trutzbox
back to privacy

IT Lunch

Webinar des IT Klub Mainz & Rheinhessen e.V.

am 20.05.2020 um 14:00 Uhr

„Machen Sie Webmeeting? Aber sicher!“

Hintergründe zur passiven Gefährdung

Dieter Carbon, Comidio GmbH

Privacy made in Germany

Gestatten …

trutzbox
back to privacy

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

VDI

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

Privacy made in Germany

Der Werbeblock …

Sichere Kommunikation für **Unternehmen**

Die TrutzBox® bietet filterbare und pseudonymisierte Webzugriffe, verschlüsselten E-Mail-Austausch und sichere, autarke Webmeetings!

VDI Arbeitskreis Internet-Sicherheit

trutzbox
back to privacy

Datum	Zeit	Inhalt / Titel	Referent	Firma / "Herkunft"
Mi 02.11.2016	19:00 - 21:00	Sie kennen dich! Sie haben dich! Sie steuern dich! Die wahre Macht der Datensammler	Markus Morgenroth	IT Berater, Buchautor, Speaker
Mi 07.12.2016	19:00 - 21:00	Wie werden unsere Internetaktivitäten von kommerziellen Firmen mitbeobachtet?	Hermann Sauer	GF Comidio GmbH
Mi 01.02.2017	19:00 - 21:00	Bilder von jedem – überall? Öffentliche und private Videoaufzeichnungen	Prof. Dr. Dieter Kugelmann	der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Mi 01.03.2017	19:00 - 21:00	Browser Fingerprinting: mich kennt doch keiner!	Gaston Pugliese	Friedrich-Alexander-Universität Erlangen-Nürnberg
Sa 29.04.2017	13:00 - 17:00	Workshop: Browser und Surfen	Hermann Sauer	GF Comidio GmbH
Mi 03.05.2017	19:00 - 21:00	Forensik- und Internetkriminalität	Prof. Dr. Harald Baier	Hochschule Darmstadt
Mi 07.06.2017	19:00 - 21:00	Herausforderungen bei der Einführung von Mailverschlüsselung im Unternehmen	Hans-Joachim Giegerich	Geschäftsführer Giegerich & Partner GmbH
Sa 19.08.2017	13:00 - 17:00	Workshop: E-Mail und -Verschlüsselung	Dieter Carbon	
Mi 06.09.2017	19:00 - 21:00	Tatort Internet – Schwachstelle Mensch!	Markus Wortmann	Kriminologe und Polizeiwissenschaftler, Geschäftsführer SICHERES NETZ HILFT e.V.
Mi 04.10.2017	19:00 - 21:00	IT-gestützte Wirtschaftsspionage	Timo Keim, Guido Jost	Landesamt für Verfassungsschutz Hessen, Verfassungsschutz Rheinland-Pfalz
Mi 06.12.2017	19:00 - 21:00	Daten als „wohlerworbene Rechte“	Prof. Dr. Michael Ronellenfitsch	der Hessische Datenschutzbeauftragte
Mi 07.02.2018	19:00 - 21:00	Warum wir es Hackern zu leicht machen	Frank Ewert	Sicherheitsberater
Mi 07.03.2018	19:00 - 21:00	Technologie-Folgenabschätzung	Dieter Carbon	
Sa 21.04.2018	13:00 - 17:00	Workshop: Browser und Surfen	Hermann Sauer	Comidio GmbH
Mi 02.05.2018	19:00 - 21:00	Delikte rund um das Tatmittel Internet	Markus Wortmann	Kriminologe und Polizeiwissenschaftler, Geschäftsführer SICHERES NETZ HILFT e.V.
Mi 13.06.2018	19:00 - 21:00	(Un-)Sicherheit bei default und weitere Gründe für Defense in depth	Christoph Linck	ESWE (Stadtwerke Wiesbaden)
Mi 03.06.2020	18:00 - 21:00	AKIS-34: Digitaler Nachlass - Vorbeugen statt nachsehen!	Markus Wortmann	
Mi 01.07.2020	18:00 - 21:00	AKIS-35: Cyber - Angriffe, Auswirkungen und Abwehr	Hermann Sauer	
Mi 02.09.2020	18:00 - 21:00	AKIS-36: Verschlüsselung für KMUs in der Praxis	Hans-Joachim Giegerich	
Mi 04.11.2020	18:00 - 21:00	AKIS-37: Realität ist, was Du draus machst: Risiken der Meinungsbildung im Netz	Prof. Dr. Birgit Stark und Pascal Jürgens M.A.	
Mi 02.12.2020	18:00 - 21:00	AKIS-38: Neues aus der Welt der Unmanned Aerial Vehicles	Dr. Frank Fuchs	
Mi 04.12.2019	18:00 - 21:00	Algorithmen entscheiden nicht	Prof. Dr. Joachim Fetzer	Deutsches Netzwerk Wirtschaftsethik
Mi 05.02.2020	18:00 - 21:00	AKIS-30: Kommunikations-Analyse: Forensik & Gefahren-Abwehr	Frank R. Walther	Geschäftsführer Synapse Networks GmbH, Gau-Algesheim
Mi 04.03.2020	18:00 - 21:00	AKIS-31: Technische Gestaltungsmöglichkeiten von Uploadfiltern	Prof. Dr. Martin Steinebach	Fraunhofer SIT, Darmstadt, Head of Media Security and IT Forensics
Mi 01.04.2020	18:00 - 21:00	AKIS-32: Rechtliche Rahmenbedingungen bei der Detektion und Abwehr von Drohnen im Bereich kritischer Infrastrukturen	Eva Skobel	Wissenschaftliche Mitarbeiterin am Lehrstuhl für Öffentliches Recht und Informationsrecht, JGU Mainz
Mi 06.05.2020	18:00 - 21:00	AKIS-33: VoIP- und IoT-Hacking, angesichts Home Office	Frank Ewert	Sicherheitsberater, Vorstand SICHERES NETZ HILFT e.V.
Mi 03.06.2020	18:00 - 21:00	AKIS-34: Digitaler Nachlass - Vorbeugen statt nachsehen!	Markus Wortmann	Kriminologe und Polizeiwissenschaftler, Geschäftsführer SICHERES NETZ HILFT e.V.
Mi 01.07.2020	18:00 - 21:00	AKIS-35: Cyber - Angriffe, Auswirkungen und Abwehr	Hermann Sauer	Geschäftsführer Comidio GmbH, Eltville
Mi 02.09.2020	18:00 - 21:00	AKIS-36: Verschlüsselung für KMUs in der Praxis	Hans-Joachim Giegerich	Geschäftsführer Giegerich & Partner GmbH
Mi 04.11.2020	18:00 - 21:00	AKIS-37: Realität ist, was Du draus machst: Risiken der Meinungsbildung im Netz	Prof. Dr. Birgit Stark und Pascal Jürgens M.A.	Direktorin des Mainzer Medieninstituts und wissenschaftlicher Mitarbeiter am Institut für Publizistik JGU
Mi 02.12.2020	18:00 - 21:00	AKIS-38: Neues aus der Welt der Unmanned Aerial Vehicles	Dr. Frank Fuchs	Geschäftsführer Frank Fuchs Consulting

privacy made in Germany

Siddhartha Gautama

Bitte glauben Sie nicht mir …

Siddhartha Gautama aus dem Adelsgeschlecht der Shakya wurde ca. 560 v. Chr. in Lumbini, Indien geboren. Nach seiner Erleuchtung unter dem Bodhi-Baum lehrte er während 45 Jahren als Buddha im Nordosten Indiens bevor er im Alter von ca. 80 Jahren starb.

Glaube nichts, weil ein Weiser es gesagt hat.
Glaube nichts, weil alle es glauben.
Glaube nichts, weil es geschrieben steht.
Glaube nichts, weil es als heilig gilt.
Glaube nichts, weil ein anderer es glaubt.
Glaube nur das, was Du selbst als wahr erkannt hast.

https://zenartblog.wordpress.com/buddha/

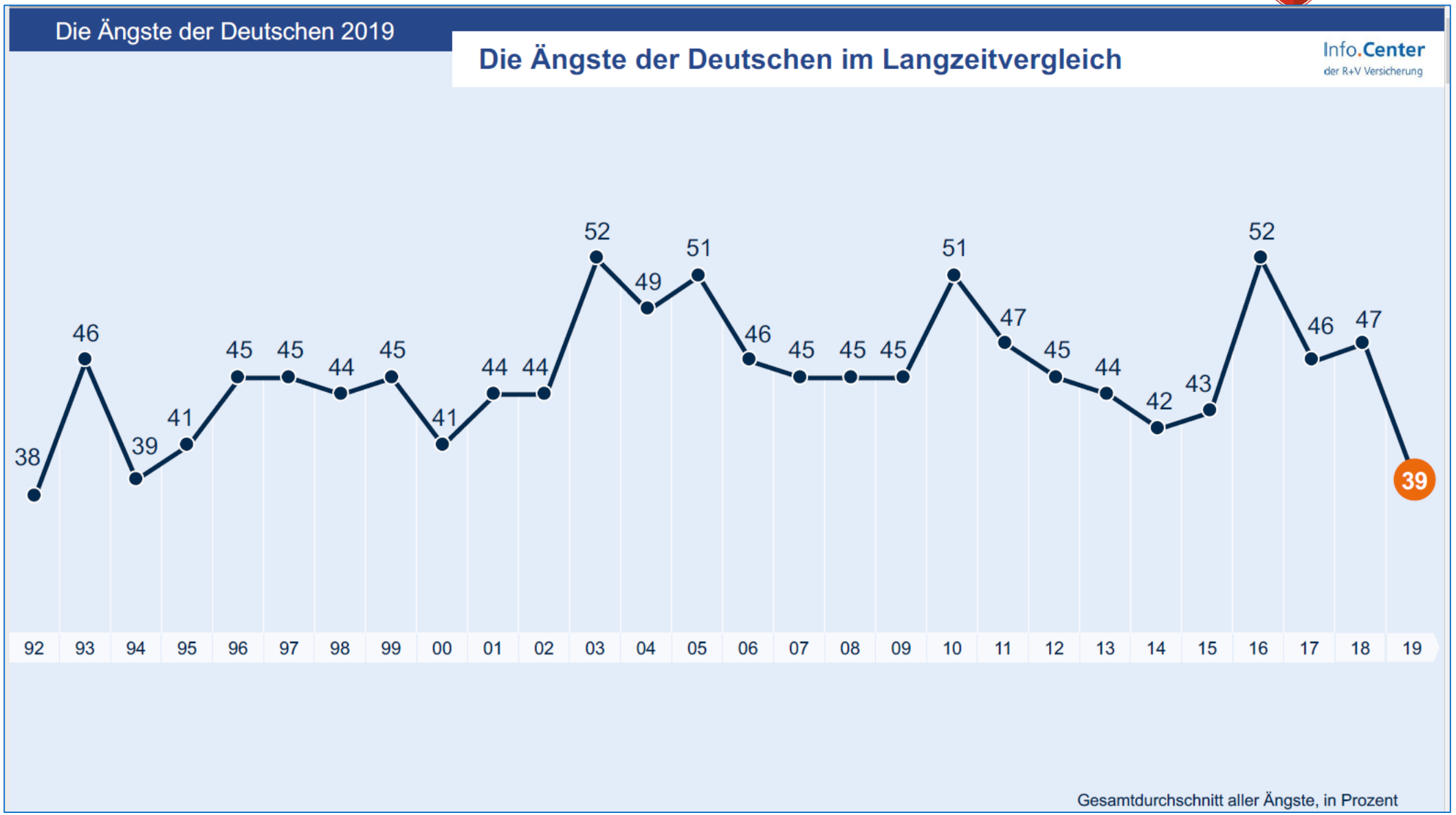
„Aktive“ Gefährdung

Die sieben größten Ängste 2018	
Angst vor	
Gefährlichere Welt durch Trump-Politik	69 %
Überforderung Deutsche / Behörden durch Flüchtlinge	63 %
Spannungen durch Zuzug von Ausländern	63 %
Überforderung der Politiker	61 %
Terrorismus	59 %
Kosten für Steuerzahler durch EU-Schuldenkrise	58 %
politischer Extremismus	57 %

Die sieben größten Ängste 2019	
Angst vor	
Überforderung Deutsche/Behörden durch Flüchtlinge	56 %
Spannungen durch Zuzug von Ausländern	55 %
Gefährlichere Welt durch Trump-Politik	55 %
Überforderung der Politiker	47 %
Politischer Extremismus	47 %
Wohnen in Deutschland unbezahlbar	45 %
Pflegefall im Alter	45 %

https://www.ruv.de/presse/aengste-der-deutschen/aengste-der-deutschen-langzeitvergleich

„Aktive“ Gefährdung



https://www.ruv.de/presse/aengste-der-deutschen/aengste-der-deutschen-langzeitvergleich

„Aktive“ Gefährdung

Wenn es ein Angreifer (Hacker, Krimineller, Nachrichtendienst, Exekutivorgan) auf „mich“ (über Firmen-Netzwerk, privates Netzwerk, meinen PC, mein Smartphone) abgesehen hat, bin ich über kurz oder lang unterlegen.

