MIKE KUKETZ 1. MÄRZ 2021 8 ERGÄNZUNGEN

Ungewöhnliche IT-Sicherheits- und Datenschutztipps – Teil2

1. Follower-Power

Im ersten Teil habe ich euch einige unc IT-Sicherheits- und Datenschutztipps von Lesern vorgestellt, die über das Fediverse (Mastodon) genannt wurden. Ohne viel Umschweife kommen wir nun zum zweiten Teil, bei dem ich es mir ebenfalls erlaubt habe kleine Rechtschreib- und Grammatikfehler der Einsender zu korrigieren.

Vorab der Disclaimer: Es gibt keine allgemeingültigen Vorgehensweisen und Tipps, mit denen ihr euch vor allen Gemeinheiten schützen könnt, die in der IT-Welt lauern. Die vorgestellten Tipps können euch aber dabei helfen, euer persönliches Risiko zu minimieren. Allerdings solltet ihr immer bedenken, dass IT-Sicherheit und auch Datenschutz ein ständiger Prozess ist, der es notwendig macht, umgesetzte Maßnahmen regelmäßig kritisch zu hinterfragen und sich an neue Herausforderungen bzw. Gegebenheiten anzupassen.

Und nun viel Spaß beim Lesen. Ein Beitrag von Lesern für Leser – mit

> Account-Sharing macht Profiling schwer. Nur eine Person gibt bei der Anmeldung/Registrierung Daten an und alle anderen nutzen es mit.

Dieser Tipp ist mit Vorsicht zu genießen. Denn unter Umständen verstößt das Account-Sharing gegen die allgemeinen Geschäftsbedingungen eines Dienstes / Unternehmens. Und er kann auch für den eigentlichen Account-Inhaber **unangenehme** Folgen haben, bspw. dann, wenn die »Mitnutzer« rechtlich fragwürdig handeln. Persönlich würde ich diesen Tipp nicht umsetzen – aber womöglich gibt es Anwendungszwecke, die dafür infrage kommen.

> Nicht immer muss es eine Ausweis-Kopie sein, grundsätzlich muss ein Abgleich der aufgeschrieben Daten mit dem Ausweis reichen. Eine Ausweis-Kopie sollte grundsätzlich geschwärzt sein und ist ohne explizite Einwilligung des Ausweisinhabers illegal.

Ein komplexes Thema, das ich nur kurz anreißen möchte. Was viele nicht wissen: Nur in wenigen Fällen seid ihr wirklich verpflichtet, den Ausweis bzw. eine Kopie vorzulegen. Dennoch stimmen viele leichtfertig zu oder kommen dem »Wunsch« von Anbietern bzw. Unternehmen nach, zur Identifikation eine Kopie des Ausweises vorzulegen / zu senden. Ich fasse mal kurz zusammen:

- Nach eurem Ausweis fragen dürfen Telekommunikationsanbieter (TKG § 95 Vertragsverhältnisse), wenn diese Angaben für die Überprüfung der Angaben erforderlich sind
- Nach dem Geldwäschegesetz (§ 8 GwG) stehen ebenfalls Kredit- und Finanzdienstleistungsinstitute oder Versicherungsunternehmen in der Pflicht, eine vollständige Kopie des Personalausweises anzufertigen
- Nur der Ausweisinhaber (oder ein Vertreter) darf eine Kopie / Ablichtung des Personalausweises vornehmen und auch nur der Inhaber darf die Kopie weitergeben
- Die Ablichtung muss eindeutig als Kopie erkennbar sein
- Sofern personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet werden, darf dies nur mit Einwilligung des Ausweisinhabers geschehen

Des Weiteren dürfen die Kopien / Ablichtungen zu Teilen auch geschwärzt werden –

und zwar jene Teile, die für den jeweiligen Zweck nicht erforderlich sind. Das sind bspw. Informationen wie:

- Zugangsnummer
- Seriennummer
- Maschinenlesbare Zone (Seriennummer, Prüfnummer etc.)
- Sicherheitsfaden

Ihr solltet euch genau überlegen bzw. informieren, ob ein Anbieter eine Ausweiskopie einfordern kann. Weitere Infos zum Thema: Wann ist das Kopieren des Personalausweises erlaubt?

