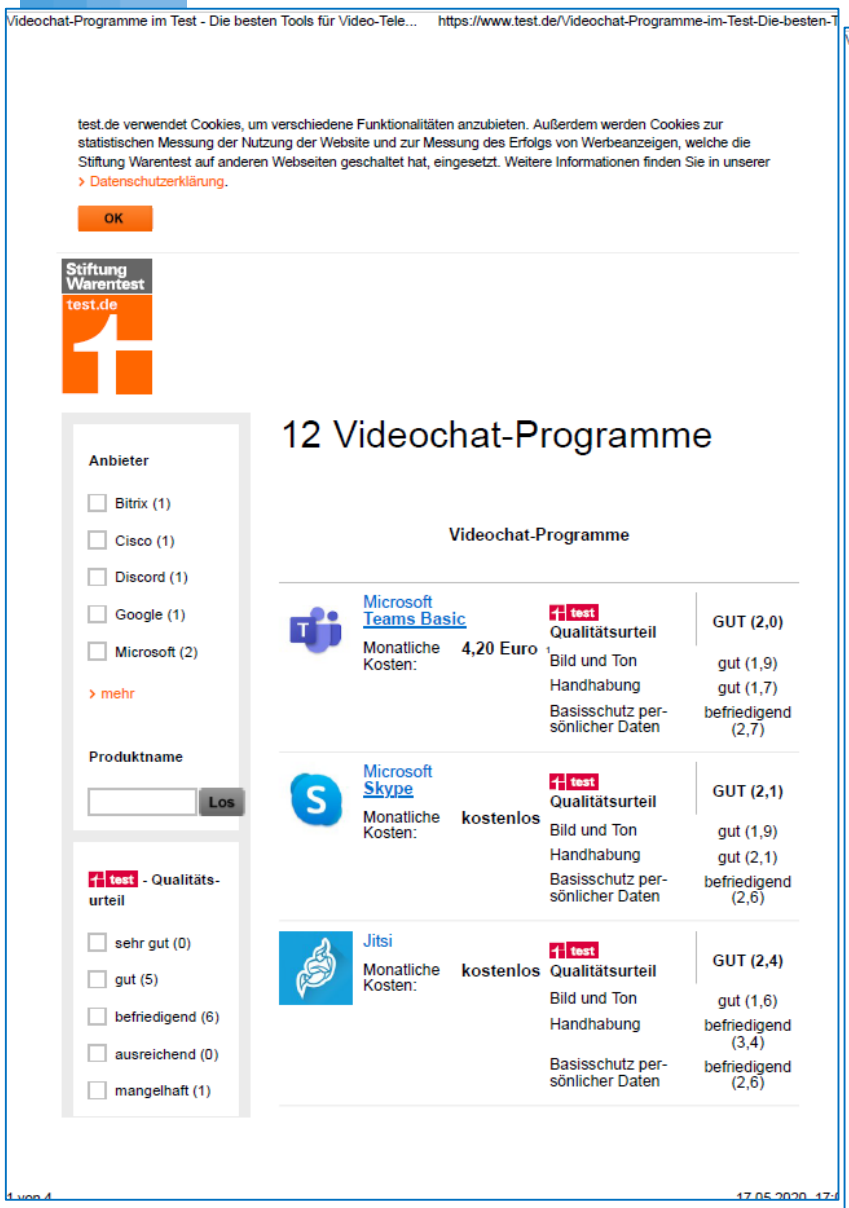
Chat-, Audio-, Video-Kommunikations-Anbieter

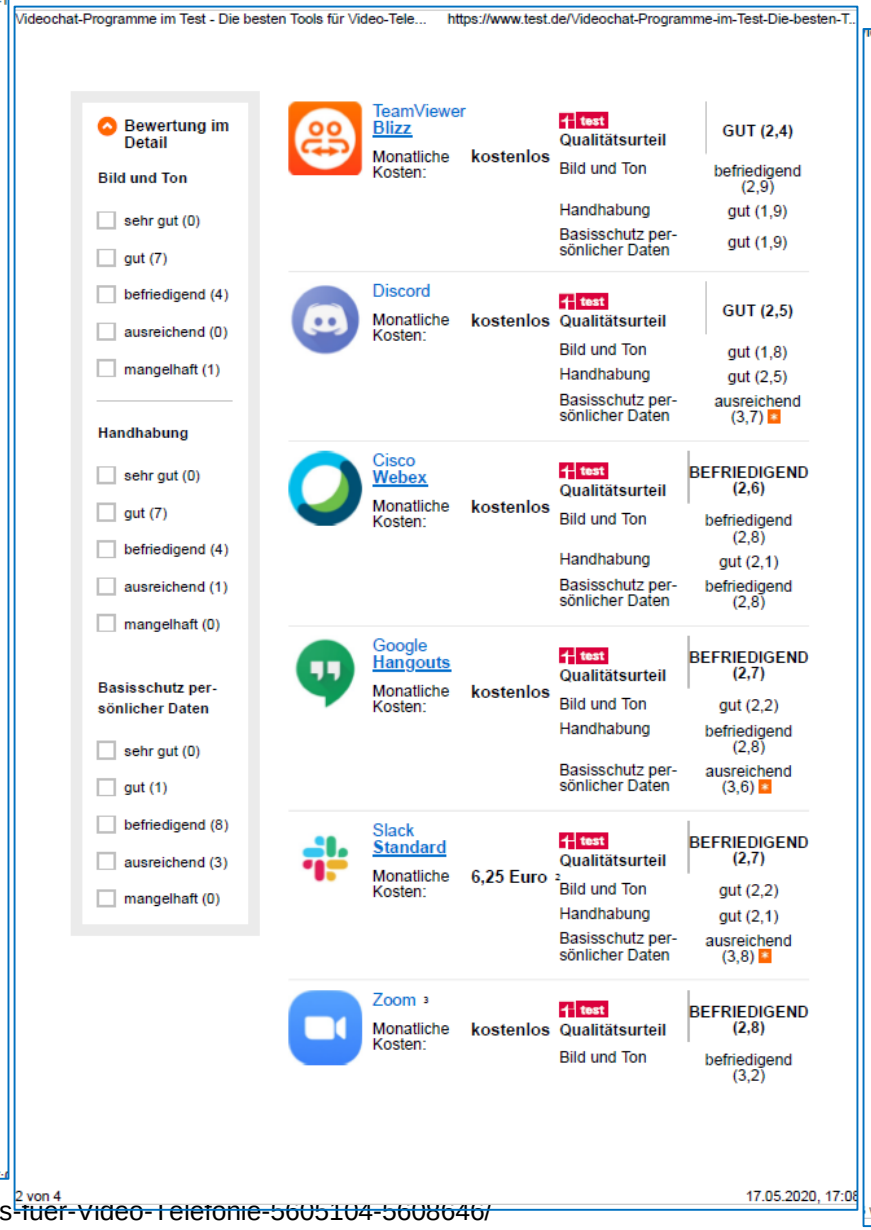


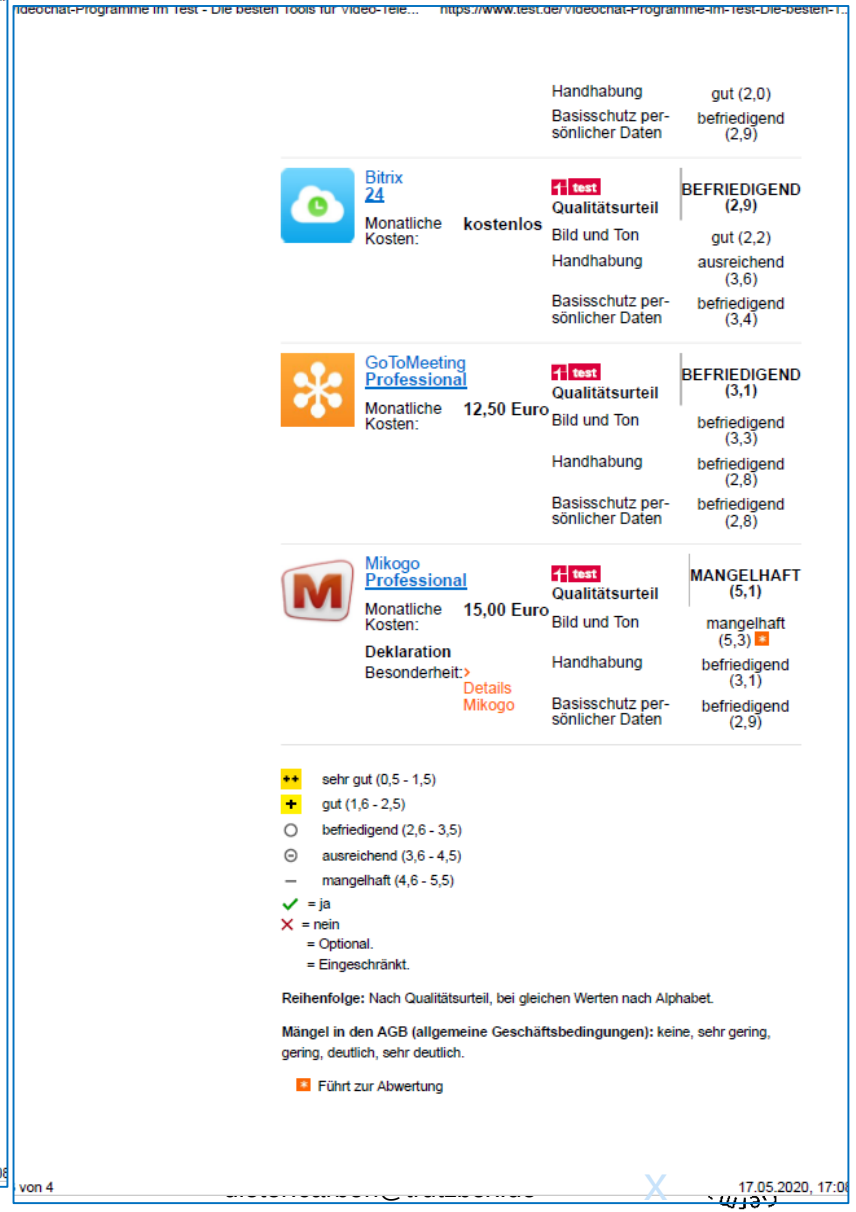
dieter.carbon@trutzbox.de

Webmeeting Anbieter

13.05.2020







https://www.test.de/Videochat-Programme-im-Test-Die-besten-Tools-fuer-Video-Telefonie-5605104-5608646/

Webmeeting Anbieter

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen

Die Vorsorgemaßnahmen zur Eindämmung der Corona-Pandemie führen in nahezu allen Bereichen des täglichen Lebens zu Einschränkungen. Um physische Nähe zwischen Menschen möglichst zu vermeiden, gehört hierzu in sehr vielen Fällen, dass berufliche Kontakte nicht mehr persönlich, sondern über das Netz gehalten werden. Wenn mehr als zwei, drei Personen eine gemeinsame Unterredung führen wollen, werden nun Telefon- und Videokonferenzen abgehalten. Viele Unternehmen und Behörden suchen gut funktionierende Angebote für deren Durchführung und stellen zunächst die Prüfung zurück, ob sie auch datenschutzgerecht in Anspruch genommen werden können.

Mit diesem Text möchte die Berliner Beauftragte für Datenschutz und Informationsfreiheit den Unternehmen, Behörden und anderen ihrer Aufsicht unterliegenden Institutionen Hinweise zu den Anforderungen an die Nutzung von Videokonferenzsystemen geben und die Risiken beschreiben, die entstehen, wenn sie nicht eingehalten werden. Um diese Risiken zu vermeiden oder zumindest zu mindern und die datenschutzrechtlichen Vorgaben einzuhalten, sind die Verantwortlichen aufgerufen, kurzfristig eingesetzte, aber nicht datenschutzgerechte Lösungen sobald wie möglich durch datenschutzgerechte zu ersetzen.

Personenbezogene Daten in Videokonferenzen

Personenbezogene Daten spielen bei der Durchführung von Videokonferenzen auf zwei Weisen eine Rolle: Erstens kann das gesprochene Wort selbst Informationen über einzelne Personen enthalten. Zweitens fallen bei der Durchführung einer Videokonferenz auch Daten über die Teilnehmerinnen und Teilnehmer an, d. h. ihre Kontaktdaten, ihre Namen sowie Angaben über Zeit und Ort ihrer Teilnahme an der Konferenz. Darunter sind auf jeden Fall Daten über Beschäftigte der Institution, die die Videokonferenz organisiert, und ggf. Daten über ihre Gesprächspartner/-innen, seien es Geschäftspartner/-innen, Mitarbeiter/-innen anderer Institutionen oder Privatpersonen.

Grundlegende Anforderungen und Empfehlungen

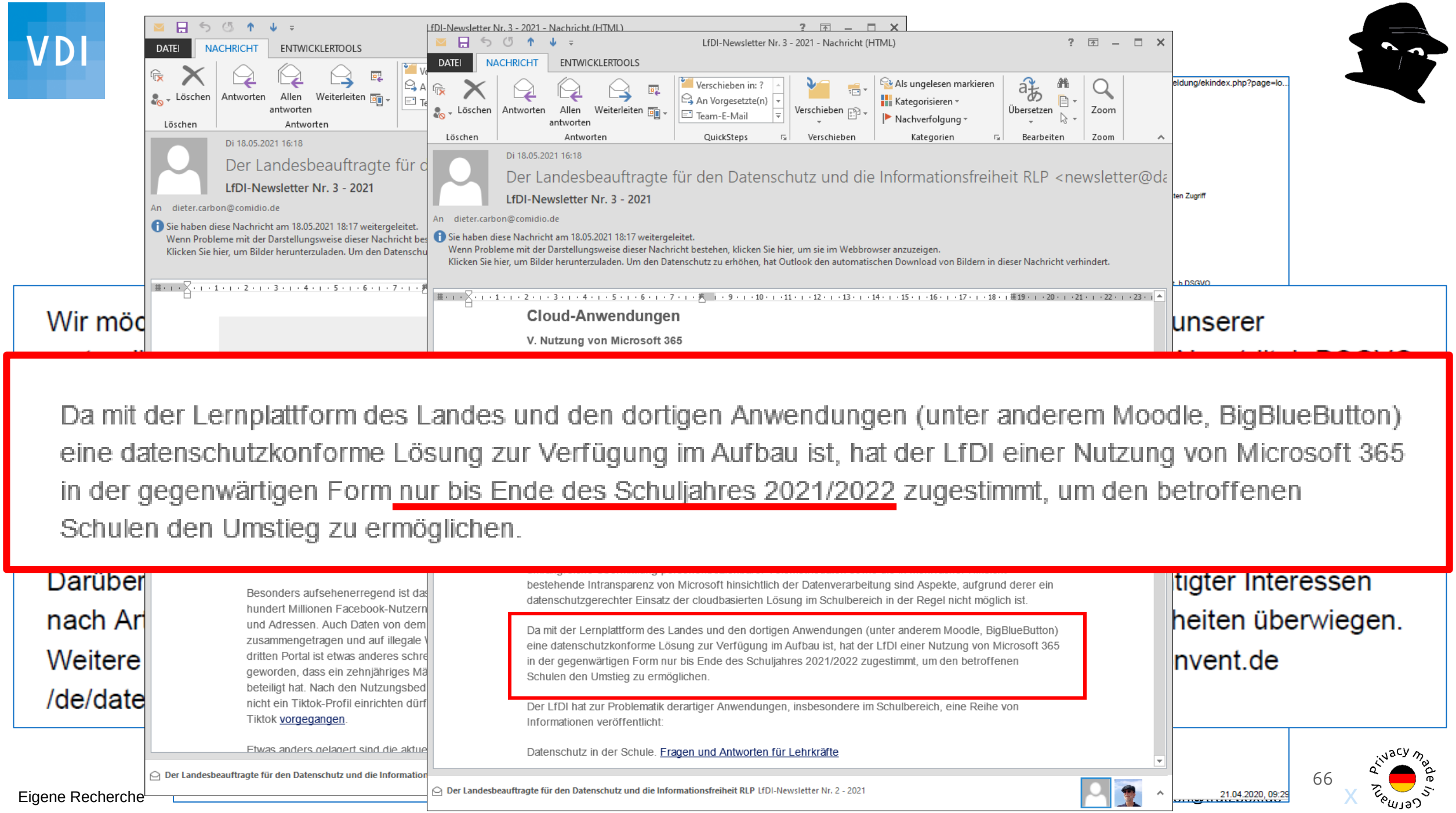
- Videotelefonie und Videokonferenzen sollen über verschlüsselte Kanäle abgewickelt werden. Dies betrifft sowohl die Vermittlung der Verbindungen als auch die Übertragung der Ton- und Bilddaten.
- Wenn Sie die Videokonferenzlösung nicht selbst sicher und mit angemessenem Aufwand betreiben können (was vorzuziehen wäre), dann können Sie einen zuverlässigen Videokonferenzdienst damit beauftra-

Der Anbieter muss Ihnen auch darlegen, ob er außereuropäische Dienstleister zur Erbringung der Leistung hinzuzieht. Einige Anbieter fungieren lediglich als Wiederverkäufer von Leistungen US-amerikanischer Unternehmen. Andere lassen einen wesentlichen Teil der Dienstleistung von außereuropäischen Unternehmen der gleichen Unternehmensgruppe erbringen. In den beiden letztgenannten Fällen gewinnen Sie zwar einen europäischen vertraglichen Ansprechpartner. Die oben beschriebenen Risiken verbleiben jedoch. Prominentes Beispiel sind die Dienstleistungen der Unternehmensgruppe von Microsoft Corporation (z. B. Microsoft Teams) einschließlich seiner Tochter Skype Communications SARL mit Sitz in Luxemburg (mit dem gleichnamigen Produkt).

Im letztgenannten Fall wie auch bei der direkten Beauftragung eines der außereuropäischen Anbieter mit signifikantem Marktanteil – in der Regel mit Sitz in den USA – müssen Sie neben den Fragen, die auch bei rein europäischen Anbietern eine Rolle spielen, die zusätzlichen Risiken bedenken und die rechtlichen Garantien prüfen. Leider erfüllen auch einige der Anbieter, die technisch ausgereifte Lösungen bereitstellen, die datenschutzrechtlichen Anforderungen bisher nicht. Dies trifft derzeit (Stand 2. April 2020) z. B. auf Zoom Video Communications, Inc. zu.