☞ Das heißt aber nicht, dass ich mich nicht gegen **passive Gefährdung** sichern sollte.

Bewusstsein für Gefährdung steigt …

trutzbox
back to privacy

Mord durch Herzschrittmacher?

FAZ

Sicherheitslücken bei Medizinprodukten / Von Sandro Gaycken u

BERLIN, 16. August. Im Jahr 2013 sah Dick Cheney, der ehemalige Vizepräsident der Vereinigten Staaten, in der Serie „Homeland", wie ein Vizepräsident durch einen Hackerangriff auf den Herzschrittmacher getötet wird. Und er sah sich bestätigt. Schon im Jahr 2007, als er noch Vizepräsident war, hatte sich Cheney in einer komplizierten Operation die Wireless-Funktion seines Defibrillators abschalten lassen.

Die schlagzeilenträchtige Geschichte setzte sich fort. Immer wieder gab es Meldungen über angreifbare Medizinprodukte. Erst im Januar dieses Jahres warnte die amerikanische Arzneibehörde FDA vor potentiell tödlichen Lücken in Defibrillatoren von St. Jude Medical. Der Aktienkurs der Firma brach ein. Aber erst seit kurzem ist bekannt, wie schlimm das Problem im Ganzen ist. Zwei neue Studien haben sich intensiv mit dem Thema befasst. Die Ergebnisse sind katastrophal.

Die erste Studie stammt von der Firma WhiteScope. Sie hat technische Tests an Herzschrittmachern vier großer Hersteller durchgeführt. Die Geräte haben insgesamt 8665 bekannte und offene Sicherheitslücken. Da tut sich ein Abgrund auf. Die jüngsten Massenangriffe mit Erpressersoftware, die Weltkonzerne in Not gebracht haben, brauchten nur zwei solcher Schwächen. Und: Diese Lücken können kaum behoben werden. Riskante Geräte wie Herzschrittmacher, Waffensysteme, Flugzeuge, Bremsen müssen teure und monatelange Zulassungstests bestehen, um zu garantieren, dass keine oder zumindest nicht die falschen Menschenleben gefährdet werden, auch bei kleinen Änderungen. Wöchentliche Sicherheits-Updates sind da nicht möglich. Das ist ein Strukturkonflikt, den es nicht geben darf. WhiteScope hat die Gefahren nachgewiesen. Die Firma konnte Programmiergeräte der Hersteller auf Ebay ersteigern und die Herzschrittmacher zu Tötungsmaschinen umprogrammieren. Das ging sogar via Internet. Viele Schrittmacher sind mit internetbasierten Home-Monitoring-Systemen verbunden, die das ermöglichen.

Der erschreckende Befund: Man kann Herzschrittmacherpatienten gezielt töten. Ein solcher Mord wäre zumindest am Patienten nicht mal als solcher erkennbar, geschweige denn gerichtlich nachweisbar. Denn die Geräte zeichnen solche Zugriffe nicht auf.

Ob auch deutsche Patienten betroffen sind, lässt sich nicht sagen. Die Hersteller wurden nicht benannt, vermutlich um Klagen abzuwenden. Schon 2016 gab es aber eine belgische Studie an Geräten im europäischen Markt, die bei einem weniger tiefgehenden Test an zehn Herzschrittmachern der „Next Generation" erhebliche Mängel in der IT-Sicherheit feststellte. Viele Hersteller scheinen also zumindest ähnliche Probleme zu haben.

Die zweite Studie stützt diesen Eindruck. Sie kommt aus dem Ponemon Institute und schließt Insulinpumpen, Intensivstationen, Operationssäle und weitere Geräte ein. 67 Prozent der Hersteller von Medizingeräten glauben, dass noch dieses Jahr ein schwerer Vorfall passieren wird, aber nur fünf Prozent ebendieser Hersteller machen regelmäßige Tests zur Cybersicherheit. 49 Prozent von ihnen berücksichtigen nicht einmal die einfachsten Empfehlungen für Sicherheitsmaßnahmen.

Die Politik hat das Problem langsam erkannt, ist aber zu zögerlich, wie so oft beim Thema Cybersicherheit. Die FDA etwa hat seit 2014 zwei Anforderungskataloge veröffentlicht, und Sicherheits-Updates müssen keinen aufwendigen neuen Zulassungsprozess durchlaufen. Aber es mangelt an der Verwirklichung.

Auch in der EU ist das ein Problem. Seit kurzem ist eine neue Medizinprodukte-Verordnung in Kraft, nach der die IT-Sicherheit von Medizingeräten dem „Stand der Technik" entsprechen muss. Konkrete Vorgaben dazu machen jedoch weder die EU noch die deutschen Aufsichtsbehörden für Medizinprodukte. Hersteller, Prüfstellen und Betre
geltenden
dards für
sich aber n
übertragen
eingebette
tiges Prob
Vieles ist u
in diesen F
sere Siche
nem Offic
Was mu
sche Gerä
und indire
getrennt w
das Einzig
kann: die V
nitoring-Sy
als Kehrse
bunden sin
nem lieber
mord. Selb
wirklich n
transparen
den, wie
Technolog
öffnen ab
terne Sic
eine Black
Die grö
sen in die
den. Ihre
werden, u
tionale S
müssen di
geht etwa
die unang
brauchen.
teidigung
auch in D
aber daue
weigern,
ve Proble
heit könn
ten werde
müssen, d

Sandro Gaycken ist Direktor, Isabel Skierka wissenschaftliche Mitarbeiterin am Digital Society Institute der ESMT Berlin.

Sicherheitslücken in Wahl-Software

F.A.Z. FRANKFURT, 7. September. Der Bundeswahlleiter Dieter Sarreither hat die Landeswahlleiter aufgefordert, mit zusätzlichen Maßnahmen eine mögliche Manipulation der Wahlergebnisse der Bundestagswahl zu verhindern. Zuvor hatten Sicherheitsforscher gravierende Mängel in der Software gefunden, mit der in etlichen Kommunen die Wahlergebnisse zusammengetragen und an den Landeswahlleiter übermittelt werden. Nach den Untersuchungen eines Informatikers aus Darmstadt und des Chaos Computer Clubs gibt es in dem Programm „PC Wahl" des Anbieters Vote IT Sicherheitslücken, wie „Die Zeit" berichtete. Der Bundeswahlleiter empfiehlt, die Software zu aktualisieren sowie übermittelte Ergebnisse telefonisch zu überprüfen. *(Kommentar Seite 10.)*

Tallinn hat ein Problem

Estland demonstriert, wie gefährlich Digitalisierung ist

FAZ D. 7.9.2017

Für die Prediger der Digitalisierung liegt das Nirwana im Baltikum. Genauer gesagt im kleinsten der baltischen Staaten, der von sich behauptet, die erste digitale Gesellschaft der Welt zu sein. „e-Estonia" nennt sich das Projekt des Landes der unbegrenzten digitalen Möglichkeiten und empfiehlt sich mit „Yes, we can"-Pathos als Vorbild: „We have built a digital society and so can you." Die Esten seien Pioniere, heißt es in der Selbstdarstellung der Regierung, sie schüfen ein „effizientes, sicheres und transparentes Ökosystem". In diesem setzen die Menschen alles auf eine Karte – einen Personalausweis, auf dem alles gespeichert ist, was einen Staatsbürger ausmacht, und mit dem er alles Erdenkliche anstellen kann, von der Steuererklärung bis zur Stimmabgabe bei der Wahl.

Das Dumme ist nur: Die Karte hat, wie Sicherheitsspezialisten jetzt herausgefunden haben wollen, ein Loch. Man hätte es erwarten können, ja müssen, schließlich ist in der digitalen Welt nur sicher, dass Daten niemals sicher sind. Irgendein Hacker wird ihrer habhaft, irgendein Geheimdienst kommt an sie heran. Das hätten die Esten eigentlich wissen müssen, zumal sie es mit einem gefährlichen, digital hochgerüsteten Nachbarn zu tun haben. In Sachen „Cyberwar" zählt Russland zur Avantgarde und scheint für eine Kriegsführung vorbereitet, die zu immensen Schäden führt, Infrastrukturen und Institutionen lahmlegt, ohne dass die Verursacher je ausfindig, geschweige denn dingfest gemacht werden. Dafür waren die geleakten Dokumente der Demokraten im amerikanischen Wahlkampf nur ein Beispiel.

Durch die Sicherheitslücke im estnischen ID-Card-System könnten Hacker, wie die „Financial Times" schreibt, an die Daten von 750 000 Menschen gelangen, welche den neuen Ausweis schon besitzen. Das ist bei einer Gesamtbevölkerung von rund 1,3 Millionen Menschen mehr als jeder Zweite, der nun befürchten muss, dass seine digitale Identität gestohlen und mit dieser wer weiß was angestellt wird. Vor knapp drei Jahren hat Estland damit begonnen, seine Verwaltung auf diesen Digitalpass umzustellen, mit dem man sogar eine sogenannte „E-Residency" erwerben und als Ausländer Bürger der Digitalrepublik Estland werden kann. Die Bürger sollen eine nie dagewesene Schlüsselgewalt haben – Zugang zu allem, was man vom Staat erwartet. Dass dies auch in umgekehrter Richtung funktioniert, intimste Dinge transparent macht und die Menschen entschlüsselt, dürfte jetzt auch dem Letzten klar sein. Doch wird das im allgemeinen E-Governance-Gestaune nicht nur von den Kapitalverwertern der Digitalisierung wie Facebook und Google konsequent ausgeblendet. Sie versprechen mehr Demokratie, von der aber gar nicht klar ist, worin sie bestehen soll. Von mehr Teilhabe ist stets die Rede, davon, dass die Menschen ihre Stimme hörbar und zählbar machen könnten, dabei geht es doch zunächst einmal um ein effizientes Service-System.

Und bei dem muss man erst einmal dafür sorgen, dass die Prinzipien und Errungenschaften der analogen Demokratie – Grundrechte, freie Wahlen, Gewaltenteilung, Rechtsstaatlichkeit – nicht ausprogrammiert werden und sich die Herrschaft des Volkes in eine der Datenkonglomerate verwandelt. Wie großartig man mit dem Demokratie-Versprechen der Digitalisierung scheitern kann, wenn man die Technik mit der Verfasstheit der Gesellschaft verwechselt, haben hierzulande vor Jahren die „Piraten" gezeigt, deren kometenhaftem Aufstieg ein innerparteilicher „Terreur" folgte, der jedem zeigte, wie „E-Demokratie" aussehen kann, wenn sie von den falschen Leuten betrieben wird.