> Für Seiten, die sinnloserweise einen Login wollen, gibt es: https://bugmenot.com/

BugMeNot ist eine Plattform, die sich rechtlich gesehen vermutlich irgendwo im Graubereich bewegt. Der Online-Dienst bietet Benutzernamen und Passwörter für **registrierungspflichtige** Webseiten an. Man muss sich also nicht selbst registrieren, sondern nimmt einfach bereits vorhandene Anmeldedaten, um sich einzuloggen. Es gibt sogar ein Firefox-Add-on (DontBugMe) das euch die Suche nach den Anmeldedaten auf der Webseite von BugMeNot abnimmt. Wie gut das in der Praxis funktioniert, habe ich bis dato nicht getestet.

> Wenn man gezwungen wird eine Telefonnummer anzugeben, niemanden zum Cold-Call-Ziel machen will und dem Betreiber mitteilen möchte, was er einen mal kann: Telefonpaul bzw. 0176-34636276

Bei wie vielen Online-Shops oder Dienstanbietern ist die Angabe der Telefonnummer ein Pflichtfeld? Nach meiner Erfahrung: Bei sehr vielen, obwohl meist nicht wirklich erforderlich. Wer nicht gerade etwas per Spedition bestellt, der wird kaum vom Online-Shop oder einem Transportdienstleister telefonisch kontaktiert. Es ist für einige daher ärgerlich, wenn man Informationen angeben muss, die zur eigentlichen Diensterbringung nicht erforderlich sind. Für die Telefonnummer gibt es da eine einfache Lösung: Telefonpaul. Ein Dienst, der automatisch Anrufe entgegennimmt und »abwimmelt« bzw. darauf hinweist, dass eine telefonische Kontaktaufnahme nicht gewünscht ist.

Hinweis: Ob es rechtlich immer einwandfrei ist eine falsche Nummer anzugeben, sei mal dahingestellt – Nutzung auf eigene Gefahr.

3. E-Mail

> Niemals einen Link in einer E-Mail anklicken.

Links in E-Mails beinhalten oftmals Phishing- oder Tracking-Links – und auch andere Gemeinheiten. Daher ist der Tipp durchaus sinnvoll, muss aber noch etwas präzisiert werden. Mein Tipp: Anstatt den Link in einer E-Mail (oder auch einer Messenger-Nachricht) anzuklicken, solltet ihr ihn kopieren und erst mal in eine Text-Datei einfügen. Dort könnt ihr den Link in aller Ruhe analysieren, ohne eine Aktion zu triggern. Ein kopierter Link kann bspw. so aussehen:

```
www.news-site.com/scan.php?page=news_item&px=privacy_nightmare&utm_sourc
```

Er beinhaltet also zwei Tracking-Parameter (`&utm_source` und `&utm_medium`) von Google. Diese Parameter tun nichts anderes als bspw. Google Analytics mit Daten zu beliefern, die ein Webseitenbetreiber wiederum auswerten kann. Ein Webseitenbetreiber kann so bspw. feststellen, woher (die meisten) Zugriffe auf seine Inhalte stammen und entsprechend seiner Strategie anpassen. Aus der Sicht eines Anwenders ist das reines Tracking und unerwünscht.

Bevor ihr also unbedacht auf Links klickt, schaut sie euch zuvor genau an – egal von welcher Quelle sie stammen. Achtet darauf, dass ihr Links, die ihr mit anderen Leuten teilen wollt, keine Tracking-Parameter wie

utm_[…] (Google)
fbclid (Facebook)
[…]

enthalten. Das sind Identifier, die zur Linkverfolgung dienen und geben den Betreibern unter Umständen Auskunft darüber, wer den Link anklickt.

Das Kopieren und Einfügen von Links in Text-Dateien ermöglicht aber nicht nur die Erkennung von Tracking-Parametern, sondern auch Phishing-Links. Weitere Details zu dieser Thematik: Phishing: Das Abfischen von Zugangsdaten vermeiden

> Ich betreibe meinen eigenen E-Mail-Server. Jeder Dienst, egal ob App oder Website, bekommt eine andere Adresse von mir (MD5-Hash der Domain). Sollte auf einer der Adressen Spam auftauchen, weiß ich sofort, welche Seite die Daten verkauft hat. Wenn ich den Account lösche, kommt auch die Adresse weg, und damit auch keine Chance auf Bettel-„Komm-zurück“-Mails.

