Private Daten

Einfach & sicher

Egon Leitner

Private Daten – Einfach & sicher

Zweite Auflage – Version 14. Januar 2023

Credits:
Icon designed by Smashicons from Flaticon

Inhaltsverzeichnis

Hallo verehrter Leser,

Tobias Hartmann, damals Vorstandschef 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?

Keine Sorge, wenn du bei diesen Fragen etwas ins Grübeln kommst. Nachdem du dieses Buch gelesen und hoffentlich die wesentlichen Grundsätze auch in die Tat umgesetzt hast, wirst du mit Recht behaupten können, dass deine Daten mindestens so sicher wie Gold gelagert sind.

Und du wirst auch einen anderen Blick auf deine Daten bekommen, dein "Goldschatz" wird für dich noch wertvoller werden.

Viel Spaß beim Lesen und bei der Umsetzung wünscht dir dein Autor

Egon Leitner

Das vorliegende kleine Sicherheitshandbuch gibt dir als Privatperson einen Überblick, wie du deine Geräte und Daten sicher handhaben kannst.

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

Sobald du mit dem Thema IT-Sicherheit etwas direkter in Berührung kommst, stellst du dir sicher früher oder später unweigerlich die Frage, welches der verschiedenen verfügbaren Systeme denn das sicherste sei ...?

Ich will an dieser Stelle nicht irgendeinen Glaubenskrieg (Betriebssystem A ist sicherer als Betriebssystem B) vom Zaun brechen, sondern möchte dir einige Überlegungen mit auf den Weg geben.

Sicherheit ist ein Prozess

Du solltest IT-Sicherheit als einen Weg sehen, auf welchen du dich begibst und auf dem du nach und nach Verbesserungen erzielst. Ein Gerät bzw. System gilt nicht von vornherein als sicher (oder auch unsicher), sondern es kommt darauf an, wie es benutzt bzw. konfiguriert wird.

Sicherheit hat viele Komponenten

IT-Sicherheit wird in der Regel nicht durch eine einzelne Komponente oder ein einzelnes Gerät erreicht, sondern hat meistens mehrere Schichten. Dementsprechend wichtig ist es, dass alle Komponenten bzw. Teile eines Systems möglichst gut abgesichert sind.

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

Sicherheit hängt vom Umfeld ab

Die relative Sicherheit eines Systems hängt von seinem Umfeld ab. Damit meine ich, dass ein System in einer relativ freundlichen Umgebung sicher genug, in einer sehr feindlichen Umgebung hingegen nicht ausreichend sicher sein kann. Natürlich hängt dies auch damit zusammen, wie interessant es für jemanden ist, das System anzugreifen, bzw. wieviel Aufwand/Ressourcen in einen Angriff gesteckt wird.

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

Absolute Sicherheit gibt es nicht

Auch diesen Satz hast du bestimmt schon oft gehört. Was du jedoch hauptsächlich berücksichtigen solltest: Stecke nicht sämtliche Energie bzw. Bemühungen in die Abwehr, sondern investiere auch in Ressourcen zur Entdeckung und vor allem zur Wiedererstellung bzw. Eingrenzung von Schäden im Falle eines mehr oder weniger erfolgreichen Angriffs.

Ein Wort zu den genannten Betriebssystemen

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

Als Gegenargument kann man anführen, dass in kleinen (Teil-)Projekten der Quellcode oft nur von wenigen Personen überprüft wird, oder den Quellcode nicht alle, die ihn sich ansehen auch verstehen. Nicht zuletzt kann man oft auch nicht mit absoluter Sicherheit sagen, ob das verwendete Programm auch genau aus diesem Quellcode entstanden ist. Wenn in diesem Buch an der ein oder anderen Stelle ein Betriebssystem genannt wird, hat dies einfach damit zu tun, dass der Autor sich mit `macOS` und mit `Linux` etwas besser auskennt, als mit anderen Betriebssystemen.

Letztlich hängt die Sicherheit eines Systems oder eines Programmes wesentlich von dem Benutzer ab.

Deshalb solltest du bevorzugt solche Systeme benutzen, mit denen du dich gut auskennst.

Anders formuliert: Sorge dafür, dass du dich mit den Systemen, welche du bevorzugt benutzt, auch gut auskennst!

Konventionen in diesem Buch

Ausgabe

```
FileVault is On.
```

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

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

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

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 mit einer Umrandung gekennzeichnet.
Einstellungen > Sicherheit	Besteht eine Eingabe/Konfiguration aus mehreren Schritten, werden diese gemeinsam umrandet dargestellt.
<CTRL-R> <ENTER>	Spezielle Tasten, wie etwa die Steuertasten (Umschalttaste, Tab, Alt, Strg) oder die Eingabetaste werden mit gelber Farbe hinterlegt dargestellt.

