IT-Sicherheit im Büro

Michael Georg Schmidt
Ein Beitrag der studentischen Gruppe ***ITS Us.***
der ***TH Lübeck***

7. September 2023

Kontakt
Threema ID: WYH86UFA
E-Mail: mail@its-us.info

Zusammenfassung

Dieser Artikel zeigt Ihnen Möglichkeiten auf, Ihre Daten und Ihre IT zu schützen. Dafür reicht die Lektüre des ***Abschnitts 1***. Er weist auf Alternativen zu Microsoft hin und erklärt in einer auch für ***absolute Laien*** verständlichen Weise, warum diese Maßnahmen sinnvoll sind. Die blauen Textstellen führen zu externen Links, die roten Textstellen führen Sie zu Verlinkungen im Text.
Alle Einträge im Inhaltsverzeichnis sind verlinkt, genauso in den Quellen. Wenn Sie schnell etwas nachsehen möchten, finden Sie alle Quellen verlinkt am Ende dieses Artikels.
Ab ***Abschnitt 2*** finden Sie Erklärungen und Erläuterungen, die auch jede/r verstehen kann.

Inhaltsverzeichnis

1 Empfehlungen

Hier finden Sie einige Empfehlungen.

1.1 Betriebssystem

Das Betriebssystem eines Computers ist das Programm, das es möglich macht, den Rechner zu nutzen.Meistens sind dies ***Windows*** von ***Microsoft*** oder ***iOS*** von ***Apple***. Sofern Sie ***Windows*** einsetzen, entsteht für Sie ab dem ***09. Oktober 2024*** Handlungsbedarf. Am ***08. Oktober 2024*** endet nämlich der Support für Windows 11, dem jüngsten Windows. Das heißt, dass Sie ab diesem Tag keine Sicherheitsupdates mehr bekommen und deshalb auf die nächste Version von Windows umsteigen sollten.
Leider soll diese Version jedoch ein Online-Betriebssystem werden (1, 2, 3, 4, 5). Da Microsoft mit Ihren Daten ausgesprochen nachlässig und leichtfertig umgeht, ist Windows ab diesem Zeitpunkt kein Betriebssystem mehr, das man nutzen sollte.
Alternativ können Sie stattdessen auf ***Apple*** mit ***iOS*** oder ***Linux*** umsteigen.

1.2 Office Suite / Programme

Als Office Suite empfehle ich ***LibreOffice***. LibreOffice bietet Ihnen alles, was Sie im Büroalltag benötigen. Alle Dateien können Sie in einem ***Microsoft kompatiblen*** Format abspeichern. Dies ist ***voreinstellbar***.
Die Installation ist lokal, somit vermeiden Sie eine Übertragung von Daten in die USA oder außerhalb Europas.

1.3 Verschlüsselung

Die ***notwendige Verschlüsselung*** betrifft sechs Bereiche. Dies sind

1. Verschlüsselung personenbezogener Daten auf der Festplatte
2. Verschlüsselte Speicherung in der Cloud
3. Verschlüsselung von E-Mails
4. Verschlüsselte (gemeinsame) Kalender
5. Verschlüsselte Aufbewahrung von Passwörtern
6. Verschlüsselte Messenger

Die verschlüsselte Speicherung von Daten auf der Festplatte lässt sich bei einem ***Linux-Betriebssystem*** bereits bei der Installation einstellen.
Eine ***Alternative*** ist die verschlüsselte Speicherung von einzelnen Dateien und Ordnern. Diese lässt sich mit ***Vera Crypt*** umsetzen.
Als ***sicheren*** und ***Ende-zu-Ende-Verschlüsselten Cloudspeicher*** empfehle ich ***ProtonDrive***. Am besten als Paket ***ProtonMail Plus*** oder ***ProtonMail Unlimited***, da Sie damit gleichzeitig auch ***verschlüsselte Kalender*** für die gemeinsame Nutzung erhalten und Ihren Datenverkehr ins Internet auf bis zu ***zehn*** Geräten mit einem ***VPN - Virtual Private Network*** absichern können.
Sie sollten für *jeden Zugang* ein ***eigenes, sicheres*** Passwort haben. Da sich das niemand merken kann, gibt es so genannte ***Passwort-Tresore***. Das sind Programme, die Ihre Passwörter sicher verschlüsselt speichern und bei Bedarf für Sie in Websites einsetzen. Hier sind ***KeePassXC*** als ***lokaler*** Passwort-Tresor und ***ProtonPass*** als ***online*** Passwort-Tresor empfehlenswert. ProtonPass bekommen Sie kostenlos oder im Paket mit ProtonMail.
Als Messenger empfehle ich Ihnen ***Signal*** oder ***Threema***.

