Empfehlungen

- Overprovisioning-Deletion
- Passwort-Manager
- Messenger
- Graphene-Os

Overprovisioning-Deletion

Unter Besonderheiten in der Datenhygiene habt ihr schon gesehen, dass zum sicheren Löschen von Daten auf SSD's auch die Reserveblöcke gelöscht werden müssen, die aber für herkömmliche Software nicht zu erreichen sind.
Die meisten Hersteller liefern verschiedene Tools aus, mit denen das umgesetzt werden kann. Hier sind die gängigsten aufgelistet. Falls ihr Ergänzungen habt, schreibt uns gerne!

- Samsung
- Kingston
- Seagate
- Sk hynix
- Western Digital
- Crucial
- Sabrent
- Adata

Passwort-Manager

Info

Der Passwortmanager ist das essenzielle Tool, um den nötigen Sicherheitsvorkehrungen bezüglich sicherer Passwörter gerecht zu werden. Hier kannst du dir anschauen, was gute Passwörter sind und wie wir damit umgehen sollten: Gegenmaßname Passwörter

KeePassXC und Bitwarden sind beide Open-Source und haben Anwendungen für alle üblichen Betriebssysteme / Browser.

KeePassXC funktioniert Offline, Bitwarden online. Aber auch KeePassXC lässt sich mittels externer Dienste über mehrere Geräte synchronisieren.

Praktikable Passwortmanager für PCs:

- KeePassXC: Linux, Windows, MacOS
- Bitwarden: Linux, Windows, MacOS

KeePass für Mobilgeräte

Empfehlung aus KeePassXC docs für Handys:

- Android: keepassDX, Keepass2Android
- iOS: Strongbox, KeePassium

Die in Browser und Betriebssysteme integrierten Passwortmanager sind nicht unbedingt zu empfehlen, da diese oftmals proprietär und überwiegend auf Komfort ausgelegt sind. Das führt regelmäßig zu Sicherheitslücken. Besonders Browser sind stets im Fokus von Angreifer*innen und bieten viele Angriffsvektoren.

KeePassXC

KeePassXC ist einer der bekanntesten und verbreitetsten Passwortmanager. Er ist Open-Source, wird regelmäßig durch Expert*innen auf Schwachstellen untersucht und bietet eine Vielzahl von sehr praktischen Features. Diese ermöglichen es uns die Lücke zwischen Sicherheit und Komfort zu schließen.

Browserintegration

Es gibt für alle gängigen Browser *(außer Safari*) eigene Plugins für KeePassXC, um die auto-fill Funktion komfortabel nutzen zu können. Damit werden auf jeder Webseite, für die Passwörter gespeichert wurden, automatisch die richtigen Login-Daten vorgeschlagen.

Das verhindert, dass Du, wenn du auf einen Phishing-Link klickst, aus Versehen dein Passwort eingibst, weil das Plugin merkt, dass Du auf einer falschen URL gelandet bist.

Schlüsseldatei

Es empfiehlt sich eine Passwortdatenbank sowohl mit Passwort, als auch mit einem zweiten Faktor abzusichern. Die einfachste Methode dafür ist die Schlüsseldatei *(eng:Key-File). (Weiter unten gibt es ein Beispiel Szenario.)*

Im folgenden sind verschiedene Methoden aufgelistet, wie die Schlüsseldatei als zweiter Faktor genutzt werden kann.

Schlüsseldatei als 2. Faktor

Es gibt die Möglichkeit, die Datenbank neben dem Passwort zusätzlich noch mit einer separaten Schlüsseldatei zu verschlüsseln. Das heißt man braucht dann, um an die Passwörter zu kommen, immer sowohl das Passwort, als auch die Schlüsseldatei.

Eine Anleitung dazu findest du hier.

Schlüsseldatei als Hauptschlüssel

Du kannst deine Passwortdatenbank auch nur mit einer Schlüsseldatei verschlüsseln, ohne Passwort. Dann musst du beim öffnen der Datenbank in KeePassXC immer die Schlüsseldatei auswählen.

Schlüsseldatei als Hauptschlüssel mit 2. Faktor Passwort

Ein häufiger Anwendungsfall dafür ist das Speichern der Schlüsseldatei auf einem verschlüsselten USB-Stick, den zB an deinem Schlüsselbund, immer mit sich geführt wird.