Ein guter Tipp. Den man allerdings noch etwas vereinfachen kann und nicht unbedingt einen eigenen E-Mail-Server voraussetzt. Fast jeder E-Mail-Provider unterstützt die Verwendung von Delimiter-Zeichen – also Trennzeichen, die zur Abgrenzung dienen. Angenommen ihr wollt euch bei einem Online-Shop registrieren. Üblicherweise gebt ihr dazu eure E-Mail-Adresse (bspw. `maxmustermann@gmx.de`) an. Ihr könnt aber auch mit dem Plus-Zeichen arbeiten und euch mit folgender Adresse registrieren:

```
maxmustermann+onlineshop@gmx.de
```

Der Bezeichner `onlineshop` wird mit dem +-Zeichen von eurer E-Mail-Adresse getrennt. Versendet der Online-Shop dann an die E-Mail-Adresse `maxmustermann+onlineshop@gmx.de` eine Nachricht, wird euch die E-Mail einfach an euer reguläres Postfach, also maxmustermann@gmx.de, zugestellt. Mit einem entscheidenden Unterschied: Ihr könnt nun (zumindest eingeschränkt) feststellen, ob eure E-Mail-Adresse in die falschen Hände gerät. Spammer oder andere Bösewichte machen sich meist nämlich nicht die Mühe die Delimiter zu entfernen. Wenn ihr dann von einem anderen Absender als dem Online-Shop eine E-Mail an die Adresse `maxmustermann+onlineshop@gmx.de` erhaltet, dann könnte das ein Indiz für einen Datenleak sein.

Leider gibt es hin und wieder auch Seiten, die bei der Registrierung keinen Delimiter zulassen oder diesen Teil einfach entfernen. Für diese Fälle kann man dann mit speziellen Aliases arbeiten, wie sie unter anderem mailbox.org anbietet.

> E-Mail-Anhhänge nie direkt öffnen, immer erst speichern und z.B. über VirusTotal extern überprüfen lassen.

Ich würde gar keine Anhänge von E-Mails öffnen, wenn ich keine Anhänge von irgendwem erwarte und den Absender nicht eindeutig verifizieren kann.

Der Tipp ist ein zweischneidiges Schwert. Einerseits kann es durchaus sinnvoll sein, E-Mail-Anhänge vor dem Öffnen auf Schadsoftware zu prüfen, andererseits muss man beachten, dass die Anhänge von Drittanbietern überprüft werden. Das bedeutet: Die Datei wird zur Prüfung an VirusTotal hochgeladen, um sie zu analysieren. Anhänge, die sensible Informationen beinhalten, sollte man nicht einfach irgendwo hochladen – damit ist die Datei bzw. der Inhalt quasi in **fremden** Händen. Vor der Nutzung von VirusTotal oder ähnlichen Tools solltet ihr daher zumindest die Datenschutzerklärung gelesen haben – VirusTotal gehört übrigens seit 2012 zu Google.

Abgesehen von den Datenschutzbedenken kann der Dienst durchaus sinnvoll sein. Immerhin wird die hochgeladene Datei von über 70 verschiedenen Antivirenprogrammen analysiert. Dabei gilt allerdings zu beachten: Die Erkennung ist nur dann sichergestellt, wenn die Schadsoftware bereits bekannt ist. Erkennungstechniken wie Heuristiken, Verhaltensanalysen und Co. funktionieren in der Praxis oftmals nicht zufriedenstellend. Damit geht ein Dilemma einher: Die Scanner produzieren eine Menge an False-Positive-Meldungen. Im übertragenen Sinne bedeutet das: Der Patient ist gesund, aber der Test hat ihn fälschlicherweise als krank eingestuft.

Das Ergebnis von VirusTotal und vergleichbaren Plattformen lässt Nutzer daher oftmals ratlos zurück. Ist die Datei nun infiziert oder nicht?