2 Weshalb der ganze Aufwand?

Eine berechtigte Frage.

2.1 DSGVO - Datenschutzgrundverordnung

Art. 25 Abs. 1 DSGVO fordert „(1) Unter Berücksichtigung ***des Stands der Technik***, [...] der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen [...] die Datenschutzgrundsätze [...] wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“
Geeigent zum Schutz der Daten betroffener Personen ist die ***Verschlüsselung personenbezogner Daten*** mit sicheren Verfahren.

Microsoft und die Datensicherheit

Am ***11. Juli 2023*** wurde bekannt, dass Hacker sich einen „Generalschlüssel“ zu vermutlich sämtlichen Clouddiensten von Microsoft verschafft haben. Das Problem verschärft sich, weil Microsoft bereits drei Monate vorher von dieser Sicherheitslücke wusste und nichts dagegen unternommen hat. Im Folgenden versucht Microsoft so viel wie möglich zu vertuschen. Das amerikanische ***Cyber Safety Review Board*** hat am 11. August 2023 begonnen, den Vorfall aufzuklären.

2.2 Verschlüsselung

Als ***Stand der Technik*** ist eine ***Ende-zu-Ende-Verschlüsselung - E2EE (End-to-End-Encryption)*** anzusehen. Dies gilt für jegliche Datenübertragung und heißt, dass die Daten auf dem Ausgangsgerät mit einem sicheren Verfahren verschlüsselt werden, verschlüsselt transportiert und gespeichert werden, und nur der rechtmäßige Empfänger die Daten erneut entschlüsseln kann. Dies ist bei M 365 ***vollständig ausgeschlossen***, da Microsoft keine E2EE anbietet. Dies gilt sowohl für die Speicherung von Daten als auch für die Übertragung von E-Mails.

Die ***Eintrittswahrscheinlichkeit*** ist mit dem ***Hackerangriff auf die Clouddienste von Microsoft*** bereits umgesetzt worden.
Die ***Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen*** ist ***unabsehbar***, da nicht einschätzbar ist, wieviele und welche Daten durch den Angriff auf die Microsoft Cloud kompromittiert wurden. Letztlich hängt dies im Einzelfall von Ihnen ab, welche Daten Sie verarbeiten.
Ein dem ***Risiko angemessenes Schutzniveau*** ist mit M 365 ***nicht*** zu erreichen, da die Daten, wenn sie diese bearbeiten, zwangsläufig in der Cloud unverschlüsselt vorliegen. Damit haben Microsoft, amerikanische Behörden und potentielle Angreifer vollen Zugriff auf Ihre Daten.

2.3 Datenübertragung in die USA

Seit dem 10. Juli 2023 ist es wieder einmal zulässig Personen bezogene Daten in die USA zu transferieren. Dies ermöglicht der Beschluss der Europäischen Kommission. Dennoch gibt es Stimmen, die das kritisch sehen. Dazu gehören

- der ***Thüringer Landesbeauftragte für Datenschutz und Informationsfreiheit*** - Pressemitteilung vom 14.07.2023
- der Landesbeauftragter für den Datenschutz in Niedersachsen - Datenübermittlung in die USA: EU erläßt neuen Angemessenheitsbeschluss
- ***Datenschutz Hessen*** Angemessenheitsbeschluss zum EU-US Data Privacy Framework in Kraft getreten
- Heise Security - Krtik an „Wahnsinn“ : EU-Kommission gibt Datentransfer in die USA wieder frei