Auch damit ist eine 2-Faktor-Authentifizierung gewehrleistet. Es wird:

1. Faktor: das Passwort für den Stick
2. Faktor: der Stick (mit der Schlüsseldatei)

benötigt, um an die Passwörter zu kommen. Dabei muss unbedingt drauf geachtet werden, das es einen Backup-USB-Stick gibt, falls der eigentliche Stick mal verloren geht!

Neue Passwörter generieren

Eines der Kernfeatures eines Passwortmanagers ist, dass die starke Passwörter oder Passphrasen nach euren eigenen Vorgaben generieren können. Damit ist sichergestellt, dass ihr nicht doch aus Bequemlichkeit immer das gleiche Passwort wiederverwendet.

Passwörter in der Cloud synchronisieren und backupen

Ist das nicht gefährlich?

Die Passwortdatenbank ist immer, zu jeder Zeit verschlüsselt. Sie wird zu keiner Zeit in der Cloud entschlüsselt, sodass die Cloud-Betreiber etwas daraus lesen könnten.

Allerdings könnte die Polizei eventuell eine Kopie deiner Datenbank klauen wie im folgenden Beispiel Szenario beschrieben.

Beispiel-Szenario

Nehmen wir an, deine Passwortdatenbank ist "nur" mit einem (starken) Passwort geschützt. Hat nun die Polizei Zugriff auf deine Cloud (oder kommt anderweitig an deine Datenbank), hat sie nur die verschlüsselte Datei erbeutet und kann damit erst mal nichts anfangen. Sollten sie aber in Zukunft dein Passwort auf irgendeine Art erfahren (sie beobachten Dich zB heimlich, wie du es eintippst), dann können sie die verschlüsselte Datenbank wieder rausholen und jetzt entschlüsseln.

Wäre die Datenbank zusätzlich mit einer Schlüsseldatei verschlüsselt, reicht es nicht aus, nur das Passwort zu kennen, sondern es braucht auch die Schlüsseldatei. Würdest du diese Schlüsseldatei nun zerstören, gäbe es keinerlei Möglichkeit mehr, die geklaute Datenbank jemals zu entschlüsseln.

How To

Du könntest zum Beispiel deine Datenbank seelenruhig in der Cloud lagern und somit auch gleichzeitig mit all deinen Geräten darauf zugreifen.

Die Schlüsseldatei hast du jeweils **nur lokal** auf deinen Geräten gespeichert.

Falls du jetzt einmal den Verdacht bekommen solltest, dass die Behörden eine Kopie deiner Passwortdatenbank bekommen haben

1. machst Du eine Kopie deiner Datenbank
2. erstellst dafür sowohl ein neues Passwort,
3. als auch eine neue Schlüsseldatei
4. und kannst danach die **alte Schlüsseldatei** auf alle deinen Geräten löschen.

Damit ist die kompromittierte Datenbank für immer nutzlos.

Achtung
Bevor du deine alte Schlüsseldatei löschst, stelle sicher: 1. dass die neue Datenbank mit der neuen Schlüsseldatei funktioniert 2. Du das neue Passwort nicht direkt vergisst!

In beiden Fällen wären all deine Passwörter unwiederbringlich weg.

KeePassXC als 2-Faktor-App

KeePassXC kann auch als 2FA-App mit TOTP genutzt werden. Das funktioniert sogar auf den Apps für Handy.

Anleitung

Hier findet sich eine Anleitung mit weiteren Verweisen.

Hinweis

Wir schreiben hier konsistent von KeePassXC.

Ältere Versionen wieKeePassX und KeePass sollten nicht mehr benutzt werden.

Messenger

Um verschlüsselt zu kommunizieren, eignen sich neben verschlüsselten Mails einige Messenger. Vorteilhaft gegenüber Mails sind (gute) Messenger, weil bei ihnen Verschlüsselung und sichere Kommunikation von vornherein mit gedacht wurden. Dafür sind sie, vor allem die besseren, aber weniger verbreitet.

Kriterien, was einen guten Messenger auszeichnet, finden sich z.B. bei Digitalcourage. Für Aktivist*innen ist (je nach Threat Model) vor allem eine möglichst sichere, Daten-sparsame und anonyme Kommunikation wichtig.

Hierfür soll auf zwei in Aktivismuskreisen recht weit verbreitete Messenger, die mit Einschränkungen zu empfehlen sind, eingegangen werden: Signal und Matrix.

Signal

Signal wurde von dem Anarchisten Moxie Marlinspike entwickelt und ist eine der bekanntesten Alternativen zum Monopolisten WhatsApp.

