Dein persönlicher Sicherheitsplan

Hier findest du:

- Einen Leitfaden wie du deine digitale Sicherheit ausbauen kannst.
- Ganz konkrete Tipps zu einem möglichen Vorgehen und empfohlene Programme.

Verschaffe dir einen Überblick

„Ich habe auf einer Busfahrt angefangen, die Einstellungen in meinem Smartphone durchzuschauen. Anscheinend war mein Smartphone bereits standardmäßig verschlüsselt - ein Todo konnte ich also schon abhaken. Ich hab mal ein Software-Update gemacht (war anscheinend veraltet), mir dann die Berechtigungen der Apps durchgeschaut (google-maps hatte mein Bewegungsprofil der letzten 3 Jahre gespeichert!), und überlegt von welchen Apps ich mich verabschieden kann. Das war mein Anfang..“

Im Alltag verwenden wir eine Vielzahl an Informationstechnologien und jede Person muss für sich überlegen, welche Schritte Sinn ergeben, um sich zu schützen. Wir möchten dich dabei unterstützen, deinen eigenen kleinen Selbstverteidigungsplan zu Gestalten. Wir geben dir ein paar Fragen mit für eine Bestandsaufnahme deiner Anforderungen und haben dann zwei Empfehlungen für dich für eine Mindeststandard-Sicherheit und die Erweiterte Sicherheit. Du bist eingeladen, die Empfehlungen an deine Situation und Bedürfnisse anzupassen und deinen eigenen Sicherheitsplan aufzustellen.

Für die Erstellung deines persönlichen Sicherheitsplanes beginnst du damit, mal eine Bestandsaufnahme zu machen.

Geräte

- Was für Geräte (PC, Laptop, Tablet, Smartphone,..) benutzt du?
- Welche Geräte, die du früher benutzt hast oder kaputt sind, liegen denn noch bei dir herum?
- Welche Speichermedien (CDs, USB-Sticks, Festplatten, Foto-Speicherkarten,...) verwendest du?
- Welche Speichermedien liegen noch mit altem Stuff in deinen Schubladen rum?

Webnutzung

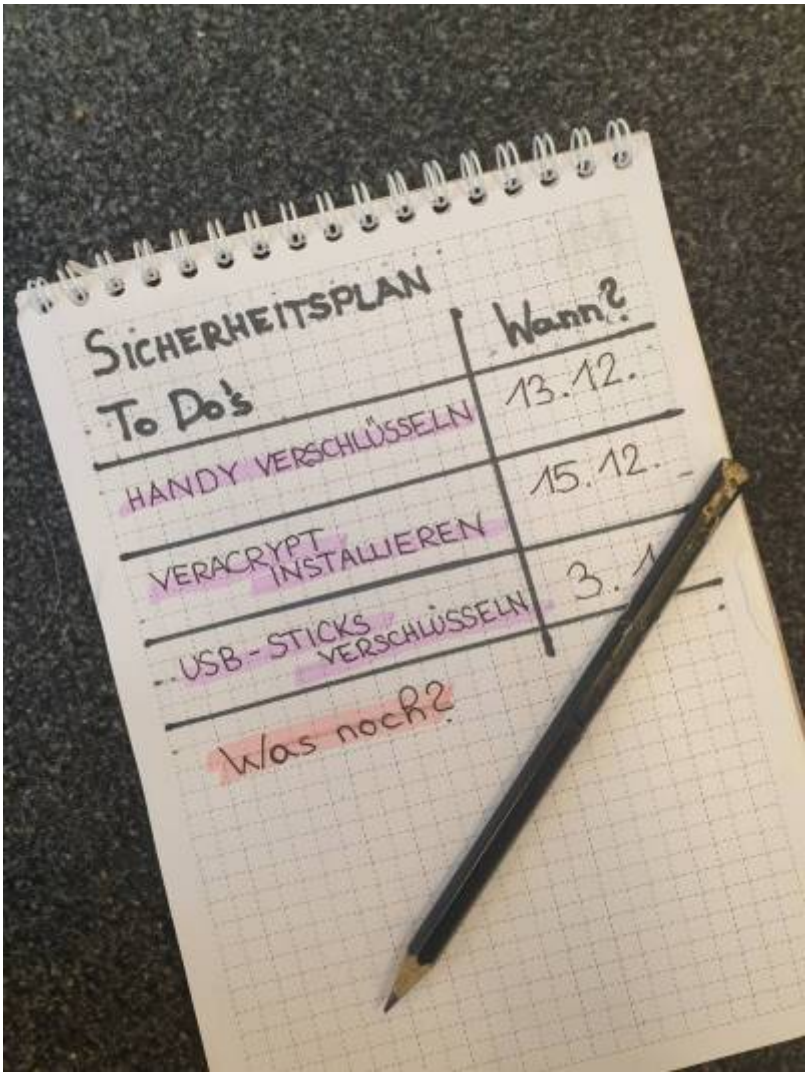
- Mit welchen Programmen surfst du im Web?
- Welche Apps verwendest du um Inhalte aus dem Web zu sehen (Twitter, Facebook, Insta, ...)?
- Welche Apps und Programme hast du installierst, aber verwendest du nicht mehr?

