Private Daten

Einfach & sicher

Egon Leitner

Private Daten – Einfach & sicher

Dritte Auflage – Version 1. Februar 2023

Credits:
Icon designed by Smashicons from Flaticon

Inhaltsverzeichnis

Hallo verehrter Leser,

Tobias Hartmann, damals Vorstandsvorsitzender des weltweit viertgrößten Marktforschungsunternehmens, sagte 2014:

„Daten sind das Gold des 21. Jahrhunderts."

Nun frage ich dich: Wie würdest du Gold lagern?

Vermutlich möglichst sicher, zum Beispiel in einem guten Tresor oder in einem Schließfach einer vertrauenswürdigen Bank.

Und wie speicherst du eine Daten?

Oder anders gefragt: Weißt du, wie du deine Daten vergleichbar sicher speichern und verwalten kannst?

Mach dir keine Sorgen, wenn du bei diesen Fragen ins Grübeln kommst. Nach der Lektüre dieses Buches und der hoffentlich praktischen Umsetzung der Grundprinzipien kannst du mit Recht behaupten, dass deine Daten mindestens so sicher wie Gold sind.

Und du bekommst einen anderen Blick auf deine Daten, dein "Goldschatz" wird für dich noch wertvoller.

Viel Spaß beim Lesen und Umsetzen wünscht dir dein Autor

Egon Leitner

Dieses kleine Sicherheitshandbuch gibt dir einen Überblick, wie du als Privatperson sicher mit deinen Geräten und Daten umgehen kannst.

Vereinzelt sind einige Anleitungen produktspezifisch, generell habe ich aber versucht, möglichst herstellerunabhängig zu schreiben, so dass eine sinngemäße Übertragung auf andere Systeme meist möglich ist.

Sobald man etwas direkter mit dem Thema IT-Sicherheit in Berührung kommt, stellt man sich früher oder später unweigerlich die Frage, welches der verschiedenen verfügbaren Systeme das sicherste ist...?

Ich will hier keinen Glaubenskrieg anzetteln (Betriebssystem A ist sicherer als Betriebssystem B), sondern dir ein paar Gedanken mit auf den Weg geben.

Sicherheit ist ein Prozess

Du solltest IT-Sicherheit als einen Weg sehen, auf welchen IT-Sicherheit sollte als ein Weg betrachtet werden, auf dem schrittweise Verbesserungen erzielt werden. Ein Gerät oder System ist nicht a priori sicher (oder unsicher), sondern es hängt davon ab, wie es verwendet oder konfiguriert wird.

Sicherheit hat viele Komponenten

IT-Sicherheit wird in der Regel nicht durch eine einzelne Komponente oder ein einzelnes Gerät erreicht, sondern hat meist mehrere Ebenen. Daher ist es wichtig, dass alle Komponenten bzw. Teile eines Systems so gut wie möglich gesichert sind.

Ein Teil des Systems bist übrigens du selbst, als Benutzer.

Sicherheit hängt vom Umfeld ab

Die relative Sicherheit eines Systems hängt von seiner Umgebung ab. Damit meine ich, dass ein System in einer relativ freundlichen Umgebung sicher genug sein kann, während es in einer sehr feindlichen Umgebung nicht sicher genug sein kann. Natürlich hängt dies auch davon ab, wie interessant es für jemanden ist, das System anzugreifen, bzw. wie viel Aufwand/Ressourcen in einen Angriff investiert werden.

Beachte auch, dass sich das Umfeld (kurzfristig) verändern kann.

Absolute Sicherheit gibt es nicht

Auch diesen Satz hast du sicher schon oft gehört. Was du aber vor allem bedenken solltest, ist, dass du nicht deine ganze Energie und deinen ganzen Aufwand in die Abwehr stecken solltest, sondern auch in Ressourcen zur Erkennung und vor allem zur Wiederherstellung bzw. Schadensbegrenzung im Falle eines mehr oder weniger erfolgreichen Angriffs.

Ein Wort zu den genannten Betriebssystemen

Im Zusammenhang mit der vieldiskutierten Sicherheit von Betriebssystemen hört man immer wieder, dass Open-Source-Betriebssysteme sicherer seien, weil der Quellcode eingesehen und kontrolliert werden könne.

Als Gegenargument kann angeführt werden, dass in kleinen (Teil-)Projekten der Quellcode oft nur von wenigen Personen eingesehen wird oder nicht jeder, der sich den Quellcode ansieht, diesen auch versteht. Nicht zuletzt kann man oft nicht mit absoluter Sicherheit sagen, ob das verwendete Programm auch genau aus diesem Quellcode entstanden ist. Wenn in diesem Buch an der einen oder anderen Stelle ein Betriebssystem genannt wird, liegt das einfach daran, dass sich der Autor mit `macOS` und `Linux` etwas besser auskennt als mit anderen Betriebssystemen.

Letztendlich hängt die Sicherheit eines Systems oder Programms sehr stark vom Benutzer ab. Daher sollte man Systeme, mit denen man vertraut ist, bevorzugen.

Mit anderen Worten: Stelle sicher, dass du mit den Systemen, die du am liebsten verwendest, gut vertraut bist!

Konventionen in diesem Buch

Ausgabe

```
FileVault is On.
```

Ausgaben in der Eingabeaufforderung bzw. in der `Linux` / `macOS` Kommandozeile werden in dicktengleicher (nichtproportionaler) Schrift dargestellt.

```
Format: APFS (Encrypted)
```

Generelle Ausgaben (am Bildschirm) werden in dicktengleicher Schrift mit blauem Hintergrund dargestellt.

Eingabe

```
$ sudo fdesetup status
```

(Kommandozeile bzw. Eingabeaufforderung)

Eingaben, welche in der Eingabeaufforderung oder auf der `Linux` / `macOS` Kommandozeile erfolgen sollen, werden mit vorangestelltem $ und

ebenfalls in dicktengleicher Schrift dargestellt.

Wenn der Befehl mit Admin- bzw. Root Rechten ausgeführt werden muss, ist dies durch vorangestelltes # erkennbar.

Eingabe (Tastatur und Maus)

i *	Die Eingabe eines einzelnen Zeichens ist durch eine Umrandung gekennzeichnet.
Einstellungen > Sicherheit	Besteht eine Eingabe/Konfiguration aus mehreren Schritten, werden diese zusammen umrandet dargestellt.
<CTRL-R> <ENTER>	Spezielle Tasten wie die Steuertasten (Shift, Tab, Alt, Strg) oder die Eingabetaste sind gelb hinterlegt.

Textdarstellung

Linux	Diese Beschreibung gilt für das Betriebssystem Linux.
macOS	Diese Beschreibung gilt für das Betriebssystem macOS von Apple.
Mozilla Firefox	Diese Beschreibung gilt für ein spezifisches Programm.

Symbole

Dieses Symbol weist auf eine Warnung oder einen sehr wichtigen Hinweis hin.

Dieses Symbol weist darauf hin, dass die beschriebene Situation Vor- und Nachteile hat, die es abzuwägen gilt.

Dieses Symbol kennzeichnet besondere Tipps und Tricks.

2 Dein Bewusstsein für IT- bzw. Daten-Sicherheit

Sei dir bei der Benutzung von Computern und IT-Systemen der damit verbundenen Risiken bewusst.

Stelle sicher, dass du sowohl mit den aktuellen Sicherheitsrisiken als auch mit den Standards und Verfahren zur Verbesserung der Sicherheit vertraut bist.

Maßnahme

- Informiere dich regelmäßig über aktuelle Bedrohungen, die die von dir genutzten Systeme oder Plattformen betreffen. Dies kannst du z.B. über die Newsletter anerkannter öffentlicher Institute (SANS, BSI, BürgerCERT) oder über spezielle Nachrichtenportale zum Thema Sicherheit (Heise-News) tun.