Faktisch ist davon auszugehen, dass der ***EuGH - Europäische Gerichtshof*** auch diese Vereinbarung für rechtswidrig erklärt, denn es hat sich in den USA nichts zum Positiven verändert. Im Gegenteil, es sind neue schwere Verstöße gegen den Datenschutz bekannt geworden

- Heise Security FBI beschlagnahmt unbeteiligten Mastodon Server - und behält ihn
- Heise Security Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert

2.4 Cloudspeicher

Für die Zusammenarbeit ist es wichtig, dass man gemeinsam auf Daten zugreifen kann. Hierfür bietet sich ***Cloudspeicher*** an. Der ***Cloudspeicher von Microsoft*** weist gleich mehrere Probleme auf

- Er bietet keine E2EE - das bedeutet, dass Ihre Daten beim Transport in die Cloud nur auf dem Transportweg verschlüässelt sind. Das geschieht mit ***TLS - Transport Layer Security***.
- Microsoft setzt ***TLSv1.2*** ein. Aktuell ist die Version ***TLSv1.3***. Die eingesetzte Version hat bekannte kryptographische Schwächen.

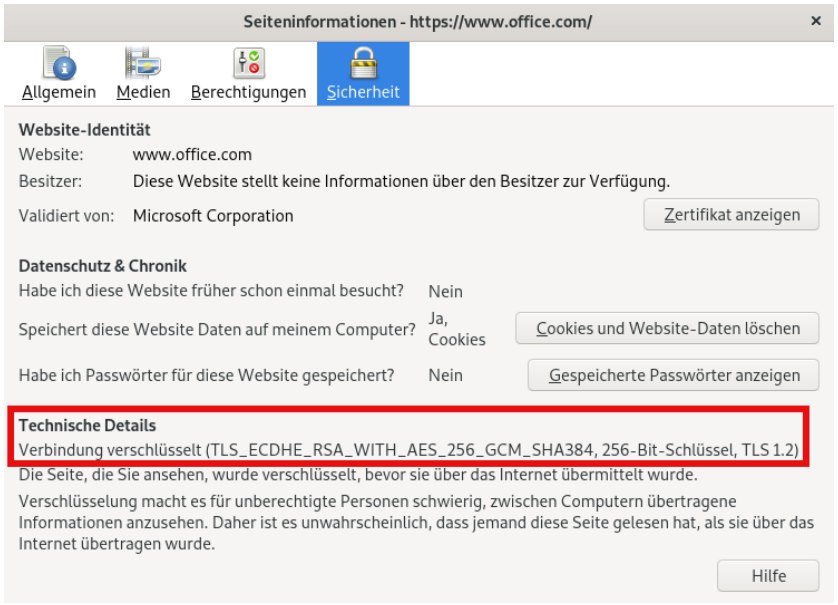

Abbildung 1: Rechts im Rahmen sehen Sie die TLS Version - abgerufen am 18.08.2023

- Ihre Daten passieren bis zu ***40 Hops - Zwischenstationen*** - auf dem Weg zur Microsoft Cloud. Die Transportweg-Verschlüsselung greift nur von Hop zu Hop. Jeder Hop entschlüsselt Ihre Daten, inspiziert diese und verschlüsselt sie neu. Es ist nicht geregelt und unbekannt, was mit Ihren Daten während der Zeit, die diese im Klartext auf einem Hop vorliegen, passiert. 2017 scheiterte der Versuch der obersten Regulierungsinstanz ***IETF - Internet Engeneering Task Force*** des Internets diesen Vorgang zu regeln, am Widerstand vieler Hop-Betreiber. Diesem Problem

könnte man jedoch mit dem Einsatz eines ***VPN - Virtual Private Network*** begegnen, bei dem Ihre Daten auf dem Ausgangsgerät verschlüsselt und ohne Zwischenstationen direkt ans Ziel transportiert werden, wo sie schließlich entschlüsselt werden.