Die Sicherheitslücke zu schließen werde mehrere Monate dauern, teilte nun die estnische Regierung mit. Die von IT-Sicherheitsexperten beschriebene Gefahr sei zwar erheblich, doch auch eine theoretische. Noch habe kein Hacker zugeschlagen, die digitalen Speicherpässe sollen bis auf weiteres im Umlauf bleiben. Digitalisierung – darauf will Estland, das am 1. Juli (anstelle der Briten, die eigentlich dran gewesen wären) die Präsidentschaft im Ministerrat der EU übernommen hat, die Europäer trimmen. In Tallinn beginnt heute eine Konferenz der EU-Verteidigungsminister, auf der es um den Cyberkrieg gehen soll. Für ein realistisches Szenario sorgen die Gastgeber selbst. MICHAEL HANFELD

Passive Gefährdung

trutzbox
back to privacy

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? …

Privacy made in Germany

Nutzungs-Daten und/oder Meta-Daten

Nutzungs-Daten	Meta-Daten
Inhalte	Informationen über Daten
Video (-Datei) Audio (-Datei) Text (-Datei) Foto (-Datei) … (-Datei)	Absender Adressat Angerufener Anrufer Autor Betreff Dauer Länge Rufnummer Teilnehmer-E-Mail-Adresse Teilnehmer-Name Zeitpunkt …

„Prof. Edward Felten, der an der renommierten Universität Princeton Informatik lehrt, belegte im Rahmen der Prozessvorbereitung, warum „Metadaten“ quasi alles über die Bürgerinnen und Bürger verraten. (1) Metadaten seien sehr einfach automatisch zu analysieren im Gegensatz zu den komplizierten Einzelheiten eines Anrufs mit seinen Variationen in Sprache, Stimme und Gesprächsstil. Moderne Analyse-Software ermöglicht, aus Metadaten Beziehungen, persönliche Daten, Gewohnheiten und Verhaltensweisen herauszulesen. Es gibt bereits Programme, die für Strafverfolgung und Geheimdienste solche Daten analysieren, etwa IBM Analyst‘s Notebook. IBM bietet sogar Kurse an, die lehren, wie man Anrufdaten mit IBM Analyst‘s Notebook auswertet. (2) Im Gegensatz zum tatsächlichen Inhalt der Anrufe, SMS und E-Mails lassen sich die Metadaten zu diesen Anrufen kaum schützen. Dafür sind diese Metadaten oft aufschlussreicher als der eigentliche Inhalt.“

https://www.datensicherheit.de/abhoerskandal-metadaten-inhalt

Nutzungs-Daten und/oder Meta-Daten

FRANKFURTER ALLGEMEINE SONNTAGSZEITUNG, 19. MAI 2019, NR. 19

Die geheime Macht der Metadaten

Sichere Kommunikation ist nur eine Seite der Medaille. Was Facebook und Whatsapp trotzdem über uns wissen.

Von Michael Spehr

Die geheime Macht der Metadaten

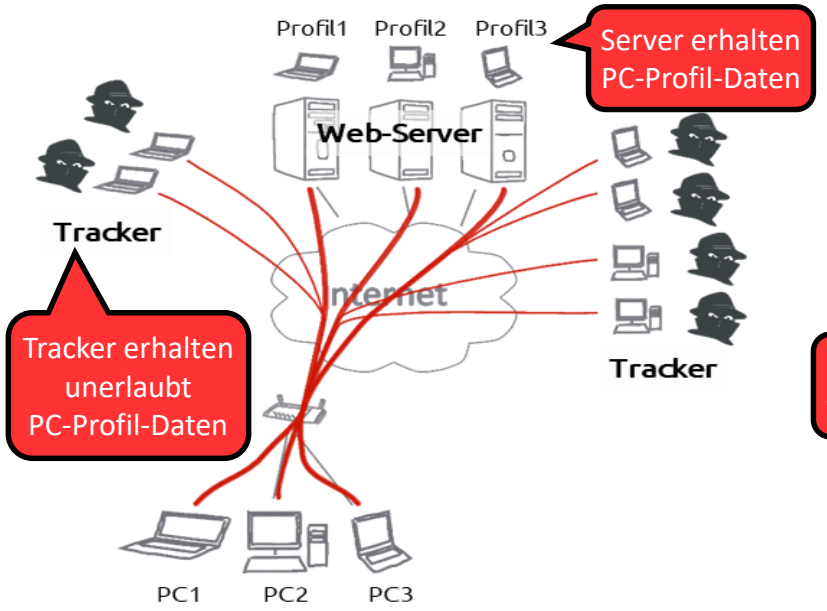
Sichere Kommunikation ist nur eine Seite der Medaille. Was Facebook und Whatsapp trotzdem über uns wissen.

Von Michael Spehr

Passive Gefährdung

trutzbox
back to privacy

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



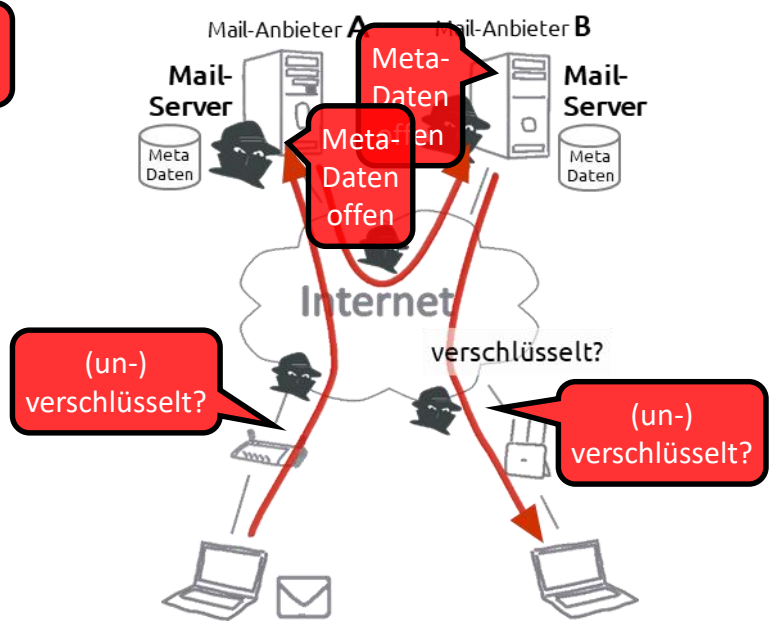


Foto: Comidio GmbH

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

Privacy made in Germany

Webmeeting Anbieter

Frankfurter Allgemeine
RHEIN-MAIN
ZEITUNG FÜR FRANKFURT UND DIE REGION

Die Begriffsverwirrung hat ein Ende: *Die Schau „Neuland" erklärt die Sprache der digitalen Welt.* Foto Museum für Kommunikation Frankfurt

Auf dem digitalen Corona-Pfad

FRANKFURT Die Sonderausstellung „Neuland" im Museum für Kommunikation

Es ist das Thema der Stunde. Dank der digitalen Medien waren die vergangenen acht Wochen zwischendurch immer wieder einmal erträglich. Und nicht nur die Videoclips zur Lage, die durch sie verbreitet wurden, trugen zur Aufheiterung der zu Kontaktsperre und Heimarbeit Verurteilten bei, sondern auch die Technik selbst, zumal sich viele Ungeübte erstmals an ihr versuchten. Übertragungsschwierigkeiten, Bedienungsfehler, Nutzerscherze allenthalben: Für Kurzweil war gesorgt, wenn Schüler sich zum Chat mit der Lehrerin unter dem Namen der Rektorin einloggten oder die Großmutter als kopflose Dame munter drauflosplauderte. Nachdem sie endlich den Mikrofon-Button gefunden hatte.

Dass die Gesellschaft wirklich auf eine solche Situation vorbereitet war, lässt sich schwerlich behaupten. So lief der Unterricht an Laptop oder Tablet in vielen Fällen alles andere als reibungslos. Manch einer betrat das „Neuland", wie die Bundeskanzlerin die digitale Welt vor nicht allzu langer Zeit bezeichnete, auf recht unsicheren Beinen und leicht orientierungslos. Da hätte die Ausstellung, die den Begriff der Regierungschefin als Titel trägt, womöglich Abhilfe schaffen können. Wäre sie denn rechtzeitig eröffnet worden. Aber zum Kummer der Kuratorinnen kam die Corona-Krise dazwischen, und es gab im Netz nur eine Ahnung von einer Ausstellung über das Digitale, die doch in den real existierenden Räumen des Frankfurter Museums für Kommunikation erlebt werden muss.

Das ist jetzt möglich. Die Ausstellung ist so aktuell, wie eine solche Schau nur sein kann. Denn seit Dienstag können sich die Besucher auf eine Corona-Spur begeben, die mit Altrosa als Leitfarbe zu den allerjüngsten Entwicklungen in der neuen schönen, vor allem aber ungemein nützlichen Digitalwelt führt. Und die Verbindungen zwischen Menschen trotz des Gebots unterstützt, sozialen Abstand zu üben.

Bis zu 20 Personen sind im Ausstellungsraum zugelassen, man kann ein bestimmtes Zeitfenster buchen, um ohne Verzögerung ins Haus am Schaumainkai zu gelangen. Ein freundlicher Herr mit Gesichtsvisier fordert einen auf, mit einem kräftigen Spritzer Desinfektionsmittel aus dem Spender die Finger auf allerlei interaktive Stationen vorzubereiten. Er händigt den Besuchern auch Touch-Pens aus, mit denen sie Schaltflächen und Knöpfe berühren können, ohne sich Keimen auszusetzen.

Es ist ruhig im Museum. Das ist für dieses Haus eher ungewöhnlich, denn wie in kaum einem anderen wimmelt es hier sonst vor Kindern. Schulklassen tummeln sich sonst im Behnisch-Gebäude, bewegen sich von einer Themen-Insel der Dauerausstellung zur nächsten, amüsieren sich etwa über Telefone mit Kabel und Gabel. Nun aber müssen sich die Besucher auf einen Rundgang begeben. Die Freiheit herumzustreunen, wie es einem gefällt, ist eingeschränkt. Und die Aufforderung, sich öfter die Hände zu waschen, ergeht in regelmäßigen Intervallen. „Ich finde es wichtig, dass wir aufeinander aufpassen", sagt Kuratorin Tine Nowak, die zusammen mit Silke Zimmermann und Anjuli Spieker die Sonderausstellung „Neuland" konzipiert hat. Es sei aber traurig gewesen, acht Wochen allein in der Ausstellung gewesen zu sein, und die Eröffnung, auf die sie fieberhaft hingearbeitet hätten, absagen zu müssen.