Ich könnte dir hier und an vielen anderen Stellen in diesem Buch URLs zu den genannten Informationen nennen, würde damit aber zum einen in Kauf nehmen, dich eventuell auf veraltete oder gar nicht mehr existierende Seiten/Quellen zu führen. Zum anderen möchte ich dich ermutigen, selbst aktiv zu werden und das Thema IT-Sicherheit in die Hand zu nehmen.

Deshalb mein Tipp: Benutze einfach die Suchmaschine Deiner Wahl, um aktuelle Informationen zu finden - Du wirst sehen, es ist gar nicht so schwer und lohnt sich!

3 Deine Geräte sind deine Daten

Überlege dir gut, ob und wem du Zugriff auf deine Geräte bzw. Daten gibst.

Grundsätzlich solltest nur du Zugriff auf deine persönlichen Geräte, wie zum Beispiel dein Handy, haben. Das bedeutet, dass du die PIN nicht weitergeben solltest, auch nicht an deinen Partner.

Auf die leider weit verbreitete Unsitte, den Kindern ein eigenes Gerät zum Spielen zu überlassen, solltest du gänzlich verzichten.

Überlege dir auch, ob und in welcher Form du Gästen Zugang zu deinem WLAN gewährst. Dabei geht es nicht nur darum, was sie in deinem Namen im Internet machen können, sondern auch darum, ob sie z.B. unerwünscht in deinem Heimnetzwerk “herumschnüffeln”...

Maßnahmen

- Gib anderen nur in absoluten Ausnahmefällen Zugang zu deinen persönlichen Geräten oder Daten.
- Wenn es notwendig war, einer anderen Person vorübergehend Zugriff auf ein persönliches Gerät oder deine Daten zu geben, entferne so schnell wie möglich die Zugriffsmöglichkeit und ändere das entsprechende Passwort oder die PIN.

- Wenn nötig, richte auf deinem Router ein separates WLAN (separate SSID) ein, über das Besucher ins Internet gehen können. Die meisten Router bieten diese Möglichkeit. Hier kannst du auch Einschränkungen vornehmen, so dass Benutzer nicht auf das lokale Netzwerk zugreifen oder nur bestimmte freigegebene Dienste über deinen Internetzugang nutzen können.

4 Schütze deine Geräte

Lass deine Geräte nicht unbeaufsichtigt und bewahre sie geschützt auf.

Überwache, kontrolliere und schütze deine Geräte zu Hause und unterwegs.

Das gilt in öffentlichen Verkehrsmitteln genauso wie im Auto oder bei Veranstaltungen wie Kongressen oder Messen.

Maßnahmen

- Achte besonders in Bussen und Bahnen immer auf deine Ausrüstung und dein Gepäck.
- Lass deine Geräte nicht für alle sichtbar im Auto liegen.
  Achtung: Generell sollten Geräte an heißen Tagen möglichst nicht im Kofferraum oder gar im Fahrzeuginneren aufbewahrt werden. Dort können Temperaturen von über 60 °C erreicht werden.
-  Überlege, ob du den Raum, in dem du deine technischen Geräte aufbewahrst oder betreibst, nicht videoüberwachen möchtest.

5 Der Zugriff auf deine Geräte und Daten

Verwende ein starkes Passwort für deine Zugänge und sperre deine Geräte oder Sitzungen, wenn du sie nicht verwendest.

(Mehr zum Thema Passwort siehe Kapitel „Bist du wirklich du?“)

Beschränke den Zugriff auf deinen Computer oder deine Geräte generell auf angemeldete Benutzer.

Maßnahmen

- Beschränke und kontrolliere den Fluss und die Präsenz von deinen Daten.
  Überlege dir, welche Daten du über welches Netz abrufst.
- Wenn du nicht immer die aktuellsten Daten auf deinem Handy brauchst, deaktiviere die Hintergrundaktivitäten. Bei iOS geschieht dies in der Regel automatisch, wenn der Stromsparmodus aktiviert ist.
- Wenn du gerade keine Netzwerkverbindung benötigst, deaktiviere diese, d.h. ziehe das Netzwerkkabel ab oder versetze dein Gerät in den

sogenannten Flugmodus. Dies gilt auch für Bluetooth-Verbindungen.

- Unterteile deine (Internet-)Aktivitäten in solche, die mit deinem Namen verbunden sind, und solche, die du anonym oder pseudonym durchführen kannst. Verwende je nach Aktivität verschiedene Geräte, verschiedene virtuelle Systeme oder zumindest verschiedene Browser.

Achte auf eine strikte Trennung, d.h. verwende immer dasselbe Gerät oder virtuelle System für dieselbe Art von Aktivität.

- Verwende für die tägliche Arbeit auf den Geräten einen nicht privilegierten Benutzer ohne administrative Rechte.
- Benutze für administrative Tätigkeiten einen speziell geschützten Admin-Account.
- Stelle sicher, dass nicht privilegierte Benutzer keinen Zugriff auf die Funktionen/Dateien der privilegierten Benutzer haben.
- Schränke die Anzahl der möglichen Loginversuche ein, stelle eine Verzögerung bei fehlgeschlagenen Anmeldeversuchen ein bzw. lass dich darüber benachrichtigen.
   Überlege dir, ob du eventuell die Daten auf deinem Gerät nach einer größeren Anzahl von

fehlgeschlagenen Anmeldeversuchen automatisch löschen lassen möchtest und konfiguriere dies entsprechend den Möglichkeiten deines Systems.

- Konfiguriere die automatische Aktivierung des Bildschirmschoners nach einer bestimmten Zeit der Inaktivität oder das zuverlässige Sperren des Bildschirms und der Benutzersitzung.
  Stelle sicher, dass der Zugang nur durch Eingabe des richtigen Passworts wiederhergestellt werden kann.

- Achte bei Fernzugriff auf deine Geräte, dass die Datenübertragung mit starker Kryptographie und der Zugriff mit Benutzername und Passwort geschützt sind. Auf vielen Systemen kannst du mit SSH (beziehungsweise `openssh`) verschlüsselt Zugreifen oder Daten übertragen.

- Setze auf mobilen Geräten und externen Speichermedien Verschlüsselung ein, bevorzugt eine Technologie, welche das gesamte Gerät verschlüsselt.

- Überprüfe und kontrolliere die Verbindungen, die dein Gerät nach außen herstellt oder benutzt.

- Sei vorsichtig mit fremden Speichergeräten, welche du an deinen Geräten benutzt.
  Sei auch vorsichtig und umsichtig bei der Verwendung deiner Speichermedien auf fremden Systemen.

- Sei besonders vorsichtig bei der Auswahl der Informationen, die du veröffentlichst oder ins Internet

stellst.
Lass die Informationen, die du veröffentlichen willst, von mindestens einer anderen Person überprüfen.

- Prüfe regelmäßig, ob und welche Daten von dir auf externen IT-Systemen bzw. im Internet veröffentlicht sind und lass sie gegebenenfalls entfernen, sofern sie nicht für extern bestimmt sind/waren.

6 Bist du wirklich du?

Stelle sicher, dass du und alle anderen Bsenutzer eindeutig identifiziert werden, wenn du ein Gerät oder einen Dienst benutzt.

Maßnahmen

- Verwende eine sichere, möglichst mehrstufige Authentifizierung sowohl für privilegierte als auch für nicht privilegierte Benutzerkonten.
- Aktiviere eine Zwei-Faktor-Authentifizierung (2FA), wo immer dies möglich ist.
  Die Faktoren sind dabei, ein bestimmter Gegenstand, geheimes Wissen oder eine (biometrische) Eigenschaft (Haben, Wissen, Sein).
- Verwende Sicherheitsfragen zur Sicherung von Benutzerkonten, z. B. bei Online-Diensten.

Von der Verwendung sogenannter Sicherheitsfragen wird oft abgeraten, da die Antworten meist aus dem persönlichen Umfeld des Nutzers stammen und daher leicht zu erraten sind.