> Wegwerf-Adressen benutzen wie dispostable.com und Konsorten.
>
> Lasse ich mir in Firefox schon direkt beim Ausfüllen von Registrierungsformularen mit einem Mausklick anlegen: Bloody Vikings!

Oftmals möchte man bei einer Registrierung (Foren etc.) nicht seine private / eigene E-Mail-Adresse angeben. Die Gründe hierfür können unterschiedlich sein:

> kein Vertrauen in den Anbieter, dass dieser damit sorgsam umgeht
> Verschleierung gegenüber dem Anbieter
> Angst davor, unerwünschte E-Mails bzw. Spam zu erhalten
> […]

Abhilfe können Wegwerf-Adressen sein, die E-Mails für einen gewissen Zeitraum empfangen können. Ein Nutzer kann den angelegten (Foren-)Account dann über den **Verifizierungslink** freischalten, den er via E-Mail auf die Wegwerf-Adresse erhalten hat. Aus Nutzersicht sind solche Wegwerf-Adressen natürlich sinnvoll – für Betreiber

allerdings oftmals ein Ärgernis, weshalb solche Adressen oftmals nicht mehr akzeptiert werden. Mit Wegwerf- / Spam-Adressen entstehen bspw. in Foren diverse Probleme:

> Kein Passwort-Reset möglich
> Keine Benachrichtigung möglich, wenn man eine private Nachricht erhält bzw. ein Thema abonniert hat
> E-Mail-System des Forums benachrichtigt über E-Mail-Rückläufer, weil die Zustellung fehltschlägt
> […]

Als Alternative schlage ich daher eine Nutzung des Tor Browsers mit einer regulären E-Mail-Adresse bei einem Anbieter vor. Das Vorgehen ist simpel:

> Man benutzt den Tor Browser
> Registriere dir eine reguläre E-Mail-Adresse (bei einem Anbieter deiner Wahl) über das Tor-Netzwerk
> Verwende diese E-Mail-Adresse anschließend bei der Registrierung in Foren bzw. anderen registrierungspflichtigen Diensten

Sofern man sich dann konsequent über den Tor Browser in das Konto bzw. Forum einloggt, ist man gegenüber dem Betreiber praktisch »anonym« und die private / eigene E-Mail-Adresse bleibt außen vor.

---

4. Fazit

Einige Tipps waren euch sicherlich noch unbekannt bzw. eventuell war euch bisher nicht klar, weshalb es sinnvoll sein kann, diese umzusetzen. Ob ein Tipp letztendlich in eurem Kontext bzw. Umfeld umgesetzt werden kann, müsst ihr selbst entscheiden. Es ist wie so oft in der IT: Die Verbesserung der IT-Sicherheit / Datenschutz geht meist mit dem Verlust von Komfort einher.

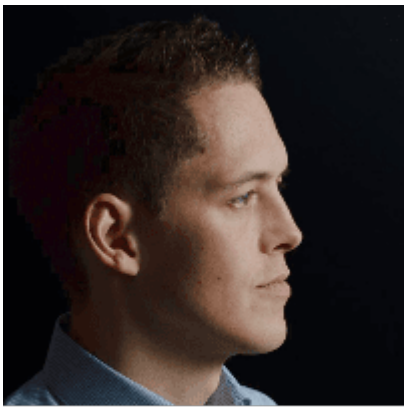
Als Ergänzung zu den hier genannten Tipps habe ich im Kuketz-Forum ein neues Thema erstellt und angepinnt, in dem ihr weitere (ungewöhnliche) Tipps nennen und

diskutieren könnt. Viel Spaß dabei!

Weitersagen | Unterstützen

Wenn dir der Beitrag gefallen hat, dann **teile** ihn mit deinen Freunden, Bekannten und Mitmenschen. Nutze dafür soziale Netzwerke, Foren, Messenger, E-Mails oder einfach die nächste Feier / Veranstaltung. Gerne darfst du meine Arbeit auch unterstützen!