Die Fragen aber, um die es in der Schau gehe, hätten durch Corona an Brisanz gewonnen. Als da etwa wären: Wer sind wir im Internet und wie viele? Wie verändert sich unsere Kommunikation, wenn wir gar nicht mehr wissen, ob wir mit Mensch oder Maschine reden? Was ist, wenn wir uns dem Zwang zur Optimierung des eigenen Körpers entziehen, der in den sozialen Medien herrscht? Was wird aus der Liebe, wenn wir sie im Internet suchen? Wie lernen wir Wahrheit und Fake News zu unterscheiden? „Die digitalen Tools haben gerade einen Schub erfahren", sagt Silke Zimmermann. Und so stellen sich prompt neue Fragen. Wie die nach der künftigen Nutzung von Homeoffice. Und der Verbesserung von Konferenz-Apps. Die Kuratorin ist bei der Vorstellung der um den Corona-Pfad erweiterten Schau ebenso digital zugeschaltet wie Ralf Nemetschek, Chef der Nemetschek-Stiftung, Partner des Museums beim Erarbeiten von Ausstellungen. Er spricht von der gesellschaftlichen Veränderung, die mit der Digitalisierung einhergeht. Bis die Technik streikt: „Ich sehe Sie nur noch als eine Art Barcode." MICHAEL HIERHOLZER

Die Fragen aber, um die es in der Schau gehe, hätten durch Corona an Brisanz gewonnen. Als da etwa wären: Wer sind wir im Internet und wie viele? Wie verändert sich unsere Kommunikation, wenn wir gar nicht mehr wissen, ob wir mit Mensch oder Maschine reden? Was ist, wenn wir uns dem Zwang zur Optimierung des eigenen Körpers entziehen, der in den sozialen Medien herrscht? Was wird aus der Liebe, wenn wir sie im Internet suchen? Wie lernen wir Wahrheit und Fake News zu unterscheiden? „Die digitalen Tools haben gerade einen Schub erfahren", sagt Silke Zimmermann. Und so stellen sich prompt neue Fragen. Wie die nach der künftigen Nutzung von Homeoffice. Und der Verbesserung von Konferenz-Apps. Die Kuratorin ist bei der Vorstellung der um den Corona-Pfad erweiterten Schau ebenso digital zugeschaltet wie Ralf Nemetschek, Chef der Nemetschek-Stiftung, Partner des Museums beim Erarbeiten von Ausstellungen. Er spricht von der gesellschaftlichen Veränderung, die mit der Digitalisierung einhergeht. Bis die Technik streikt: „Ich sehe Sie nur noch als eine Art Barcode." MICHAEL HIERHOLZER

Magic Quadrant for Meeting Solutions

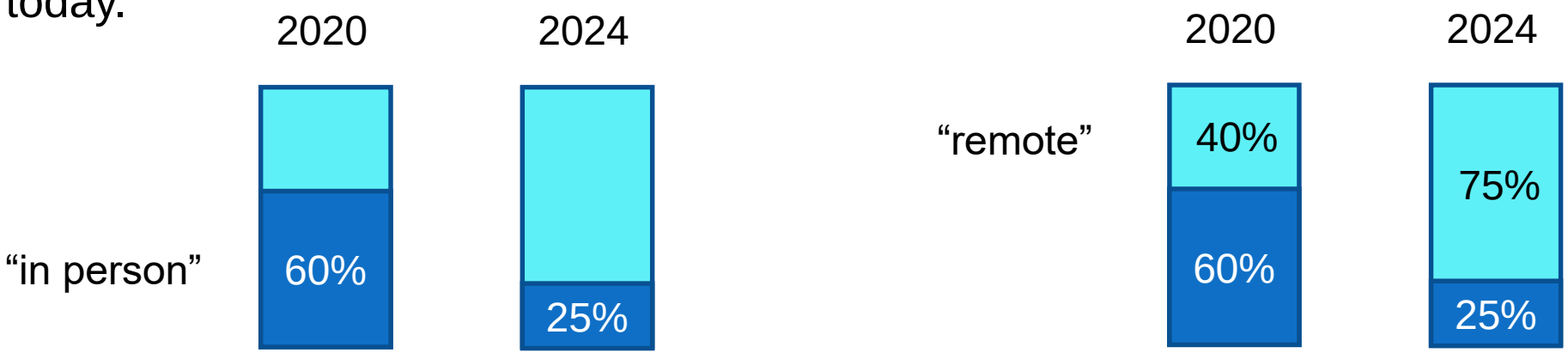
Published 5 September 2019 - ID G00354093

https://www.gartner.com/doc/reprints?id=1-1OH1GWOA&ct=190909&st=sb

Strategic Planning Assumptions

By 2022, 40% of formal meetings will be facilitated by virtual concierges and advanced analytics.

By 2024, remote work and changing workforce demographics will impact enterprise meetings so that only 25% will take place in person, down from 60% today.



Magic Quadrant for Meeting Solutions

Published 5 September 2019 - ID G00354093

https://www.gartner.com/doc/reprints?id=1-1OH1GWOA&ct=190909&st=sb

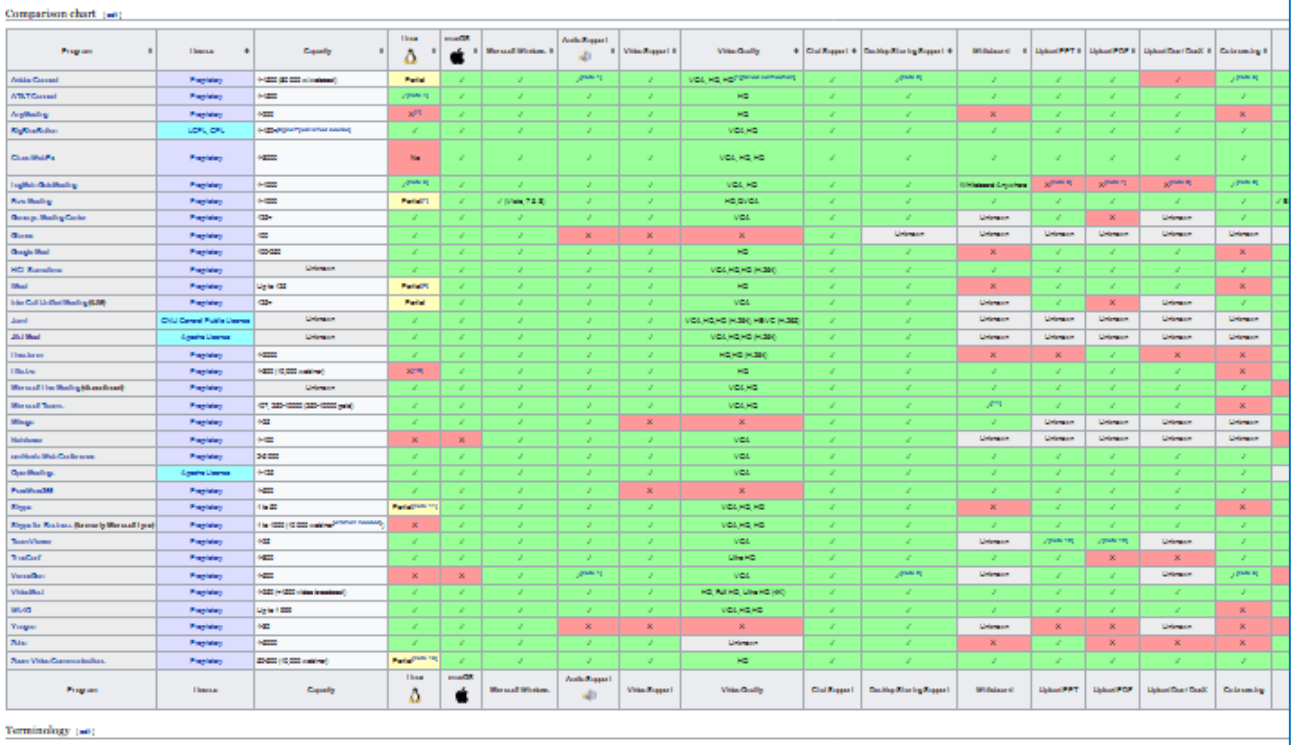
Microsoft
Zoom
Cisco

… as best

Webmeeting Anbieter

trutzbox
back to privacy

Comparison of web conferencing software



https://en.wikipedia.org/wiki/Comparison_of_web_conferencing_software

Liste von Webkonferenz-Lösungen

Anbieter	Produkt	Plattform	Maximale Teilnehmerzahl (nicht Webinar)	Dauerhaft kostenfreie Version verfügbar	Maximale kostenfreie Teilnehmerzahl (nicht Webinar)	Terminplanung von Meetings möglich	Aufzeichnung von Meetings möglich
Adobe	Connect Meetings[1]	Win, Mac, iOS, Android, Browser	100	Ja	3	Ja	Ja
Amazon	Chime[2]	Win, Mac, iOS, Android	10	Nein		Ja	Ja
AnyMeeting	AnyMeeting[3]	Browser	30	Ja	30	Ja	Ja
BlueJeans	BlueJeans[4]	Win, iOS, Android	100	Nein		Ja	Ja
Cisco	WebEx[5]	Win, Mac, Linux, iOS, Android, Browser	100	Ja	3	Ja	Ja
Dialpad	UberConference[6]	Browser	100	Ja	?	Ja	Ja
Expert Travel	baldaja CONNECT[7]	Win, Mac, Browser	1000	Nein		Ja	Ja
FreeConferenceCall.com	FreeConferenceCall.com[8]	Win, Mac, Linux, Browser	1000	Ja	?	Ja	Ja
Google	Google Meet[9]	iOS, Android, Browser	250	Nein		Ja	Ja
Google	Hangouts[10]	iOS, Android, Browser	25	Ja	25	Nein	Nein
Highfive	Highfive[11]	Browser	50	Nein		Ja	Ja
Jitsi	Jitsi Meet[12]	Win, Mac, Linux, iOS, Android, Browser	?	Ja	?	Ja	Ja
Livestorm	Livestorm[13]	Win, Mac, Linux, iOS, Android, Browser	1000	Ja	10	Ja	Nein
LogMeIn	GoToMeeting[14]	Win, Mac, Linux, iOS, Android, Browser	100	Ja	3	Ja	Ja
LogMeIn	Join.Me[15]	Win, Mac, iOS, Android, Browser	250	Ja	10	Ja	Ja
Microsoft	Skype[16]	Win, Mac, Linux	25	Ja	2	Nein	Nein
Microsoft	Skype for Business[17]	Win, Mac	250	Nein		Ja	Ja
PGi	GlobalMeet[18]	Win, Mac, iOS, Android, Browser	125	Nein		Ja	Ja
ReadyTalk	ReadyTalk[19]	Win, Mac, Browser	100	Nein		Ja	Ja
TeamViewer	Blizz[20]	Win, Mac, iOS, Android, Browser	300	Ja	5	Ja	Ja
TurboMeeting	TurboMeeting[21]	Win, Mac, iOS, Android, Linux, Browser	6000	Ja	5	Ja	Ja
TrueConf	TrueConf[22]	Win, Mac, iOS, Android, Linux, WebRTC, Browser	3000	Ja	12	Ja	Ja
Zoho	Zoho Meeting[23]	Browser	100	Nein		Ja	Ja
Zoom Video Communications	Zoom[24]	Win, Mac, Linux, iOS, Android, Browser	1000	Ja	100	Ja	Ja

https://de.wikipedia.org/wiki/Liste_von_Webkonferenz-L%C3%B6sungen

Privacy made in Germany

Webmeeting Anbieter

trutzbox
back to privacy

Videokonferenz-Tools im Überblick

Tools für Videokonferenzen gewinnen immer mehr an Bedeutung. Und die Programme bieten eigentlich schon längst alle Funktionen an, die Treffen in persona - besonders über die Ländergrenzen hinweg - überflüssig machen. Die Auswahl der Tools für Videokonferenzen ist groß. Wir zeigen in unserem Beitrag, welche Anbieter es gibt.

Hinweis: Mehrere Anbieter, darunter Microsoft, Google, Slack, Zoom oder Cisco, bieten aufgrund der aktuellen Lage um COVID-19 einige ihrer Chat-, Videokonferenz- und anderen Kollaborationsdienste kostenlos an.

- Microsoft Teams
- Cisco Webex Meetings
- Skype
- Zoom
- GoToMeeting
- Jitsi
- BigBlueButton

https://www.heise.de/tipps-tricks/Videokonferenz-Tools-im-Ueberblick-4688243.html

The Best Videoconferencing Service

wirecutter
A New York Times Company

Reviews for the real world | Electronics | Home & Garden | More categories... | Deals

Everything we recommend

Our pick

cisco Webex

Also great

jitsi

Jitsi Meet

For hanging out with friends

Free, secure, and remarkably easy to use, Jitsi Meet is perfect for quick meetings among family or friends. Those who need absolute privacy can also install it as a private server.