Dieses Problem kann jedoch leicht umgangen werden, indem du entweder eine falsche Antwort auf eine Frage gibst oder, wie es bei einigen Diensten möglich ist, indem du selbst eine Frage mit der entsprechenden Antwort vorgibst.

Im Idealfall ist die Antwort auf deine Sicherheitsfrage genauso komplex und lang wie deine Passwörter. Und natürlich verwahrst du auch diese Information nach den gleichen Kriterien wie deine Passwörter.

- Wenn es auf deinem Gerät oder Computer Benutzerkonten gibt, die nicht oder nicht mehr benötigt werden, entferne sie.

- Schütze Passwörter beim Speichern und Übertragen ausschließlich mit anerkannter Kryptographie.

- Stelle sicher, dass die verwendete oder selbst programmierte Software während der Authentisierung keine kompromittierenden Informationen an den Benutzer weitergibt, die durch Rückschlüsse eine Überwindung oder Manipulation des Systems ermöglichen.

Thema: Passwörter

- Benutze für jeden Zugang/Dienst unterschiedliche Passwörter.

- Wähle bei der Verwendung von Kennwörtern eines mit einer gewissen Länge und/oder Komplexität (Stichwort Entropie).
  Die Länge ist noch wichtiger als die Komplexität.

-  Konfiguriere dein System so, dass es die Verwendung von Passwörtern mit einer bestimmten Länge und Komplexität erzwingt.

- Erstelle oder befolge keine unsinnigen Regeln, die sehr spezifische Anforderungen an Groß-/Kleinschreibung, Zahlen und Sonderzeichen stellen, aber oft relativ kurze Passwörter erlauben.

- Schreibe keine Mindest- und/oder Höchstdauer für die Gültigkeit von Passwörtern vor. Periodisch erzwungene Passwortänderungen führen zwar zu häufig geänderten, aber oft schwachen und vorhersehbaren Passwörtern.

  Wenn dein Passwort stark ist und nur dir oder befugten Personen bekannt ist, gibt es keinen Grund, es ständig zu ändern.

Wenn anzunehmen ist, dass das Passwort kompromittiert wurde oder Unbefugten bekannt ist, sollte es natürlich so schnell wie möglich geändert werden.

Wenn du dein Passwort änderst, solltest du es vollständig ändern und ein neues Passwort wählen, das so wenig Ähnlichkeit wie möglich mit deinem alten Passwort hat.

Und in diesem Zusammenhang: Man braucht keinen Mechanismus, der die Wiederverwendung von Passwörtern für eine bestimmte Anzahl von Generationen verhindert, wenn man seine Passwörter aus zufälligen Zeichen/Satzteilen erstellen lässt.

Thema: Passwörter (Fortsetzung)

- Bewahre deine Passwörter sorgfältig und sicher auf. Es spricht nichts dagegen, sich Passwörter aufzuschreiben und sie physisch sicher zu verwahren, zum Beispiel in einem Tresor.

  Bei einer größeren Anzahl von Passwörtern empfiehlt sich der Einsatz eines Verwaltungsprogramms (Passwortmanager).

  Nutze bei der Verwendung eines Passwortmanagers möglichst Open-Source-Software und achte darauf, dass die Daten lokal und nicht bei einem proprietären Anbieter gespeichert werden.

   Sofern die gespeicherten Passwörter ausreichend durch starke Kryptographie geschützt sind, kannst du diese eventuell bei einem allgemeinen Cloud-Anbieter oder – noch besser – auf einem eigenen Server ablegen.

  Als Passwortmanager kann ich dir eines der folgenden Programme empfehlen: `KeePass` verfügbar für `Linux`, `macOS` und weitere Betriebssysteme, oder `pass` bzw. `gopass`, ebenfalls für diverse Betriebssysteme verfügbar.

7 Kontrolliere was passiert

Kontrolliere welche Daten oder Programme auf welchen Geräten verwendet werden.
Wenn du Programme oder Daten aus nicht vertrauenswürdigen Quellen verwenden musst, öffne sie in einer so genannten Sandbox-Umgebung.

Konfiguriere die Geräte möglichst so, dass Aufzeichnungen über Benutzer- und Programmaktivitäten erstellt werden.
Achte darauf, dass die von verschiedenen Anwendern durchgeführten Aktionen eindeutig zugeordnet werden können.

 Wäge den Nutzen gegen das Risiko ab, dass die Aufzeichnungen sensible Informationen enthalten und in falsche Hände geraten könnten.

Maßnahmen

- Halte für das Ausführen beziehungsweise Installieren von Programmen aus nicht vertrauenswürdigen Quellen oder für das Öffnen von verdächtigen Dateien eine sogenannte Sandbox-Umgebung bereit. Dies kann zum Beispiel ein isoliertes physisches oder virtuelles System sein.

- Synchronisiere möglichst alle internen Uhren deiner Geräte mit der Atomzeit (Stichwort NTP).

- Schütze die Protokolle und die Werkzeuge zur Protokollierung vor unbefugtem Zugriff, unbefugter Änderung und unbefugter Löschung.

- Sichere die Überwachungsprotokolle mit kryptographischen Methoden ab und zeichne diese gegebenenfalls auf einem System auf, welches sich physisch an einem anderen Ort als das überwachte System selbst befindet.

Thema: Keylogger

Was ist ein Keylogger?

Ein Keylogger ist eine Software oder Hardware, die alle Tastatureingaben an einem Computer aufzeichnen kann.

Insbesondere auf fremden Rechnern, die du nicht vollständig kontrollieren kannst, aber auch auf deinen eigenen Rechnern besteht die Gefahr, dass vertrauliche Daten gegen deinen Willen ausgespäht werden.

Mögliche Maßnahmen gegen Hardware-Keylogger

- Kontrolliere deine Tastatur und deren Anschlüsse regelmäßig auf Veränderungen oder zusätzlich eingesteckte Geräte/Adapter.

Mögliche Maßnahmen gegen Software-Keylogger

- Befolge die in Kapitel 11 empfohlenen Maßnahmen, insbesondere die zeitnahe Installation verfügbarer Sicherheitsupdates.

- Falls du ein Betriebssystem benutzt, auf

dem Viren relevant sind: Einige Virenscanner können auch Software-Keylogger erkennen.

-  Verwende einen Passwortmanager

  Dieser trägt den Benutzernamen/Passwort entweder automatisch in das entsprechende Programm bzw. in das entsprechende Feld auf der Webseite ein oder du kannst ihn per Copy & Paste einfügen.

  Beachte jedoch, dass ein Keylogger auch das Master-Passwort kompromittieren kann. Ein Gegenmittel wäre die Verwendung einer zusätzlichen Schlüsseldatei für den Passwortmanager.

- Falls du die Präsenz eines Software-Keyloggers nicht vollständig ausschließen kannst:

  - **Mische relevante mit nicht relevanten Eingaben**
    Setze dafür, zum Beispiel bei der Passworteingabe, den Fokus (mit der Maus) abwechselnd auf das Passwortfeld und dann auf ein nicht relevantes Feld bzw. eine nicht relevante Stelle in der Anwendung.
    Achte darauf, dass du nur den Fokus innerhalb des Programms änderst und nicht die gesamte Anwendung, da einige Keylogger die Eingaben pro Programm separat aufzeichnen.

  - **Benutze eine Bildschirmtastatur**
    Dabei handelt es sich um ein Hilfsprogramm, das in der Regel vom Betriebssystem zur Verfügung gestellt wird und es ermöglicht, eine visuell dargestellte Tastatur nur mit der Maus oder dem Touchpad zu bedienen.

  - **Überwache ausgehende Verbindungen**
    Wie in Kapitel 11 beschriebenen, achte generell auch auf ausgehende Datenverbindungen. Es ist wahrscheinlich, dass der Keylogger die gesammelten Eingaben über das Netzwerk nach außen sendet.