Textdarstellung

Linux	Diese Beschreibung gilt für das Betriebssystem Linux.
macOS	Diese Beschreibung gilt für das Betriebssystem macOS von Apple.

Textdarstellung

`Mozilla Firefox`	Diese Beschreibung gilt für ein spezifisches Programm.

Symbole

	Dieses Symbol zeigt eine Warnung oder einen sehr wichtigen Hinweis an.
	Mit diesem Symbol wird darauf hingewiesen, dass der beschriebene Sachverhalt Vor- und Nachteile hat, welche es abzuwägen gilt.
	Mit diesem Symbol werden besondere Tipps und Tricks gekennzeichnet.

2 Dein Bewusstsein für IT- bzw. Daten-Sicherheit

Sei dir bei der Nutzung von Computern bzw. IT-Systemen der mit der Benutzung verbundenen Risiken bewusst.

Stelle sicher, dass du aktuelle Sicherheitsrisiken genauso kennst, wie Standards und Verfahren zur Erhöhung der Sicherheit.

Maßnahme

- Informiere dich regelmäßig über aktuelle Bedrohungen, welche die von dir benutzten Systeme bzw. Plattformen betreffen. Dies kannst du zum Beispiel über die Newsletter von anerkannten öffentlichen Instituten (SANS, BSI, BürgerCERT) oder über spezifische Nachrichtenportale zum Thema Sicherheit (Heise-News).

Ich könnte dir an dieser Stelle und etlichen anderen Stellen diese Buches 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 animieren, aktiv zu werden und das Thema IT-Sicherheit selbst in die Hand zu nehmen.

Deshalb gebe ich dir lieber den Ratschlag, einfach die Suchmaschine deiner Wahl zum Auffinden von aktuellen Informationen zu benutzen - du wirst sehen, es ist nicht so schwierig und lohnt sich!

3 Deine Geräte sind deine Daten

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

Generell solltest eigentlich nur du selbst Zugriff auf deine persönlichen Geräte, wie zum Beispiel dein Mobiltelefon haben. Das heisst, du solltest von der Weitergabe des PINs, auch etwa an deinen Partner, absehen.

Auf eine leider sehr verbreitete Unsitte, Kindern zum Spielen ein persönliches Gerät gänzlich zu Überlassen, solltest du komplett verzichten.

Überlege dir auch, ob und in welcher Form du Gästen Zugriff auf dein WLAN gibst. Es geht nicht nur darum, was sie im Internet alles in deinem Namen anstellen könnten, sondern auch, ob sie sich zum Beispiel in deinem Heimnetzwerk auf unerwünschte Weise “etwas umsehen” …

Maßnahmen

- Gib nur in absoluten Ausnahmefällen anderen Zugriff auf deine persönlichen Geräte bzw. Daten.
- Falls es notwendig war, jemand anderen temporär Zugriff auf ein persönliches Gerät bzw. deine Daten zu geben, entferne die Zugriffsmöglichkeit sobald wie möglich, ändere das entsprechende Kennwort bzw. die entsprechende PIN.

- Falls notwendig, richte auf deinem Router ein gesondertes WLAN (separate SSID) ein, über welches Besucher auf das Internet zugreifen können. Diese Möglichkeit besteht auf den meisten Routern. Auch kannst du darüber Einschränkungen vornehmen, sodass 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.

Beaufsichtige, überwache und schütze deine Geräte sowohl zu Hause, als auch wenn du unterwegs bist.

Dies gilt in öffentlichen Verkehrsmitteln genauso, wie in deinem Auto oder auf Veranstaltungen wie Kongressen oder Messen.

Maßnahmen

- Beaufsichtige besonders in Bus und Bahn deine Geräte, bzw. deine Gepäckstücke ständig.
- Lass deine Geräte nicht für jeden offen sichtbar im Auto liegen.
  Achtung: Lass deine Geräte generell an heißen Tagen möglichst nicht im Kofferraum oder gar im Innenraum des Autos liegen. Dort können Temperaturen von mehr als 60 °C erreicht werden.
-  Überlege dir, ob du den Raum, in welchem du deine technischen Geräte aufbewahrst bzw. betreibst nicht videoüberwachen möchtest.

5 Der Zugriff auf deine Geräte und Daten

Verwende ein starkes Passwort für deine Zugänge und sperre deine Geräte bzw. Sitzungen wenn du sie nicht benutzt.

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

Beschränke den Zugriff auf deinen Computer bzw. auf 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 Netzwerk abrufst.
- Sofern du auf deinem Mobil-Telefon nicht immer aktuellste Daten brauchst, deaktiviere die Hintergrundaktivitäten. Bei iOS ist dies in der Regel bei aktiviertem Stromsparmodus automatisch der Fall.
- Sofern du zu einem gewissen Zeitpunkt keine Netzwerkverbindung benötigst, deaktiviere diese, das heißt ziehe das Netzwerkkabel ab oder versetze dein

Gerät in den sogenannten Flugmodus. Beachte dies auch für Verbindungen über Bluetooth.