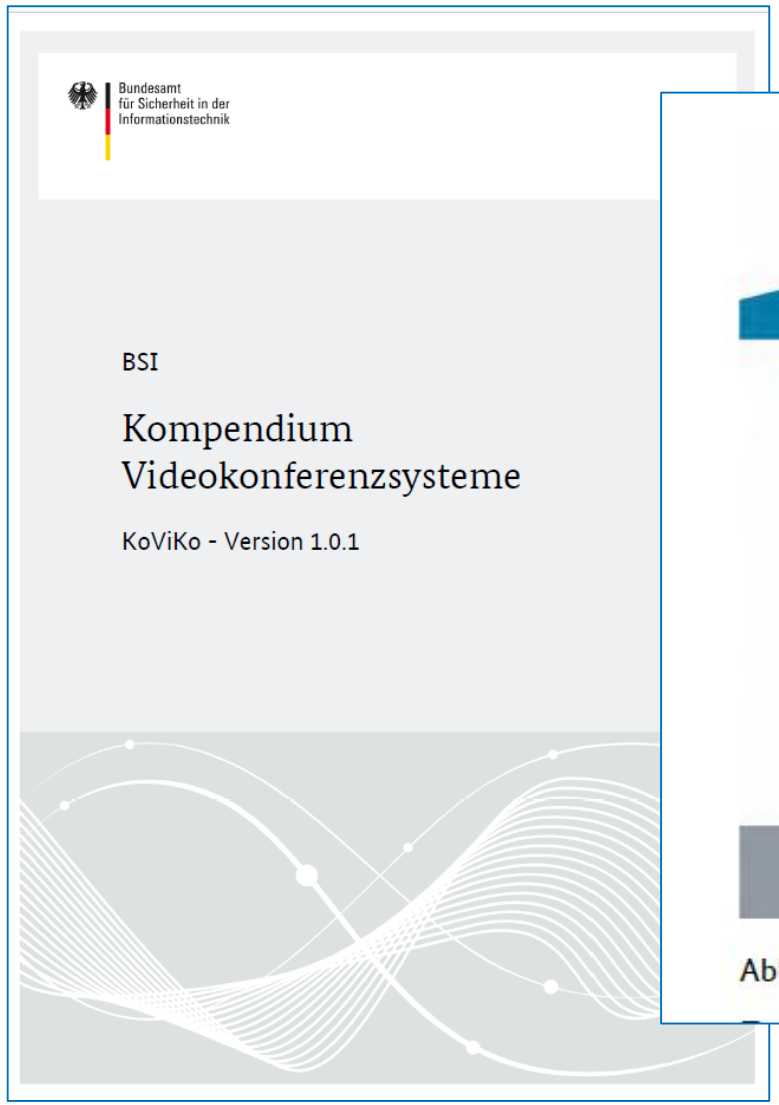
https://thewirecutter.com/reviews/best-video-conferencing-service/

> Zoom's self-advertised mission is to "make video communications frictionless," but it seems clear at this point that the service's impressive ease of use came at the cost of security and privacy. Security researchers, reporters, and hobbyist infosec geeks have found numerous flaws with the service, including a Mac installer that acted like malware, Facebook and LinkedIn integrations that shared user data without consent, false claims of end-to-end encryption, involuntarily shared user email addresses and photos, and cloud recordings left exposed to prying eyes. Zoombombing became an ugly trend, seeing everything from elementary school classes to graduate dissertation presentations disrupted with pornography and racist attacks.

Privacy made in Germany

Webmeeting Anbieter

BSI, Kompendium Videokonferenzsysteme, KoViKo - Version 1.0.1, 01.04.2020, 173 Seiten



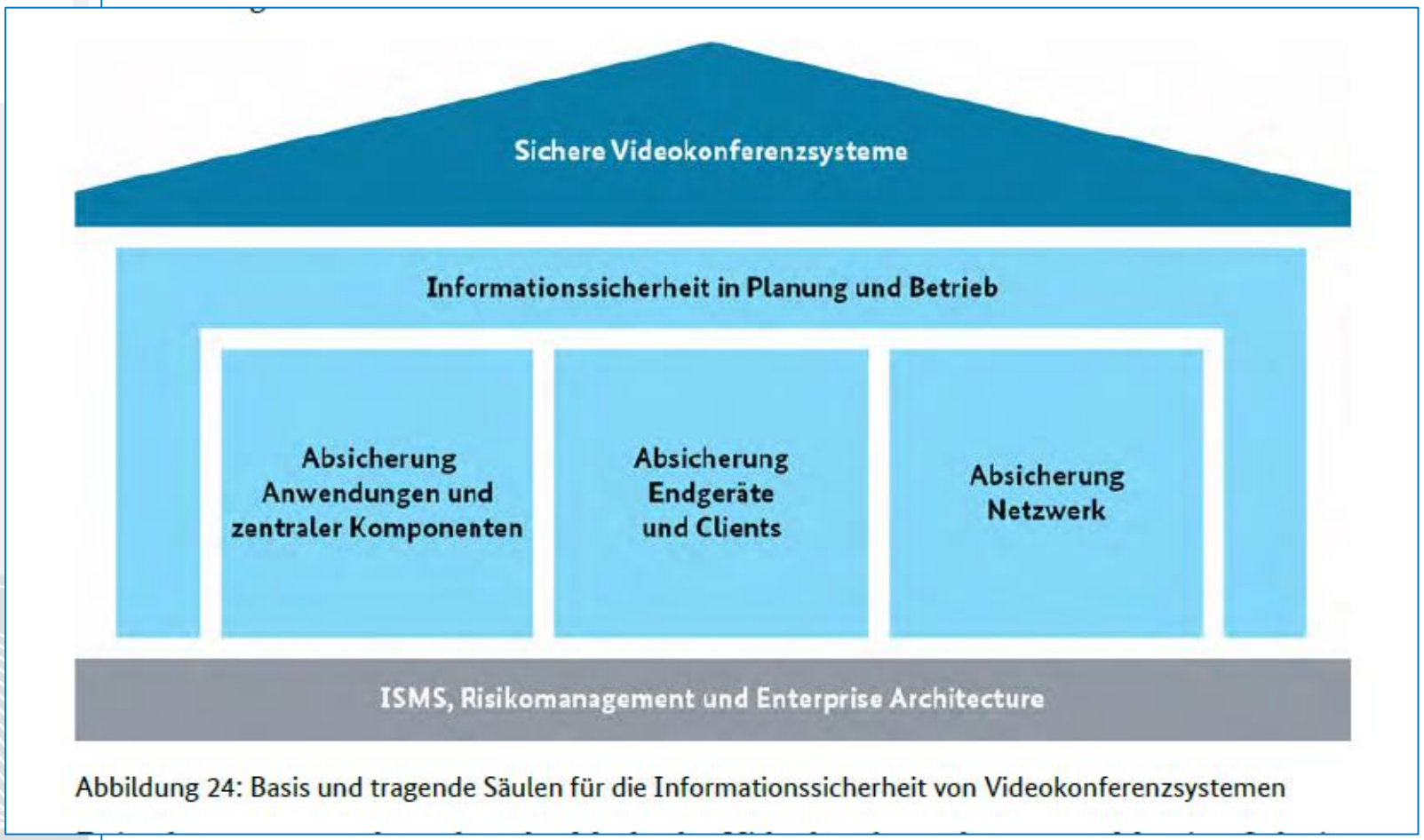


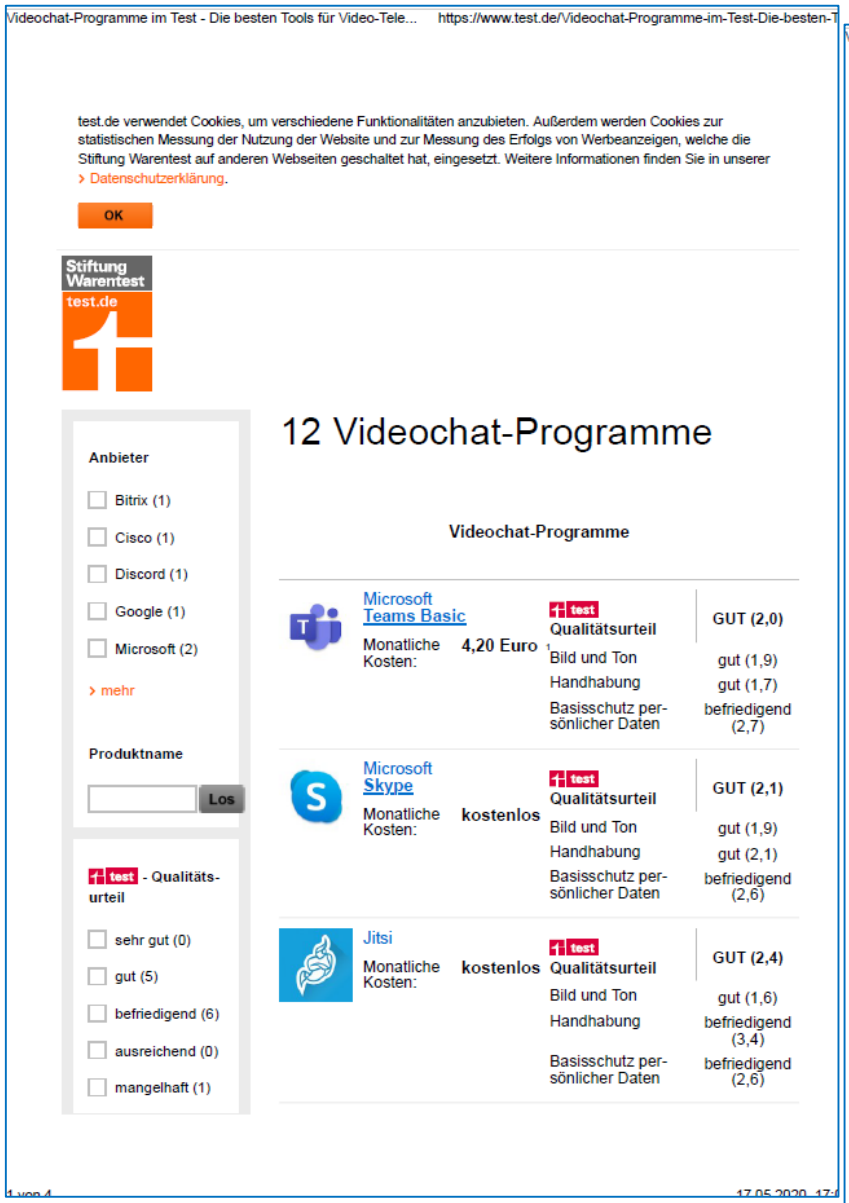
Abbildung 24: Basis und tragende Säulen für die Informationssicherheit von Videokonferenzsystemen