8 Deine Geräte, deine Konfiguration

Erstelle, verwalte und dokumentiere die Konfiguration deiner Geräte, und verwende dabei so weit wie möglich automatisierte Werkzeuge für das Konfigurationsmanagement.

Führe auch ein Inventar von deiner Hard- und Software.

Maßnahmen

- Verfolge eine konkrete Sicherheitsrichtlinie für die Konfiguration von all deinen Geräten und halte dich zwingend an diese.
-  Überprüfe geplante Konfigurationsänderungen an deinen Geräten vor der Durchführung (!) unter expliziter Berücksichtigung der Auswirkungen auf die Sicherheit.(!!)
- Protokolliere die Änderungen an deinen Geräten.
- Schütze den physischen und logischen Zugriff für das Durchführen von Änderungen auf deinen Geräten.
- Beschränke die Funktionalität deiner Geräte durch geeignete Konfiguration auf das absolut Notwendige.

- Untersage und/oder beschränke die Verwendung von definierten Diensten, Funktionen, Protokollen und/oder Ports.
  Wie in Kapitel 11 beschrieben, kann dies durch die Konfiguration einer “personal firewall” erfolgen.

- Bestimme für dich selbst, welche Software du auf deinen Geräten verwenden willst.

- Lege die Kriterien fest, die eine Software erfüllen muss, damit sie für den Einsatz auf deinen Geräten geeignet ist, und überprüfe bei jeder neuen Software, ob sie diese Kriterien erfüllt.

- Wenn du ein Gerät mit mehreren Benutzern teilst, lege genau fest, wer Software installieren/konfigurieren darf, und konfiguriere eine Überwachung oder Benachrichtigung, wenn eine nicht autorisierte Installation von Software erfolgt.

9 Die Wartung deiner Geräte

(Instandhaltung, Pflege)

Plane etwaige notwendige Wartungen bzw. Reparaturen von deinen Geräten im Voraus und lasse sie nur von vertrauenswürdigen autorisierten Dienstleistern durchführen.

Lass notwendige Reparaturen – wenn immer möglich – vom Hersteller selbst ausführen.

Maßnahmen

- Stelle sicher, dass auf jeglichen Geräten, welche du zur Wartung bzw. zur Reparatur gibst, alle Daten entfernt wurden.
- Wenn du jemandem Fernzugriff auf ein Gerät gewährst, um Wartungsarbeiten durchzuführen, überwache die Sitzung und beende sie sofort, wenn die Wartungsarbeiten abgeschlossen sind.
- Achte darauf, wem du bei Wartungs-/Reparaturarbeiten Zugang zu deiner Wohnung oder deinem Haus gewährst.
- Unterziehe jedes Gerät, das von einer Wartung/Reparatur zurückgekehrt ist, vor der Wiederinbetriebnahme einer gründlichen Prüfung. Wenn es ohne weiteren Verschleiß möglich ist, führe

einen Dauertest durch, um zu überprüfen, ob der Fehler/das Problem tatsächlich behoben wurde.

- Sofern machbar, installiere sämtliche Software auf dem gewarteten/reparierten Gerät komplett neu bzw. formatiere den vorhanden Speicher gründlich.

10 Deine Datenträger sind deine Daten

Erarbeite für dich selbst eine Richtlinie für den Umgang mit Datenträgern bzw. Medien, seien sie digital oder nicht.

Dies betrifft die Erstellung, die Verwaltung und die Entsorgung bzw. Vernichtung.

Maßnahmen:

- Beschränke den Zugang zu Medien mit relevanten Daten (auch physisch) auf die gewünschten Personen und verwahre diese in geschützten Bereichen.

  Überlege dir, wo du deine Dokumente und Datenträger sicher aufbewahren möchtest. Hochsensible Inhalte auf Papier sind natürlich am besten in einem Bankschließfach oder einem privaten Tresor aufgehoben.

  Bei einzelnen Datenträgern, die ausreichend mit starker Kryptographie geschützt sind, ist das primäre Kriterium für den Zugriff/Zugang die Verfügbarkeit. Mit anderen Worten, wenn die Daten ausreichend verschlüsselt und mehrfach an verschiedenen Orten vorhanden sind, ist der physische Schutz nicht so kritisch.

- Bereinige Medien vor der Wiederverwendung oder Entsorgung bzw. vernichte sie mit technisch anerkannten Methoden.

  Papier muss zwingend mit einem Aktenvernichter mit Kreuzschnitt vernichtet werden.

  Kleinere Mengen können aber auch durchaus durch Verbrennung sicher vernichtet werden.

  Für Datenträger gilt das bereits im vorigen Punkt Beschriebene: Sofern der Datenträger vollständig mit starker Kryptographie verschlüsselt ist, genügen bei der Entsorgung einfachere Maßnahmen wie einfaches Überschreiben oder Löschen.
  Wenn die Datenträger jedoch unverschlüsselt sind/waren, müssen je nach Sensibilität der Daten aufwändigere Maßnahmen ergriffen werden.

  Im Zweifelsfall sind magnetische Datenträger mit hochsensiblen Daten durch anerkannte technische Verfahren, wie z.B. professionelles Degaussen, vollständig zu vernichten.

  Wenn dies nicht möglich ist, kann in Ausnahmefällen die Löschung per Software durch zertifizierte Methoden erfolgen (siehe DoD 5220.22-M Wiping Standard bzw. entsprechende FIPS-Standards).

- **Vorsicht bei Datenträgern mit Speicherzellen:** Durch die ausgefeilte Technik der internen Organisation der Speicherzellen durch den Controller

auf dem Gerät ist es praktisch nicht mehr möglich, alle Speicherinhalte von außen zuverlässig zu löschen. Damit bleibt bei der Entsorgung unverschlüsselter Inhalte praktisch nur noch die Vernichtung als ausreichende Maßnahme.

- Kennzeichne Medien bzw. Informationen deutlich mit entsprechenden Hinweisen zu Handhabung, Schutzbedarf und Verbreitungseinschränkungen.
  Hier geht es darum, dass du selbst und eventuell auch andere die Medien bzw. Informationen und ggf. deren Schutzbedürftigkeit auf den ersten Blick klar erkennen können.
  Das bedeutet nicht, dass man jedes Dokument nach Sicherheitsklassen eines Nachrichtendienstes klassifizieren muss, aber man sollte im Bedarfsfall z.B. Familienmitgliedern mitteilen können, wenn sie ein besonders sensibles Dokument von einem in den Händen halten oder man sollte z.B. bei mehreren Festplatten/Speichermedien deren Inhalt anhand der vorhandenen Kennzeichnung von außen zuordnen können.

- Behalte den Überblick über den Aufbewahrungsort deiner Medien.

- Verwende starke Verschlüsselung, um die Daten auf deinen digitalen Medien zu schützen.
  Starke Verschlüsselung schützt den Inhalt deiner Medien zuverlässig.

Bei kleineren Informationsmengen auf Papier kann es auch sinnvoll sein, diese verschlüsselt darzustellen, z.B. mit GPG-Verschlüsselung und Darstellung mittels QR-Code.

Bei elektronischen Datenträgern solltest du möglichst immer den gesamten Datenträger verschlüsseln.

Unter `Linux` ist dies mit `dm-crypt/luks` möglich, unter `macOS` kannst du bei jeder Partitionierung/Formatierung eines Datenträgers die Verschlüsselung wählen bzw. mit `FileVault` für die komplette Verschlüsselung deiner internen Festplatte sorgen.

Unter `macOS` siehe dazu:

```
Systemeinstellungen > Sicherheit > FileVault
```

Wenn es nicht möglich ist, den gesamten Datenträger oder eine Partition vollständig zu verschlüsseln, erstelle eine verschlüsselte Containerdatei der gewünschten Größe und speichere alle Daten darin. Achte darauf, dass keine Daten außerhalb des Containers gespeichert werden und verwende auch hier starke Kryptographie.