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf

dieter.carbon@trutzbox.de

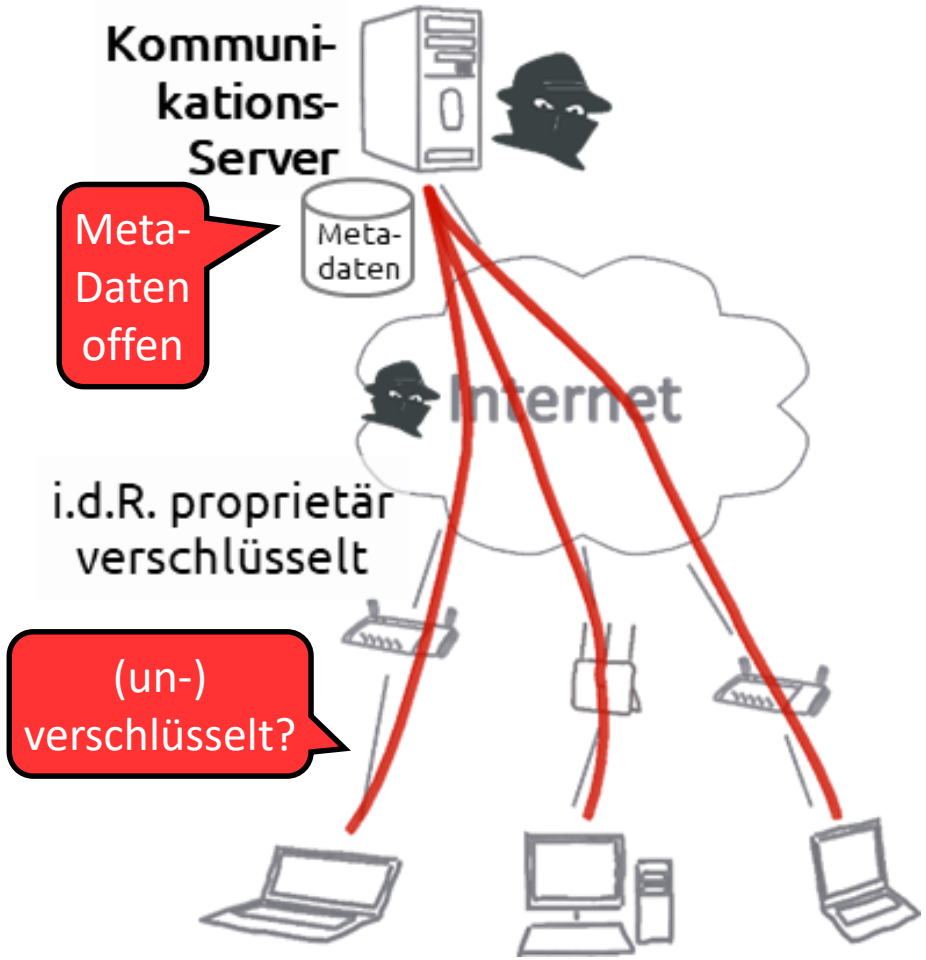


Eigene Recherche

Passive Gefährdung … und Abhilfe

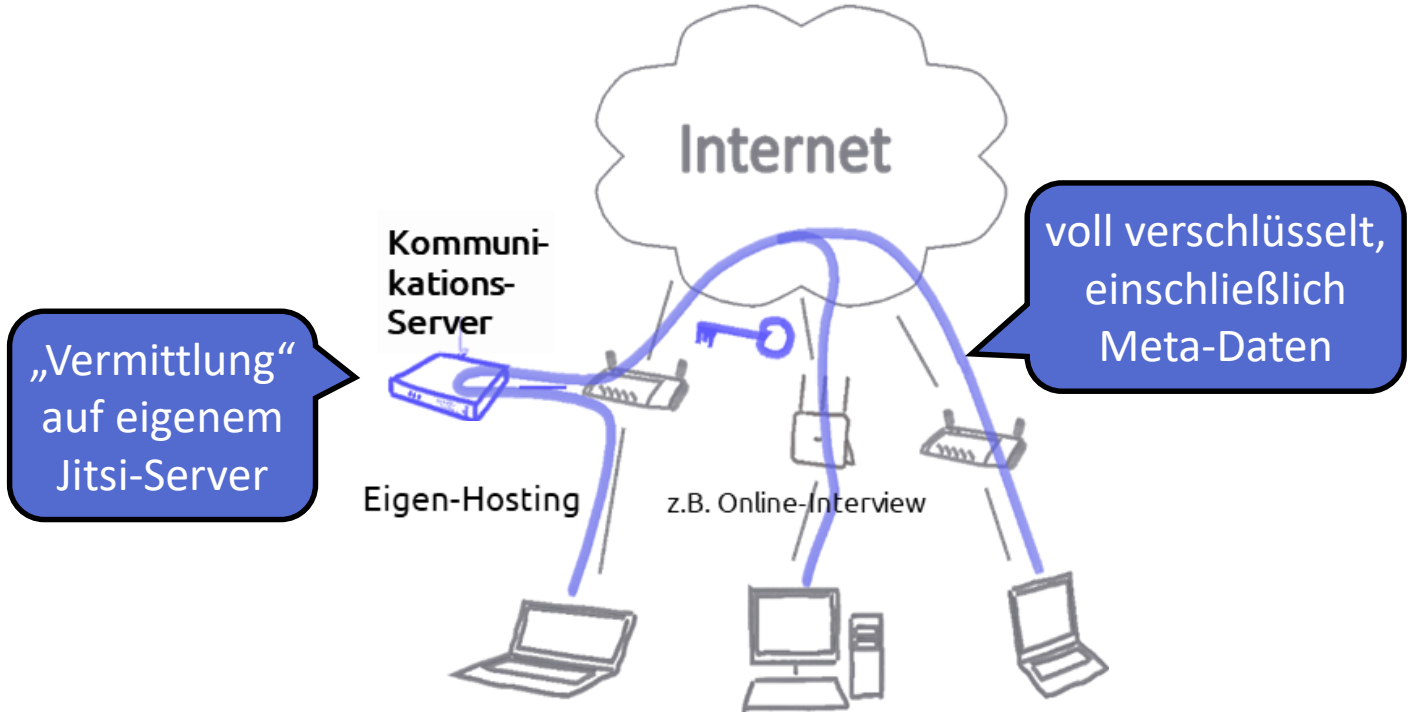
offene Metadaten und ggf. Inhaltsdaten beim Anbieter

Chat-, Audio-, Video-Kommunikations-Anbieter



verschlüsselter Video- und Audio-Chat

ohne externen Chat-, Audio-, Video-Kommunikations-Anbieter



dieter.carbon@trutzbox.de

Privacy made in Germany

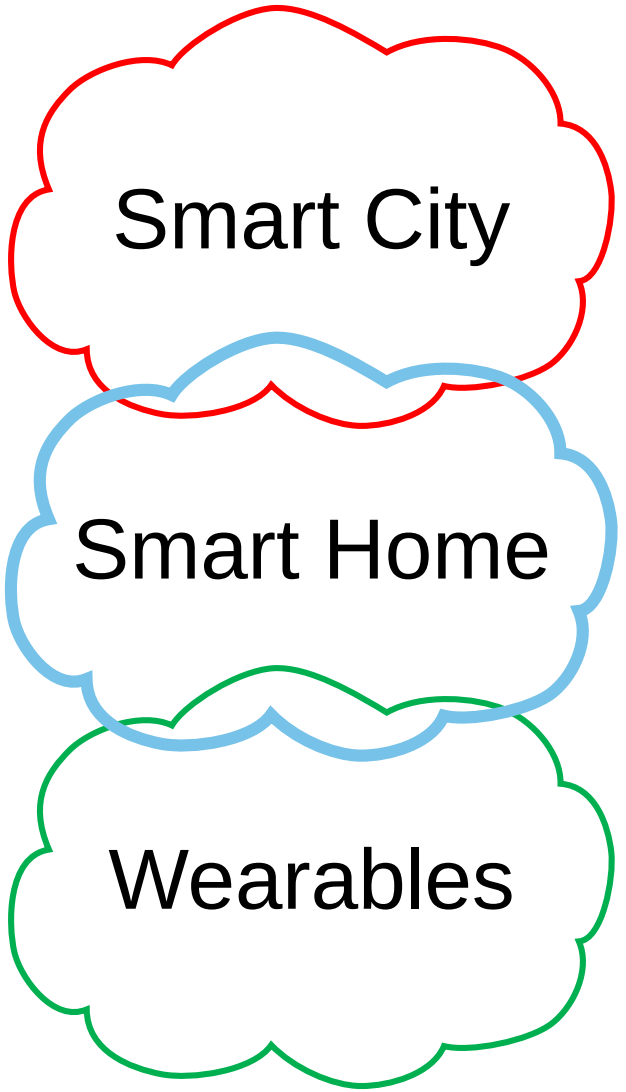
Smart Home Definition DKE

Damit eine strukturierte Darstellungsweise möglich ist, wird das gesamte Thema in sechs Domänen unterteilt.

Als Domänen werden die Anwendungsgruppen

1. Smart-Home-Infrastruktur,
2. Energiemanagement,
3. Gesundheit,
4. Wohnkomfort,
5. Wohnungssicherheit und
6. Informationssicherheit

bezeichnet, die einer Gliederung der vielfältigen und smarten Funktionen dient.

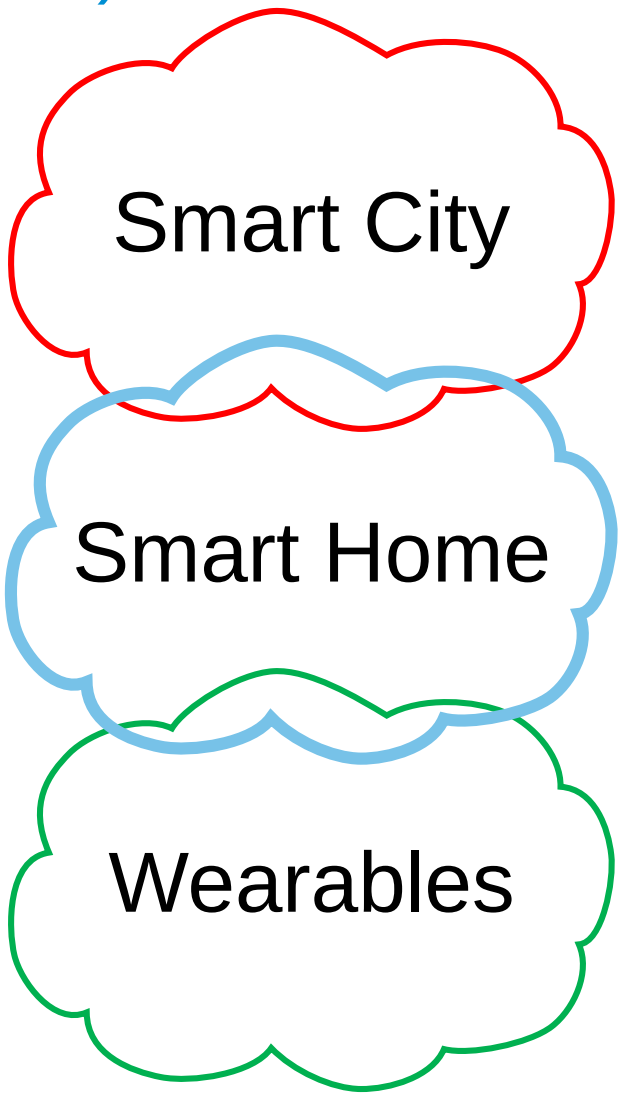


DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

https://www.dke.de/de/arbeitsfelder/home-building/normung-roadmap-smart-home-living

Smart Home Herausforderungen (DKE)

- Mangelnde Zuverlässigkeit im Betrieb
- Mangelndes Vertrauen in den Datenschutz
- Mangelndes Vertrauen in die Nutzung der Daten
- Mangelndes Wissen zu Kosten-Nutzungsverhältnis
- Berührungsängste (Know-how wie Geräte funktionieren und in Betrieb genommen werden)
- Hohe Komplexität
- Fehlende Langlebigkeit und Investitionsrisiko
- Unsichere Geräte bezüglich der Datensicherheit
- Proprietäre Lösungen versus Interoperabilität
- Ständiger Wechsel der Interoperabilität



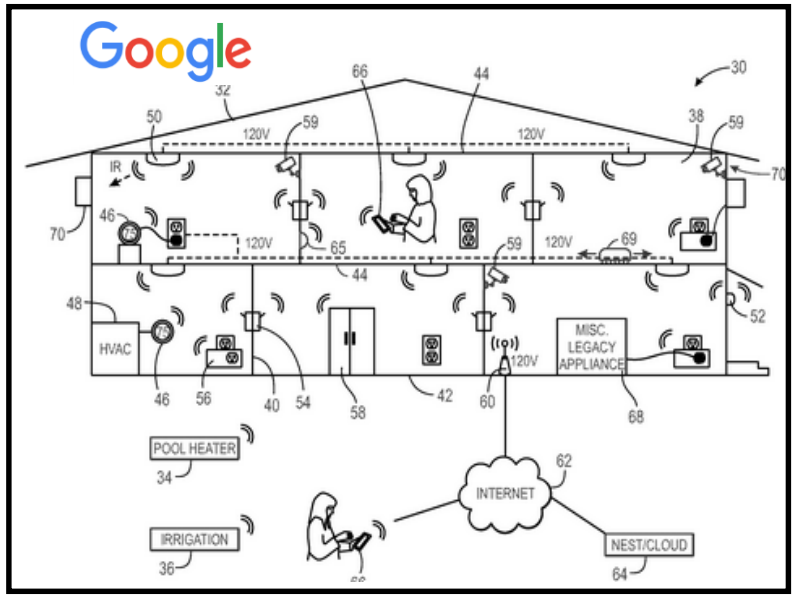
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

https://www.dke.de/de/arbeitsfelder/home-building/normung-roadmap-smart-home-living

dieter.carbon@trutzbox.de

Wie geht es weiter ?

Google Patent (2015):
Überwachung und Berichterstattung der Haushaltsaktivitäten im Smart Home

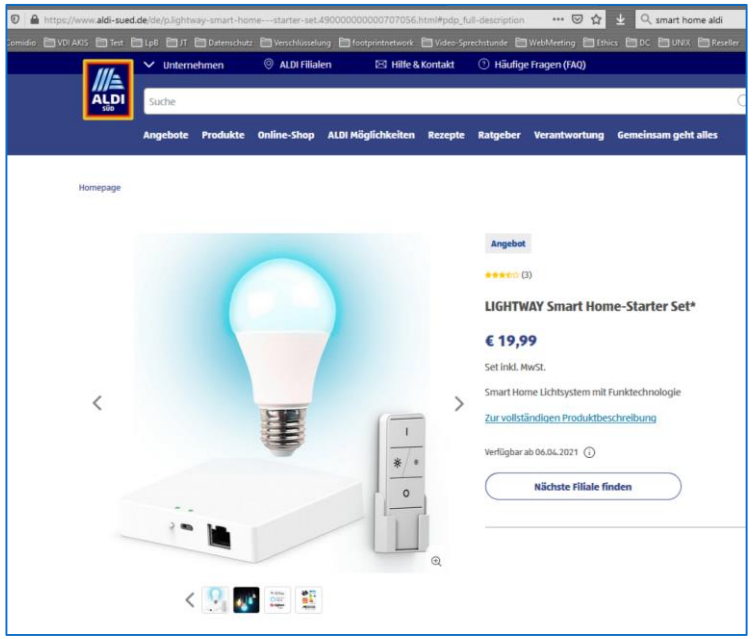


https://patents.google.com/patent/US20160261932A1/en

dieter.carbon@trutzbox.de

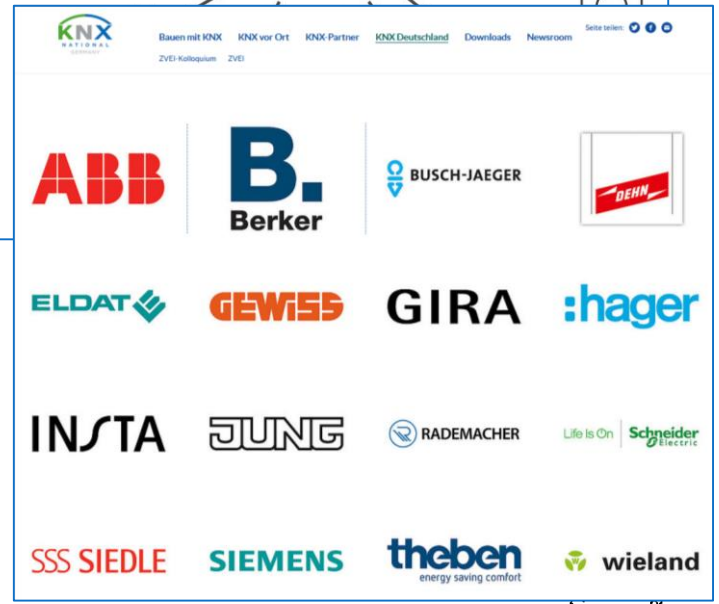
Privacy made in Germany

Smart Home Anbieter …



Aldi:
LIGHTWAY Smart Home-Starter Set

Apple:
Home App steuerst HomeKit Zubehör



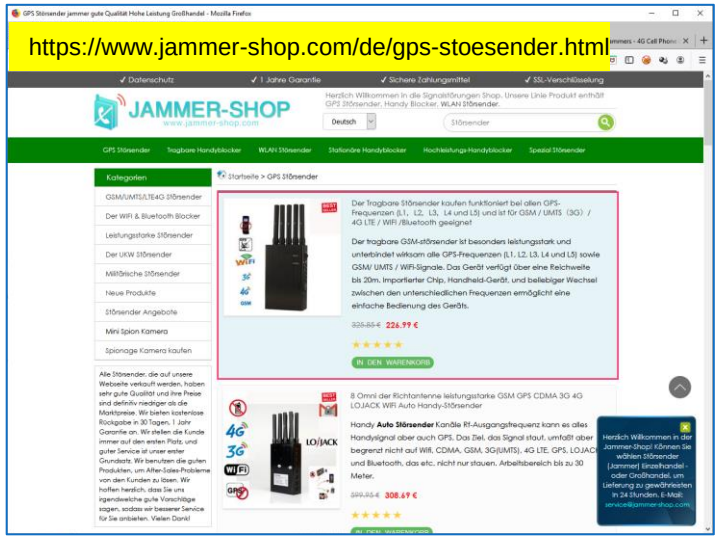
https://www.aldi-sued.de/de/p.lightway-smart-home---starter-set.490000000000707056.html#pdp_full-description https://www.apple.com/de/ios/home/ https://www.knx.de/knx-deutschland/