- Microsoft bietet eine Verschlüsselung in der Microsoft Cloud an - der Schlüssel muss aber bei Microsoft gespeichert sein. Damit hat Microsoft Zugriff auf Ihre Daten.
- Microsoft bietet bei einer Lizenz, die Möglichkeit den Schlüssel für Daten lokal vorzuhalten - aber dies muss auf Hard- oder Software von Microsoft geschehen. Damit hat Microsoft auch da Zugriff auf Ihre Schlüssel.

2.5 Kalender

Microsoft bietet über ***Outlook / Exchange*** Kalender an, die von mehreren Personen genutzt werden können - aber die Daten in diesen Kalendern sind ebenfalls ***nicht verschlüsselt***. Damit hat Microsoft einen weiteren Ansatzpunkt, um Profile seiner Nutzer anzufertigen.

2.6 Windows geht in die Microsoft Cloud

Mit dem ***Ende des Supports für Windows 11***, das am ***08. Oktober 2024*** erreicht ist, plant Microsoft, sein Betriebssystem Windows in die Microsoft Cloud zu verlagern (1, 2, 3, 4, 5). Das bedeutet, dass die Daten der Nutzer ***vollständig und ausnahmslos*** der Kontrolle und dem Zugriff Microsofts und der amerikanischen Behörden auf Grund entsprechender Gesetze (FISA, Patriot Act) ausgesetzt sind.

2.7 Profilbildung

Wenn Sie im Internet surfen, fallen automatisch Daten an, die Ihnen zuzuordnen sind. Datenhändler wie ***Acxiom*** sammeln diese Daten und erstellen hieraus Profile, die sie verkaufen. Um das zu vermeiden, empfiehlt es sich, ein ***VPN - Virtual Private Network*** einzusetzen. Bei dieser Technik verbinden Sie sich mit einem Server Ihres VPN-Anbieters, der Ihre Anfrage ins Internet weiterleitet. Gleichzeitig wird Ihre Anfrage auf Ihrem Ausgangsgerät verschlüsselt und erst beim Empfänger, dem VPN-Server, wieder entschlüsselt. Da ***sehr viele*** Nutzer über diesen Server Anfragen stellen, kann eine Website nicht mehr nachvollziehen, welcher „Person“ diese Anfrage zuzuordnen ist. Damit macht man es Datenhändlern nahezu unmöglich seine eigenen Daten zu einem Profil zusammen zu führen. Als VPN-Anbieter ist ***ProtonVPN*** im Paket ***Proton Mail Plus*** oder ***Proton Unlimited*** empfehlenswert.

3 Alternative Vorschläge

3.1 Datenübertragung in die USA

Um eine Übertragung von (personenbezogenen) Daten in die USA zu vermeiden, empfiehlt es sich, eine ***Office Suite lokal*** zu installieren. Eine ***Office Suite*** ist eine Sammlung von Programmen, die für den Einsatz im Büro als sinnvoll oder notwendig erachtet werden.
Mögliche Software hierfür wären

- ETES.IO
- LibreOffice - kostenlos
- OpenOffice - kostenlos

Die Aufzählung ist beispielhaft und alphabetisch sortiert. Es gibt noch weitere Alternaitven. Für empfehlenwert halte ich ***LibreOffice***.

3.2 Verschlüsselung

Sie sollten dafür sorgen, dass die Systeme, die Sie einsetzen, vollständig eine ***E2EE*** beherrschen. Im Einzelnen bedeutet das

- Ihre ***Daten*** müssen verschlüsselt gespeichert werden, sowohl ***lokal*** als auch in der ***Cloud***
- Ihre ***E-Mailkommunikation*** muss E2EE sein, sofern sie personenbezogene Daten betrifft, was fast immer der Fall ist