Dafür kannst du, betriebssystemunabhängig, eventuell die Software `VeraCrypt` verwenden.

- Kontrolliere bzw. **vermeide** die Verwendung fremder externer Datenträger, insbesondere wenn der Eigentümer nicht eindeutig feststellbar ist.

Stell dir folgendes Szenario vor: Du findest irgendwo einen USB-Stick, bist sehr neugierig was denn wohl darauf gespeichert ist und schließt ihn an deinen Computer an ...

Mach das nicht!!!

Bei diesem Vorgehen lauern gleich mehrere Gefahren: Zum einen könnte der USB-Stick mechanisch oder elektronisch so präpariert sein, dass dein Computer beschädigt wird. Zum anderen könnte er Schadsoftware enthalten, die Software oder Daten auf deinem Computer verändert, löscht oder bei nächster

Gelegenheit von deinem Computer nach außen überträgt.

Wenn du Datenträger anderer (bekannter) Personen an dein Gerät anschließen musst, stelle sicher, dass dein Gerät ausreichend gegen Schadsoftware geschützt bzw. immun ist.

Überlege, ob du ein anderes, unkritisches Gerät hast, an das du den Datenträger anschließen kannst.

Thema: Backup

- Erstelle regelmäßig Backups.
- Achte darauf, dass deine Backups so aktuell wie möglich sind.
- Erstelle zwei oder mehr Sicherungskopien deiner Daten und bewahre sie an getrennten Orten auf.

  Ich habe für meine Backups den Grundsatz:

  “Einmal ist keinmal, und zweimal am selben Ort ist auch keinmal”.
- Teste regelmäßig die Wiederherstellung von Daten aus Backups.

  Das Backup deiner Daten muss auf jeden Fall die folgen- den drei Kriterien erfüllen:

  “Vertraulichkeit, Integrität und Verfügbarkeit!”
- Schütze deine Backupdaten durch Verschlüsselung, insbesondere an externen Speicherorten.
  Sofern du starke kryptographische Methoden verwendest, ist die Vertraulichkeit und Integrität deiner Daten selbst eigentlich immer gewährleistet. Bedenke aber, dass bei der Übertragung von Daten immer auch Metadaten

entstehen, die ihrerseits sensibel sein können.

- Bei der externen Datenspeicherung (Cloud) ist zu beachten, in welchem Land sich die Daten letztlich befinden bzw. welches Recht zur Anwendung kommt.

Beachte die **3-2-1-Backup-Regel** von Peter Krogh:

• Mindestens drei Kopien von Daten,
• Speichern der Kopien auf zwei unterschiedlichen Medien,
• Aufbewahren einer Backup-Kopie an einem externen Speicherort.

11 Deine Geräte, deine Kommunikation

Sichere jegliche Informationsübertragung, sowohl extern als auch intern, so gut wie möglichst ab, am besten durch starke Verschlüsselung.

Achte bei der Auswahl von Geräten, Software und Netzwerk auf den „Stand der Technik“ bzw. auf anerkannte Anbieter. Achte auch darauf, dass du die gewählte Technik nach anerkannten Standards anwendest.

Maßnahmen

- Setze bevorzugt Software ein, die von Haus aus eine Trennung von Benutzer- und Administratorrolle vorsieht.
- Achte darauf, dass diese Rollen auch im Laufe der Zeit bzw. mit der fortwährenden Nutzung der Software oder des Gerätes strikt getrennt bleiben und nicht gegenseitig auf die Informationen oder Ressourcen der jeweils anderen Rolle zugreifen (können).
- Überlege, ob es möglich und sinnvoll ist, verschiedene Geräte in verschiedenen Netzwerken mit unterschiedlichen Sicherheitsniveaus zu platzieren.

- Setze gegebenenfalls an zentralen Punkten/Schnittstellen Firewalls ein, welche du so konfigurierst, dass sie standardmäßig den kompletten Netzwerkverkehr verbieten und nur definierte Ausnahmen erlauben (deny all, permit exception).

- Verhindere möglichst, dass ein Gerät gleichzeitig Verbindung zu getrennten Netzwerken herstellt.

- Verhindere ebenfalls, dass ein Gerät gleichzeitig Verbindung zu mehreren entfernten Geräten aufbaut.

- Benutze anerkannte, starke Verschlüsselung um jegliche Datenübertragung zu schützen.

- Trenne Netzwerkverbindungen einer Kommunikationssitzung am Ende der Sitzung oder nach einer definierten Zeit der Inaktivität.
  Dies gilt zum Beispiel für SSH-Sitzungen.

- Achte bei der Verwendung von kryptographischen Schlüsseln darauf, dass du methodisch nach (für dich) definierten Mechanismen für die Erzeugung, Verteilung, Speicherung und Löschung vorgehst.
  Erstelle z.B. bei der Generierung von GPG-Schlüsseln gleichzeitig einen Rückrufschlüssel und bewahre deinen privaten Schlüssel sorgfältig auf.

- Wähle und setze Kryptographie nach anerkannten Richtlinien, wie etwa dem FIPS, um.

- Achte darauf, dass niemand deine Geräte unbemerkt von außen aktivieren oder benutzen kann.

Achte hierbei besonders auf eventuell eingebaute Kameras oder Mikrofone.

Bei tragbaren Computern oder Tablet-PCs kann die Frontkamera oft ganz einfach mit einem Stück mattem, leicht haftendem Klebeband abgedeckt werden, wenn sie nicht benötigt wird.

Manche Geräte haben auch eine eingebaute Klappe, die vor die Kamera geschoben werden kann.

- Überwache und beschränke die Ausführung von mobilem Code bzw. die Technologie/Produkte zur Ausführung von mobilem Code.
  Dazu gehören z.B. Javascript und Ähnliches, aber auch Postscript und PDF.
  Vielleicht wusstest du noch nicht, dass in PDF-Dateien komplette Programme eingebettet sein können, die dann über den Viewer ausgeführt werden...

- Wähle die Nutzung von VoIP-Technologien (FaceTime, WhatsApp, Skype/Teams, Zoom usw.) mit Bedacht und setze wenn möglich solche mit integrierter Ende-zu-Ende-Verschlüsselung ein.

- Schütze die Authentizität von Kommunikationssitzungen. Vergewissere dich, dass dein Browser dich zuverlässig warnt, wenn das

Zertifikat einer Website nicht mit ihrem Namen übereinstimmt.

- Vergewissere dich, dass auch bei SSH-Verbindungen eine zuverlässige Identifizierung der Gegenseite stattfindet bzw. überprüfe manuell den sogenannten Fingerprint.

- Schütze Backups bzw. archivierte Daten in angemessener Weise durch starke Verschlüsselung. Siehe hierzu speziell das Sonderthema **Backups** auf Seite 43.

Thema: Verschlüsselung

Starke Verschlüsselung hilft

Starke Verschlüsselung hilft dir, die Vertraulichkeit und Integrität deiner Daten zu wahren.

Aber was ist starke Verschlüsselung?

Unter starker Verschlüsselung versteht man Algorithmen und Methoden, die Inhalte nach dem Stand der Technik so gut schützen, dass sie gegen kryptographische Analyse und Entschlüsselung sicher sind.

Generell wird bei der Verschlüsselung zwischen symmetrischer und asymmetrischer Verschlüsselung unterschieden.

Symmetrische Verschlüsselung verwendet einen einzigen Schlüssel für das Verschlüsseln und das Entschlüsseln der Information. Dieser Schlüssel muss, zum Beispiel in Form eines Passwortes, zwischen den beteiligten Teilnehmern ausgetauscht werden.

Bei der **asymmetrischen Verschlüsselung** hingegen wird ein Schlüsselpaar erzeugt, das aus einem öffentlichen Schlüssel zum Verschlüsseln und einem privaten Schlüssel zum Entschlüsseln besteht. Der öffentliche Schlüssel kann, wie der Name schon sagt, problemlos offenbart werden, während der private Schlüssel geheim gehalten werden muss.