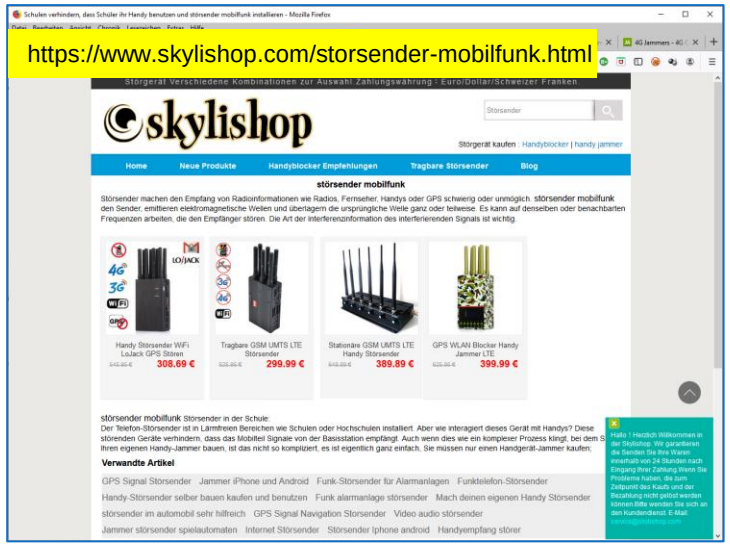
dieter.carbon@trutzbox.de

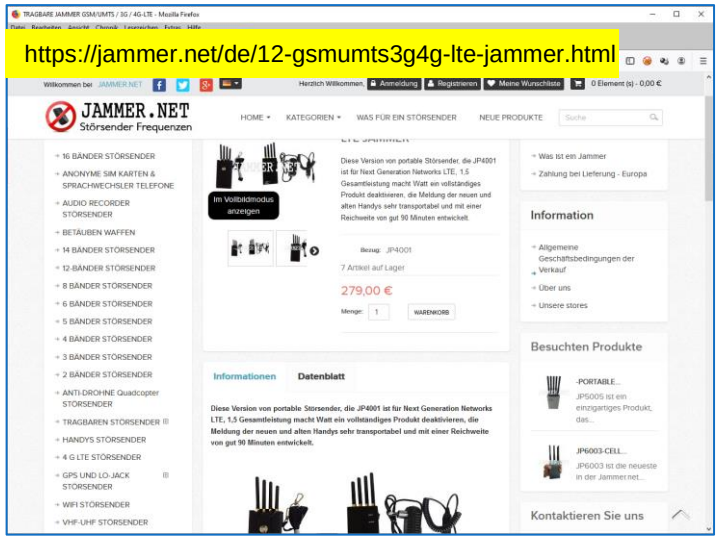
WLAN, UMTS, 5G …

Aber: Vorsicht bei Funkkommunikation …

Bezugsquellen für Störsender



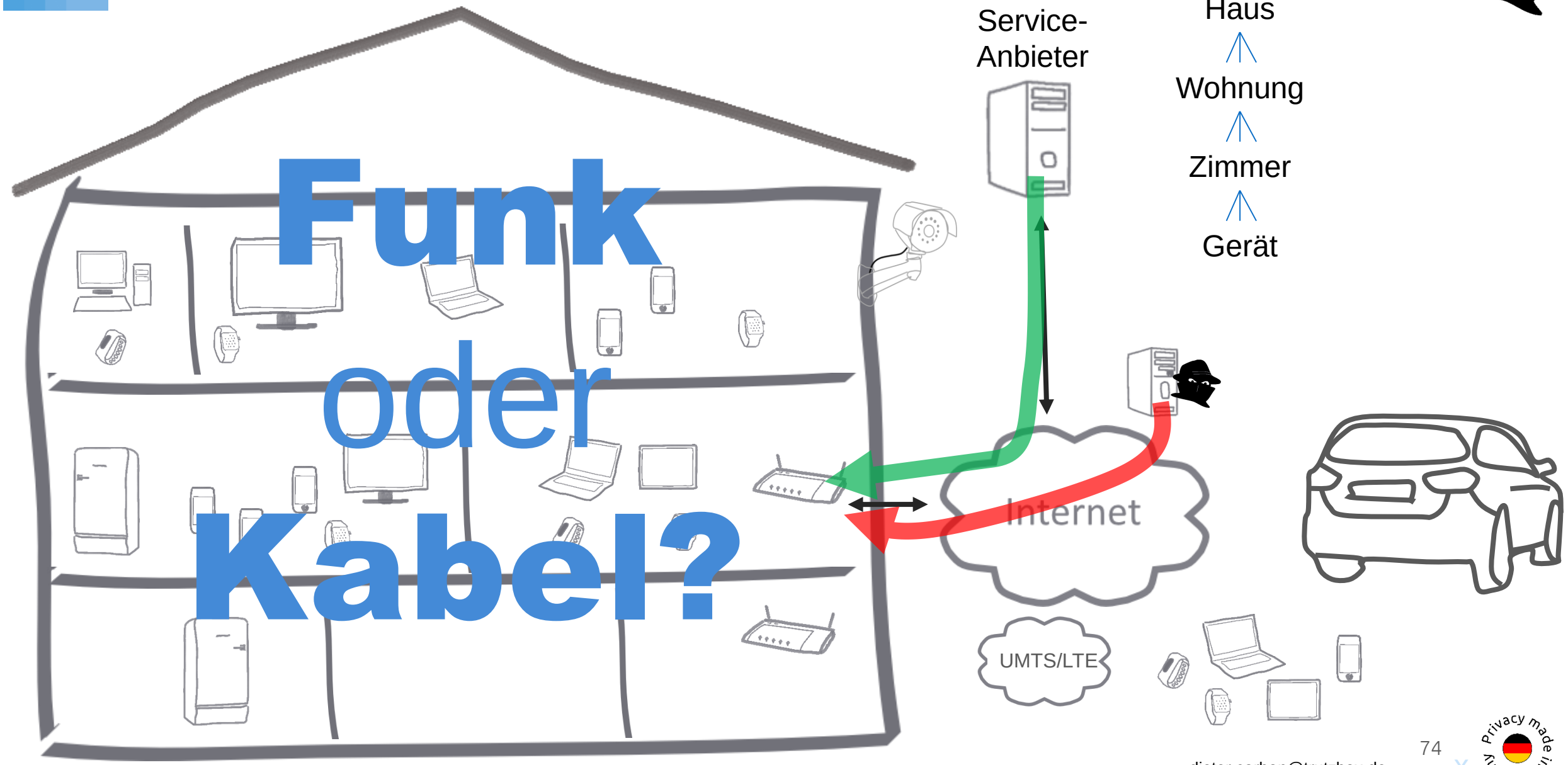




dieter.carbon@trutzbox.de

Privacy made in Germany

Smart Home Struktur



Funk
oder
Kabel?

dieter.carbon@trutzbox.de

Smart Home Geräte

1 Abflusssensor
2 Anwesenheitssimulation
3 Außenbewegungsmelder
4 Auto
5 Beleuchtung
6 Belüftung
7 Bewässerung
8 Bewegungsalarm HausTiere
9 Bewegungsmelder
10 Fensterkontakte
11 Fernseher
12 Feuchtemesser
13 Fitness Uhr
14 Fotoapparat
15 Futterautomat
16 Garagentore
17 Gasmelder
18 Geschirrspüler
19 Haarbürste
20 Heimtrainer
21 Heizung
22 Kaffeebecher
23 Kaffeemaschine
24 Kameras
25 Kinderpuppe
26 Klimatisierung
27 Küchenmaschine
28 Kühlung
29 Lautsprecher
30 Licht
31 Luftbefeuchter
32 Luftmessung
33 Luftreiniger
34 Mähroboter
35 Markise
36 Musikanlage
37 Navigationssystem
38 Ofen
39 Pflegeroboter
40 Radio
41 Rasensprenger
42 Rauchmelder
43 Schalter
44 Schlösser
45 Schnarchmelder
46 Schnellkochtopf
47 Sensoren
48 Sicherheitssystem
49 Smart Lock
50 Sprach-Assistent
51 Steckdose
52 Strom-Verbrauchsmessung
53 Temperaturmesser
54 Thermomix
55 Thermostat
56 Toaster
57 Türklingel
58 Türkommunikation
59 Uhr
60 Umfeldsteuerung
61 Ventilator
62 Verschattung
63 Videokameras
64 Visualisierung
65 Waage
66 Wasserhahn
67 Wasserkocher
68 Wassermelder
69 Wecker
70 Wetterstation
71 Windelsensor

https://ak.vdi-rheingau.de/index.php/ABCDEH_Ressourcen

dieter.carbon@trutzbox.de
Privacy made in Germany

NachLese 19.03.2021

Brand bei Europas größtem Cloud-Anbieter OVH

5 Etagen

Platz für 12.000 Server

betraf 16.000 Kunden

3,6 Mill. Websites offline

… darunter staatliche Portale, Banken Newskanäle, das Centre Pompidou und die Regierungsseite data.gouv.fr

Das war einmal eine Cloud: Data Center wie das von OVH in Straßburg sind die kollektiven G…

Am Rhein brennt das Wal…

Ein ikonisches Bild: Europas größtes Rechenzentrum geht in F…

Daten abgebrannt

CLOUD-DIENST: Der Brand eines Rechenzentrums von Europas Cloud-Riesen OVHCloud zeigt, wie anfällig Infrastrukturen sein können.

VON REGINE BÖNSCH

Letzte Woche brannte es bei Europas größtem Cloud-Anbieter OVHCloud. Zwei von vier Serverhallen in Straßburg waren betroffen, eine brannte ganz nieder, die andere teilweise. Das meldete die österreichische Nachrichtenagentur Apa. Der Brand betraf bis zu 16 000 Kunden, teilte das Unternehmen selbst mit. Laut Medienberichten gingen 3,6 Mio. Webseiten zumindest kurzzeitig offline. Zahlreiche Kunden verloren alle Daten. Denn Back-ups gab es bei OVH nur gegen Extragebühr – die viele im Glauben an die Sicherheit der Cloud einsparten.

Bei dem Feuer wurden nach Angaben von Firmenchef Octave Klaba vor allem zwei der vier Rechenzentren in Straßburg in Mitleidenschaft gezogen. Die Server von OVH nutzen etwa Unternehmen oder staatliche Organisationen, um große Datenmengen zu speichern und zu verwalten. Die 1999 von Klaba gegründete französische OVH hat nach eigenen Angaben rund 1,5 Mio. Kunden weltweit und betreibt unter anderem 15 Rechenzentren in Europa.

Zu den prominenteren Opfern gehören das Centre Pompidou, die offizielle Webseite der französischen Regierung, data.gouv.fr, der französische Bitcoin-Anbieter Coinhouse und die britische Spielefirma Facepunch. Letztere meldete ebenso den Totalverlust ihrer Daten wie die französische Großkanzlei Leroi & Associés. Dabei sollen auch Kunden mit Back-up alle Daten verloren haben. Denn auch diese Server in einer anderen Halle seien vom Feuer betroffen gewesen. Wie viele Unternehmen ihre Daten endgültig verloren haben, wird erst erhoben. OVH ist europäischer Marktführer im Hosting-Bereich und galt als einer der großen Hoffnungsträger für eine europäische Antwort auf die Cloud-Angebote aus den USA und China.

Der Brand zeigt, wie anfällig die Cloud-Infrastruktur sein kann. Noch immer gelten speziell deutsche Unternehmen als zögerlich, wenn es um die Migration in die Cloud-Umgebung geht. Auch im Jahr 2021 sind viele von ihnen noch immer nicht vollumfänglich von der Cloud überzeugt: Jedes zehnte Unternehmen setzt diese Technik überhaupt nicht ein, fast ein Drittel arbeitet noch klassisch mit lokalen Vor-Ort-Serverlösungen und verwendet nur punktuell die Cloud. Aber die Reise hin zur Cloud nimmt in Deutschland an Fahrt auf. Zu diesem Ergebnis kommt eine Studie von Techconsult im Auftrag von Mimecast, einem britischen Anbieter für Daten- und E-Mail-Security. Im Dezember 2020 befragten die Sicherheitsexperten rund 200 Entscheider in deutschen Unternehmen. Cloud-Adoption ist auf jeden Fall branchen- und größenabhängig. Unternehmen mit bis zu 999 Mitarbeitern setzen zu 68,7 % überwiegend oder nahezu zu 100 % auf die Cloud. Damit liegen sie deutlich vor Unternehmen mit 1000 bis 4999 Mitarbeitern (56,9 %), bei größeren Konzernen sind es hingegen nur noch 47,5 %. Geht es um die Branchen, dann hat die Telekommunikation mit 93,8 % die Nase vorne. Auf Platz zwei und drei folgen Industrie (69 %) und der Handel (66,7 %).

Foto: dpa Picture-Alliance/MAXPPP/Jean-Marc Loos

Geschmolzen: Verkohlte Containerhüllen zeugen von dem Brand des Cloud-Zentrums in Straßburg. Geschmolzen ist dabei auch so mancher IT-Traum von den sicheren Daten in der Wolke.

dieter.carbon@trutzbox.de

Software-Arten

Microsoft 365 (Teams)

Google Chrome OS

Zoom

gmx.net

Iridium

gmail.com

web.de

Firefox

Office 2013

TrutzBox

Thunderbird

LibreOffice

jitsi

Proprietäre Software

Quelloffene Software

Open Source Software

Eigen Hosting

Fremd-Betrieb in Europa

Fremd-Betrieb außerhalb Europa

Als Open Source (aus englisch open source, wörtlich offene Quelle) wird Software bezeichnet, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann. Open-Source-Software kann meistens kostenlos genutzt werden.

https://de.wikipedia.org/wiki/Open_Source

dieter.carbon@trutzbox.de

Privacy made in Germany

Update Trick

Meines Erachtens gilt generell (leider) folgende Logik (welche zukünftig von immer mehr Anbietern angewandt wird):

1. Benutzt ein Gerät zur Funktions-Steuerung eine Software, welche nicht isoliert (also IT-unkommunikativ) betrieben wird?
   Im Allgemeinen daran erkennbar (und meistens dann der Fall), wenn das Gerät einen (W)LAN-Anschluss besitzt.
2. Falls ja gilt, die Nutzungsmöglichkeit eines Software-gesteuerten Gerätes ist von der Informations-Sicherheit der eingesetzten Software abhängig.
3. Diese Software ist nur dann „möglichst sicher“, wenn sie in dem neusten Release-Stand betrieben wird.
4. Der Geräte-Nutzer ist für die Informations-Sicherheit seines Gerätes verantwortlich; daher muss er prüfen
   a. Ist dieses Gerät noch „update-fähig“?
   b. Welches ist seitens des Anbieters das aktuelle Software-Release?
   c. Ist dieses aktuelle Software-Release auf meinem Gerät im Einsatz?
   d. Falls nicht, was muss der Geräte-Nutzer tun, um das aktuelle Software-Release auf seinem Gerät zum Einsatz zu bringen?
5. Wie kann der Geräte-Nutzer sicherstellen, …
   a. dass er über neue Releases informiert wird
   b. dass er neue Releases (ggf. automatisch) erhält?
   c. dass er neue Releases (ggf. automatisch) installiert?
6. Sollte das untersuchte Gerät „nicht mehr Update-fähig“ sein, ist ein zunehmend IT-technisch unsicherer Betrieb zu erwarten, von welchem dringend abgeraten wird.
   Es besteht die Gefährdung des fremden Zugriffs auf das eigene Home-Netzwerk.
   Eine (meistens wenig hilfreiche) Alternative besteht in der informationstechnischen Trennung des Gerätes von IT-Netzen.
7. Falls es keine Updates (mehr) gibt, sollte das Gerät
   a. vom IT-Netzen getrennt („Insel-Betreib“) betrieben werden, oder
   b. außer Betrieb genommen werden,
   c. ggf. ersetzt werden.

Diese Logik gilt m.E. für Smartphones, WLAN-xyz-Geräte (wie Birnen, Kameras, alle Smart-Home- oder IoT-Geräte) smart Autos, usw.

Also: Wenn es keine Updates für ein Gerät mehr gibt … entweder (W)LAN abschalten oder Gerät ersetzen.

dieter.carbon@trutzbox.de

Update Dilemma

Mache ich Updates …

… kann es sein, dass ich
- allgemein-gefaktes Update
- personalisiert-gefaktes Update

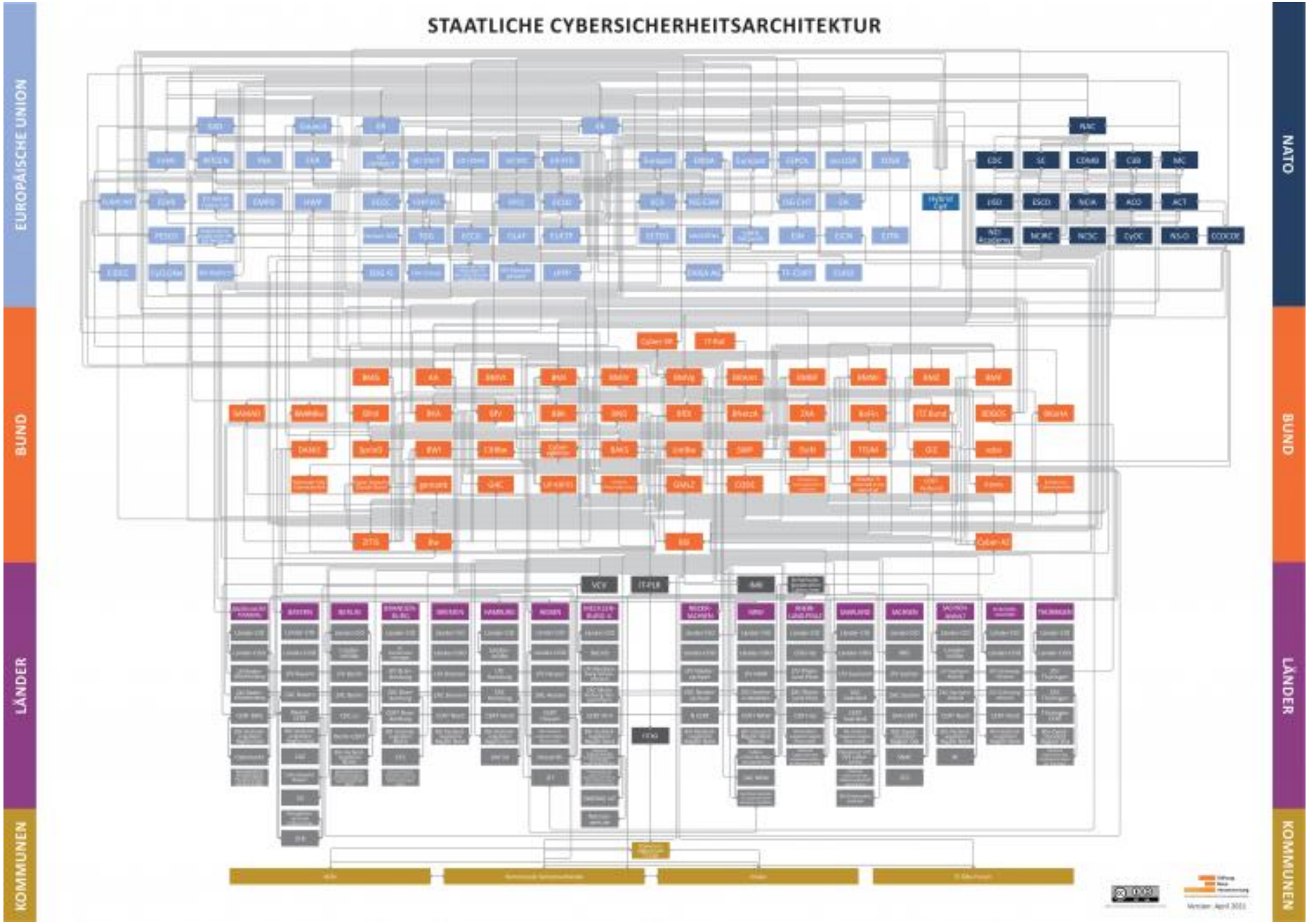
erhalte.

Mache ich keine Updates …

… kann es sein, dass
- mir Sicherheits-Updates fehlen,
- ich leichter Schadsoftware erhalte.