Über den Autor | Kuketz



In meiner freiberuflichen Tätigkeit als Pentester / Sicherheitsforscher (Kuketz IT-Security) schlüpfe ich in die Rolle eines »Hackers« und suche Schwachstellen in IT-Systemen, Webanwendungen und Apps (Android, iOS). Des Weiteren bin ich **Lehrbeauftragter** für IT-Sicherheit an der dualen Hochschule Karlsruhe, schärfe durch Workshops und Schulungen das **Sicherheits-** und **Datenschutzbewusstsein** von Personen und bin unter anderem auch als Autor für die Computerzeitschrift c't tätig.

Der Kuketz-Blog bzw. meine Person ist regelmäßig in den Medien (heise online, Spiegel Online, Süddeutsche Zeitung etc.) vertreten.

Mehr Erfahren ➡

Unterstützung erhalten

Wenn du Fragen hast oder Hilfe suchst sind das offizielle Forum oder der Chatraum geeignete Anlaufstellen, um den Sachverhalt dort zu erörtern.

FOLGE DEM BLOG

Wenn du über aktuelle Beiträge informiert werden möchtest, hast du verschiedene Möglichkeiten, dem Blog zu folgen:

Bleib aktuell ➡

ÄHNLICHE BEITRÄGE

19. FEBRUAR 2021

Ungewöhnliche IT-Sicherheits- und Datenschutztipps – Teil1

Ungewöhnliche IT-Sicherheits- und Datenschutztipps: Von sinnvoll über skurril bis hin zu gefährlich - da ist für jeden etwas dabei.

18. SEPTEMBER 2017

Android: Viele VPN-Apps sind ein Sicherheits- und Datenschutzproblem

Die Studie »An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps« ist zwar schon etwas älter…

28. FEBRUAR 2014

Grundstein legen – Android ohne Google?! Teil2

Your phone your data - Legen wir den Grundstein für ein freies Android System

19. MÄRZ 2019

LineageOS – Take back control! Teil2

Mit einem Custom-ROM wie LineageOS koppeln wir uns von den herstellereigenen Android-Systemen bzw. Google ab.

15. MAI 2018

Umgang mit Daten im Arbeitsalltag – Datensouveränität Teil2

Wie ich in meinem Arbeitsalltag die größtmögliche Datensouveränität erreiche.

WEITERE THEMEN

Android | Audit | Autonomie | Backup | Browser | Cloud

Datenschutz Digitalpolitik E-Mail Firewall Hacking

Härten iOS Kuketz-Blog Linux macOS Messenger

OpenWrt Passwort Pentest RaspberryPi

Sicherheitslücke Sicherheitsmaßnahme Tor Tracking

Überwachung Verschlüsselung Windows WordPress

XMPP

ERGÄNZUNGEN

8 Ergänzungen zu “Ungewöhnliche IT-Sicherheits- und Datenschutztipps – Teil2”

Hace sagt:

1. März 2021 um 08:21 Uhr

Zur Telefonnummer:
Wenn man doch eine echte benötigt, können einen Anbieter wie satellite.me helfen.
Somit schützt man seine Nummern, die man für Tan-SMS oder Einmalpasswörter leider manchmal noch benötigt.

Nils sagt:

1. März 2021 um 08:39 Uhr

zu frankgehtran.de:
Wie der Betreiber der Seite schreibt, geht Frank leider nicht mehr ran. Nach einer Provider-Umstellung gibt es nicht mehr die Möglichkeit, die Anrufer nur noch eine Ansage hören zu lassen, ohne dass sie auf die Mailbox sprechen können.

Stattdessen kann aber der Telefonpaul verwendet werden.
Ausprobiert habe ich aber beides noch nie ;-)

Alexander sagt:

1. März 2021 um 09:24 Uhr

Zu Virustotal noch ein Tipp:

Man kann auch nach einem Hash suchen: https://www.virustotal.com/gui/home/search
Also Hash der Datei am Computer erstellen und hochladen…falls man Treffer hat, dann ist es schon sehr wahrscheinlich, daß etwas faul ist und man muss nicht die Datei hochladen.

Unter Windows im DOS-Fenster mit dem Befehl (was oft unbekannt ist):
certutil -hashfile

Justin sagt:

1. März 2021 um 13:44 Uhr

(mMn) WICHTG:
Bei virustotal – *insb.* bei angeblichem Virenbefall immer auch mal einen Blick in die Community-Bewertung (links oben) werfen.
Jüngstes Beispiel bei mir: CheatEngine 7.2, die sogar OpenSource ist, wurde von VT hoch negativ bewertet, von der Community aber entwarnt.