Asymmetrische Verschlüsselung ist in der Regel etwas rechenintensiver als symmetrische Verschlüsselung, bietet aber einige Vorteile.

Wenn bei der Verschlüsselung in einem Verfahren sowohl symmetrische als auch asymmetrische Verschlüsselung zum Einsatz kommt, wird dies **hybride Verschlüsselung** genannt.

Wenn du mehr über die Klassifizierung oder die technischen Hintergründe erfahren möchtest, empfehle ich dir die entsprechenden Artikel bei Wikipedia.

Schlüssellänge

Die Sicherheit von Verschlüsselungsverfahren hängt oft (aber nicht immer) von der Länge des verwendeten Schlüssels ab, die in Bit angegeben wird. Je länger der Schlüssel ist, desto mehr Schlüssel oder Variationen sind möglich.

Thema: Verschlüsselung Fortsetzung

Empfehlungen für symmetrische Verschlüsselung

Twofish oder AES

- **Twofish** ist ein Verschlüsselungsalgorithmus, der bereits 1998 von dem Kryptographieexperten Bruce Schneier veröffentlicht wurde und Schlüsselgrößen von 128, 192 und 256 Bit unterstützt.

  Obwohl der Algorithmus seit vielen Jahren bekannt ist und vielfach analysiert wurde, existieren bisher nur theoretische Angriffsszenarien.

- AES (Advanced Encryption Standard) ist der derzeit weltweit am häufigsten verwendete Verschlüsselungsalgorithmus. Er ging im Jahr 2000 als Sieger aus einem Wettbewerb hervor, den das NIST (National Institute of Standards and Technology) ausgeschrieben hatte, um einen Nachfolger für den geknackten DES-Algorithmus zu finden.

  Auch für AES existieren bisher praktisch nur theoretische Angriffsszenarien.

  Allerdings wird häufig kritisiert, dass der Wettbewerb von einer US-Bundesbehörde organisiert wurde und es zu einer

Einflussnahme durch die NSA (National Security Agency = Auslandsgeheimdienst der USA) gekommen sein könnte.

AES kann auf modernen Prozessoren Geschwindigkeitsvorteile erzielen, da es hardwareseitig durch spezielle Befehlssätze, die sogenannten AES New Instructions (AES-NI), unterstützt wird.

Betriebsmodus

Soll eine Nachricht, die länger als ein Block ist, mit einem Blockchiffre (symmetrische Verschlüsselung) verschlüsselt werden, muss ein entsprechendes Verfahren definiert werden. Das heißt, es wird festgelegt, wie der Schlüssel für die Verschlüsselung weiterer Blöcke verwendet werden soll. Würde man immer den gleichen Schlüssel verwenden, so würde man bei gleichen Daten auch immer die gleichen verschlüsselten Daten erhalten.

 Dies macht der Modus ECB, welchen du deshalb meiden solltest.

Bei Wahlmöglichkeit empfiehlt sich der **GCM** (Galois Counter Mode). Bei `GPG` kommt generell eine Variante des Cipher Feedback Mode (**CFB**) zum Einsatz.

Empfehlungen für asymmetrische Verschlüsselung

RSA (mit mindestens 4096 Bit und DH) oder ECC

Einer der bekanntesten Anwendungsfälle für asymmetrische Verschlüsselung ist GPG. Wenn du dies mit mit RSA einsetzt, solltest du mindestens einen Schlüssel mit 4096 Bit Länge und das Diffie-Hellman-Protokoll (DH) für den Schlüsseltausch verwenden.
Leider bietet RSA mit zunehmender Rechenleistung von Computerclustern immer mehr Angriffsfläche. Um mit einer gewissen Reserve für die nächsten Jahre zu verschlüsseln, müsstest du heute schon eine Schlüssellänge von 15360 Bit verwenden.
Das wiederum würde die Ver-/Entschlüsselung um etwa den Faktor 500 verlangsamen.

Deshalb solltest du einen Blick auf ECC (Elliptic Curve Cryptography) werfen. Obwohl das Verfahren seit einigen Jahren standardisiert und in GPG integriert ist, ist es noch nicht überall implementiert und daher manchmal inkompatibel mit anderen Anwendern/Programmen.

Empfehlungen für Hashverfahren

SHA-2 (zum Beispiel SHA-256 oder SHA-512) oder SHA-3, eventuell auch RIPEMD-160.

Hashverfahren sind eine Art Prüfsumme, die über eine beliebige Menge von Daten berechnet werden kann und sozusagen deren Fingerabdruck darstellt.

Für die Kryptographie geeignete Hashverfahren müssen verschiedene Anforderungen erfüllen, u.a. irreversibel und kollisionsresistent sein. Letzteres bedeutet, dass verschiedene Daten nicht den gleichen Hash haben dürfen.

Weiterführende Informationen zu kryptographischen Hashfunktionen kannst du auf Wikipedia finden.

12 Die Integrität deiner Geräte und deiner Daten

Identifiziere und korrigiere Schwachstellen der von dir verwendeten Geräte und Software.

Sofern du gezwungen bist, Geräte mit Betriebssystemen zu verwenden, welche üblicherweise von Viren bzw. Malware befallen werden können, dann setze zentrale Mechanismen zum Schutz vor schädlichem Code an.

Bedeutet in der Praxis: Zentraler Virenscanner, Überprüfung der E-Mails noch auf dem Mailserver.

Informiere dich regelmäßig über aktuelle Sicherheitswarnungen und Empfehlungen zu den von dir verwendeten Geräten bzw. der von dir verwendeten Software und ergreife zeitnah (!) die notwendigen Maßnahmen.

Maßnahmen

- Installiere alle verfügbaren Updates für die eingesetzte Software, insbesondere Sicherheitsupdates, zeitnah - oder je nach Bedrohungslage innerhalb weniger Tage.
- Wenn du einen Virenscanner verwendest, aktualisiere ihn regelmäßig.

- Wenn du einen Virenscanner verwendest, lass alle Dateien auf deinem Gerät regelmäßig und heruntergeladene, geöffnete oder ausgeführte Dateien in Echtzeit scannen.

- Überwache ein- und ausgehenden Datenverkehr um Angriffe oder Hinweise auf potentielle Angriffe zu erkennen.

  Dies kannst du zum Beispiel besonders gut mit einer sogenannten „personal firewall“, welche nicht nur pauschal den ein- und ausgehenden Netzwerkverkehr regelt, sondern dabei auch noch nach Anwendung differenziert.

  Unter macOS kannst du dafür Little Snitch verwenden.

- Entwickle Methoden, um die unrechtmäßige Nutzung deiner Geräte aufzudecken.
  Dies kann z. B. durch die Überprüfung der Systemlogs auf fehlgeschlagene Anmeldeversuche geschehen.

- Überwache auch die von dir genutzten externen IT-Systeme, wie z.B. Webdienste, auf unrechtmäßige Nutzung.
  Bei den meisten Webdiensten kannst du dir anzeigen lassen, von welchem Standort bzw. von welcher IP-Adresse aus die letzten Zugriffe erfolgt sind oder wie viele Benutzersitzungen gerade aktiv sind.

 Bei einigen (Web-)Diensten ist es an dieser Stelle auch möglich, sich offene Sitzungen von anderen Geräten anzeigen zu lassen. Sofern solche noch aktiv sind und nicht mehr benötigt werden, schließe sie.

13 Überprüfe deine Sicherheit

Überprüfe regelmäßig deine Sicherheitsvorkehrungen bzw. Einstellungen, um festzustellen, ob sie in ihrer Anwendung wirksam sind.

Entwickle Plänen zur Identifizierung, Verringerung oder Beseitigung von Schwachstellen.