Kommunikation

- Mit welchen Messenger-Programmen kommunizierst du?
- Welche (Video-)Telefonieprogrammen nutzt du?
- Über welche Inhalte schreibst du in den Messengern?
- Besprichst du sensible Informationen am Telefon?
- Benutzt du eine Cloud und File-Sharing-Dienste?

Leg dir einen Plan zurecht

Es ist völlig ok, wenn du dich nach dem Durchkämpfen durch die Bestandsaufnahme überfordert fühlst. Wir alle haben uns Schritt für Schritt an die ganze Thematik herangetasten. Das wichtigste, um einen selbstbestimmten Umgang mit deinen Daten zu erlangen, ist, dass du irgendwo anfängst. Such dir am besten das aus, was für dich am greifbarsten klingt und klick dich dann durch die Anleitungen durch.



Womit du anfangst, ist natürlich ganz dir überlassen. Zum Beispiel kann das ein Wechsel der Suchmaschine oder der Abschied von WhatsApp sein. Wir haben Tipps für eine Basis Sicherheit ausgearbeitet, an denen du dich orientieren kannst.

Step-by-Step: Lass dich nicht überfordern von den vielen Aufgaben und nimm dir nicht alles auf einmal vor! All diese Dinge brauchen Zeit.

Das Handy, den Computer und alle Festplatten zu verschlüsseln und auch noch ein gutes Konzept für deine Passwörter anzugehen, wird sich nicht alles an einem Wochenende ausgehen. Lass dich davon nicht entmutigen, sondern beginn mal damit, dir einen Plan zu machen und arbeite die Dinge, die du erledigen möchtest, anhand einer TODO-Liste Schritt für Schritt ab.

Tipps für die Basis Sicherheit

Wir schlagen dir für alltägliche Nutzung ein paar Programme und Verhaltensweisen vor. Die Links führen dich zu Anleitungen und Erklärungen.

o Passwortsicherheit
Ein der größten Sicherheitslücken sind unsichere, veraltete und schlecht verwaltete Passworte. Erstelle also gute Passworter und verwende für jedes Login ein eigenes. Damit du dabei nicht durcheinanderkommst gibt es Passwort-manager (zB KeePassXC). Im Passwortmanager kannst du dir auch sichere passwörter erstellen.Wir haben dir hier im Wiki einiges dazu aufgeschrieben, wie du sichere Passworte erstellen kannst, wie du dir die Passworte merkst und wie du sie verwalten kannst.

o Verschlüssle deine Geräte und Datenspeicher
Um andere den Zugriff auf deine Daten zu verwehren, hilft nur eine Verschlüsselung.

o Datensicherung
Sicherungen von deinen Daten machen immer Sinn – Auch hier auf die Verschlüsselung achten. Backup/Datensicherung wirkt oft überfordernder als es ist. Oft reicht ein einfaches kopieren der wichtigsten Daten auf eine externe (verschlüsselte) Festplatte. Tipps dazu findest du auch hier im Wiki

o Verwende als Internetbrowser Firefox mit Addons
Der Browser ist deine Tür ins Internet und sollte vertrauenswürdig und sicher sein! Firefox sammelt weniger Daten als andere Browser und sein Quellcode ist offen einsehbar, was ihn auch überprüfbar macht. Installiere dazu noch Privacy Erweiterungen wie ublock origin, https everywhere und privacy badger. Im Wiki gibt es einen eigenen Artikel zur Verwendung von Firefox.

o Anonymität im Netz über Tor
Falls du dich noch mal ganz anonym im Internet bewegen willst, verwende den Tor-Browser. Er ist auf allen Plattformen installierbar.

o Social Media Sicherheit
Mache dich mit den Sicherheits- und Datenschutzeinstellungen der Socialmedia-Plattformen vertraut und achte darauf, was du postest.

o Entferne Metadaten und verpixle Gesichter
Fotos und Dokumente: Wenn du Dinge veröffentlichst, entfernt die Metadaten und verpixel Gesichter!

o Datenvermeidung
Oft ist es nicht sinnvoll, alles zu speichern. Auch gehören manche Inhalte nur über die richtigen Kanäle kommuniziert. Die meisten Daten müssen nicht für immer aufbewahrt werden. Lösche also regelmäßig Daten. Bei vielen Programmen, wie zB Signal, kannst du dies einfach einstellen.

o Nutze (so weit möglich) Alternativen zu Google, Microsoft,…
Oft gibt es gute Freie Software Alternativen zu Anwendungen der großen Anbieter wie Google und Microsoft. So ist leichter überprüfbar, was die Programme tatsächlich machen. Als Betriebssystem gibt es unterschiedliche Linux-Distributionen und zu fast allen (leider nicht ganz allen) Programmen gibt es gute Alternativen.

o Updates & Systemsicherheit
Mache regelmäßig Updates! Sowohl das Betriebssystem als auch die Programme müssen stetig upgedated werden. Achte außerdem darauf, dass du auch wirklich nur die Programem installiert hast,

die du auch wirklich brauchst.