VT rapportiert Konzernmeinungen (nichts Anderes sind AV-Vendors) mit Blick auf Unternehmenskunden – und in ein Unternehmensumfeld gehört viele Software tatsächlich nicht. Das sagt aber wenig über ihre tatsächliche ‚Gefährlichkeit' aus.

Anonymous sagt:

1. März 2021 um 09:45 Uhr

Um das Linkziel zu sehen reicht es eigentlich aus, mit der Maus über Link zu fahren (ohne anklicken). Dann wird das Ziel normalerweise unten links angezeigt. GMX & Web.de sind da leider nicht hilfreich, da man den Orginallink kaum noch erkennen kann. (nebenbei: man kann Skip Redirect nutzen, um den Dereferer zu überspringen).

Für das Entfernen von Trackingparameter aus der URL gibt es für Firefox auch eine Erweiterung: ClearURLs.

Robert sagt:

1. März 2021 um 12:15 Uhr

Niemals das Ausloggen (Beenden von Online-Diensten) vergessen! In der täglichen Praxis erlebe ich es immer wieder: Selbst wenn bestimmte Dienste gerade nicht benötigt werden (FB/Google/Microsoft/Dropbox etc. etc.) surfen eine ganze Menge von Leuten ganz selbstverständlich normal weiter im Internet, während sie noch in diversen Diensten eingeloggt sind. Sie erhöhen damit nicht nur die potentielle Angriffsfläche sondern ermöglichen mit ihrem Verhalten auch ein viel detailiertes Tracking ihrer Online-Aktivitäten, sind sich dessen aber nie bewusst. Zum Teil verständlich, weil das natürlich unsichtbar passiert.
Hier gibt es dafür einen kostenlosen Service, der automatisch viele Dienste überprüfen kann: https://superlogout.com/ Keine Ahnung ob man dem trauen kann, aber die Idee ist natürlich sinnvoll!
Außerdem sollte man regelmäßig, also von Zeit zu Zeit, überprüfen ob man alle seine Online-Dienste wirklich noch benötigt oder ob man nicht den einen oder anderen Dienst aussortieren, abmelden, kündigen und schließen kann. Auch dafür gibt es zum Glück einige kostenlose Seiten:
1. https://justdeleteme.xyz/
2. https://www.accountkiller.com/
3. https://unroll.me/
Bei Unroll muss man angeben nicht in der EU zu wohnen, dann läufts.

Peterson sagt:

4. März 2021 um 12:03 Uhr

Eine Alternative für VirusTotal könnte

https://virusscan.jotti.org/
sein, der Dienst besteht schon sehr lange, hat bei mir immer gut funktioniert. Man bekommt als Ergebniss die einzelnen Bewertungen der verschiedenen Virenscanner aufgelistet.

C. sagt:

27. März 2021 um 09:48 Uhr

Tracking-Links werden bei FairEmail beim Anklicken zunächst im Klartext dargestellt und danach alle Tracker entfernt.
Ein weiteres Plus für dieses excellente Programm (FOSS).

Ergänzungen sind geschlossen / Aktualität

Dieser Beitrag ist älter als vier Wochen. **Hinweis**: Die Blog-Beiträge haben nicht wie Enzyklopädie-Einträge (bspw. Wikipedia) den Anspruch, dauerhaft aktuell und richtig zu sein, sondern beziehen sich wie Zeitungsartikel auf den Informationsstand zum Redaktionsschluss.

Wenn du Fragen hast oder Hilfe suchst sind das offizielle Forum oder der Chatraum geeignete Anlaufstellen, um den Sachverhalt dort zu erörtern. Kritik, Anregungen oder Korrekturvorschläge zum Beitrag nehme ich gerne per E-Mail entgegen.

Kuketz-Forum

Artikel (293)

Datenschutz (161) Sicherheitsmaßnahme (83)

NACH OBEN ⬆

SITEMAP IMPRESSUM DATENSCHUTZHINWEIS