- Ihre ***(gemeinsamen) Kalender*** sollten verschlüsselt gespeichert werden, weil gerade Kalender viele personenbezogene Informationen enthalten
- Ihre ***Passwörter*** sollten verschlüsselt gespeichert werden
- Sofern Sie ***Messenger*** einsetzen, müssen auch diese permanent eine E2EE einsetzen und den Datenschutzbestimmungen entsprechen

3.3 Lokale Verschlüsselung

Sie können ein Betriebssystem auf Ihrer Hardware installieren, das standardmäßig alle Daten auf der Festplatte im Ruhezustand verschlüsselt. Mit Linux ist das kein Problem.
Alternativ können Sie das kostenlose Programm ***VeraCrypt*** dafür einsetzen, um einzelne Dateien oder Ordner zu verschlüsseln.

3.4 Cloudspeicher

Als Alternative zur Microsoft Cloud ist ***E2EE Cloudspeicher in Europa oder der Schweiz*** empfehlenswert. In der Schweiz gilt ein ähnlich strenges Datenschutzrecht wie es die DSGVO bietet. Hier sind aktuell zwei Anbieter besonders interessant

- Proton mit seinem Produkt ProtonDrive
- Tresorit - Tresorit zum kostenlosen Ausprobieren mit ***2GB*** Speicher

Sowohl ProtonDrive als auch Tresorit bieten ***Desktop-Apps*** an, über die Sie direkt auf Ihren Cloudspeicher zugreifen können. Zusätzlich können Sie Ihre lokalen Daten hierüber automatisch mit dem Cloudspeicher synchronisieren. Damit haben Sie ein ***automatisches Backup***, ohne großen Aufwand betreiben zu müssen.
Der Anbieter ***Tutanota*** arbeitet an einem Cloudspeicher der sogar „quantensicher“ sein soll, aber das Ziel soll erst in etwa dem Jahr 2026 erreicht sein.

3.5 E-Mailkommunikation

Mit dem E-Mailprovider ***ProtonMail*** können Sie auf einfache Art, E-Mails ***Ende-zu-Ende-Verschlüsseln*** und Ihre Domain bei dem bisherigen Domain-Provider belassen. Die verschlüsselte E-Mailkommunikation funktioniert auch mit einem Gegenüber, das von E-Mailverschlüsselung noch nie etwas gehört hat.

Alternativ könnten Sie auch die Anbieter ***Tresorit*** oder ***Tutanota*** nutzen.

3.6 Kalender

Verschlüsselte Kalender mit Zugriff durch mehrere Personen haben alle drei eben erwähnten Anbieter im Portfolio

- ProtonCalendar
- Tresorit
- Tutanota - im Zusammenhang mit einem (kostenlosen) E-Mailkonto

Alle drei bieten auch ***Apps*** für den ***Desktop*** und ***Mobilgeräte*** an. Sie müssen also nicht auf Webanwendungen zugreifen, was alle Verfahren noch sicherer macht.

3.7 Passwörter - Passwort-Tresore

Es kann immer einmal passieren, dass ein Passwort von Ihnen kompromittiert wird. Wenn das passiert, ist es unschön, aber ***wichtig***, dass Sie dieses Passwort ***nur für ein Konto*** verwendet haben, denn sonst kann der Angreifer auch auf alle anderen Konten von Ihnen zugreifen, die das gleiche Passwort verwenden. Im schlimmsten Fall könnte man Ihre ***digitale Identität*** übernehmen.

Sichere Passwörter

Sichere Passwörter sollten

- GROSS- und kleinbuchstaben enthalten
- Zahlen einbinden 0...9
- Sonderzeichen verwenden !?=’$ ...
- vor allem aber ***lang*** sein, möglichst 16 Zeichen als Minimum

Entgegen früheren Vorgaben gilt inzwischen, dass man ein Passwort gerne lebenslang verwenden kann, ***wenn es gut und sicher ist***. Da sich niemand solche Passwörter merken kann, gibt es so genannte ***Passwort-Tresore***.
Bei Passwort-Tresoren unterscheidet man zwischen ***lokalen*** und ***online*** Passwort-Tresoren. Die hier vorgestellten Passwort-Tresore erstellen für Sie auf Wunsch auch sichere Passwörter. Alternativ können Sie das Programm ***PWGen*** verwenden.