… schlecht für mich

dieter.carbon@trutzbox.de



Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

Version: April 2021

Der Dilettant …

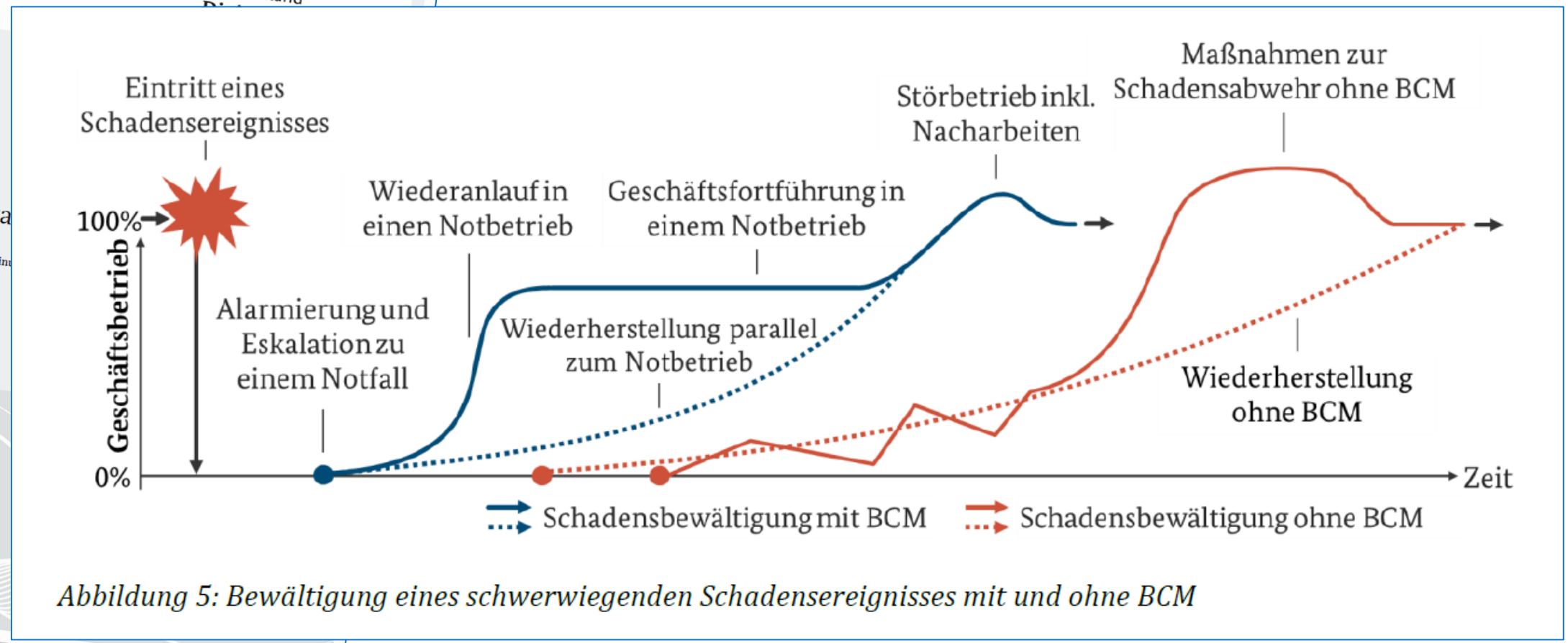


Abbildung 5: Bewältigung eines schwerwiegenden Schadensereignisses mit und ohne BCM

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

Nutzwert-Analyse

Ziel: Vergleich von Optionen und Bestimmung der besten Lösung

- Bestimmung von (Vergleichs-)Kriterien
- Punktebeschreibung für Kriterien-Erfüllung (0 – 10 Punkte)
- subjektive Festlegung von KO-Schwellen der einzelnen Kriterien (0 – 10 Punkte)
- „objektive“ Bepunktung der einzelnen Kriterien (0 – 10 Punkte) der verschiedenen Optionen
- subjektive Gewichtung der einzelnen Kriterien
- Aufsummierung der einzelnen Kriterien-Erfüllungen zu Vergleichs-Werten
- höchster Vergleichs-Wert -> beste Lösung

Nutzwert-Analyse

Nutzwertanalyse zum Vergleich von Optionen						Option 1				
10,00	1	Gewich-tung in %	gelbe Felder mit Werten ausfüllen, orangene Felder mit Text ausfüllen; Ergebnis: Vergleich blauer Summenfelder, oben rechts; höherer Wert "gewinnt"			KO-Schwelle 0-10	KO ?	Beschreibungstext zur Kriterien-Erfüllung	Punkte 0 - 10	Vergleichs-Wert
	Kriterien	100%	<- muss 100% sein		Punktebeschreibung für Kriterien-Erfüllung		1	Option 1 = Name	Erfüllung	10,00
1		13%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	1,30
2		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
3		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
4		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
5		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
6		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
7		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
8		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
9		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
10		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
11		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
12		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
13		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
14		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
15		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30
16		3%			0 Punkte= 5 Punkte= 10 Punkte=	0	1		10	0,30

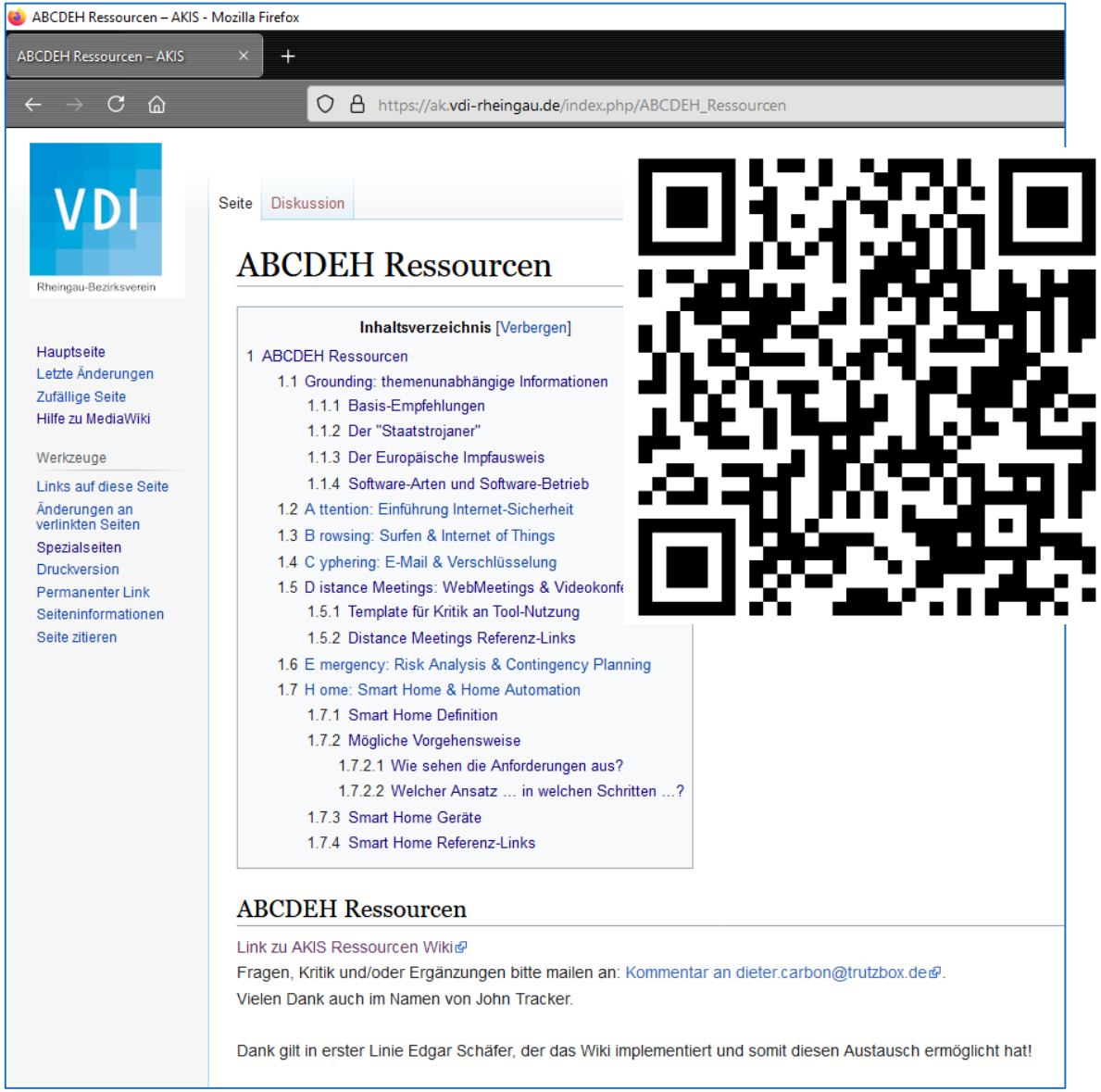
	Option 2				
	KO-Schwelle 0-10	KO ?	Beschreibungstext zur Kriterien-Erfüllung	Punkte 0 - 10	Vergleichs-Wert
		1	Option 2 = Name	Erfüllung	10,00
1	0	1		10	1,30
2	0	1		10	0,30
3	0	1		10	0,30
4	0	1		10	0,30
5	0	1		10	0,30
6	0	1		10	0,30
7	0	1		10	0,30
8	0	1		10	0,30
9	0	1		10	0,30
10	0	1		10	0,30
11	0	1		10	0,30
12	0	1		10	0,30
13	0	1		10	0,30
14	0	1		10	0,30
15	0	1		10	0,30
16	0	1		10	0,30

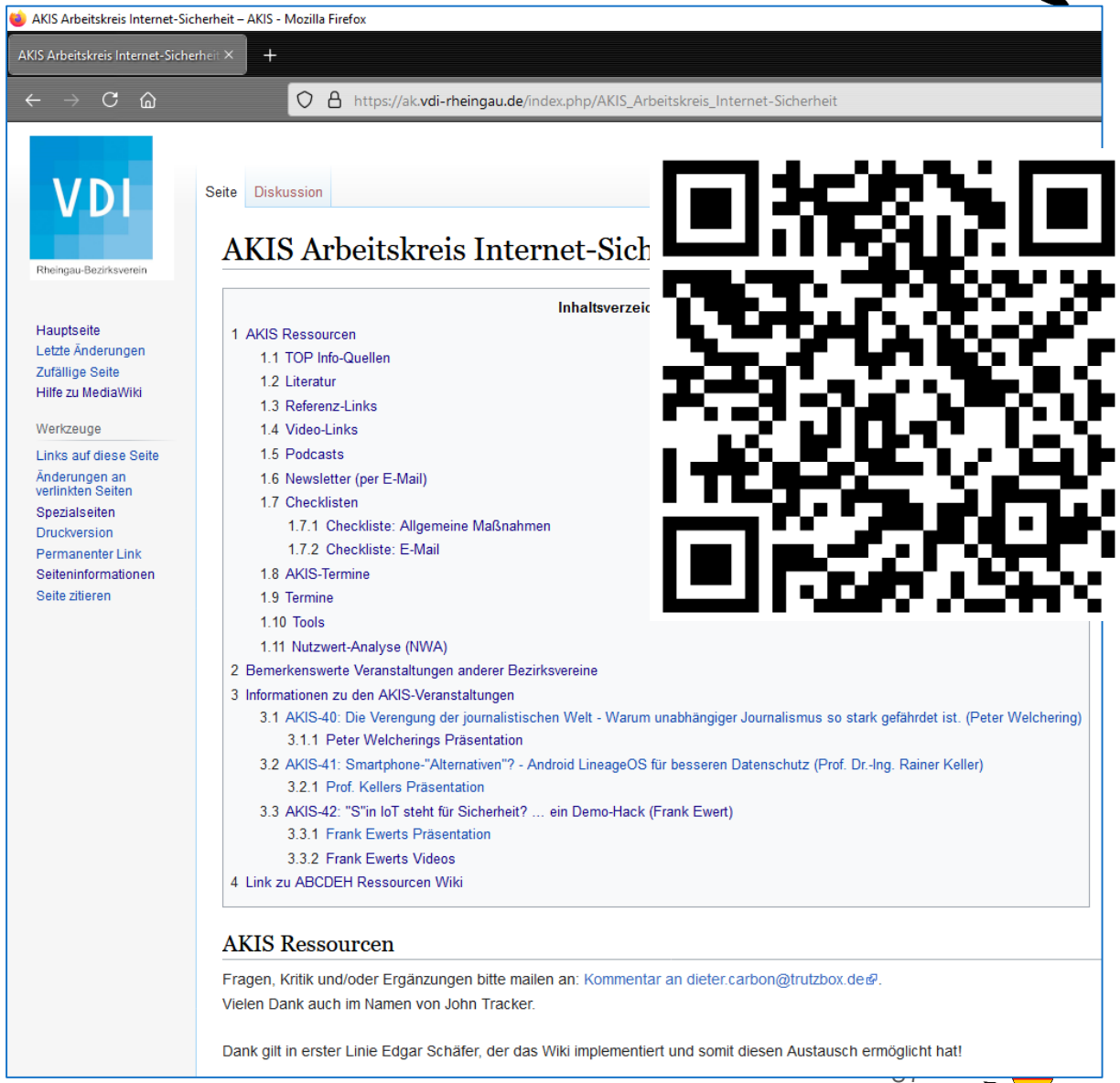
	Option 3				
	KO-Schwelle 0-10	KO ?	Beschreibungstext zur Kriterien-Erfüllung	Punkte 0 - 10	Vergleichs-Wert
		1	Option 3 = Name	Erfüllung	10,00
1	0	1		10	1,30
2	0	1		10	0,30
3	0	1		10	0,30
4	0	1		10	0,30
5	0	1		10	0,30
6	0	1		10	0,30
7	0	1		10	0,30
8	0	1		10	0,30
9	0	1		10	0,30
10	0	1		10	0,30
11	0	1		10	0,30
12	0	1		10	0,30
13	0	1		10	0,30
14	0	1		10	0,30
15	0	1		10	0,30
16	0	1		10	0,30

	Option 4				
	KO-Schwelle 0-10	KO ?	Beschreibungstext zur Kriterien-Erfüllung	Punkte 0 - 10	Vergleichs-Wert
		1	Option 4 = Name	Erfüllung	10,00
1	0	1		10	1,30
2	0	1		10	0,30
3	0	1		10	0,30
4	0	1		10	0,30
5	0	1		10	0,30
6	0	1		10	0,30
7	0	1		10	0,30
8	0	1		10	0,30
9	0	1		10	0,30
10	0	1		10	0,30
11	0	1		10	0,30
12	0	1		10	0,30
13	0	1		10	0,30
14	0	1		10	0,30
15	0	1		10	0,30
16	0	1		10	0,30

	Option 5				
	KO-Schwelle 0-10	KO ?	Beschreibungstext zur Kriterien-Erfüllung	Punkte 0 - 10	Vergleichs-Wert
		1	Option 5 = Name	Erfüllung	10,00
1	0	1		10	1,30
2	0	1		10	0,30
3	0	1		10	0,30
4	0	1		10	0,30
5	0	1		10	0,30
6	0	1		10	0,30
7	0	1		10	0,30
8	0	1		10	0,30
9	0	1		10	0,30
10	0	1		10	0,30
11	0	1		10	0,30
12	0	1		10	0,30
13	0	1		10	0,30
14	0	1		10	0,30
15	0	1		10	0,30
16	0	1		10	0,30

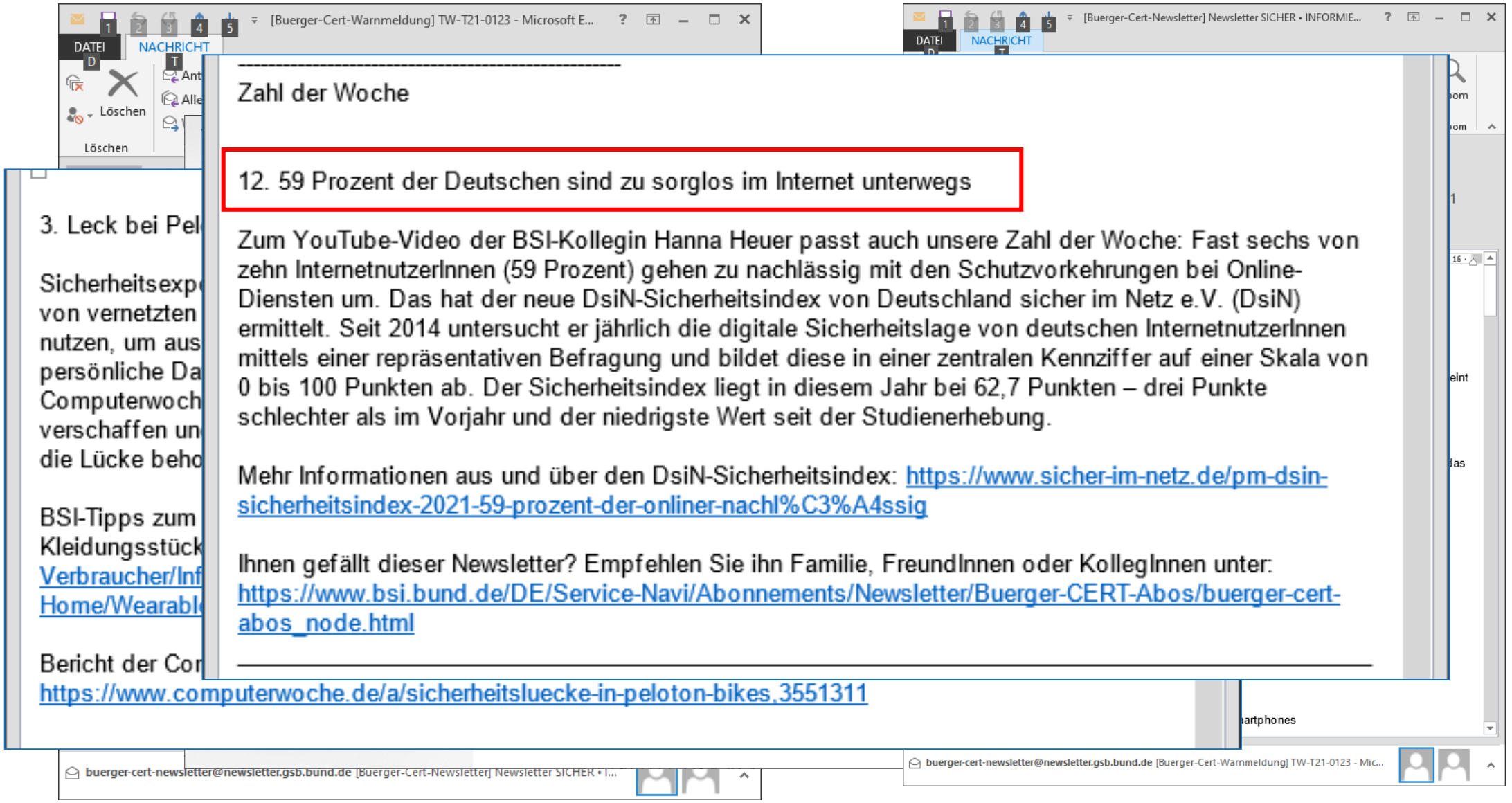
Ressourcen Wikis





https://ak.vdi-rheingau.de/index.php/ABCDEH_Ressourcen https://ak.vdi-rheingau.de/index.php/AKIS_Arbeitskreis_Internet-Sicherheit dieter.carbon@trutzbox.de