Vorteile von Signal

- **Einfache Nutzung**: Signal ist simpel zu installieren und "funktioniert einfach". Mensch kann nicht viel falsch machen, was die Sicherheit gefährden würde.
- **Weite Verbreitung**: 2022 hatte Signal 40 Millionen aktive Nutzer*innen. Damit liegt es zwar noch immer weit hinter den 2 Milliarden Nutzer*innen von WhatsApp, ist aber dennoch weit verbreitet.
- **Sichere Verschlüsselung**: Signal hat ein eigens Kommunikationsprotokoll, das quell-offen ist und regelmäßig geprüft wird. Einige andere Messenger, wie WhatsApp haben das Protokoll ebenfalls übernommen, sodass sich das Protokoll durch die Nutzung von Milliarden von Menschen bewährt. Die Kommunikation in Signal ist demnach sicher Ende-zu-Ende-verschlüsselt.
- **Daten-Sparsamkeit**: Signal speichert möglichst wenig über die Nutzer*innen und kann demnach auch nur wenige Informationen preisgeben. Die einzigen Daten, die Signal in vergangenen Gerichtsprozessen raus *konnte*, waren das Erstellungsdatum des Accounts und das Datum, als der Account zuletzt genutzt wurde.

- **Möglichkeit der automatischen Löschung**: Chats können so eingestellt werden, dass sich die Nachrichten automatisch nach einer bestimmten Zeit löschen. So sind sie selbst dann sicher, wenn Cops (nach dieser Zeit) Zugriff auf das Gerät erhalten.

Nachteile von Signal

- **Anonymität**: Signal wurde nicht entwickelt um anonym zu sein, sondern um sichere Verschlüsselung anzubieten. Stand heute (Januar 2024) ist eine Telefonnummer notwendig, um sich zu registrieren; diese muss (rein rechtlich) auf eine real existierende Person registriert sein. Die Telefonnummer ist sichtbar für alle, mit denen mensch kommuniziert. Die konkrete Gefahr ist hier, dass entweder ein Cop in einem sensiblen Chat ist und mensch so identifiziert wird, oder dass ein Handy mit Zugriff auf sensible Chats konfisziert wird.
- **Sitz in den USA**: Die Signal Foundation hat ihren Sitz in den USA und kann demnach gezwungen werden, Daten an Geheimdienste weiter zu geben.
- **Zentralität**: Signal läuft nur über die eigene Infrastruktur (die bei Amazon, Microsoft, Google und Cloudflare liegt) und lässt sich nicht selber hosten. Somit muss mensch Signal ein Stück weit vertrauen, dass sie ihren Job gut machen. Außerdem gibt es somit eine zentrale Stelle, die angegriffen werden kann.

Signal Gruppen

Signal Gruppen werden gerne und häufig genutzt um sich in größeren Gruppen *(bis zu ~150 Kontakten)* auszutauschen. Generell bieten Signal-Chats automatisches Löschen von Nachrichten nach einem eingestellten Zeitraum X ein, was auch dringend für Gruppen eingestellt werden sollte, die einem gewissen Gefahrenpotential unterliegen.

Leider gibt es noch keine Funktion, die ganze Gruppen automatisch nach Zeitraum X löscht. Daher muss besonders bei Beschlagnahmung von Geräten überlegt werden, welche Kontakte zusammen in welchen Gruppen *(bzw. welchen Gruppennamen!)* in Zusammenhang stehen und eventuell ebenfalls kompromittiert wären.

Daher empfehlen wir *(Für alle Gruppenchats, nicht nur auf Signal)*: Unter dem Prinzip der *plausible deniability* sämtlichen Gruppen möglichst unscheinbare Namen geben, die nicht gegen euch verwendet werden können! Es hilft leider nichts, die Gruppennamen im Nachhinein zu ändern, weil diese im Chat angezeigt wird, zB: "*Du hast den Gruppennamen von* '*Randale*' *auf* '*Spaziergang*' *geändert*". Am besten erstellt ihr also die Gruppen neu, wenn die Namen ein Problem sein könnten.

Matrix

Matrix ist ein Kommunikationsprotokoll (ähnlich wie Mail, bzw. genauer so was wie IMAP, eines ist).

Für dieses Protokoll gibt es diverse Clients, der bekannteste ist Element. Vor allem in letzter Zeit findet Matrix mehr Verbreitung in Aktivismus- und Hackerkreisen.