Lokale Passwort-Tresore

Ein ***Lokaler Passwort-Tresor*** hat den ***Vorteil***, dass nur Personen, die einen ***physischen Zugang*** zu dem Gerät haben, auf dem dieser Tresor gespeichert ist, diesen angreifen könnten.
Der ***Nachteil*** ist, dass Sie diesen Tresor auch nur von ***einem*** Gerät aus nutzen können.

Online Passwort-Tresore

Online Passwort-Tresore haben den ***Vorteil***, dass Sie diese mit ***beliebig vielen*** Geräten nutzen können.
Der ***Nachteil*** ist, dass eine unbestimmbare Anzahl von Personen Ihren Passwort-Tresor angreifen könnte.

Empfehlung

Welche Lösung für Sie die richtige ist, müssen Sie selbst entscheiden. Zwei (kostenlose) Passwort-Tresore halte ich für empfehlenswert. Sie sind beide ***Open Source***. Es kann also jeder sehen, was diese Tresore machen. Die Sicherheit entsteht durch die jeweils verwendeten kryptographischen Verfahren.

- KeePassXC - ein ***lokaler*** Passwort-Tresor
- ProtonPass - ein ***online*** Passwort-Tresor

3.8 Messenger

Wenn Sie ***Messenger*** nutzen, müssen diese auch ***Ende-zu-Ende-Verschlüsselt*** arbeiten.

Empfehlenswert

Empfehlenswerte Messenger sind

- Signal für Mobilgeräte und Signal für den Desktop
- Threema und Threema für den Desktop

Erläuterungen

Signal ist in den USA beheimatet, von da her eher fragwürdig, aber eine Bürgerrechtsorganisation betreibt den Messenger. Signal speichert nur das Datum der Installation und das Datum der letzten Kommunikation. Das sind so wenige Daten, dass man Signal vertrauen kann.
Threema können Sie auch ***vollständig anonym*** nutzen, denn Sie müssen weder Ihre Telefonnummer, noch Ihre Kontakte preisgeben.
Bedauerlich bei ***Threema*** ist der Umgang mit einem Fehler, der entdeckt wurde. Statt den Fehler zu beheben und sich für den Hinweis zu bedanken, hat Threema recht harsch reagiert. Das hat dem Unternehmen einen Negativpreis, den „Pwnie Award“ der IT Sicherheitskonferenz ***Black Hat 2023*** eingebracht.
Das Problem ist inzwischen behoben und somit erhalten beide Messenger eine Nutzungsempfehlung.

Warnung

Eine ausdrückliche ***Warnung*** gilt dem Einsatz von

- Telegram
- Tiktok

Beide ignorieren die Privatsphäre der Nutzer vollständig. ***Telegram überträgt sämtliche Eingaben in Echtzeit*** an die Telegram Server. Damit werden auch die Eingaben übertragen, die Sie vor dem Absenden gelöscht haben. Privatsphäre ist damit nicht möglich, genauso wenig wie eine E2EE.
Tiktok spioniert Nutzer aus und verfolgt sogar Journalisten.

4 Quellen

Hier finden Sie alle im Text erwähnten Quellen.