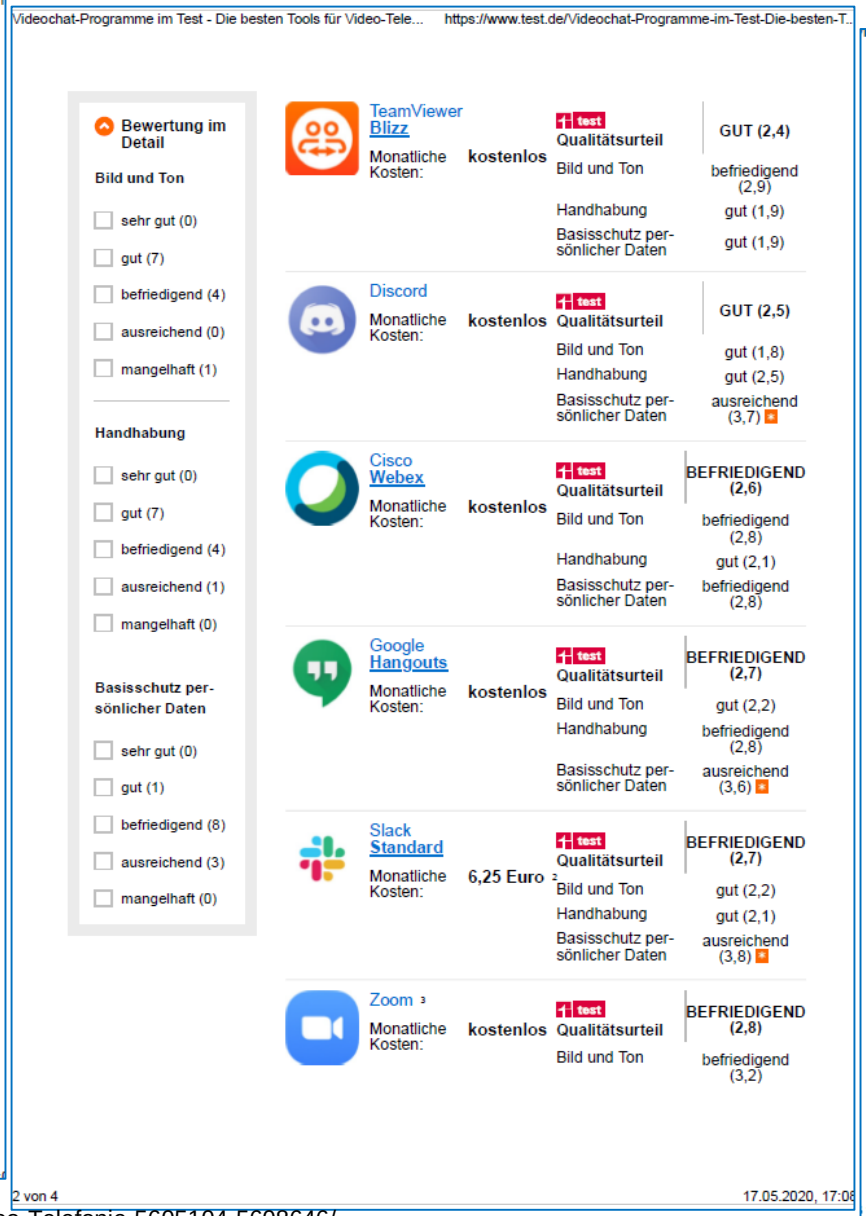
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4

Webmeeting Anbieter

13.05.2020

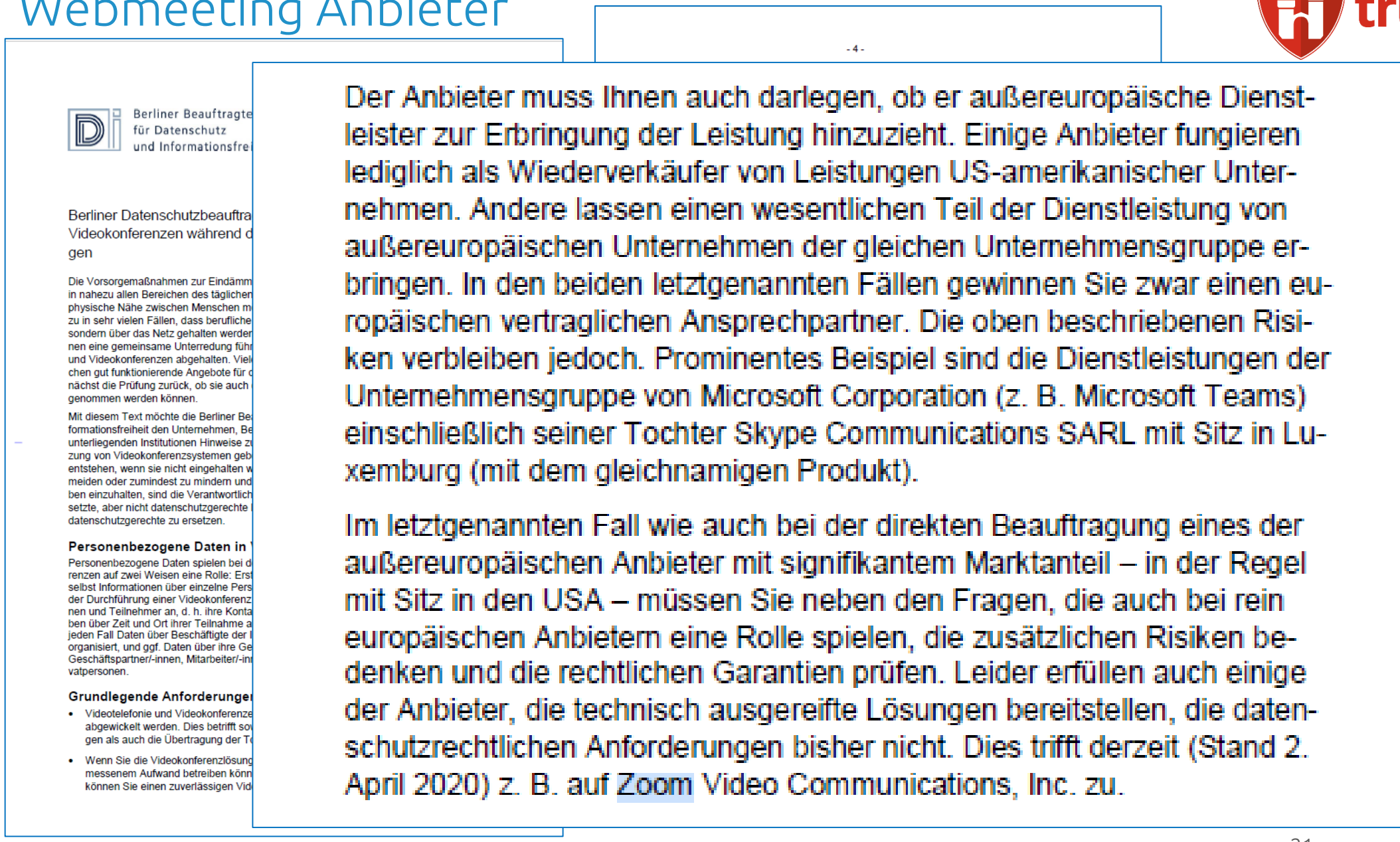
trutzbox
back to privacy





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

Webmeeting Anbieter



Berliner Beauftragte
für Datenschutz
und Informationsfrei

Berliner Datenschutzbeauftra
Videokonferenzen während d
gen

Die Vorsorgemaßnahmen zur Eindämm
in nahezu allen Bereichen des täglichen
physische Nähe zwischen Menschen m
zu in sehr vielen Fällen, dass berufliche
sondern über das Netz gehalten werden
nen eine gemeinsame Unterredung führ
und Videokonferenzen abgehalten. Viel
chen gut funktionierende Angebote für d
nächst die Prüfung zurück, ob sie auch
genommen werden können.

Mit diesem Text möchte die Berliner Be
formationsfreiheit den Unternehmen, Be
unterliegenden Institutionen Hinweise zu
zung von Videokonferenzsystemen geb
entstehen, wenn sie nicht eingehalten w
meiden oder zumindest zu mindern und
ben einzuhalten, sind die Verantwortlich
setzte, aber nicht datenschutzgerechte
datenschutzgerechte zu ersetzen.

Personenbezogene Daten in

Personenbezogene Daten spielen bei d
renzen auf zwei Weisen eine Rolle: Erst
selbst Informationen über einzelne Pers
der Durchführung einer Videokonferenz
nen und Teilnehmer an, d. h. ihre Konta
ben über Zeit und Ort ihrer Teilnahme a
jeden Fall Daten über Beschäftigte der
organisiert, und ggf. Daten über ihre Ge
Geschäftspartner/-innen, Mitarbeiter/-in
vatpersonen.

Grundlegende Anforderunge

- Videotelefonie und Videokonferenze
abgewickelt werden. Dies betrifft so
gen als auch die Übertragung der T
- Wenn Sie die Videokonferenzlösung
messenem Aufwand betreiben könn
können Sie einen zuverlässigen Vid