Funktionsweise

Der wichtigste Unterschied von Matrix im Vergleich zu anderen Messengern, wie z.B. Signal, ist die Dezentralität, bzw. *Föderation*. Ähnlich wie bei Mails gibt es viele verschiedene Server ("*Homeserver*") (wie z.B. *matrix.org* oder *matrix.systemli.org*). Kommuniziert ein Aktivisti mit einem Matrix-Account bei matrix.org mit einem Aktivisti mit einem Matrix-Account bei matrix.systemli.org, so müssen die (verschlüsselten) Nachrichten zwischen den beiden Servern synchronisiert werden.

Matrix Föderation Funktionsweise

Vorteile von Matrix

- **Sichere Verschlüsselung**: Matrix nutzt eine eigene Implementation des Signal-Protokolls. Es hat Nachteile im Vergleich zum Signal-Protokoll, ist aber dennoch ähnlich sicher.
- **Dezentralität**: Matrix ist föderiert und damit dezentral. Es gibt viele verschiedene Server, die miteinander kommunizieren; somit gibt es viele Stellen, die angegriffen werden müssten, um ganz Matrix lahm zu legen.
- **Anonymität**: Bei einigen Servern werden keine persönlichen Informationen zur Erstellung eines Accounts benötigt. Somit ist es prinzipiell möglich, Matrix anonym zu nutzen.
- **Offenheit**: Der Quelltext von Matrix, sowie von Element ist quelloffen und kann (und wird) regelmäßig überprüft.

Nachteile von Matrix

- **Komplizierte Nutzung**: Zuweilen ist es kompliziert, Matrix zu nutzen. Das Prinzip der Föderiertheit ist unintuitiv, es gibt viele sehr verschiedene Clients und vieles funktioniert nicht einfach.
- **Noch nicht weit verbreitet**: Menschen müssen häufig erst mal dazu überredet werden, sich einen Matrix-Account einzurichten.
- **Mangelnde Daten-Sparsamkeit**: Weil Matrix föderiert ist, müssen alle Daten auf allen föderierten Servern synchronisiert werden. Das bedeutet auch, dass es praktisch unmöglich ist, Daten wieder zu löschen. Auf allen Servern werden standardmäßig für immer die Matrix ID persönliche Informationen, Nutzungsdaten, IP-Adressen, Geräteinformationen, andere Server mit denen kommuniziert wird und Raum-IDs

gespeichert. (Die Quelle bezieht sich auf eine ältere Matrix-Version. Inwiefern die standardmäßig gespeicherte Datenmenge und das Löschverhalten auf aktuelle Versionen übertragbar sind, ist unklar.)

Resümee

Für den aktivistischen Alltag, in dem mensch nicht anonym sein möchte, eignet sich Signal sehr gut. Insbesondere im Vergleich zu kommerziellen Alternativen ist es Privatsphäre-freundlich und sicher. Sollte aber doch mal Anonymität (und gleichzeitig eine sichere Verschlüsselung) in der digitalen Kommunikation wichtig sein, eignet sich Matrix besser. Hier sollte dann aber darauf geachtet werden, dass keine persönlichen Informationen (wie die IP-Adresse) preis gegeben werden, da diese auf den Servern liegen bleiben.

Graphene-Os

GrapheneOS ist ein mobiles Betriebssystem, welches auf Android basiert. Häufig wird es empfohlen, da es eine Alternative zu vorinstallierten (OEM) Betriebssystemen darstellt, welche gänzlich ohne Google-Services genutzt werden kann. Neben diesem Merkmal, welches die Privatsphäre von Nutzer*innen schützt, bietet GrapheneOS in Kombination mit unterstützten Geräten hochmoderne Sicherheitsfeatures, wegen derer wir die Nutzung an dieser Stelle stark empfehlen.