1. Althammer & Kill (18.08.2023) - https://www.althammer-kill.de/
2. Althammer & Kill zu Microsoft 365 in Kirche und Wohlfahrt v2 - https://web.tresorit.com/l/6IrH1#MhRoUtpryZpiQRDN1koyVg
3. Angemssenheitsbeschluss EU - USA (18.08.2023) - https://germany.representation.ec.europa.eu/news/datenverkehr-zwischen-der-eu-und-den-usa-europaische-kommission-erlasst-neuen-2023-07-10_de
4. Angemessenheitsbesschluss zum EU-US Data Privacy Framework in Kraft getreten (18.08.2023) - https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/eu-us-data-privacy-framework-in-kraft-getreten
5. Acxiom - Datenhändler (22.08.2023) - https://www.acxiom.com/
6. Computerwoche - Microsoft auf Irrwegen (18.08.2023) - https://www.computerwoche.de/a/windows-aus-der-cloud-im-ernst,3614914
7. CSRB Cyber Safety Review Board (18.08.2023) - https://www.dhs.gov/news/2023/08/11/department-homeland-securitys-cyber-safety-review-board-conduct-review-cloud
8. Cyber Safety Review Board (24.08.2023) - https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb
9. Datenschutz Hessen (18.08.2023) - https://datenschutz.hessen.de/
10. Datenübermittlung in die USA: EU erläßt neuen Angemessenheitsbeschluss (18.08.2023) - https://lfd.niedersachsen.de/startseite/themen/internationaler_datenverkehr/datenubermittlung_in_die_usa_eu_erlasst_neuen_angemessenheitsbeschluss/datenubermittlung-in-die-usa-eu-erlasst-neuen-angemessenheitsbeschluss-223847.html
11. Dell (19.08.2023) - https://www.dell.com/de-de?c=de&l=de&s=gen&mp=dell.de/&redirect=1
12. Der Standard - Microsoft plant, Windows 11 komplett in die Cloud zu heben (18.08.2023) - https://www.derstandard.de/story/3000000176663/microsoft-plant-windows-11-komplett-in-die-cloud-zu-heben
13. ETES.IO (18.08.2023) - https://www.etes.de/etes.io/

14. EU-DSGVO (22.08.2023) - https://dejure.org/gesetze/DSGVO
15. Heise Online, Frank Schröer - Microsoft will Windows komplett in die Cloud verlagern (18.08.2023) - https://www.heise.de/news/Microsoft-will-Windows-11-komplett-in-die-Cloud-verlagern-9200869.html
16. FISA Foreign Investigative Surveiliance Act (18.08.2023) - https://www.law.cornell.edu/uscode/text/50/1881a
17. Heise Security, Stefan Krempl - FBI beschlagnahmt unbeteiligten Mastodon-Server und behält ihn (18.08.2023) - https://www.heise.de/news/Mastodon-FBI-und-Admins-in-der-Kritik-nach-Server-Beschlagnahme-9227813.html
18. Heise Security, Jürgen Schmidt (18.08.2023) - Gestohlener Cloud-Master-Key: Microsoft schweigt - so fragen sie selbst - https://www.heise.de/news/Gestohlener-Cloud-Master-Key-Microsoft-schweigt-so-fragen-Sie-selber-9229395.html
19. Heise Security, Monika Ermert, Dusan Zivadinovic - IETF: TLS-Middleboxen, Verschlüsselung und die Rauferei um das „richtige"Internet (18.08.2023) - https://www.heise.de/news/IETF-TLS-Middleboxen-Verschluesselung-und-die-Rauferei-um-das-richtige-Internet-3695607.html
20. Heise Security, Stefan Krempl (18.08.2023) - Kritik an „Wahnsinn" : EU-Kommision gibt Datentransfer in die USA wieder frei - https://www.heise.de/news/Kritik-an-Wahnsinn-EU-Kommission-gibt-Datentransfer-in-die-USA-wieder-frei-9212124.html
21. Heise Security, Jürgen Schmidt (18.08.2023) - Microsoft Cloud: Weitere kritische Lücke - scharfe Kritik an Microsoft - https://www.heise.de/news/Microsoft-Cloud-Weitere-kritische-Luecke-scharfe-Kritik-an-Microsoft-9234573.html
22. Heise Security, Jürgen Schmidt (18.08.2023) - Microsofts gestohlener Schlüssel mächtiger als vermutet - https://www.heise.de/news/Neue-Erkenntnisse-Microsofts-Cloud-Luecken-viel-groesser-als-angenommen-9224640.html
23. Heise Security, Stefan Krempl - Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert (18.08.2023) - https://www.heise.de/news/Trotz-Verbot-FBI-hat-ueber-Vertragsfirma-NSO-Spyware-finanziert-9231066.html
24. Heise Security, Jürgen Schmidt - Telegram-Chat: der sichere Datenschutzalbtraum - eine Analyse und ein Kommentar (19.08.2023) - https://www.heise.de/hintergrund/Telegram-Chat-der-sic