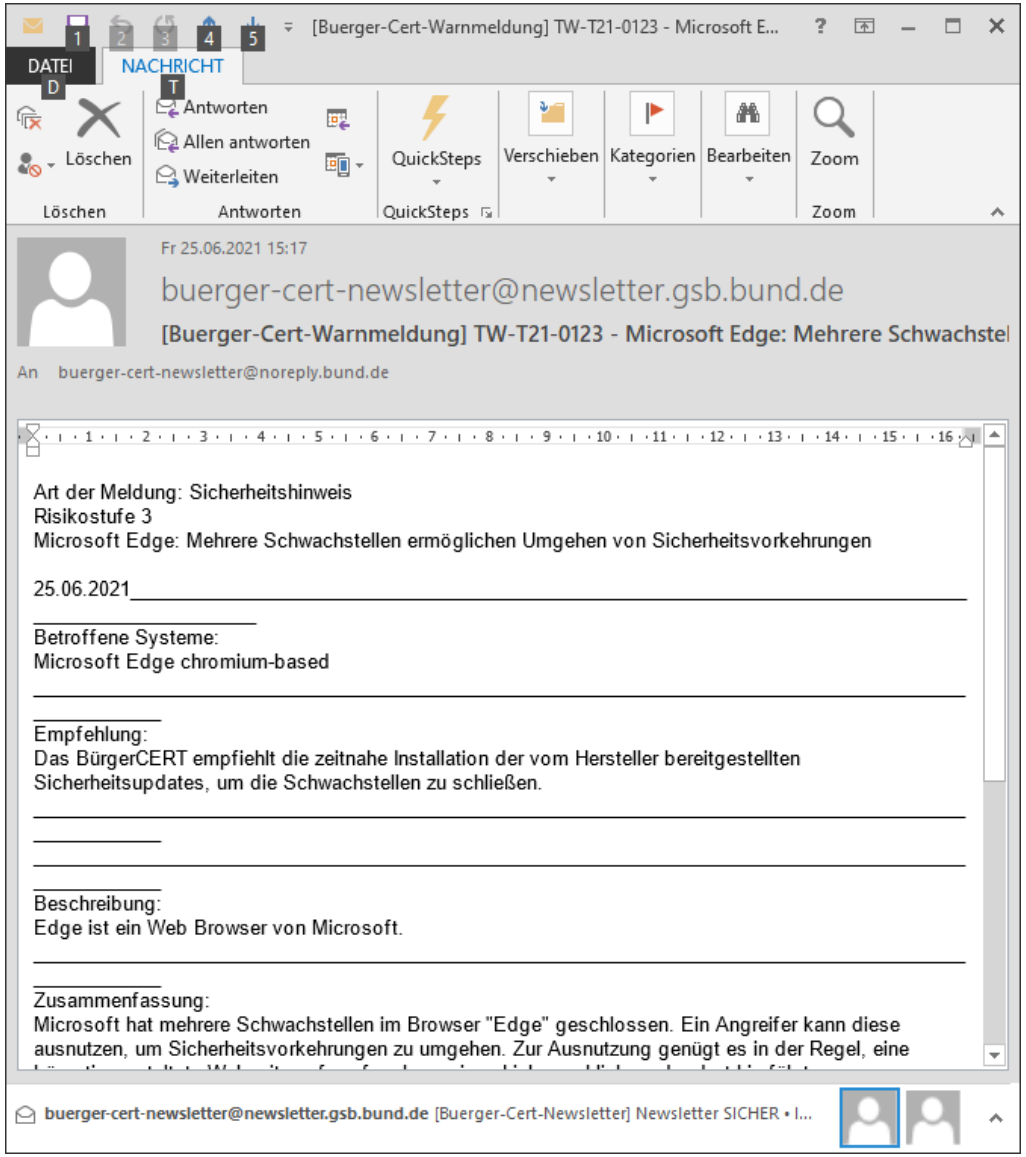
#1 der AKIS TOP-Empfehlungen

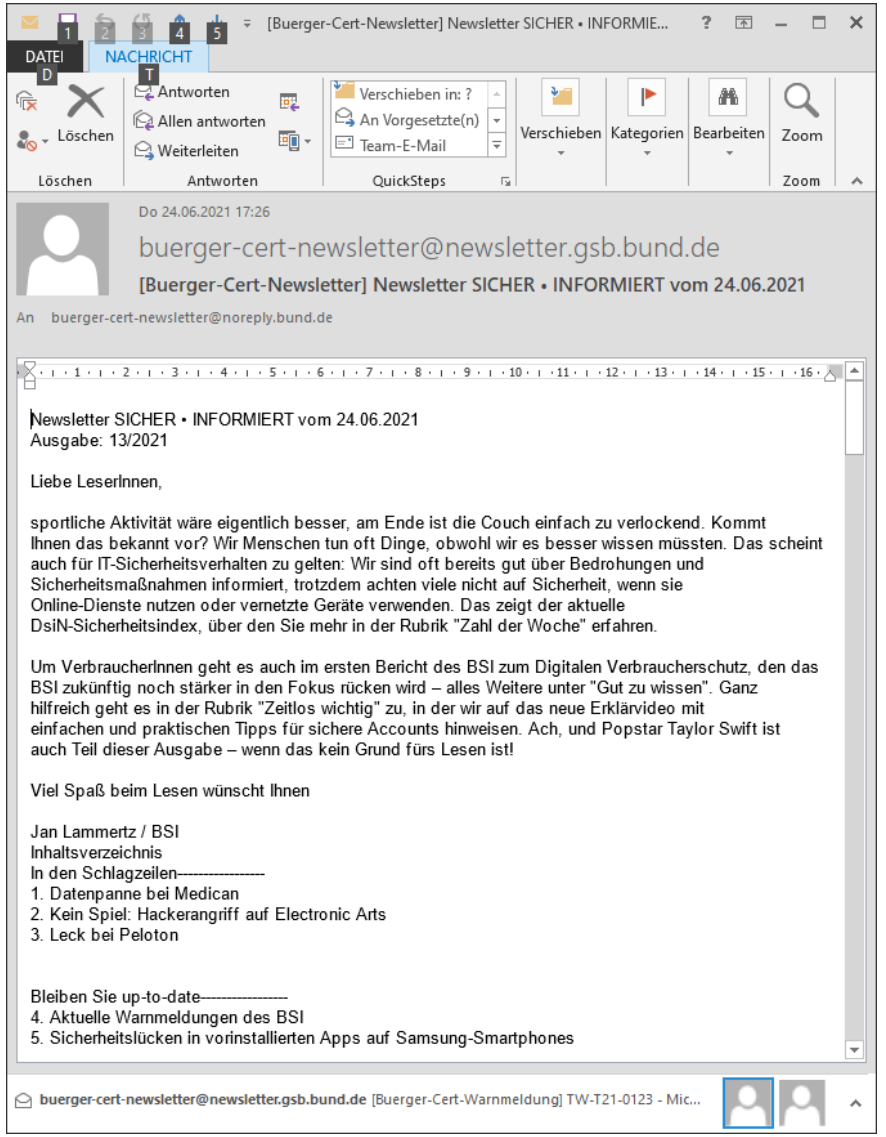


https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/Abonnieren/abonnieren_node.html

dieter.carbon@trutzbox.de

#1 der AKIS TOP-Empfehlungen





https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Buerger-CERT-Abos/Abonnieren/abonnieren_node.html

dieter.carbon@trutzbox.de

Erkenntnisse

There is no free breakfast.
Soll heißen: sofern der Erbringer einer kostenlosen Leistung weder wohltätig noch selbstlos, sondern betriebswirtschaftlich handelt, kann ich davon ausgehen, dass die vermeintlich kostenlose Leistung von mir, z.B. mit meinen Nutzungsdaten, bezahlt wird -> **DEAL**.

dieter.carbon@trutzbox.de
Privacy made in Germany

Erkenntnisse

Nach dem Motto "If you can’t be rememebered, you needn’t be forgotten” kann etwas, was nicht von mir bekannt ist, auch nicht im Netz gespeichert werden und folgerichtig auch nicht – weder jetzt noch zukünftig - gegen mich verwendet werden.

dieter.carbon@trutzbox.de

12 ProThesen zur Internet-Sicherheit: von Hörigkeit zur Mündigkeit

1. Digit~~al~~us first. Bedenken second
2. Wir wollen doch nur Dein Bestes
3. CIA: man schütze mich vor meinen Freunden
4. Seekabel ist Sehkabel
5. Ich bin Mittelpunkt (-> Ich bin Mittel .)
6. Bitte (k)ein Bid
7. Wer verschlüsselt, hat was zu verbergen
8. Frau Merkel skypt
9. Smart Home - alone, nur mit Strom
10. Offenes Visier; sieh, das Gute liegt so nah
11. Der Dilettant bringt was auf die Waage
12. Wer schreibt, der bleibt; Grüße von der Insel

Prothese von altgriechisch πρόσθεσις *prósthesis*, ‚Anfügung', aus πρός ‚hinzu, obendrein, außerdem' und τίθημι ‚setzen, stellen, legen

https://de.wikipedia.org/wiki/Prothese

Abgrenzung?

Wirtschaftsförderung

Als Wirtschaftsförderung bezeichnet man die von öffentlichen Organen oder privaten Unternehmen bzw. Initiativen betriebenen Anstrengungen, die Wirtschaft in einer bestimmten Region zu beleben.

Dies geschieht in Form von materieller, personeller und finanzieller Unterstützung.

Bei erfolgreicher Förderung amortisieren sich die Fördermaßnahmen durch Beschäftigungszuwachs, Steuermehreinnahmen und Attraktivitätsgewinn des Standorts.

Auch private Wirtschaftsförderung wird in Einzelfällen betrieben.

Wirtschaftsspionage

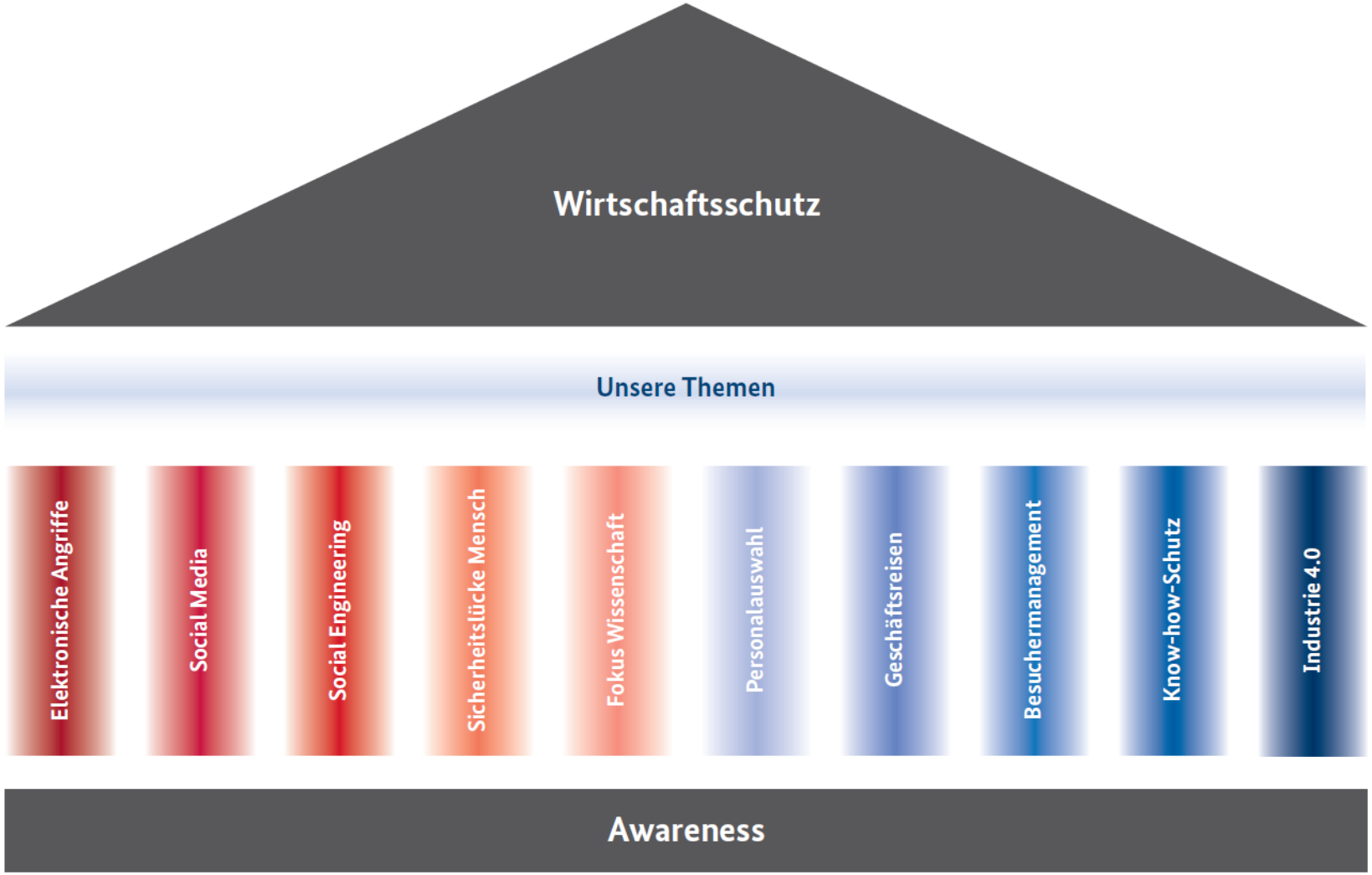
Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung im Zielbereich Wirtschaft.

In der öffentlichen Diskussion und Medienberichterstattung werden die Begriffe Wirtschaftsspionage und Konkurrenzspionage sowie Industriespionage häufig nicht präzise voneinander abgegrenzt.

So handelt es sich bei der Industrie- und Konkurrenzspionage um die illegale Beschaffung von Know-how und Waren durch konkurrierende Unternehmen.

Ziel ist es, durch früheren Erhalt der Informationen entweder sich selbst einen Vorteil zu verschaffen oder früh (genug) Gegenmaßnahmen einleiten zu können.

Bundesamt für Verfassungsschutz



https://www.verfassungsschutz.de/DE/themen/cyberabwehr/cyberabwehr_node.html;jsessionid=1E3F72ADDB32E797732F584D92DE9D7C.intranet381

dieter.carbon@trutzbox.de

Privacy made in Germany

Bundesamt für Verfassungsschutz

Die zunehmende Entwicklung technischer Möglichkeiten hat unsere Gesellschaft rasant verändert: Nicht nur Inhalte des Privatlebens werden zunehmend im Internet gespeichert oder geteilt, sondern auch branchenübergreifende Prozesse wie die Kommunikation oder Arbeitsabläufe im beruflichen Kontext unterliegen der digitalen Transformation. E-Mails und Cloud-Dienste sind längst Bestandteil des Informationsaustausches in Politik, Wirtschaft und Wissenschaft.

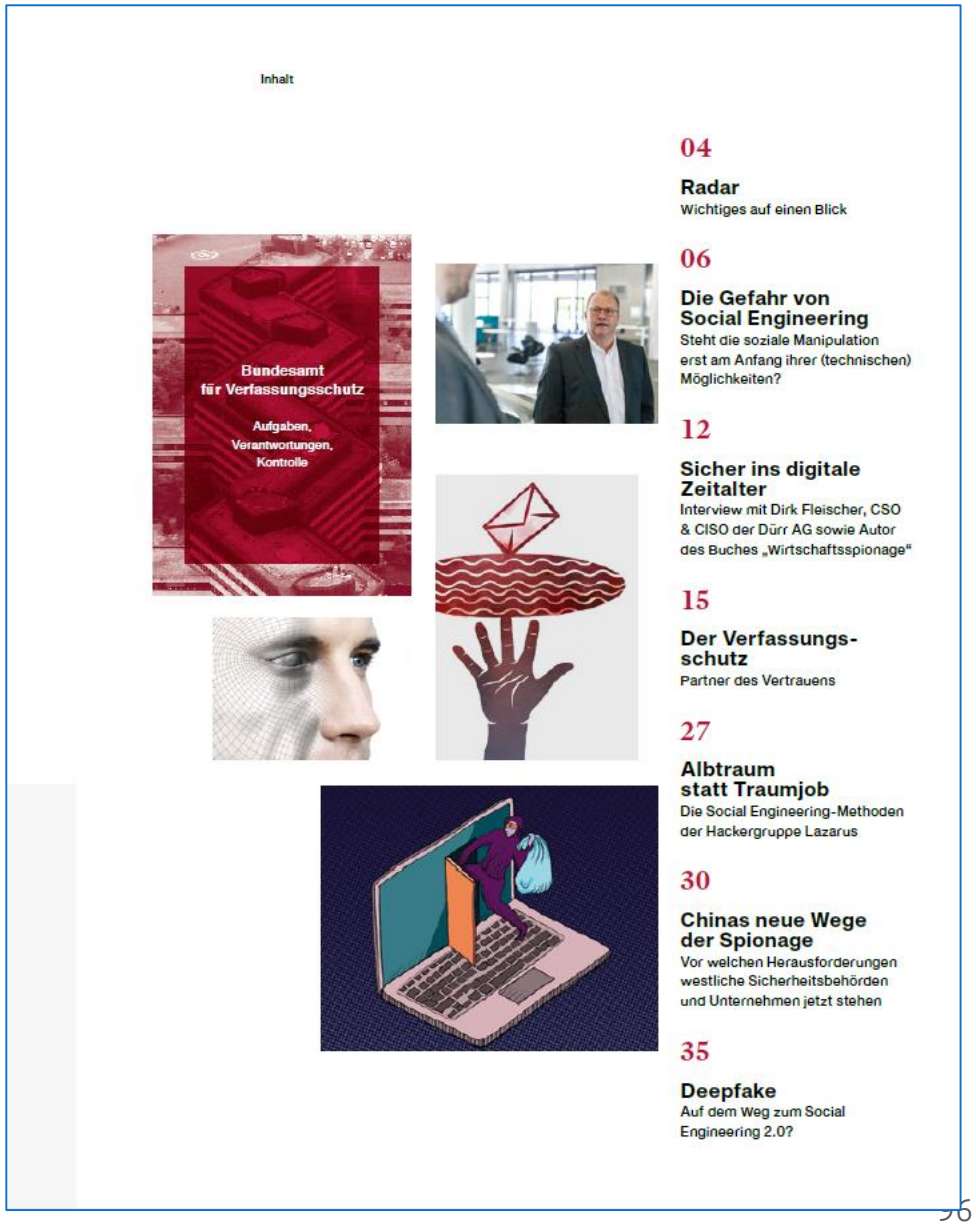
Unsere Gesellschaft ist dadurch vernetzter und dynamischer, aber auch verletzlicher geworden. Denn moderne Technologien bieten eine große Angriffsfläche und durch die Anonymisierungsmöglich-keiten des Internets können potenzielle Angreifer weitgehend im Verborgenen agieren.

Die Bundesrepublik Deutschland als offene und pluralistische Gesellschaft ist aufgrund ihrer geopolitischen Lage, ihrer Rolle in der Europäischen Union und NATO, ihrer ökonomischen Stabilität und nicht zuletzt durch ihre Führungsrolle in einigen Segmenten der Spitzentechnologie für fremde Nachrichtendienste ein äußerst attraktives Ziel (politisch und gesamtwirtschaftlich) - insbesondere im Cyberraum

https://www.verfassungsschutz.de/DE/themen/cyberabwehr/cyberabwehr_node.html;jsessionid=1E3F72ADDB32E797732F584D92DE9D7C.intranet381

dieter.carbon@trutzbox.de

Bundesamt für Verfassungsschutz

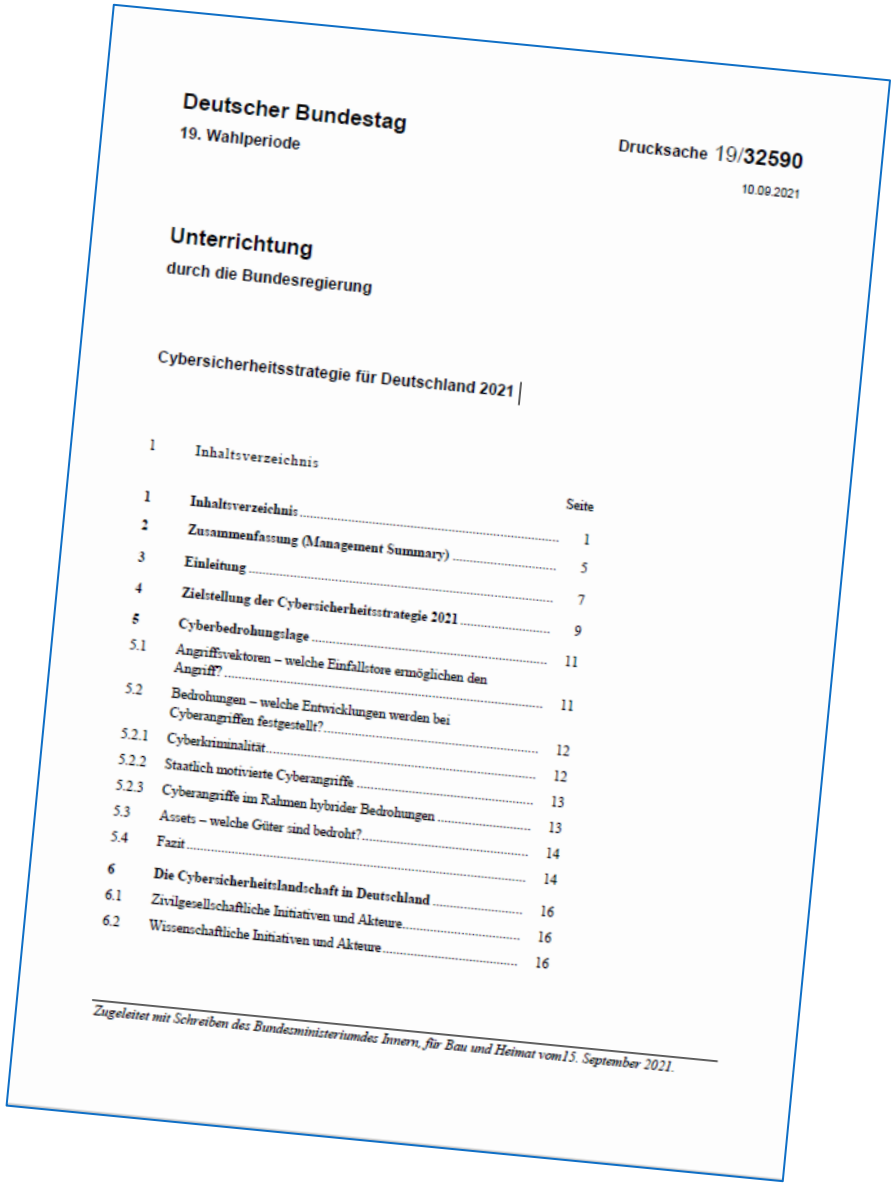


https://www.verfassungsschutz.de/SiteGlobals/Forms/Suche/Publikationensuche_Formular.html?nn=678910

dieter.carbon@trutzbox.de

Bundesministerium des Innern und für Heimat

Cybersicherheitsstrategie für Deutschland 2021



Deutscher Bundestag
19. Wahlperiode

Drucksache 19/**32590**
10.09.2021

Unterrichtung
durch die Bundesregierung

Cybersicherheitsstrategie für Deutschland 2021

1 Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriumdes Innern, für Bau und Heimat vom15. September 2021.

https://www.bundestag.de/presse/hib/kurzmeldungen-865026

dieter.carbon@trutzbox.de

5.1 Angriffsvektoren – welche Einfallstore ermöglichen den Angriff?

Unsichere IT-Systeme – sowohl Hard- als auch Software – stellen ein zentrales Einfallstor für Cyberangriffe dar. Je größer und komplexer Softwareprojekte werden und je mehr Personen dabei in die Erstellung eingebunden sind, desto häufiger entstehen Fehler in der Software, die als Schwachstellen durch Angreifer ausgenutzt werden können. Zwar sorgen zahlreiche Hersteller mittlerweile mit regelmäßigen oder kurzfristigen Updates dafür, festgestellte Schwachstellen zu schließen (Patchen). Jedoch lassen sich nicht immer alle Schwachstellen schließen und auch die schiere Anzahl an Schwachstellen verdeutlich den Bedarf, durch verbesserte Qualitätssicherungsprozesse das Aufkommen von Schwachstellen bereits vor Veröffentlichung zumindest zu reduzieren.