14 Wurdest du gehackt?

Überlege dir im Voraus, was du tun würdest, wenn eines deiner Geräte tatsächlich gehackt oder deine Daten kompromittiert, gestohlen, manipuliert oder gelöscht würden.

Teste regelmäßig deine Fähigkeit, auf einen möglichen Sicherheitsvorfall zu reagieren.

Grundsätzlich gibt es zwei Arten von Hackerangriffen:

I) Irgendjemand hackt irgendwen, und in diesem Fall hat es (auch) dich getroffen.

Der Angriff war nicht individuell auf dich als Opfer zugeschnitten, sondern zielte auf die Masse, du warst einer von vielen. Diese Art von Hackerangriffen wird oft sogar mit öffentlich verfügbaren Tools durchgeführt und wäre in den meisten Fällen vermeidbar.

- Wenn du die Ratschläge in diesem Buch befolgst oder in die Tat umsetzt, wird es dich wahrscheinlich kaum treffen können.
- Für den Fall, dass du doch betroffen sein solltest, wirst du mit Hilfe von Backups deiner Daten in kurzer Zeit wieder ein funktionierendes System haben.
- Falls du von einem Verschlüsselungstrojaner betroffen bist:

Sichere auf alle Fälle auch die verschlüsselten Daten, oft können diese in Zukunft wieder entschlüsselt werden.

II) Jemand hackt genau dich

Wow, was für eine Ehre! ;-)

Im Ernst: Du hast dir keine Freunde gemacht, d.h. jemand will dir schaden, oder du hast etwas, das für den anderen sehr wertvoll ist und das er unbedingt haben will.

In jedem Falle hast du es wahrscheinlich mit einem versierten Angreifer zu tun.

Generelles Vorgehen

- Wenn du etwas Verdächtiges entdeckst oder Spuren findest, nimm nach Möglichkeit alle deine Geräte sofort vom Netz, d.h. trenne sie sowohl vom Internet als auch vom lokalen Netzwerk.
- Sobald die Geräte vom Netzwerk getrennt sind, beginne sorgfältig damit, alle Daten und Zustände zu sichern bzw. darauf zu achten, dass sie nicht weiter verändert werden.
- Vorrangiges Ziel muss es sein, herauszufinden, auf welchem Weg der Angreifer eingedrungen ist.
  Nur so kannst du eine Wiederholung in Zukunft vermeiden.

- Ein weiteres wichtiges Ziel sollte es sein, alle vorhandenen Spuren bzw. Beweise möglichst unverändert zu sichern.
  Wenn du die Analyse des Angriffs oder Einbruchs selbst durchführst, analysiere, welche Geräte betroffen sind und welche möglicherweise nicht. Analysiere sowohl verdächtige Programme/Prozesse als auch ungewöhnlichen Datenverkehr.

  Wenn ein erheblicher Schaden entstanden ist oder du den Täter noch nicht kennst, aber hoffst, dass du ihn mit Hilfe anderer ausfindig machen kannst, solltest du erwägen, den Vorfall der Polizei oder einer anderen zuständigen Behörde zu melden.

Grundsätzlich können im Zusammenhang mit individuellen Angriffen im Folgenden zwei mögliche Hypothesen aufgestellt werden.

Annahme A: Der Angreifer hat sein Ziel (noch) nicht erreicht

Falls der- oder diejenige sein Ziel noch nicht vollständig erreicht hat, ist es wahrscheinlich, dass er/sie zurückkehrt.

Für diesen Fall:

- Musst du besser gerüstet sein und
- kannst du dem Angreifer eventuell einen sogenannten „Honigtopf“ hinstellen.

Du kannst auch versuchen, den Angreifer glauben zu lassen, dass er sein Ziel bereits vollständig erreicht hätte.
Falls er dir Schaden zufügen wollte, könntest du zum Beispiel, deinen Computer oder deine EDV-Anlage heimlich weiterlaufen lassen und einen längeren Ausfall vortäuschen.

Annahme B: Der Angreifer hat sein Ziel erreicht

- Versuche den Schaden bestmöglich zu begrenzen
- Baue deine Systeme wieder auf
- Sei das nächste Mal besser gerüstet

15 Lass keine (unnötigen) Daten entstehen

Überlege immer, wenn Daten erzeugt werden, ob sie wirklich notwendig und nützlich sind.

Obwohl es in der Datenschutz-Grundverordnung der Europäischen Union einen Artikel zur Datenminimierung und speziell in Deutschland in § 71 des Bundesdatenschutzgesetzes das Gebot der Datensparsamkeit gibt, sind Dienste, Programme und mobile Anwendungen oft nicht so gestaltet, dass sie generell oder in den Voreinstellungen datenschutzfreundlich sind.

Maßnahmen

- Wenn du bei der Nutzung eines Dienstes oder einer Anwendung um die Angabe persönlicher Daten gebeten wirst, gib nur die unbedingt erforderlichen Daten an.
- Prüfe wann immer möglich auch die Verwendung eines Pseudonyms.
- Wenn du neue Dienste, Programme oder mobile Anwendungen (Apps) verwendest, kontrolliere unmittelbar vor oder bei der ersten Nutzung alle Einstellungsmöglichkeiten, insbesondere diejenigen, die die verarbeiteten Daten oder den Datenschutz betreffen.

 Im Falle von lokalen Programmen bzw. Apps kannst du folgendermaßen vorgehen:

- Programm/App herunterladen/installieren
- Internet- bzw. Netzwerkverbindung trennen
- Programm/App öffnen und gewünschte Einstellungen vornehmen
- Programm/App schließen
- Einstellungen kontrollieren
- Internet- bzw. Netzwerkverbindung wiederherstellen

Thema: Datenspuren

Hinterlasse keine unnötigen Datenspuren (im Internet)

Jeder Mensch hinterlässt bei der Nutzung des Internets, aber auch sonst im täglichen Leben, Datenspuren. Vielen von uns ist gar nicht bewusst, in welchen Situationen unseres Alltags wir Datenspuren hinterlassen.
Deshalb geht es auch hier in erster Linie darum, dass du ein Bewusstsein dafür entwickelst.

- Überlege, in welchen Alltagssituationen du welche Datenspuren hinterlässt?
- Welche davon könntest du vermeiden?
- Welche Bedeutung könnten diese Daten in Zukunft erlangen?

Beachte, dass manche Daten bereits zum Zeitpunkt ihrer Entstehung eine bestimmte Bedeutung oder einen bestimmten Kontext haben, während andere erst in der Zukunft in einen bestimmten Kontext gestellt werden.

Sich im Internet oder auch im Alltag komplett oder weitgehend anonym zu bewegen ist sehr schwierig bis fast unmöglich. Dennoch gibt es einige Vorkehrungen bzw. Verhaltensweisen, die du treffen kannst, um deine Datenspuren so gering wie möglich zu halten.

Vermeidung von Datenspuren im Alltag

Jeder Mensch hinterlässt in seinem Alltag bewusst oder unbewusst Datenspuren. Häufig lassen wir sogar zu, dass Daten entstehen, weil wir im Gegenzug einen (vermeintlichen?) Vorteil sehen oder suggeriert bekommen. Sehr oft sind es auch Annehmlichkeiten, die wir gegen unsere Daten eintauschen.

 In der folgenden Aufzählung liefere ich dir (ohne Anspruch auf Vollständigkeit) eine Liste von Alltagssituationen, in denen du wahrscheinlich schon Daten erzeugt oder hinterlassen hast.

Aufnahmen durch Überwachungskameras

- Praktisch auf Schritt und Tritt werden wir heute gefilmt und damit überwacht.
  Sei es auf öffentlichen Plätzen, auf Straßen und Autobahnen, in Bahnhöfen, auf Flughäfen, in Banken, beim Juwelier oder in anderen Geschäften, aber auch durch (schlecht angebrachte) private Überwachungskameras.
- Neuerdings werden wir auch von Body-Cams der Polizei erfasst.