Einstellungs Empfehlungen

Datenschutz & Sicherheit

Exploit protection

- auto reboot: so niedrig wie möglich, aber für die Anwendenden noch komfortabel! (nach Reboot kommen ohne erstmaliges Entsperren z.B keine Signalnachrichten/anrufe mehr an)
- USB - C Port: hier sollte mindestens "Charging only" gewählt werden. "Charging only when locked" ist nochmal eine Stufe strenger (potentiell besser), führt aber dazu, dass das Handy nicht mehr geladen werden kann, wenn es gleichzeitig benutzt werden muss.
  - Hier könnte es sich empfehlen standardmäßgig "Charging only when locked" auszuwählen und im Zweifel direkt zu wissen, wie die Einstellung auf "Charging only" geändert werden kann, wenn dies nötig ist.
- WiFi & Bluetooth automatisch ausschalten: Hier sollte bei Beiden eine noch komfortable Zeitspanne gewählt werden.
- Geräteentsperrung

Geräteentsperrung

- Duress Passwort: Dieses Passwort sorgt dafür, dass wenn es eingegeben wird, das Handy komplett auf Werkseinstellungen zurückgesetzt wird. Das ist sehr praktisch, solltet ihr einmal gegängelt/gezwungen o.ä. werden euer Handy zu entsperren. Das funktioniert übrigens auch, falls ein Angreifer versucht euer Passwort per Brute-Force zu erraten. Voraussetzung ist natürlich, dass auf dem Gerät keine lebensnotwendigen Daten sind, von denen ihr keine Backups habt. Wählt für das Duress Passwort also am besten eins:
  - an das ihr euch im Zweifel sofort erinnert!

    - das die Polizei z.B erraten würde
    - oder: eins, dass ihr für euer richtiges Passwort niemals wählen würdet.

WiFi

Für sämtliche WiFis, über die nicht ihr selber die volle Kontrolle habt:

- In die Einstellung der jeweiligen Verbindung (Zahnrad bei WiFi-Name): nicht persistente MAC-Adress-Generierung für diese Verbindung aktivieren.

2FA für Fingerprint

Seit kurzer Zeit gibt es die Möglichkeit einen zweiten Faktor für die Entsperrung per Fingerprint zu nutzen. Das bringt einen enormen Fortschritt im Spannungsfeld zwischen Usability und Security mit sich!

Wo war bisher das Problem?

Im Normalfall ist es ja so, dass biometrische Entsperrmethoden mit äußerster Vorsicht zu genießen sind, aus dem einfachen Grund, dass sie von euch erzwingbar sind. Die Polizei kann im Zweifel euren Finger mit Gewalt auf euer Handy legen und es entsperren.

Das heißt bisher ging die Nutzung der biometrischen Entsperrung immer einher mit der Gefahr überrumpelt und zum Entsperren gezwungen zu werden, bevor das Handy ausgeschaltet werden kann.

Wie schaut die Lösung aus?

Die 2FA Option bietet die Möglichkeit einen mindestens 4-stelligen (empfohlen werden 6Stellen) Zahlen PIN einzurichten, der jedes mal nach dem Fingerprint zusätzlich einzutippen ist, um das Handy zu entsperren.

Dann muss zwar trotzdem noch etwas getippt werden, aber einen z.B 6-stelligen PIN auf dem großen Zahlen-Pad ist viel einfacher und schneller getippt, als eine 7 Wörter lange Passphrase auf der kleinen Tastatur. Außerdem lässt sich der PIN viel entspannter ändern (wenn es sein muss), da man keine große Sorge davor haben muss, jetzt ein neues langes Passwort lernen zu müssen.

Das bedeutet das Handy kann mit einem sehr starken Passwort verschlüsselt werden, ohne dass man nun dieses elendig lange Passwort etliche Male am Tag eintippen muss.

Kann der PIN nicht gebrute-forced werden?

Nur sehr eingeschränkt:

- Die gesamte Fingerprint-Methode ist nur 48h nach der letzten Eingabe des primären (langen) Passworts.

- Es sind maximal 4 * 5 Fehlversuche erlaubt. Zwischen jedem 5. Fehlversuch gibt es eine 30 sekündige Auszeit. Es gibt also maximal 20 Fehlversuche. [1]

PIN Scrambling

PIN scrambling ist ziemlich nerdig, hat aber durchaus seine Anwendungsfälle:

Anstatt dass die Ziffern immer in numerischer Reihenfolge auf dem Bildschirm angezeigt werden, werden die Ziffern bei der PIN-Eingabe an zufälligen Stellen auf dem Bildschirm angezeigt. Wenn euch also ein Angreifer aus kleiner Entfernung dabei beobachtet hat, wie ihr euren PIN eingegeben habt, in der er nur z.B. die Richtung des Daumens auf dem Bildschirm erkennen konnte, ist der PIN für ihn nicht rekonstruierbar.

PIN scrambling ist auch für die 2FA beim Fingerprint verfügbar.