Weitere Ursachen für unsichere IT-Systeme sind fehlerhafte Konfiguration, mangelnde Schutzmechanismen oder Fehlbedienungen der Nutzerinnen und Nutzer. Auch diese Ursachen ermöglichen es unberechtigten Dritten, in fremde Systeme einzudringen und diese zu kompromittieren.

Zusätzlich erweitert die schnell anwachsende Zahl von mit dem Internet verbundenen Geräten (Internet of Things –IoT), wie beispielsweise Lautsprecher, Kühlschränke, Türklingeln, Fahrstühle und Werkzeugmaschinen sowie Medizingeräte, die Möglichkeit potenzieller Cyberangriffsszenarien. Dies wiegt umso schwerer, als viele IoT-Geräte oftmals nur über ein geringes Cybersicherheitsniveau verfügen. Die Schnelllebigkeit dieses Marktes führt häufig zu schlechter Qualität der Software mit großen Sicherheitslücken. Zudem sind Patches nicht oder nicht über entsprechend lange Zeiträume oder nur stark verzögert verfügbar und gegebenenfalls in Ermangelung entsprechender Funktionen beziehungsweise Schnittstellen gar nicht erst einspielbar.

Für die Ausnutzung der Mehrzahl der Schwachstellen bedarf es zumeist auch eines aktiven Zutuns der Nutzenden. Für Angriffe über Schwachstellen wird teilweise auch fehlende Information von Nutzenden ausgenutzt. Der schnelle Klick auf einen unsicheren, schadhaften Link, die Installation von Software aus unbekannten Quellen oder das unbedachte Öffnen eines E-Mail-Anhangs sind typische Alltagsfälle für die Kompromittierung eines IT-Gerätes. Ohne sensibilisierte Nutzende wird ein hohes Niveau an Cybersicherheit daher kaum gelingen.

Bundesministerium des Innern und für Heimat

Cybersicherheitsstrategie für Deutschland 2021

Zu beobachten ist zudem ein sich verstärkender Trend zu Supply-Chain-Angriffen. Hier wird durch den Angreifer eine Soft- oder Hardware während des Herstellungs- oder Pflegeprozesses verändert. Die Manipulation des Angreifers wird dann unmittelbar vom Hersteller mit dem Produkt ausgeliefert. Zum Beispiel wurde im Dezember 2020 bekannt, dass Angreifer ein Update eines Softwareherstellers manipuliert hatten. Die Installation des Updates erfolgte automatisiert. Da die Nutzenden regelmäßig den Updatemechanismen vertrauen, können typischerweise zahlreiche Systeme betroffen sein. Derartige Angriffe stellen ein besonderes Risiko dar, da die manipulierte Software häufig mit Administratorrechten installiert oder betrieben wird und Schutzmechanismen wie Virenscanner zumeist nicht ansprechen. Kundinnen und Kunden sowie Verbraucherinnen und Verbraucher sind regelmäßig arg- und schutzlos.

Insbesondere bewusst herbeigeführte Schwachstellen der Hardware zeigen, dass Cybersicherheit auch eine Frage Digitaler Souveränität ist, da ein nationaler Fertigungsprozess besser beaufsichtigt oder reguliert werden kann. Die Abhängigkeit von Systemen, deren Vertrauenswürdigkeit nicht kontrolliert werden kann, eröffnet potenzielle Einfallstore für Cyberakteure.

Die Chancen neuer Technologien wie KI oder Quantencomputing sind unbestritten. Damit verbunden sind aber auch neue Risiken. Beispielsweise basieren KI-basierte Verfahren häufig auf einem Trainingsprozess und lassen sich in ihrem Verhalten oftmals nicht vollständig nachvollziehen. Aus diesem Grund kann die Integrität dieser Algorithmen gegebenenfalls durch geschickte Auswahl der Eingabemuster oder Trainingsdaten beeinträchtigt werden. Bei einer Verkehrszeichenerkennung führten beispielsweise geschickte Manipulationen der Verkehrszeichen zu fehlerhaften Ausgaben. Um Risiken bei neuen Informationstechnologien zu begegnen, bedarf es jedoch weiterer Forschung und neu zu entwickelnder Technologien.

Bundeskriminalamt

Das Nationale Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) mit Sitz in Bonn ist keine eigenständige Behörde, sondern stellt eine gemeinsame, behörden- und institutionenübergreifende Plattform dar. Es wurde 2011 im Rahmen der Umsetzung der Cyber-Sicherheitsstrategie (CSS) der Bundesregierung gegründet.

Ziele des Cyber-AZ

Im Cyber-AZ sollen relevante Informationen zwischen den beteiligten Behörden und Partnern schnell ausgetauscht und Schutzmaßnahmen zur Gewährleistung der Cyber-Sicherheit in Deutschland koordiniert werden.

Leitbild

Das Cyber-AZ ist DIE Kooperations-, Kommunikations- und Koordinationsplattform der relevanten (Sicherheits-) Behörden unterschiedlicher Ressorts und Ebenen, die insbesondere durch ein gemeinsames, aktuelles und umfassendes Cyber-Sicherheitslagebild für Deutschland, strategische Berichterstattungen sowie durch die koordinierende operative und interdisziplinäre Fallbearbeitung unverzichtbare Beiträge zur gesamtstaatlichen Cyber-Sicherheit und somit - auch im Krisenfall - zur Handlungsfähigkeit der Bundesregierung leistet.

Bundeskriminalamt

Aktuell arbeiten innerhalb des **Nationalen Cyber-Abwehrzentrum** die folgenden acht Kernbehörden und Partner zusammen:

Kernbehörden:
- Bundesamt für den Militärischen Abschirmdienst
- Bundeskriminalamt
- Bundesamt für Sicherheit in der Informationstechnik
- Bundesamt für Verfassungsschutz
- Bundesamt für Katastrophen- und Bevölkerungsschutz
- Bundeswehr-Kommando Cyber- und Informationsraum
- Bundespolizei
- Bundesnachrichtendienst

Partner:
- Cyberabwehr Bayern
- Schwerpunktstaatsanwaltschaften Cyber aus Bamberg und Köln
- Bundesanstalt für Finanzdienstleistungsaufsicht

https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

dieter.carbon@trutzbox.de

Privacy made in Germany

Bundesamt für Sicherheit in der Informationstechnik

Die Digitalisierung mit all ihren Vorzügen wird weiter voranschreiten. Das ist gut so. Wenn wir aber dabei weiterhin die Informationssicherheit vernachlässigen, werden wir niemals das volle Potenzial der Digitalisierung ausnutzen können. Mehr noch: Im schlimmsten Fall werden viele Digitalisierungsprojekte scheitern.

ARNE SCHÖNBOHM, PRÄSIDENT DES BUNDESAMTS FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

dieter.carbon@trutzbox.de

Bundesamt für Sicherheit in der Informationstechnik

PHISHING: CHECKLISTE FÜR DEN ERNSTFALL

WAS IST PHISHING?

Cyber-Kriminelle verschicken betrügerische Nachrichten per E-Mail, über Messenger oder über soziale Netzwerke. Sie fordern Nutzerinnen und Nutzer dazu auf, vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern preiszugeben. Angeschriebene sollen auf einen Link klicken.

Die Gefahr: Die angegebenen Links führen auf gefälschte Internetseiten, auf denen die Daten abgegriffen werden. Die Nachrichten wirken täuschend echt, die Absender seriös. Viele Empfänger schöpfen daher keinen Verdacht und geben ihre Daten den Kriminellen preis.

DAS SOLLTEN SIE TUN, WENN …

… Sie Zahlungsdaten weitergegeben haben:

- ✓ Sperren Sie Ihr Bankkonto.
- ✓ Kontrollieren Sie die Umsätze Ihres Bankkontos und setzen Sie sich mit Ihrer Bank in Verbindung.
- ✓ Nutzen Sie nach der Entsperrung ausschließlich neue Passwörter und PINs für Ihr Konto.

… Sie Zugangsdaten zu Ihrem E-Mail-Konto weitergegeben haben:

- ✓ Vergeben Sie ein neues Passwort.
- ✓ Es kann sein, dass mit dem Zugang zu Ihrem E-Mail-Postfach auch die Zugänge anderer Online-Dienste kompromittiert sind und beispielsweise geändert oder übernommen wurden. Deswegen müssen Sie diese ebenfalls zurücksetzen. Das gilt für Online-Profile, mit denen Sie sich bei anderen Diensten, z. B. einem Online-Shop, anmelden können.

… Sie Zugangsdaten zu anderen Konten, z.B. Online-Shops, weitergegeben haben:

- ✓ Vergeben Sie ein neues Passwort.
- ✓ Nehmen Sie Kontakt mit dem Anbieter auf.
- ✓ Überprüfen Sie zudem, ob Zahlungsdaten betroffen waren und nehmen Sie dementsprechend auch Kontakt mit Ihrer Bank auf.

HINWEIS

Vergeben Sie für alle Online-Account-Zugänge jeweils unterschiedliche Passwörter. Passwort-Manager können dabei hilfreich sein.

Bundesamt für Sicherheit in der Informationstechnik

Wir wollen, dass Sie sicher leben. Ihre Polizei

DAS SOLLTEN SIE TUN, WENN …

… Sie auf einen Link geklickt haben und Geldforderungen bekommen:

- ✓ Zahlen Sie kein Geld an Kriminelle.
- ✓ Wenden Sie sich bei Geldforderungen Unbekannter an die Polizei, die Verbraucherzentrale oder suchen Sie Rat bei einem Rechtsbeistand.

… den Verdacht haben, dass Ihre Daten abgeschöpft wurden:

- ✓ Erstatten Sie in jedem Fall Anzeige bei Ihrer örtlichen Polizeidienststelle – auch bei einem vagen Verdacht. Als Opfer von Internetkriminalität haben Sie die gleichen Rechte wie Opfer anderer Straftaten auch.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR PHISHING

- › Führen Sie Aktualisierungen von Software und Betriebssystemen auf allen Geräten immer sofort durch und installieren Sie Antivirenprogramme.
- › Seien Sie skeptisch bei E-Mails unbekannter Absender. Ihre Bank, Diensteanbieter oder Behörden bitten niemals per E-Mail darum, persönliche Daten wie Passwörter über einen Link zu ändern.
- › Bei Zweifeln lassen Sie sich die Echtheit einer E-Mail vom Absender telefonisch bestätigen. Nutzen Sie dafür nicht die Telefonnummer aus der E-Mail, sondern suchen Sie diese selbst heraus.
- › Vorsicht bei Anhängen mit Formaten wie **.exe** oder **.scr**. Diese können Schadsoftware direkt auf Ihr Gerät laden. Manchmal werden Nutzer oder Nutzerinnen auch durch Doppelendungen wie Dokument **.pdf.exe** in die Irre geführt.
- › Verwenden Sie für die diversen Account-Zugänge möglichst eine Zwei-Faktor-Authentisierung. Durch die zweite Stufe der Identifizierung können Kriminelle selbst dann nicht auf Ihre Daten zugreifen, wenn sie bereits Ihr Passwort erbeutet haben.

Mehr Informationen zum Schutz vor Betrüger-E-Mails unter:
www.bsi-fuer-buerger.de/phishing

Mehr Informationen für Opfer von Internetkriminalität:
www.polizei-beratung.de/opferinformationen/cybercrime/

Bundesamt für Sicherheit in der Informationstechnik

Wir wollen, dass Sie sicher leben. Ihre Polizei

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html

dieter.carbon@trutzbox.de

Privacy made in Germany

Bundesamt für Sicherheit in der Informationstechnik

INFEKTION MIT SCHADPROGRAMMEN: CHECKLISTE FÜR DEN ERNSTFALL

Ein Schadprogramm ist eine Software, die unerwünschte und meist schädliche Funktionen auf einem infizierten PC, Smartphone oder internetfähigem Gerät ausführt. Oft gelangt sie unbemerkt auf ein System, z. B. beim Surfen oder Öffnen von Dateianhängen.

Cyberkriminelle nutzen Schadsoftware als Werkzeug für Datendiebstahl, Online-Betrug oder digitale Erpressung. Täglich kommen unzählige neue Schadprogrammvarianten hinzu.

SO ERKENNEN SIE SCHADPROGRAMME

Wenn Sie einen Sperrbildschirm mit einer Zahlungsforderung sehen, handelt es sich zweifelsfrei um einen Erpressungsversuch nach einer Infektion mit einem Schadprogramm. Hinweise auf Hintergrundaktivitäten eines Schadprogramms sind auch:

Smartphones, deren Akku sich schneller entlädt, oder in Ihrem Namen versendete Spammails an Ihre Kontakte. Bereits in einer solchen Situation sollten Sie Schritte zur Überprüfung der Sicherheit Ihrer Geräte unternehmen.

DAS SOLLTEN SIE TUN, WENN …

… Sie ein Schadprogramm auf Ihrem Gerät vermuten:

- ✓ **Trennen Sie das Gerät vom Netzwerk:** Schalten Sie das WLAN aus oder entfernen Sie das Netzwerkkabel.
- ✓ **Starten Sie einen Virenscan:** Führen Sie auf dem Gerät einen Offline-Virenscan durch. Achten Sie darauf, dass Ihr Virenschutzprogramm aktuell ist.

Eine umfangreiche Schritt-für-Schritt-Anleitung für die Infektionsbeseitigung von Schadsoftware auf PC, Smartphone und Tablet sowie weiteren smarten Geräten finden Sie auf:
www.bsi-fuer-buerger.de/infektionsbeseitigung.

- ✓ **Setzen Sie das System neu auf:** Aufgrund der möglichen Änderungen am System durch das Schadprogramm sollte grundsätzlich eine Neuinstallation des Betriebssystems vorgenommen werden. Smartphone und Tablets sollten Sie auf Werkseinstellungen zurücksetzen.
- ✓ **Ändern Sie Ihre Passwörter:** Beginnen Sie mit dem E-Mail-Konto, das Sie zum Zurücksetzen anderer Passwörter benötigen. Aktivieren Sie wenn möglich eine Zwei-Faktor-Authentisierung.

Bundesamt für Sicherheit in der Informationstechnik

Wir wollen, dass Sie sicher leben. Ihre Polizei

DAS SOLLTEN SIE TUN, WENN …

… Sie mit Ransomware erpresst werden:
Ransomware kann den Zugriff auf Ihre Daten oder Ihr System einschränken bzw. komplett unterbinden. Oftmals wird der Systemzugriff gesperrt oder bestimmte Daten verschlüsselt. Für die Freigabe wird dann ein Lösegeld verlangt.

- ✓ **Zahlen Sie kein Lösegeld:** Zwar kann eine Zahlung zur Entschlüsselung der Daten führen, doch hiervon ist dringend abzuraten.
- ✓ **Anzeige bei der Polizei erstatten:** Wenden Sie sich direkt an eine zentrale Ansprechstelle für Cybercrime. Eine Übersicht finden Sie unter: www.polizei.de.
- ✓ **Entschlüsselung prüfen:** Eine Zusammenstellung kostenfreier Entschlüsselungstools gibt es auf www.NoMoreRansom.org. Das Projekt wird von Europol-EC3 in Zusammenarbeit mit behördlichen und privatwirtschaftlichen Partnern betrieben.
- ✓ **Setzen Sie das System neu auf** wie oben beschrieben.
- ✓ **Ändern Sie Ihre Passwörter.**

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR SCHADPROGRAMMEN

- › **Updates durchführen:** Installieren Sie regelmäßig und zeitnah alle bereitgestellten Sicherheitsupdates. Aktivieren Sie möglichst die Einstellung „automatische Updates".
- › **Schutzprogramme nutzen:** Halten Sie Ihr Virenschutzprogramm immer aktuell.
- › **Firewall aktivieren:** Eine Firewall kann Ihr Gerät zusätzlich vor Angriffen von außen schützen.
- › **Nutzerkonten einrichten:** Verwenden Sie zum Surfen und beim alltäglichen Arbeiten Benutzerkonten mit reduzierten Rechten, damit Schadprogramme keine Administratorenrechte erhalten.
- › **Anhänge und Links prüfen:** Seien Sie vorsichtig beim Öffnen von Links und Anhängen aus E-Mails – auch bei vermeintlich bekannten Absendern. Absenderangaben in E-Mails können einfach gefälscht werden.
- › **Vorsicht beim Download:** Laden Sie Daten, Programme und Apps nur aus vertrauenswürdigen Quellen herunter.
- › **Daten sichern:** Legen Sie regelmäßig Back-ups wichtiger Daten an, um bei Verschlüsselung oder Beschädigung die Daten selbst wiederherstellen zu können.

Mehr Informationen zu Schadprogrammen:
www.bsi-fuer-buerger.de/Schadprogramme

Mehr Informationen für Opfer von Cybercrime:
www.polizei-beratung.de/opferinformationen/cybercrime/

Bundesamt für Sicherheit in der Informationstechnik

Wir wollen, dass Sie sicher leben. Ihre Polizei

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html

dieter.carbon@trutzbox.de

Privacy made in Germany

Chaos Computer Club e. V.

Sicherheit und Vertrauen online schützen:
Gegen eine unbegrenzte Ausweitung von Überwachung und für den Schutz von Verschlüsselung

Forderungen:

Die Unterzeichner dieses gemeinsamen Briefes fordern die Bundesregierung und den Deutschen Bundestag auf, sich für starke Verschlüsselung und den Schutz privater Kommunikation einzusetzen und diese in allen Bereichen von Gesellschaft und Wirtschaft zu fördern. Dies bedeutet konkret:

- Keine weiteren gesetzlichen Maßnahmen zu ergreifen, die eine Schwächung oder das Brechen von Verschlüsselung zur Folge hätten.
- Insbesondere die Mitwirkungspflicht für Unternehmen bei der Reform des Bundesverfassungsschutzrechts zu verzichten, die Unternehmen zum verlängerten Arm der Nachrichtendienste machen und die Cybersicherheit erheblich gefährden würde.
- Die Anpassung des Verfassungsschutzrechts mit der Mitwirkungspflicht nicht in Eile durch das parlamentarische Verfahren zu treiben, sondern die Wirtschaft und Zivilgesellschaft einzubeziehen. Dies erfordert einen Dialog mit Bürgern, Zivilgesellschaft und Industrie.