here-Datenschutz-Albtraum-eine-Analyse-und-ein-Kommentar-4965774.html

25. IETF - Internet Engeneering Task Force (19.08.2023) - https://www.ietf.org/
26. KeePassXC (19.08.2023) - https://keepassxc.org/
27. LibreOffice (18.08.2023) - https://de.libreoffice.org/
28. Landesbeauftragter für den Datenschutz Niedersachsen (18.08.2023) - https://lfd.niedersachsen.de/startseite/
29. MacTechNews - Microsofts Pläne: Windows komplett in die Cloud - und eigene Prozessoren (18.08.2023) - https://www.mactechnews.de/news/article/Microsofts-Plaene-Windows-komplett-in-die-Cloud-und-eigene-Prozessoren-182820.html
30. Microsoft - Windows End-of-Live (22.08.2023) - https://learn.microsoft.com/en-us/lifecycle/products/windows-11-home-and-pro
31. Nau.ch - Windows hebt ab - in die Cloud (18.08.2023) - https://www.nau.ch/news/digital/windows-11-hebt-ab-in-die-cloud-66532852
32. OpenOffice (18.08.2023) - https://www.openoffice.org/de/
33. Patriot Act (18.08.2023) - https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act
34. Proton (18.08.2023) - https://proton.me/de
35. ProtonCalendar (18.08.2023) - https://proton.me/de/calendar
36. ProtonDrive (18.08.2023) - https://proton.me/de/drive
37. ProtonPass (19.08.2023) - https://proton.me/de/pass
38. PWGen (27.08.2023) - https://pwgen-win.sourceforge.io/
39. Pwnie Award Winner (19.08.2023) - https://docs.google.com/document/d/1H-fS7qC3dQLL6jzRFtkLVCs7nQBSJIBF4x6-98XAtRA/edit#heading=h.pnkk50rz2jgs
40. Signal (19.08.2023) - https://signal.org/de/
41. Signal Desktop (19.08.2023) - https://signal.org/de/download/
42. SWR Wissen - Diese Daten sammelt Tiktok (19.08.2023) - https://www.swr.de/wissen/daten-spionage-wird-tiktok-in-den-usa-verboten-100.html
43. Threema (19.08.2023) - https://threema.ch/de

44. Threema Desktop (19.08.2023) - https://threema.ch/de/home
45. Threema Blog Post (19.08.2023) - https://threema.ch/en/blog/posts/news-alleged-weaknesses-statement
46. Thüringer Landesbeauftragter für Datenschutz und Informationsfreiheit (18.08.2023) - https://www.tlfdi.de/
47. Thüringer Landesbeauftragter für Datenschutz und Informationsfreiheit - Pressemitteilung zum Angemessenheitsbeschluss der Europäischen Kommission - https://www.tlfdi.de/fileadmin/tlfdi/presse/Pressemitteilungen_2023/230714_PM_MS365_.pdf
48. Tresorit (18.08.2023) - https://tresorit.com/de
49. Tresorit kostenlos (18.08.2023) - https://web.tresorit.com/signup
50. Tresorit E-Mailing (19.08.2023) - https://tresorit.com/de/email-encryption-service
51. Tutanota (18.08.2023) - https://tutanota.com/de/
52. Understanding Microsoft Information Protection Encryption Key Types (18.08.2023) - https://techcommunity.microsoft.com/t5/security-compliance-and-identity/understanding-microsoft-information-protection-encryption-key/ba-p/2214589
53. VeraCrypt (18.08.2023) - https://www.veracrypt.fr/code/VeraCrypt/
54. Windows 11 Home and Pro (18.08.2023) - https://learn.microsoft.com/en-us/lifecycle/products/windows-11-home-and-pro