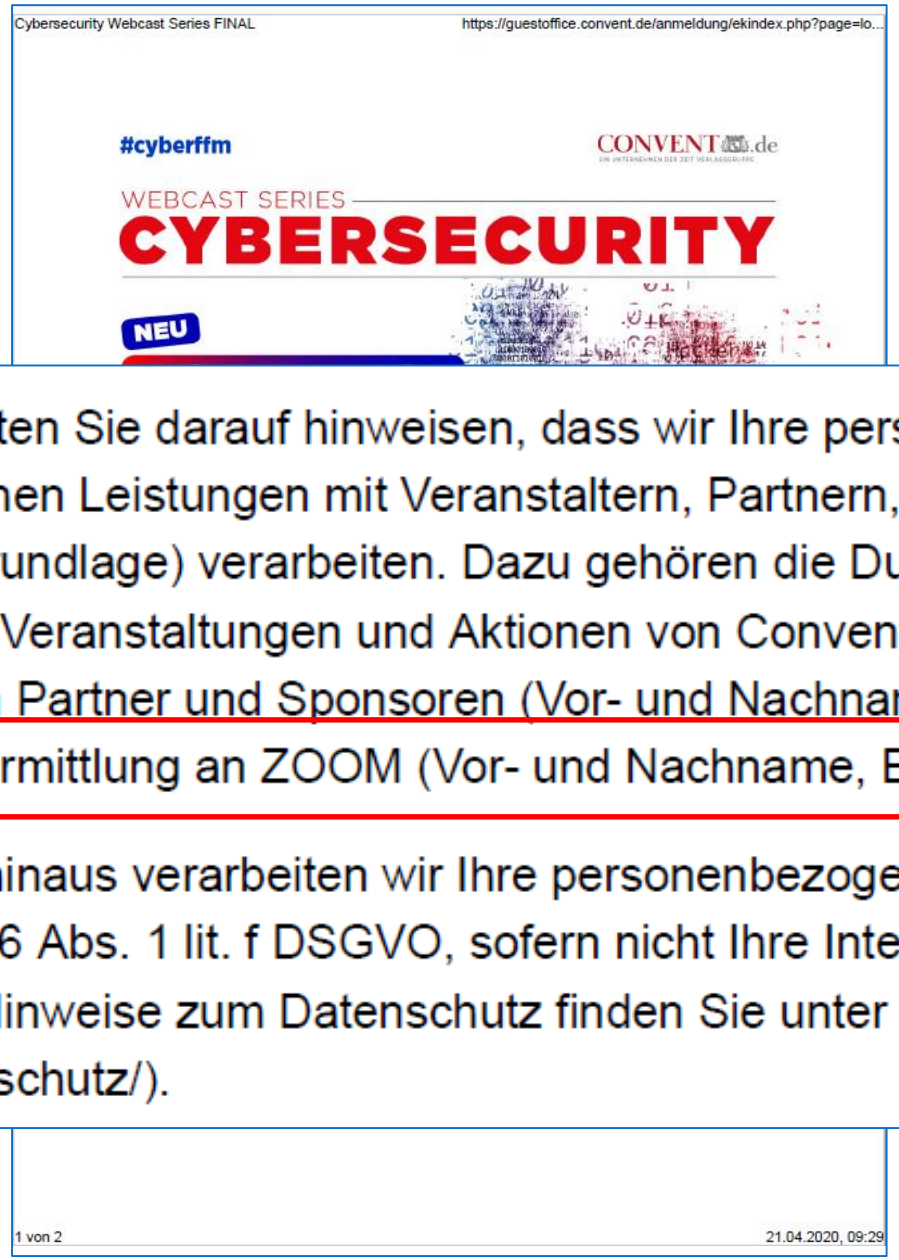
- 4 -

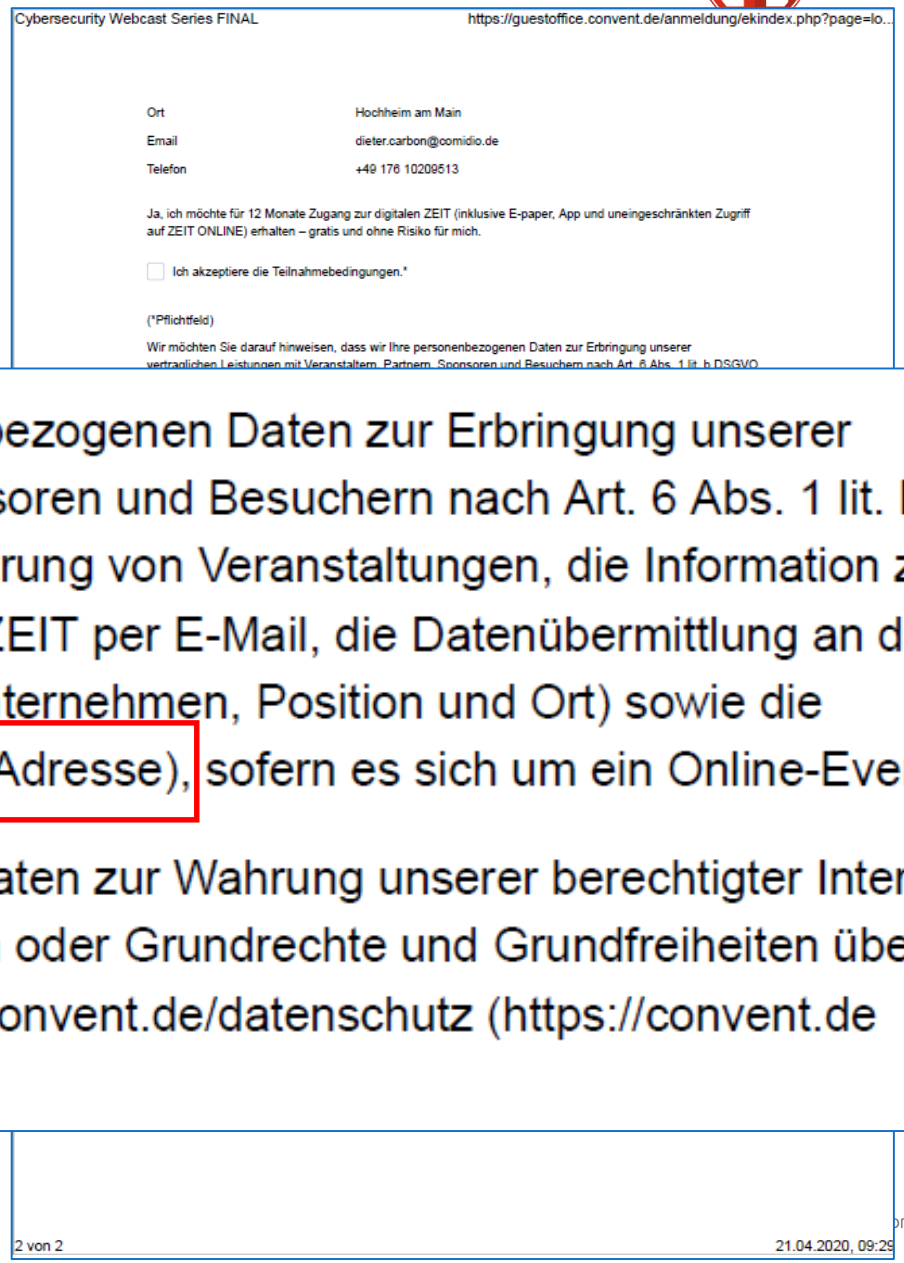
Der Anbieter muss Ihnen auch darlegen, ob er außereuropäische Dienstleister zur Erbringung der Leistung hinzuzieht. Einige Anbieter fungieren lediglich als Wiederverkäufer von Leistungen US-amerikanischer Unternehmen. Andere lassen einen wesentlichen Teil der Dienstleistung von außereuropäischen Unternehmen 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

Sammler & Jäger





Wir möchten Sie darauf hinweisen, dass wir Ihre personenbezogenen Daten zur Erbringung unserer vertraglichen Leistungen mit Veranstaltern, Partnern, Sponsoren und Besuchern nach Art. 6 Abs. 1 lit. b DSGVO (Rechtsgrundlage) verarbeiten. Dazu gehören die Durchführung von Veranstaltungen, die Information zu künftigen Veranstaltungen und Aktionen von Convent und ZEIT per E-Mail, die Datenübermittlung an die jeweiligen Partner und Sponsoren (Vor- und Nachname, Unternehmen, Position und Ort) sowie die Datenübermittlung an ZOOM (Vor- und Nachname, E-Mail-Adresse), sofern es sich um ein Online-Event handelt.

Darüber hinaus verarbeiten wir Ihre personenbezogenen Daten zur Wahrung unserer berechtigter Interessen nach Art. 6 Abs. 1 lit. f DSGVO, sofern nicht Ihre Interessen oder Grundrechte und Grundfreiheiten überwiegen. Weitere Hinweise zum Datenschutz finden Sie unter www.convent.de/datenschutz (https://convent.de/de/datenschutz/).

Passive Gefährdung

trutzbox
back to privacy

beim Surfen?

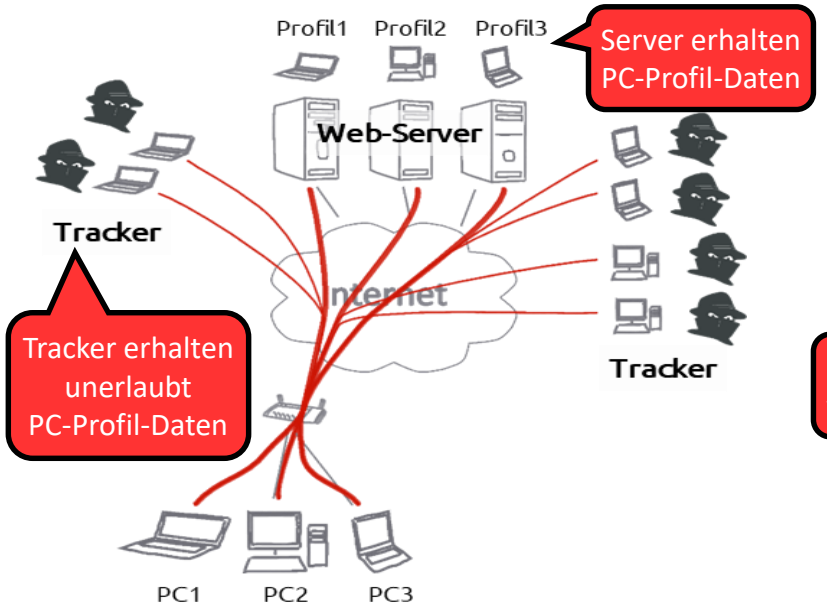
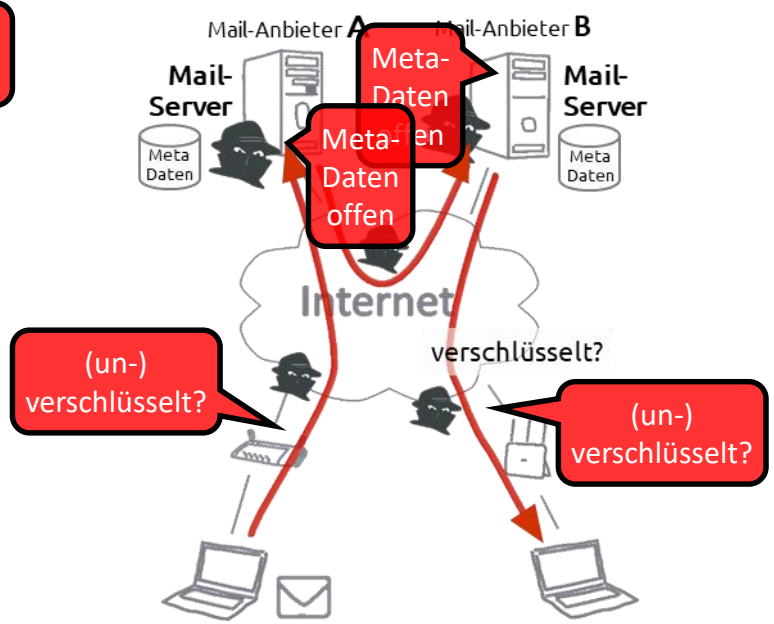


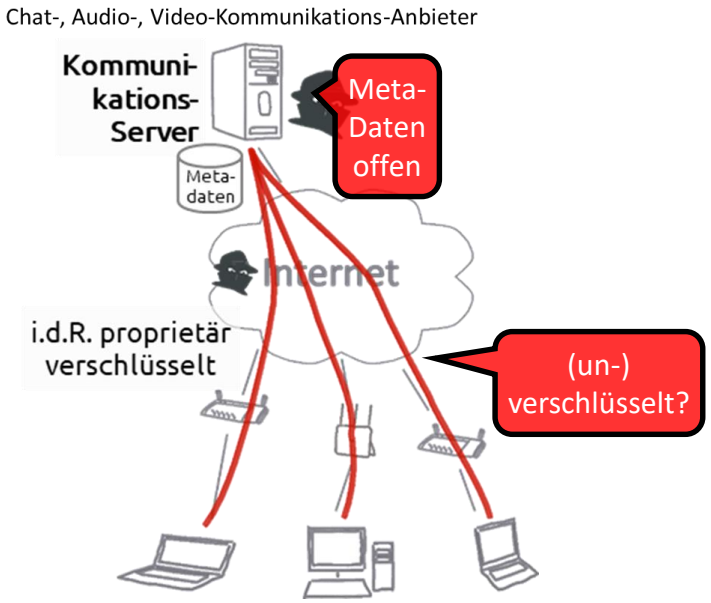
Foto: Comidio GmbH

beim Austausch von E-Mails?



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

bei Videokonferenzen/Webmeetings?



- Traue ich der Technik des Anbieters?
- Traue ich dem Anbieter?