- Teile deine Aktivitäten (im Internet) auf, in solche die namentlich mit dir verbunden sind und in solche, die du anonym oder pseudonym durchführen kannst. Verwende je nach Aktivität unterschiedliche Geräte, unterschiedliche virtuelle Systeme oder zumindest unterschiedliche Browser.

Achte dabei auf eine strikte Trennung, d. h. benutze für ein und dieselbe Art der Aktivität immer dasselbe Gerät bzw. virtuelle System.

- Nutze auf deinen Geräten für das tägliche Arbeiten einen nicht privilegierten Benutzer, welcher keine administrativen Rechte besitzt.
- Benutze für administrative Tätigkeiten einen speziell geschützten Admin-Account.
- Vergewissere dich, dass nicht privilegierte Benutzer nicht auf die Funktionen/Dateien des/der privilegierten Benutzer zugreifen können.
- Schränke die Anzahl der möglichen Loginversuche ein, stelle eine Verzögerung bei fehlgeschlagenen Anmeldeversuchen ein bzw. lass dich darüber benachrichtigen.
   Überlege dir, ob du eventuell nach einer größeren Zahl an fehlgeschlagenen Anmeldeversuchen die Daten

auf deinem Gerät automatisch löschen lassen möchtest und konfiguriere dies entsprechend der Möglichkeiten auf deinem System.

- Konfiguriere das automatische Aktivieren des Bildschirmschoners nach einem gewissen Zeitraum der Inaktivität bzw. das zuverlässige sperren der Anzeige und der Anwendersitzung.
  Stelle sicher, dass der Zugriff nur mittels Eingabe des korrekten Passwortes wieder hergestellt werden kann.

- Falls du remote auf deine Geräte zugreifst, stelle sicher dass die Datenübertragung mit starker Kryptografie und der Zugriff ebenso mit Benutzer 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, welche dein Gerät nach aussen aufbaut bzw. benutzt.

- Sei vorsichtig mit fremden Speichergeräten, welche du an deinen Geräten benutzt.
  Sei auch vorsichtig und bedacht mit der Nutzung von deinen Speichergeräten an fremden Systemen.

- Sei besonders vorsichtig damit, welche Informationen du veröffentlichst bzw. ins Internet stellst.
  Lass die zur Veröffentlichung vorgesehenen Informationen von mindestens noch einer Person ausführlich prüfen.

- 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?

Sorge dafür, dass du bzw. auch jeder andere Benutzer beim Verwenden eines Gerätes oder eines Dienstes eindeutig identifiziert wird.

Maßnahmen

- Nutze eine sichere, wenn möglich mehrstufige Authentifizierung, sowohl für privilegierte als auch für nicht privilegierte Benutzerkonten.
- Aktiviere wo mögliche eine Authentifizierung mit zwei Faktoren, eine sogenannte Zwei-Faktor-Authentifizierung (2FA).
  Die Faktoren sind dabei, ein bestimmter Gegenstand, geheimes Wissen oder eine (biometrische) Eigenschaft (Haben, Wissen, Sein).
- Benutze Sicherheitsfragen zur Absicherung von Benutzerkonten, zum Beispiel bei Online-Diensten.

Vor der Benutzung von sogenannten Sicherheitsfragen wird oft abgeraten, da die Antworten darauf meistens aus dem persönlichen Umfeld des Benutzers stammen und sich deshalb leicht erraten lassen.

Dieses Problem lässt sich allerdings leicht umgehen, indem du entweder eine falsche Antwort auf eine Frage vergibst, oder, wie bei manchen Diensten zugelassen, selbst eine Frage mit zugehöriger Antwort vergibst.

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.

- Sofern es auf deinem Gerät bzw. deinem Computer Benutzerkonten gibt, welche nicht oder nicht mehr benötigt werden, entferne diese.

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

- Achte darauf, dass von dir verwendete oder selbst pogrammierte Software während der Authentifizierung keine kompromittierenden Informationen an den Benutzer weitergibt, welche durch Rückschlüsse das Aushebeln bzw. Manipulieren des System erlauben.

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).
  Länge ist dabei noch wichtiger als Komplexität.

-  Stelle dein System so ein, dass es die Verwendung von Kennwörtern mit einer gewissen Länge und Komplexität erzwingt.

- Erstelle bzw. befolge keine sinnlosen Regeln, welche ganz spezifische Anforderungen an Groß-/Kleinschreibung, Zahlen und Sonderzeichen stellen, dafür aber oft relativ kurze Kennwörter erlauben.