Tipps zur Smartphone Sicherheit

o Verschlüssle dein Smartphone
Für den Fall, dass du dein Telefon verlierst oder es in die falschen Hände gerät: Es muss nicht sein, dass wer deine Daten lesen kann.

o Updates & Systemsicherheit
Mache regelmäßig Updates. Sowohl das Betriebssystem, als auch die Apps müssen stetig upgedated werden. Achte außerdem dass du auch wirklich nur die Apps/Programme installiert hast, die du auch wirklich brauchst.

o Einstellungen
Schau dir die Einstellungen deines Smartphones mal genauer an und entziehe nicht notwendige Berechtigungen!

Tipps zu sicheren Kommunikation

o Email
Verschlüssel deine Email Kommunikation. Dies kannst du zB über Thunderbird machen.

o Signal-Messenger
Nutze Signal für deine Kommunikation am Smartphone. Mit Signal kannst du deine Nachrichten leicht Ende-zu-Ende verschlüsseln. Falls andere Personen kein Signal haben, kannst du mit der Signal-App auch normale (unverschlüsselte!) SMS versenden, was die App sehr angenehm für den alltäglichen Gebrauch macht.

o Anrufe
Telefoniere wenn möglich auf deinem Smartphone immer verschlüsselt, zB mit Signal.

o Jitsi-meet
Jitsi-Meet ist ein Service für Sprach- und Videokonferenzen im Browser, wobei ein Server zB von Systemli gehostet wird. Für Android gibt es eine eigene App. Die Verbindung zwischen App und Server ist verschlüsselt. Die Version aus dem Google Play Store enthält einige Tracker, installiere die App also am besten über F-Droid. Jitsi-meet funkioniert für große Gruppen leider manchmal nicht so gut.

o Mumble
Mumble ist eine freie Sprachkonferenzsoftware. Mumble läuft auch bei schlechter Internet-Verbindung flüssig und stabil und schafft problemlos Telefonkoferenzen mit zehn und sogar 100 Personen. Der Datenverkehr zwischen App und Server ist vollständig verschlüsselt und damit auch deine Gespräche. Der Verkehr ist jedoch nicht Ende-zu-Ende-verschlüsselt. Nutze daher einen vertrauenswürdigen Server wie z.B. den von Systemli oder setze deinen eigenen Mumble-Server auf. Für das Smartphone gibt es hier zB die App Plumble.

Tails: Ein sicheres Betriebssystem To-Go
Installiere Tails auf einem USB-Stick, damit hast du ein portables, anonymes, amnestisches Betriebssytem, welches du auf jedem Computer nutzen kannst. Tails ist ein speziell auf Sicherheit und

Anonymität fokussiertes Betriebssystem, das bereits viele Programme und Lösungen mitbringt: Anonym Emails abrufen, anonym surfen, Verschlüsselung,...

Dran bleiben!

Technische Möglichkeiten verändern sich laufend, daher reicht es nicht aus, einmal die Festplatte zu verschlüsseln oder einen sicheren Messenger zu installieren, denn was heute als sicher gilt, kann in naher Zukunft schon wieder unsicher sein. Es ist wichtg, Software, die du verwendest, durch refeglmäßige Updates auf dem Laufenden zu halten. So werden zb allfällig enstandene Sicherheitslücken in den Systemen geschlossen. Wir finden es daher wichtig, dass wir uns kontinuierlich mit digitaler Sicherheit auseinandersetzen!

Bleib dran: Informiere dich aktiv und laufend über neue digitale Sicherheitsstandards- und entwicklungen!

- Updates: Achte darauf, dass auch deine software immer up-to-date ist :)
- Ändere regelmäßig deine Passwörter!

Die Organisation netzpolitik.org bietet einen wöchentlichen Newsletter an, um über aktuelle netzpolitische Entwicklungen zu informieren.

Zum Weiterlesen

- Eine nett gestaltete Seite zu Erstellung deines eigenen Sicherheitsplans: ein security planner
- Überlegungen zum persönlichen Sicherheitsplan auf Surveillance-Self-Defence
- Tipps zu Privacy-Settings und Sicherheitseinstellungen in deinen Social-Media-Konten