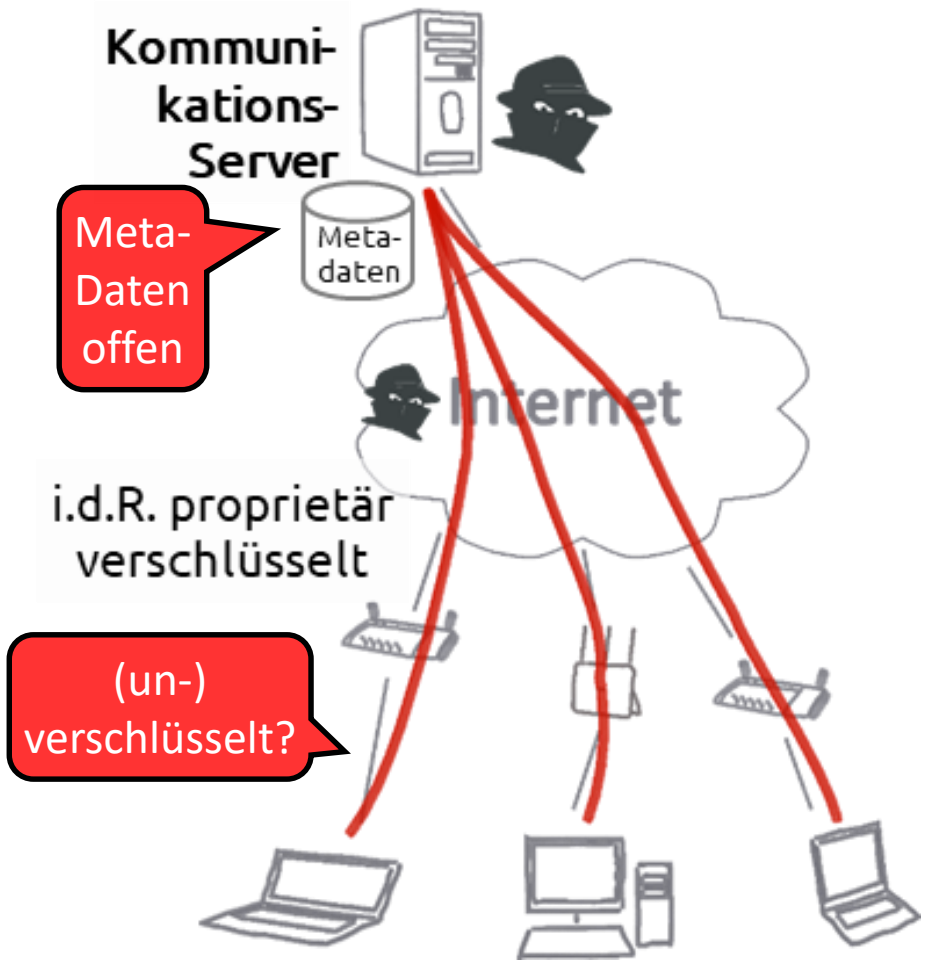
Privacy made in Germany

Passive Gefährdung … und Abhilfe

trutzbox
back to privacy

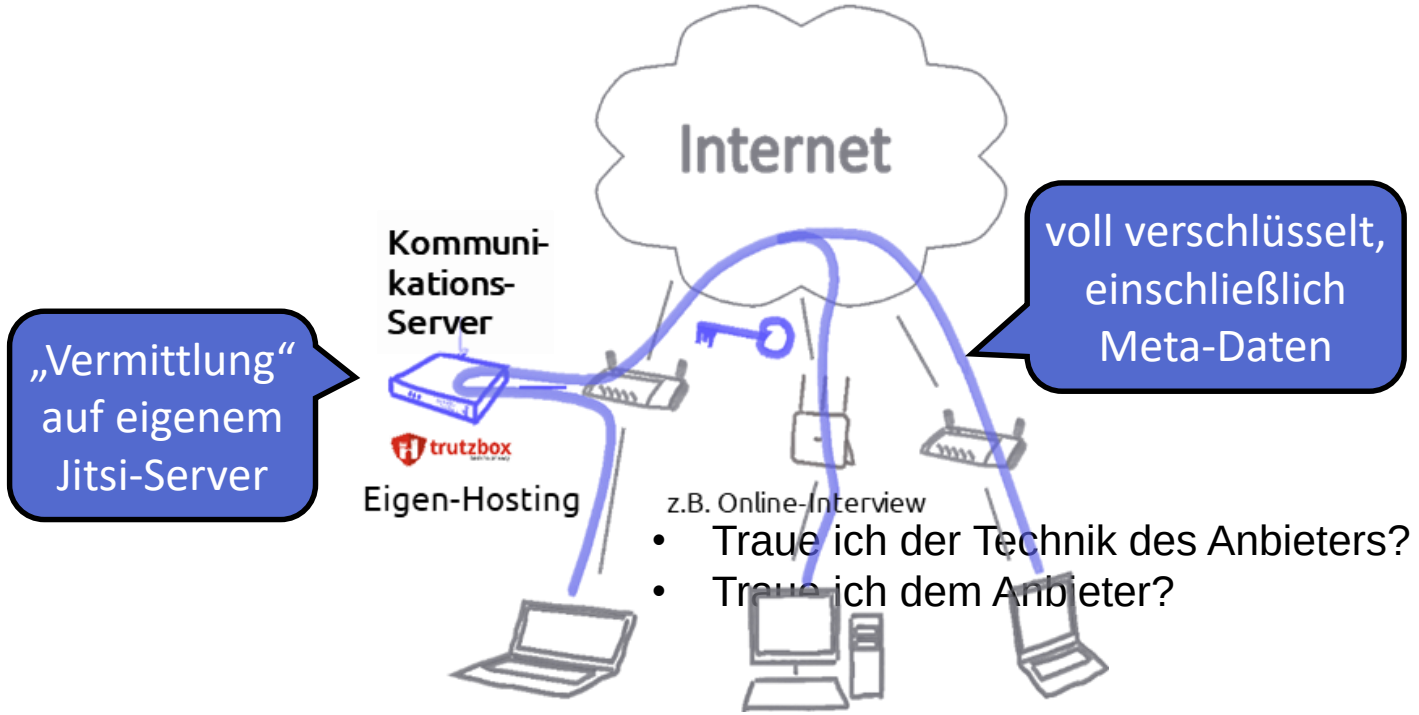
offene Metadaten und ggf. Inhaltsdaten beim Anbieter

Chat-, Audio-, Video-Kommunikations-Anbieter



verschlüsselter Video- und Audio-Chat

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



- Traue ich der Technik des Anbieters?
- Traue ich dem Anbieter?

Privacy made in Germany

Passive Gefährdung … und Abhilfe

trutzbox
back to privacy

Webmeeting-Systeme

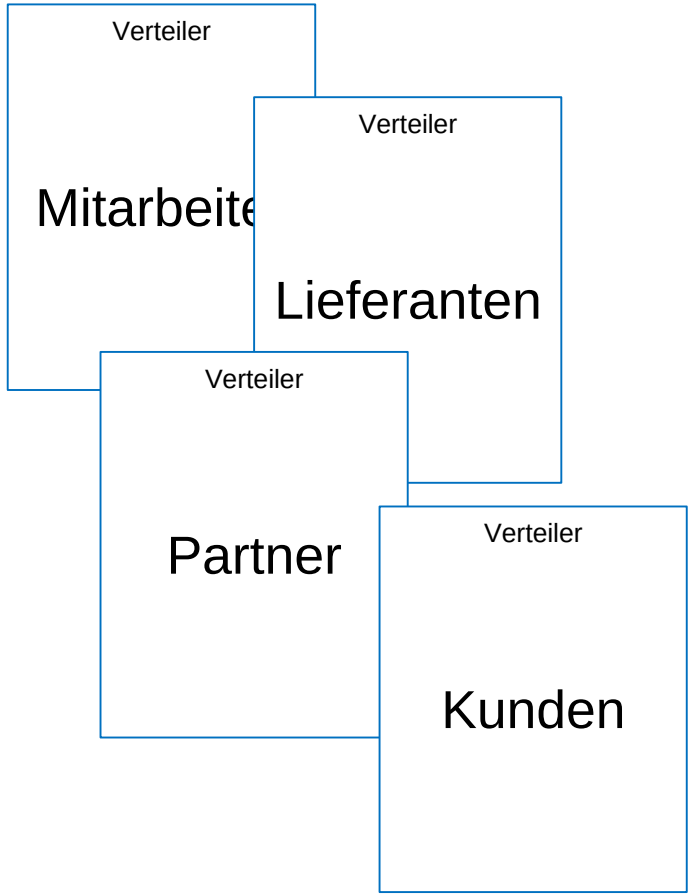
Propietäre Systeme

Quelloffene Systeme

Fremd-Betrieb außerhalb Europa

Fremd-Betrieb In Europa

Eigen-Betrieb



Privacy made in Germany

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**.

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.

Es geht um Vertrauen

trutzbox
back to privacy

https://duckduckgo.com/?q=spahn+aufzug+foto&t=iphone&ia=images&iax=images&iai=https%3A%2F%2Fwww.express.de%2Fimage%2F36569028%2F2x1%2F940%2F470%2Ffbc7865dc5e4677ba7f8596bf6f13176%2FMI%2Fjens-spahn-aufzug.jpg

Privacy made in Germany

Eigene Analyse …

Kriterien	Webmeeting, betrieben über externen Service-Anbieter	Jitsi, betrieben über eigenen Server, z.B. TrutzBox
Verschlüsselung	Anbieter verschlüsselt und kann auch selbst entschlüsseln. Was sichert er zu?	Ihre TrutzBox verschlüsselt TrutzBox zu TrutzBox und TrutzBox zu Browser.
Anzahl Räume	Wieviele Räume kosten wieviel?	Unbegrenzte Raum-Anzahl im Fix-Preis.
Anzahl Teilnehmer	Wieviele Teilnehmer kosten wieviel?	Unbegrenzte Teilnehmer-Anzahl im Fix-Preis.
Anzahl parallele Sessions (Räume)	Wieviele Räume können parallel zu welchen Kosten genutzt werden?	Unbegrenzte Anzahl paralleler Sessions (Räume)im Fix-Preis.
Datenschutz-Gesetz	Welchem Datenschutz-Gesetz (Land) unterliegt der Anbieter?	Sie betreiben Ihre TrutzBox wo immer Sie möchten und unterliegen keinem Anbieter-Gesetz.
Datenschutz	Welchen Datenschutz sagt der Anbieter zu? Viele Anbieter haben standard-mäßig Tracker (u.a. Google, Twitter, Facebook) eingebaut.	Sie wissen und bestimmen, wem Sie welche Daten weitergeben. Ihre TrutzBox sendet keine Daten weiter. Auch nicht an Comidio.
Personal-Qualität	Hat der Anbieter zuverlässiges Personal?	Sie sind Ihr eigenes TrutzBox Betriebs-Personal.
Technik-Qualität	Setzt der Anbieter zuverlässige Technik ein (oder z.B. problematischen Flash Player)?	Die TrutzBox bietet ausgezeichnete HD-Audio Qualität mit Opus und verschlüsselt sicher.
Angriffs-Attraktivität	Anbieter mit großer Kundenzahl ist lohnenswertes Angriffsziel für Hacker und Wirtschafts-Kriminelle.	Die geringe Anzahl Ihrer TrutzBox Teilnehmer macht konkreten Angriff unattraktiv für Hacker und Kriminelle.
Download Risiko	Muss Software heruntergeladen werden?	TrutzMeeting basiert auf dem neuen WebRTC Standard und funktioniert, da browserbasiert, **ohne** risiko-behafteten Software-Download für Teilnehmer.
Meta-Daten	Anbieter verwaltet und speichert Meta-Daten: wer meetet wann, wie lange, wie oft, mit wem und unter welchem „Titel“.	Selbstverständlich kennen Sie, als TrutzBox Betreiber (= Administrator) die Meta-Daten, aber eben nur Sie.
Einbruchs-Sicherheit	Wie einbruchsicher ist der Anbieter?	Sie bestimmen die Sicherung Ihrer TrutzBox selbst.
Kosten	Welche Kosten entstehen gegenüber dem Anbieter? - teilweise über 1.000 € Einrichtung, - teilweise über 300 € Jahresgebühr (je was?).	Die TrutzBox Kosten sind bekannt: - TrutzBox Set einmalig - Update Service jährlich.
Software	Quelloffen? In der Regel „proprietär“, also nicht offengelegt.	Die TrutzBox ist mit quelloffener Software erstellt, also transparent und jederzeit überprüfbar.
Zusatznutzen	Kein weiterer Nutzen!?	Mit der TrutzBox: - verschlüsseltes Mailen und - spurenarmes Surfen.

Ja, aber … (Memo an DSB)

trutzbox
back to privacy

Sehr geehrte Frau/ geehrter Herr [Datenschutzbeauftragte/r],

wir, die [], stehen mit dem Bereich [] ihres Unternehmens in geschäftlichem Kontakt.

Heute hat dieser Bereich zu einem Webmeeting / zu einer Videokonferenz auf Basis von [] eingeladen.

Der Einladende konnte uns nicht zusichern, dass die genutzten Server sich unter der Kontrolle Ihres Unternehmens befinden und/oder der DS-GVO unterliegen. Zudem bestehen unsererseits Zweifel, dass weder die eingesetzte, proprietäre Technologie noch das betreibende Unternehmen, über technische und organisatorische Zweifel erhaben sind.

Da wir an einer weitergehenden Geschäftsbeziehung mit ihrem Hause interessiert sind, werden wir zeitnah das beschriebene Meeting-Tool nutzen, möchten aber zugleich mit Nachdruck darauf hinweisen, dass es technisch-organisatorische Möglichkeiten gibt, Online-Meetings datenschutz-konform aufzusetzen und zu betreiben.

In diesem Sinne möchten wir anregen, baldmöglichst auf ein sichereres Tool umzusteigen, und so ihre und unsere Geschäftsdaten besser zu schützen.

Wir bauen auf Ihr Verständnis und bitten den Eingang dieses Schreibens zu bestätigen.
Besten Dank im Voraus.

Mit freundlichen Grüßen,

Privacy made in Germany

trutzbox
back to privacy

Danke für Ihr Interesse!

Haben Sie eine sichere Zeit …

Privacy made in Germany