Telefonieren mit Mobiltelefon

- Die Gespräche könnten von staatlichen Behörden, Geheimdiensten, Telekommunikationsunternehmen oder anderen Dritten aufgezeichnet werden.

- ! Du könntest Zuhörer haben, speziell wenn du zu laut sprichst.
- ! Jedes Handy könnte potentiell als Wanze benutzt werden.
- Metadaten fallen in Form von Positionsdaten an: Das Mobiltelefon ist quasi ein Peilsender.

Bezahlung mit EC-Karte, Kreditkarte

- Wer häufiger oder immer mit der gleichen Karte bezahlt, hinterlässt praktisch eine komplette Route seines täglichen Weges.

Sammeln von Payback Punkten

- Auch beim Sammeln von Payback-Punkten gilt wie beim Bezahlen mit Karte: Du hinterlässt praktisch eine komplette Route deines Alltags. Hinzu kommt beispielsweise die Möglichkeit, auch online Payback-Punkte zu sammeln und so Offline- und Online-Aktivitäten zu verknüpfen.

Diverse andere Kundenkarten

- Für Kundenkarten gilt das gleiche wie oben für Payback beschrieben.

Auf den Namen ausgestellte Veranstaltungstickets

- Hier weiß der Veranstalter sogar, auf welchem Platz du gesessen hast.

Auf den Namen ausgestellte Zugtickets/Flugtickets

- Bei Bahntickets kannst du die Erfassung deines Namens eventuell noch verhindern, indem du sie am Schalter kaufst.
- Bei Flugtickets ist es selbst bei Inlandsflügen praktisch nicht mehr möglich, ohne Angabe des Namens zu fliegen.

Autos mit Blackbox

Bereits heute verfügen die meisten Fahrzeuge über eine Blackbox. Sofern diese nicht bereits als dediziertes Gerät im Fahrzeug verbaut ist, kann in älteren Fahrzeugen bereits die Airbagsteuerung (ab ca. 2015) in nahezu gleichem Umfang Daten aufzeichnen.

Im einzelnen sind dies:

- Geschwindigkeit
- Geographische Lage
- Beschleunigung in Längs- und Querachse

In modernen Fahrzeugen werden jedoch noch viele weitere Ereignisse zu Fahrzeugfunktionen erfasst, z. B:

- Anschnallen bzw. Ablegen des Sicherheitsgurtes
- Betätigung der Bremse
- Setzen des Blinkers
- Ein- und Ausschalten des Lichtes
- Betätigung der Differentialsperre

Dateien mit Metadaten

Verschiedene Programme hinterlassen in den von ihnen erstellten oder bearbeiteten Dateien entweder Daten über den Benutzer oder andere Metadaten, wie z. B. an den Computer angeschlossene Drucker oder die Seriennummer des Programms.

Digitale Bilddateien mit Metadaten
In digitalen Fotos sind in der Regel verschiedene Metadaten gespeichert:

- Geographische Lage von dem Aufnahmeort
- Typ und Modell der Kamera
- Verwendetes Objektiv
- Eingestellte Belichtungszeit, Blende und Brennweite

Vermeidung von Datenspuren im Internet

Erklärung: Was ist eine IP-Adresse?

Eine IP-Adresse ist eine Netzwerkadresse, welche es erlaubt, an einem Netzwerk mit dem Internetprotokoll (IP) teilzunehmen. Dies kann ein privates Netzwerk (private IP-Adresse) oder aber das Internet (öffentliche IP-Adresse) sein.

Die öffentliche IP-Adresse für die Teilnahme am Internet wird in der Regel vom Provider (Internetdienstanbieter) zugewiesen und kann dauerhaft (statisch) oder temporär (dynamisch, für einen bestimmten Zeitraum) verwendet werden.

Bei der Kommunikation mit Gegenstellen oder Diensten im Netz wird immer die öffentliche IP-Adresse übertragen. Durch entsprechende Protokollierung und Zuordnung mit Hilfe des Internetproviders kann so der Anschlussinhaber des genutzten Internetzugangs ermittelt werden.

Erklärung: Was sind Cookies?

Cookies sind kleine Datenmengen, die von einem Server oder Dienst im Internet über den Browser des Nutzers temporär oder dauerhaft auf dessen Gerät abgelegt werden.

Der Zweck ist meist, bei der nächsten Nutzung bestimmte Daten erneut zur Verfügung zu haben oder die Nutzerin bzw. den Nutzer wieder zu erkennen.

Dies ermöglicht natürlich auch die Nachverfolgung der Aktivitäten ein und desselben Nutzers.

 Du kannst das Tracking durch Cookies mit verschiedenen Methoden weitgehendst vermeiden:

- Du stellst deinen Browser so ein, dass er gar keine Cookies akzeptiert (diverse Dienste, die zwingend Cookies benötigen, funktionieren dann aber nicht mehr).
- Du löschst die Cookies nach einem abgeschlossenen Surfvorgang (Besuch **einer** Website).
- Du verwendest für jeden Surfvorgang eine neue virtuelle Maschine oder einen Docker-Container.

Erklärung: Was ist der Referrer?

Ein Browser gibt bei jedem Aufruf einer Webseite an, über welchen Link er zu dieser Webseite gekommen ist. Dies wird als Referrer bezeichnet. Das heißt, wenn du eine Webseite nicht direkt aufrufst oder der Link

anders gestaltet ist, erhält die aufgerufene Seite in der Regel die Information, woher du kommst.

Du kannst die Übertragung des Referrers ebenso wie die Annahme von Cookies in deinem Browser einschränken.

Erklärung: Was ist VPN?

VPN steht für „Virtual Private Network“ und bezeichnet eine in der Regel verschlüsselte Verbindung zwischen Netzwerken an unterschiedlichen Standorten. So kann beispielsweise von einem mobilen Gerät aus eine Verbindung zum Heimnetzwerk oder zum internen Netzwerk einer Firma hergestellt werden.

Von dort aus ist oft auch der Zugang zum Internet möglich.
Bei einem solchen Zugriff auf das Internet sieht der Ziel-Server/Dienst dann nicht mehr die IP-Adresse des ursprünglichen Geräts, sondern die des ausgehenden Netzes.

 Um die Sicherheit zu erhöhen, kannst du von einem mobilen Gerät aus eine verschlüsselte VPN-Verbindung zum Router deines Heimnetzwerks aufbauen und von dort aus auf das Internet zugreifen.

 Im Internet gibt es zahlreiche Anbieter von so genannten VPN-Diensten, über die es möglich ist, z.B.

mit einer IP-Adresse, die einem anderen Land zugeordnet ist, auf das Internet zuzugreifen.

Oft versprechen die Anbieter gleichzeitig Anonymität und erklären, dass sie keine Logfiles über Quell- und Ziel-IP-Adressen führen.

Sei dir aber darüber im Klaren, dass man dies nicht überprüfen kann oder dass der Anbieter von den Behörden verdeckt dazu gezwungen werden kann.

Erklärung: Was ist Tor?

Tor steht für „The Onion Router“ und ist ein gemeinschaftlich betriebener, dezentraler Dienst, der es ermöglicht, im Internet zu surfen, ohne die eigene IP-Adresse preiszugeben.

Tor bzw. das Tor-Netzwerk wird durch eine Reihe von Relais, auch Knoten genannt, realisiert, über die die Zugriffe verschlüsselt weitergeleitet werden, bis sie den „Exit Node“ erreichen, der schließlich auf das Ziel zugreift.
Der Zielserver erhält also nur die IP-Adresse des „Exit Node“ und nicht die des Benutzers. Auch jedes Relay sieht nur die IP-Adresse des vorhergehenden und des nachfolgenden Knotens.

 Falls du dich doppelt absichern möchtest, überlege die Variante VPN durch Tor einzusetzen.

Stichwortverzeichnis