Insbesondere in der aktuellen globalen Pandemie,
Rolle bei der Aufrechterhaltung des wirtschaftliche
Menschen darauf vertrauen können, dass die Polit
die Integrität von verschlüsselter K

Die Unterz

Bundesverband IT-Mittelstand e.V. (BITMi)

eco – Verband der Internetwirtschaft e. V

G DATA CyberDefense AG

Dr. Sven Herpig,
Leiter Internationale Cybersicherheitspolitik, Stiftung Neue Verantwortung*

mailbox.org
mailbox.com

*Die Zugehörigkeit von Privatpersonen zu Institution

Prostasia Foundation

Chaos Computer Club e. V. (CCC)

Praxonomy

Mega Limited

Riana Pfefferkorn,
Research Scholar, Stanford Internet Observatory*

Blacknight

Software Freedom Law Center

*Die Zugehörigkeit von Privatpersonen zu Institution

Internet Society Bolivia

Law and Technology Research Institute of Recife (IP.rec)

Global Partners Digital

*Die Zugehörigkeit von Privatpersonen zu Institutionen wird nur zur besseren Identifizierung angegeben

https://www.ccc.de/system/uploads/317/original/210601_Gemeinsamer_Brief_G10_BVerfSchG_updated_.pdf

dieter.carbon@trutzbox.de

Privacy made in Germany

Chaos Computer Club e. V.

CCC veröffentlicht Formulierungshilfe für Digitales im neuen Regierungsprogramm

Überwachung

- Verbot biometrischer Überwachung im öffentlichen Raum:
  Die Verwendung von Systemen zur biometrischen Überwachung muss im öffentlichen Raum grundsätzlich und ausnahmslos untersagt sein.
- Abschied von der Vorratsdatenspeicherung:
  Die Vorratsdatenspeicherung hat sich als weitgehend ungeeignet herausgestellt und wurde immer wieder von Höchstgerichten wegen des unverhältnismäßigen Grundrechtseingriffs gekippt. Statt gebetsmühlenartig bei jeder sich bietenden Gelegenheit für die Einführung einer weitgehend unwirksamen und verfassungsrechtlich bedenklichen Methode zu plädieren, sollte von weiteren Bestrebungen in dieser Richtung endgültig Abstand genommen werden. Die Vorratsdatenspeicherung ist und bleibt ein zivilisatorischer Rückschritt und wird eine gefährliche Vorbildwirkung entfalten, die es zu verhindern gilt.
- Abschied von Kryptoverboten:
  Wer Verschlüsselung kriminalisiert, sorgt dafür, dass nur noch Kriminelle Verschlüsselung nutzen. Der Versuch, diese Technik künstlich zu schwächen oder Zweitschlüssel hinterlegen zu lassen, hebelt die Sicherheit Millionen gesetzestreuer Menschen aus, während Kriminelle weiterhin starke Verschlüsselung nutzen. Künftige Regierungen sollten sich für die Stärkung von Verschlüsselung und damit die Erhöhung der weltweiten IT-Sicherheit einsetzen. Formelle oder informelle Verpflichtungen von Betreibern von Systemen zur Aushebelung von Verschlüsselung dürfen grundsätzlich nicht stattfinden.
- Beachtung der Überwachungsgesamtrechnung:
  Die vom Bundesverfassungsgericht mehrfach angemahnte Beachtung der Gesamtheit der Überwachungsmaßnahmen und Datenerfassung muss Eingang in die konkrete Rechtssprechung finden.

Chaos Computer Club e. V.

CCC veröffentlicht Formulierungshilfe für Digitales im neuen Regierungsprogramm

- **IT-Sicherheit**
- Es bedarf einer grundlegenden Erhebung des Zustands von IT-Systemen in kritischen Infrastrukturen. Darauf aufbauend muss ein konkreter und zeitnaher Plan zum Beheben der vorgefundenen Probleme und Schwachstellen entwickelt und umgesetzt werden
- Unabhängiges BSI: Solange das BSI dem Innenministerium untersteht, kann es seinem Auftrag wegen konträrer Interessen nicht kompromisslos gerecht werden. Wenn das BSI nicht vollständig von allen Aufgaben und Abhängigkeiten im Bereich der inneren Sicherheit befreit wird, kann es keine vertrauenswürdige Instanz, z. B. für die Bearbeitung von gemeldeten Sicherheitslücken oder Überprüfungen von Software sein.
- Der Staat und seine Organe müssen alle IT-Sicherheitslücken, die ihm bekannt werden, sofort den Herstellern melden und unmittelbar zu ihrer zeitnahen Schließung beitragen.
- Verbot der Verwendung von Bundesmitteln zur Beschaffung von Angriffswerkzeugen (Staatstrojaner) durch Sicherheitsbehörden.
- Entkriminalisierung von IT-Sicherheitsforschung: Abschaffen des Hackerparagraphen § 202c StGB
- Wer IT-Sicherheitslücken aufdeckt und veröffentlicht, bleibt grundsätzlich straffrei, selbst wenn die Aufdeckung in Form eines Proof-of-Concept-Exploits passiert. Zur Inanspruchnahme dieser Regelung genügt die gleichzeitige Meldung der Sicherheitslücke an das BSI oder eine andere geeignete Stelle.

Chaos Computer Club e. V.

CCC veröffentlicht Formulierungshilfe für Digitales im neuen Regierungsprogramm

- Produkthaftung für Softwareentwicklung. Hersteller von softwarebasierten Systemen dürfen nicht länger de facto von Haftung für die Qualität und Funktionsfähigkeit ihrer Produkte ausgenommen sein.
- Herstellerhaftung für das Verschleppen der Behebung von IT-Sicherheitslücken: Nach einer kurzen Frist haftet der Hersteller für Schäden, solange kein Patch verfügbar ist.
- Wer verfügbare Security-Patches nicht einspielt, haftet für Schäden, die dadurch verursacht werden. Schäden gegenüber Dritten müssen erstattet werden. Dafür ist eine Trennung von Security- und Funktionsupdates notwendig.
- Hersteller von notorisch unsicherer Software müssen von der Beschaffung durch den Bund ausgeschlossen werden. Kein weiterer Einkauf von Komponenten aus öffentlicher Hand bei Herstellern, die keine adäquate IT-Sicherheitskultur pflegen.
- Software, die im Umfeld gesellschaftlich kritischer Vorgänge Verwendung findet (z. B. Software zur Auszählung von Wahlstimmen), bedarf einer expliziten Freigabe nach Audit durch das BSI und muss grundsätzlich quelloffen sein.

https://www.ccc.de/de/updates/2021/ccc-formulierungshilfe-regierungsprogramm

dieter.carbon@trutzbox.de

Privacy made in Germany

Hack Back

Analoges Modell (Beispiel)

1	Wir werden mit Raketen beschossen.	Wie kann man einen Angriff erkennen?
2	Wir stellen fest, von wo (Standort der Startrampen) die Raketen abgeschossen wurden.	Wie kann man den Ausgangsort des Angriffs feststellen?
3	Wir planen einen Gegenschlag mit Raketen.	Wie kann ein Gegenschlag aussehen? Wer wird wann, wie und wo bekämpft?
4	Maßnahme: wir bekämpfen die abschießenden (und weitere) Startrampen.	Welche Mittel werden gegen wen und wo eingesetzt?

Cyber - Modell

1		Wie kann man einen Angriff erkennen?
2		Wie kann man den Ausgangsort des Angriffs feststellen?
3		Wie kann ein Gegenschlag aussehen? Wer wird wann, wie und wo bekämpft?
4		Welche Mittel werden gegen wen und wo eingesetzt?

AG KRITIS, Manuel ‚HonkHase' Atug

- Unsere Arbeitsgruppe ist vollständig unabhängig von Staat oder Wirtschaft. Wir vertreten keine Interessen von Unternehmen oder Wirtschaftsverbänden, sondern unser Ziel ist es einzig und allein, die Versorgungssicherheit der Bevölkerung zu erhöhen.
- Wir sind derzeit ca. 42 Fachleute (Fachfrauen und Fachmänner) und Experten, die sich täglich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 (10) BSI-Gesetz i. V. m. BSI-Kritisverordnung beschäftigen, z. B. durch Planung, Bau, Betrieb, Beratung oder Prüfung der beteiligten IT-Systeme und Anlagen. Unsere Arbeitsgruppe KRITIS besteht u. A. aus Mitgliedern, die in den Sektoren Energie, Gesundheit, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Wasser sowie Staat und Verwaltung als auch Medien und Kultur dienstlich aktiv sind.
- Wir sind kein Wirtschaftsverband, haben keine Sponsoren und sind auch kein Unternehmen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der IT-Sicherheit kooperativ mit allen Beteiligten herbei zu führen.
- Unsere Gruppe eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen unserer Bundesrepublik zur Reaktion auf Großschadenslagen durch Cyber-Vorfälle im Bereich der Kritischen Infrastrukturen nicht ausreichen, um die Auswirkungen der dadurch verursachten Krisen und Katastrophen zu bewältigen.

AG KRITIS, Manuel ‚HonkHase‘ Atug

Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen

- Während im klassischen Katastrophenfall die überwiegend ehrenamtlichen Helfer der privaten Hilfsorganisationen und im weiteren die behördlichen Einrichtungen für den Schutz der Bevölkerung zur Verfügung stehen und gewährleisten, dass auch in außergewöhnlichen Situationen ausreichende Hilfe zur Verfügung steht, existieren ehrenamtliche Strukturen für digitale Katastrophenfälle bislang nicht.

- Die quantitative Zunahme von IT und OT, deren lange Betriebsdauer, die hohe Geschwindigkeit des technischen Fortschritts und die immer stärkere Vernetzung der Systeme vergrößern jeweils für sich die Eintrittswahrscheinlichkeit einer großflächigen oder sogar katastrophalen Störung unserer lebensnotwendigen und damit Kritischen Infrastrukturen.

- In Deutschland gibt es aktuell fast 2.000 Kritische Infrastrukturen. Dem gegenüber stehen etwa 15 hauptamtliche Mitarbeiter des BSI MIRT, die im Krisenfall unter Umständen auf ein niedriges Vielfaches dieser Zahl aufgestockt werden können. Um bei Schadenslagen, deren Größe und potentielle Auswirkungen die Kapazitäten der Behörden übersteigen, trotzdem schnelle Hilfe zur Wiederherstellung der kritischen Dienstleistungen bereitstellen zu können, müssen sich unserer Ansicht nach auch zivile Helfer organisieren und ihre Kräfte bündeln, analog zu den bereits existierenden Hilfsorganisationen auf anderen Gebieten.

AG KRITIS, Manuel ‚HonkHase' Atug

Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen

Die AG KRITIS strebt daher die Gründung eines Cyber-Hilfswerks (CHW) an. Das „Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen" kann über den nachfolgenden Link abgerufen werden:


AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Das Cyber-Hilfswerk

Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen

Version 1.0 – veröffentlicht am 07.02.2020

1

https://ag.kritis.info/chw-konzept/

https://ag.kritis.info/wp-content/uploads/2020/02/chw-konzept_v1.0.pdf

dieter.carbon@trutzbox.de

Privacy made in Germany

sichere-industrie.de

Manuel Atug
HiSolutions AG

Ransomware- und andere Cyberangriffe ↗

Gibt es eine Entwicklung im Bereich Industrial Security, die aus Ihrer Sicht für das Jahr 2021 besonders war?

Ja, es gibt da was Besonderes, leider. Es ist besonders traurig zu sehen, wie oft inzwischen im Bereich Industrial Security Ransomware- und andere Cyberangriffe erfolgreich durchgeführt werden und wie das kontinuierlich steigt. Gegenmaßnahmen haben offenbar weder das IT-SiG 2.0 bewirkt noch die ganzen Befugniserweiterungen oder offensiven Vorgehensweisen, welche die Regierung mit den Sicherheitsbehörden da als vermeintliche Allheilmittel sieht.

Wichtig ist daher, dass ein Umdenken stattfindet, hin zur Erhöhung der Cyberresilienz von ICS-Umgebungen, so dass die Widerstandsfähigkeit gegenüber Cybervorfällen kontinuierlich steigen kann.

Verändert die zunehmende Marktanforderung nach Security Ihrer Einschätzung nach etwas spürbar in den Unternehmen?

Bei kritischen Infrastruktur-Betreiberinnen kommt so langsam Bewegung in die Security-Fragestellungen da, wo es beispielsweise durch das BSI-Gesetz reguliert und vorgegeben ist. Aber auch hier könnte es deutlich zügiger gehen und es könnte deutlich mehr passieren, so dass seltener Ausfälle geschehen.

Es ist also weiterhin sehr viel zu tun. Insbesondere stelle ich fest, dass die Awareness inzwischen überall vorhanden ist, allerdings ist das Verständnis, was dies für die eigenen Risiken bedeutet, nicht sehr ausgeprägt. Hier muss also noch die Transformation passieren. Gegebenenfalls müssen auch die richtigen Anreize geschaffen werden, angereichert mit Incentivierungen, so dass Security in solchen Umgebungen verstanden und eingebracht wird und am Ende alle davon profitieren.

Verständnis, was dies für die eigenen Risiken bedeutet

»Wichtig ist daher, dass ein Umdenken stattfindet, hin zur Erhöhung der Cyberresilienz von ICS-Umgebungen, so dass die Widerstandsfähigkeit gegenüber Cybervorfällen kontinuierlich steigen kann.«

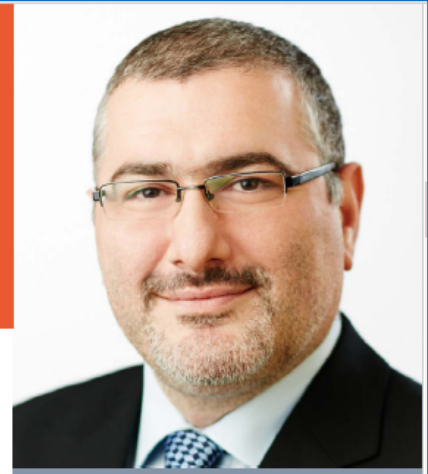
Was ist Ihrer Meinung nach die größte Herausforderung im Kontext Security für 2022?

Die desolate Cybersicherheitspolitik in Deutschland. Es ist ein Cyberwimmelbild der Verantwortungsdiffusion an verschiedensten Akteuren mit unklaren Zuständigkeiten vorhanden und ständig kommen weitere Akteure dazu.

Gefühlt müssen Sicherheitsmaßnahmen auch und insbesondere für Industrial-Security-Umgebungen - also beispielsweise kritische Infrastrukturen - gegen die Vorstellungen der Regierung eingebracht werden.

Speziell der KRITIS-Sektor Staat und Verwaltung, zu dem durchaus auch kommunale Betreiberinnen mit ICS-Umgebungen gehören, unterliegt weiterhin keinen klaren Security-Anforderungen. Hier sind immerhin schon die KRITIS-Betreiberinnen durch BSIG § 8a deutlich weiter, aber noch lange nicht am Ziel. Ohne diese Anforderungen wird es sehr herausfordernd, Security in Zukunft zu erhöhen oder besser zu etablieren und kontinuierlich zu leben.

desolate Cybersicherheitspolitik in Deutschland



Manuel Atug
Head of Business Development
HiSolutions AG

Zu beobachten ist zudem ein sich verstärkender Trend zu Supply-Chain-Angriffen. Hier wird durch den Angreifer eine Soft- oder Hardware während des Herstellungs- oder Pflegeprozesses verändert. Die Manipulation des Angreifers wird dann unmittelbar vom Hersteller mit dem Produkt ausgeliefert. Zum Beispiel wurde im Dezember 2020 bekannt, dass Angreifer ein Update eines Softwareherstellers manipuliert hatten. Die Installation des Updates erfolgte automatisiert. Da die Nutzenden regelmäßig den Updatemechanismen vertrauen, können typischerweise zahlreiche Systeme betroffen sein. Derartige Angriffe stellen ein besonderes Risiko dar, da die manipulierte Software häufig mit Administratorrechten installiert oder betrieben wird und Schutzmechanismen wie Virenscanner zumeist nicht ansprechen. Kundinnen und Kunden sowie Verbraucherinnen und Verbraucher sind regelmäßig arg- und schutzlos.

Insbesondere bewusst herbeigeführte Schwachstellen der Hardware zeigen, dass Cybersicherheit auch eine Frage Digitaler Souveränität ist, da ein nationaler Fertigungsprozess besser beaufsichtigt oder reguliert werden kann. Die Abhängigkeit von Systemen, deren Vertrauenswürdigkeit nicht kontrolliert werden kann, eröffnet potenzielle Einfallstore für Cyberakteure.

Die Chancen neuer Technologien wie KI oder Quantencomputing sind unbestritten. Damit verbunden sind aber auch neue Risiken. Beispielsweise basieren KI-basierte Verfahren häufig auf einem Trainingsprozess und lassen sich in ihrem Verhalten oftmals nicht vollständig nachvollziehen. Aus diesem Grund kann die Integrität dieser Algorithmen gegebenenfalls durch geschickte Auswahl der Eingabemuster oder Trainingsdaten beeinträchtigt werden. Bei einer Verkehrszeichenerkennung führten beispielsweise geschickte Manipulationen der Verkehrszeichen zu fehlerhaften Ausgaben. Um Risiken bei neuen Informationstechnologien zu begegnen, bedarf es jedoch weiterer Forschung und neu zu entwickelnder Technologien.

Überwachungs-Geräte



Festnetz-Abhörgerät über GSM-Funk

Artikel-Nr.: 12225

- **Live-Telefonüberwachung ohne Limit.**
- Kein Entfernungslimit zum Anschluss.
- Weltweit in allen Netzen einsetzbar.
- Alle Telefonate parallel mithörbar.
- Gespräche werden aufgezeichnet.
- **Hochleistungsakku für bis 6 Monate.**

Lieferzeit: 3-4 Tage

349,00 € zzgl. USt.

Menge

1

In den Warenkorb

dieter.carbon@trutzbox.de

Privacy made in Germany

Überwachungs-Geräte

IP-LAN HD SpyCam im Netzteil

Artikel-Nr.: 24008

- **Mini IP/LAN HD SpyCam versteckt im Netzteil.**
- **Video, Foto & Audio übers Netzwerk mittels Handy betrachten.**
- **Energieversorgung mit 220-V**, kein Akku notwendig.
- Speicherung auf **Micro SD-Karte bis zu 32 GB.**
- Automatische Aufzeichnung bei Bewegungserkennung.
- Betriebszeit: unbegrenzt durch Netzstrom.
- **Arbeitszeit: 24 Stunden, jeden Tag!**

239,00 € zzgl. USt.

Ausverkauft !

ihremail@email.de

Wenn lieferbar, bitte benachrichtigen

dieter.carbon@trutzbox.de

Privacy made in Germany

Überwachungs-Geräte

HD SpyCam getarnt in der Krawatte, 4 GB

Artikel-Nr.: 24017

- **Für diskrete, unauffällige Video-Aufnahmen mit Ton.**
- Stilvolle Krawatte mit getarnter Spionagekamera.
- Trägt nicht auf: Komplette Krawatte bleibt sehr flach.
- Kamera-Linse perfekt integriert im Muster der Krawatte.
- **4GB interner Speicher.**
- **Bedienung via mini Fernbedienung mit Abstand bis 15m.**
- Datentransfer zu PC, Notebook über USB 2.0
- Nimmt brillante Videos mit glasklarem Ton überall auf.

Lieferzeit: 3-4 Tage

219,00 € zzgl. USt.

Menge

1

In den Warenkorb

dieter.carbon@trutzbox.de

Privacy made in Germany

Überwachungs-Geräte

IP-LAN SpyCam im Rauchmelder

Artikel-Nr.: 24029

- Raum-Übersicht dank riesigem Panorama-Bildwinkel.
- **Ip-LAN-Spy-Cam Video-, Foto-, reine Tonaufnahme.**
- **Weltweite Zugriff- jederzeit und überall.**
- Speicher: **Micro-SD-Speicherkarten bis zu 64 GB.**
- Unterstützt Bewegungserkennung und Infrarot-Nachtsicht.
- **Steuerbar per App für Android und iOS.**

Lieferzeit: 3-4 Tage

249,00 € zzgl. USt.

Menge

1

In den Warenkorb

dieter.carbon@trutzbox.de

Privacy made in Germany

Überwachungs-Geräte

WIFI HD-SpyCam in LED-Lampe

Artikel-Nr.: 24036

- **HD-Kamera mit riesigem 360 ° Sichtfeld.**
- **WiFi-kompatibel, einfache Installation.**
- **Weltweiter Fernzugriff per Gratis-App für Android + iOS.**
- **2-Wege-Audio dank Mikrofon und Lautsprecher!**
- **Mit Kartensteckplatz für TF-Karte, bis 64 Gb.**
- **Mit Loop-Modus EndlosAufnahmen möglich.**
- **Für jeden E27-Lampensockel geeignet.**
- **Hohe Qualität, stabile Performance.**

Lieferzeit: 3-4 Tage

218,00 € zzgl. USt.

Menge

1

In den Warenkorb

dieter.carbon@trutzbox.de

Privacy made in Germany

Überwachungs-Geräte

GSM-Abhörgerät in Steckerleiste mit 4x USB

Artikelnummer:14907

- **GSM-Abhörgerät in funktionsfähiger Steckerleiste mit 4x USB**
- **Globale Raumüberwachung via Handy-Netz, weltweit !**
- **Weltweit einsetzbar für reine akustische Raumüberwachung.**
- **Im Dauerbetrieb mit ausgezeichneten akustischen Daten.**
- **Ideal für Dauer-Überwachungsaufgaben z.B.: als Babyfone oder zur akkustischen Überwachung von Alten und Kranken.**
- **Auch sehr gut geeignet zur akkustischen Gebäudekontrolle.**
- **Mit autom. RÜCKRUF-FUNKTION bei Geräuscherkennung.**

Lieferzeit: 3-4 Tage

298,00 € **zzgl. USt.**

Menge:

https://www.spydiscount24.com/gsm-abhoergeraet-steckerleiste-4x-usb

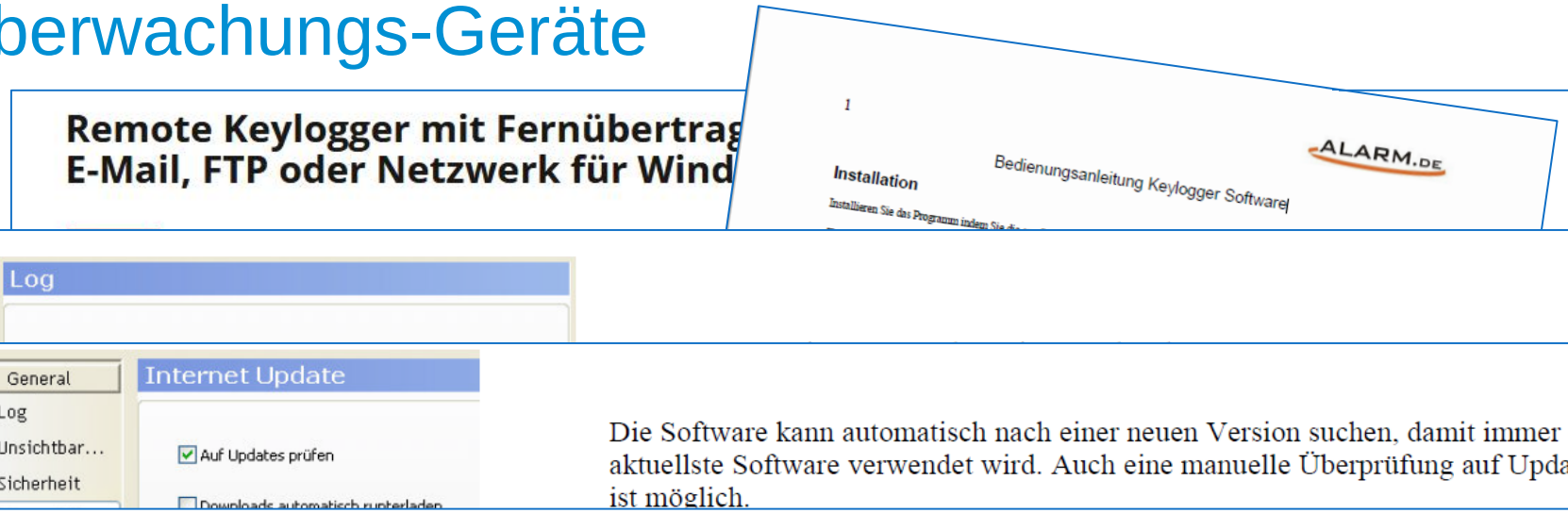
dieter.carbon@trutzbox.de

Privacy made in Germany

Überwachungs-Geräte

dieter.carbon@trutzbox.de

Überwachungs-Geräte



Rechtliche Erläuterung zum Keylogger

Der Einsatz auf fremden Rechnern ohne Einwilligung des Besitzers ist nicht erlaubt. Die Software verfügt über Überwachungsfunktionen (insbesondere "Aufnahme der Tastenanschläge" und "Bildschirmaufnahme"), die der Genehmigung der zu überwachenden Personen bedarf.

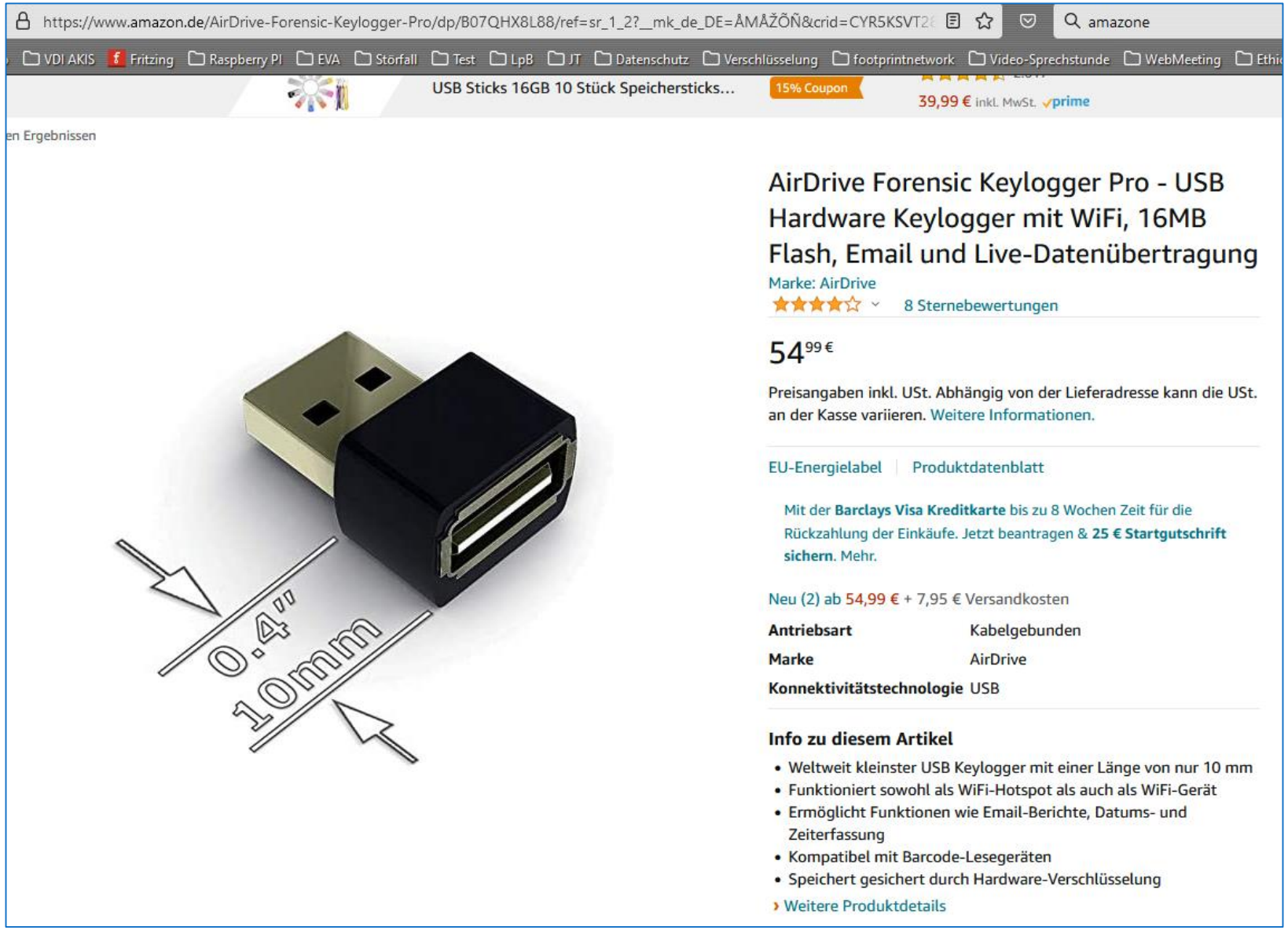
In Deutschland kann der heimliche Einsatz von Keyloggern an fremden Computern als Ausspähen von Daten gemäß § 202a des Strafgesetzbuches strafbar sein. Unternehmen, die Keylogger an den Firmencomputern einsetzen wollen, müssen zuvor die Zustimmung des Betriebsrats einholen. Gemäß Ziffer 22 des Anhangs zur Bildschirmarbeitsverordnung darf "ohne Wissen der Benutzer (...) keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden". Damit ist dem Arbeitgeber ein heimlicher Einsatz von Überwachungssoftware und -hardware wie beispielsweise Keyloggern verboten. § 87 Absatz 1 Nr. 6 des Betriebsverfassungsgesetzes bestimmt darüber hinaus, dass "Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen", der Mitbestimmung des Betriebsrats bzw. im öffentlichen Dienst des Personalrats, vgl. § 75 Abs. 3 Nr. 17 BPersVG unterliegen.

Bei Verwendung der Software in anderen Ländern müssen Sie sich über die dortigen gesetzlichen Bestimmungen informieren und diese beachten.

https://www.alarm.de/alarm/keylogger-software.pdf

dieter.carbon@trutzbox.de

Überwachungs-Geräte



dieter.carbon@trutzbox.de

Technische Werke Ludwigshafen (1/4)

- Technische Werke Ludwigshafen TWL, ca. 700 Mitarbeiter
- April 2020: Administrator stellt fest, dass Cyber Angriff erfolgt (ist)
- Interne Kommunikation, LAgebesprechung: Beauftragter für Informationssicherheit, TWL-Datenschutzbeauftragter und entsprechender Vorstand
- Externe Kommunikation: mit Polizeipräsidium Rheinpfalz, Dezernat für Cyberkriminalität K 16, Landeskriminalamt Rheinlandpfalz und TWL-beratende Security Firma
- Hinzuziehung BSI, da Kompromittierung von OT (Operation Technology; Netzleittechnik zur Steuerung der Strom-, Gas-, Wasser- und Fernwärme Versorgung und des Kraftwerks) nicht ausgeschlossen werden kann
- OT und IT (Information Technology; Mail-, CRM- und andere Büro-Anwendungen) sind über zwei Firewalls voneinander getrennt
- Am Folgetag: Informationen an den Landesdatenschutzbeauftragten und noch in der ersten Woche wird eine auf IT- und Datenschutz-Recht spezialisierte Rechtsanwaltskanzlei informiert und hinzugezogen, speziell um Fehler bei der Außenkommunikation zu vermeiden
- Unmittelbar danach wird ein K-Team gegründet, wobei das „K“ zunächst für „Krise“ steht - später für „Kompetenz“ - zunächst bestehend aus vier Personen, und dann erweitert um Vorstände, Leiterin Konzern-Kommunikation, Vertriebsleiter, Leiter Recht und weitere.

Technische Werke Ludwigshafen (2/4)

- Beratende Security Firma verifiziert , was Admins vermutet hatten: Erst-Infektion am 13. Februar durch eine E-Mail mit Hyperlink.
- Daraus wird geschlossen, dass TWL nicht Opfer eines gezielten Angriffs wurde, sondern einer breit gestreuten Kampagne durch eine einfache Phishing E-Mail, wie fast jeder schon einmal eine erhielt.
- „Die menschliche Firewall hatte vier Chancen, die Infektion zu verhindern“.
  - Die Phishing Mail war Teil einer groß angelegten Kampagne, die über ganz Deutschland lief und die E-Mail ist mit dem Absender „Kopierer“ versehen (seltsam: Auffallgrund 1). Wenn sich jemand von TWL beim Kopierer mittels Karte identifiziert und einen Scan macht, wird dieser als PDF per E-Mail mit Absender „Mitarbeiter-Mail-Adresse“ an den Mitarbeiter geschickt.
  - Zudem hat eine Überwachungssoftware in die Betreff-Zeile der besagten E-Mail „suspect“ eingefügt (seltsam: Auffallgrund 2).
  - Im Anhang war nicht ein erwartetes PDF, sondern ein HTML-Link-Dokument(seltsam: Auffallgrund 3).
  - Durch Doppel-Klick auf den Anhang wird eine Excel-Datei heruntergeladen mit der Aufforderung: „Wenn Sie den Inhalt dieser Datei sehen möchten, dann klicken Sie auf Makros aktivieren.“ (seltsam: Auffallgrund 4), was prompt vom Mitarbeiter „befolgt“ wurde.

Technische Werke Ludwigshafen (3/4)

- Dies sind vier Merkwürdigkeiten und Auffallgründe, die umso mehr befremden, als dass diese „menschliche Schwachstelle“ zwei Monate vorher ein Awareness E-Learning Modul zum Thema Mail-Phising erfolgreich absolvierte. Hierin wurden alle Fähigkeiten vermittelt, solche Angriffe zu erkennen und zu vermeiden.
- Als Sofortmaßnahme erfolgt die physische Trennung von IT und OT.
- Danach wird ein Restore aus dem Backup getestet, was funktioniert, sodass das Backup verwendet werden kann und Funktionstests sind auch erfolgreich.
- Zu dem Zeitpunkt ist unbekannt, wie tief die Angreifer im System sind und die Backups werden offline genommen.
- Im weiteren Verlauf ist nicht konkret klärbar, wie tief und verbreitet die Angreifer eindringen konnten. Daraufhin wird die Empfehlung ausgesprochen, die Microsoft-basierte Infrastruktur zu ersetzen.
- Im Februar erfolgt der Angriff, im April wird er erkannt und im Juni genehmigt der Aufsichtsrat den Ersatz und Neu- und Parallel-Aufbau der gesamten Infrastruktur mit allen dazugehöriger IT-Komponenten, wie Server und PCs.

Technische Werke Ludwigshafen (4/4)

Erkenntnisse führen zu den Fragen:

1. Sind Awareness-Maßnahmen wirkungsvoll? Reichen Schulungen aus, oder sind Trainings besser?
2. Sind IT und OT „sauber“ getrennt?
3. Ist die IT ausreichend kleingliedrig segmentiert?
4. Besteht ein ausreichendes, internes Logging?
5. Besteht ein Zero-Trust Ansatz?
6. Werden externe Penetrationstest regelmäßig und unabhängig durchgeführt?
7. Sind Backups „emergency-sicher“
8. Sind Notfallpläne aktuell und umsetzbar?
9. Besteht regelmäßiger Kontakt mit zuständigen Behörden auch zu Nicht-Vorfall-Zeiten?
10. Besteht ein Informationsaustausch mit ähnlich aufgestellten Institutionen und Unternehmen?
11. Ist die private IT-Nutzung im Unternehmen sicherheitsrelevant geregelt?
12. Sind disziplinarische Konsequenzen bei Fehlverhalten definiert und werden sie auch konkret angewandt?
13. Sind Notfallnummern definiert und operabel?
14. Gibt es ein redundantes Notfall-Kommunikationsnetz?
15. Kann Operations redundant und ggf. isoliert betrieben werden?
16. Ist das Unternehmen IT-rechtlich gut beraten?
17. Werden im Bedarfsfall die relevanten Instanzen (LDSB, BSI, LKA, Beratungsfirmen, usw.) transparent involviert?
18. Existiert ein professionelles Krisenkonzept?
19. Gibt es ein Business Continuity Konzept?
20. …

dieter.carbon@trutzbox.de

Empfehlungen

z.B.

„DHL-Mitteilung“

Dritt-Anbieter-Sperre

Empfehlungen

dieter.carbon@trutzbox.de

Empfehlungen

- Der ultimative Schutz Ihrer Accounts: Verwalten von bis zu 60 TOTP-Konten
- Sichere Zwei-Faktor-Authentisierung (2FA) mit TOTP: Wirkungsvoller Schutz vor Identitäts-Diebstahl
- Für Smartphone, Tablet, Notebook oder Desktop
- Bei allen führenden Online-Plattformen sofort nutzbar
- Sicherheit aus Deutschland

Time-based One-time Password Algorithmus

Der Time-based One-time Password Algorithmus (TOTP) ist ein Verfahren zur Erzeugung von zeitlich limitierten Einmalkennwörtern basierend auf dem Keyed-Hash Message Authentication Code, welcher im Rahmen der Authentifizierung Anwendung findet.
Das Verfahren basiert im Kern auf einer kryptografischen Hash-Funktion HMAC, mit deren Hilfe aus dem zwischen Sender und Empfänger vereinbarten und geheimen Schlüssel K und der absoluten Uhrzeit ein kryptografischer Hash-Wert berechnet wird. ... Das Einmalkennwort ist innerhalb dieser Dauer von 30 Sekunden gültig. ... Wesentlich bei diesem Verfahren ist, dass die beiden Systeme, Sender und Empfänger, über hinreichend genaue Uhren oder über einen Zugang wie dem Network Time Protocol (NTP) zu einer genauen Uhrzeitinformation verfügen müssen, da andernfalls die Authentifizierung fehlschlägt.

https://shop.reiner-sct.com/authenticator/reiner-sct-authenticator

https://de.wikipedia.org/wiki/Time-based_One-time_Password_Algorithmus

dieter.carbon@trutzbox.de

Empfehlungen

CovPass Check 12+
Corona-Impfnachweise prüfen
Robert Koch-Institut
Entwickelt für iPhone
Nr. 5 in Gesundheit und Fitness
★★★☆☆ 3,1 • 374 Bewertungen
Gratis

für iOS Geräte

https://apps.apple.com/de/app/covpass-check/id1566140314

Die CovPassCheck-App

COVID-Zertifikate der EU direkt per App prüfen

Die CovPassCheck-App ist eine sichere Lösung für unter anderem Gewerbetreibende und Behörden. Nur mit der CovPassCheck-App können digitale COVID-Zertifikate der EU zuverlässig geprüft werden.

für Android Geräte

https://play.google.com/store/apps/details?id=de.rki.covpass.checkapp&hl=en_US&gl=US

dieter.carbon@trutzbox.de

Empfehlungen

1. Backup machen! (off-line, off-site)
2. Traue ich dem Anbieter?
3. Traue ich der Technik des Anbieters?
4. Updates einspielen
5. Notfall-Planung

dieter.carbon@trutzbox.de

Danke für Ihr Interesse!

Gibt es Fragen … ?

dieter.carbon@trutzbox.de

Das war‘s …

Vielen Dank für Ihre Teilnahme,

bis zum nächsten Mal ☺,

bleiben Sie gesund

und haben Sie eine sichere Zeit!

Dieter Carbon

dieter.carbon@trutzbox.de

Privacy made in Germany