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

  Wenn dein Passwort stark und nur dir bzw. autorisierten Personen bekannt ist, gibt es keinen Grund für ständige Änderungen.

Wenn anzunehmen ist, dass das Passwort kompromittiert bzw. Unbefugten bekannt ist, soll es natürlich so schnell wie möglich geändert werden.

Du solltest bei Passwortänderungen dein Passwort komplett auf ein noch nie verwendetes abändern, welches möglichst wenig Ähnlichkeit mit dem bisherigen hat.

Und in diesem Zusammenhang: Du benötigst keinen Mechanismus, welcher das Wiederverwenden von Passwörtern für eine bestimmte Anzahl von Generationen verhindert, wenn du deine 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 Kennwörtern empfiehlt sich ein Programm zu Verwaltung (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 benutz werden.
Sofern du Programme oder Daten aus nicht vertrauenswürdigen Quellen verwenden musst, öffne diese in einer sogenannten Sandbox-Umgebung.

Konfiguriere deine Geräte möglichst so, dass Aufzeichnungen über Aktivitäten von Benutzern und Programmen erstellt werden.
Stelle dabei sicher, dass von unterschiedlichen Benutzern durchgeführte Aktionen eindeutig zuordenbar sind.

 Wäge hierbei den Nutzen und die Gefahr, dass die Aufzeichnungen sensible Informationen beinhalten und in falsche Hände gelangen könnten, gegeneinander ab.

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 nach Möglichkeit alle internen Uhren deiner Geräte mit der Atomzeit (Stichwort NTP).

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

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

Thema: Keylogger

Was ist ein Keylogger?

Ein Keylogger ist eine Soft- oder Hardware, welche alle Eingaben an der Tastatur eines Computers aufzeichnen kann.

Besonders auf fremden Computern, beziehungsweise solchen, die du nicht selbst vollständig kontrollieren kannst, aber auch auf deinen eigenen besteht die Gefahr, dass so gegen deinen Willen vertrauliche Daten von dir 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, speziell die zeitnahe Installation von verfügbaren Sicherheitsupdates.

- Falls du ein Betriebssystem benutzt, auf welchem Viren relevant sind: Einige Virenscanner können auch Software-Keylogger erkennen.

-  Verwende einen Passwortmanager

  Dieser setzt entweder den Benutzer/das Passwort sogar selbständig in das entsprechende Programm beziehungsweise in das entsprechende Feld der Webseite ein, oder du kannst es mit Copy & Paste einfügen.

  Beachte allerdings, dass bei der eventuellen Präsenz eines Keyloggers auch dein Master-Passwort kompromittiert wer- den könnte. Ein Gegenmittel wäre, für den Passwortmanager zusätzlich eine Schlüsseldatei zu verwenden.

- 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 anschließend auf ein nicht relevantes Feld beziehungsweise eine nicht relevante Stelle der Anwendung.
    Beachte dabei, nur den Fokus innerhalb des Programmes zu wechseln und nicht komplett die Anwendung, da einige Keylogger die Eingaben pro Programm separat aufzeichnen.

  - **Benutze eine sogenannte Bildschirmtastatur**
    Dies ist ein – in der Regel vom Betriebssystem zur Verfügung gestelltes – Hilfsprogramm, über welches man nur mit Maus oder Touchpad eine visuell angezeigte Tastatur bedienen kann.

  - **Überwache ausgehende Verbindungen**
    Wie in Kapitel 11 beschriebenen, achte generell auch auf ausgehende Datenverbindungen. Der Keylogger wird wahrscheinlich die gesammelten Eingaben über das Netzwerk nach aussen senden.

8 Deine Geräte, deine Konfiguration

Erstelle, pflege und dokumentiere die Konfiguration deiner Geräte, soweit möglich mit automatischen Werkzeugen zur Konfigurationsverwaltung.

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.
- Schränke die Funktionalität deiner Geräte durch entsprechende Konfiguration auf das ausschließlich Notwendige ein.

- 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.

- Definiere für dich selbst, welche Software du auf deinen Geräten einsetzen willst.

- Definiere, welchen Kriterien eine Software entsprechen muss, damit du sie für den Einsatz auf deinen Geräten als geeignet betrachtest und überprüfe bei jeder neuen Software, ob sie diese Kriterien erfüllt.

- Falls du ein Gerät mit mehreren Benutzern teilst, definiere genau, wer Software installieren/konfigurieren darf und konfiguriere eine Überwachung bzw. eine Benachrichtigung, falls eine nicht erlaubte Installation einer 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.

Lasse, wann immer möglich, notwendige Reparaturen durch den Hersteller selbst durchführen.

Maßnahmen

- Stelle sicher, dass auf jeglichen Geräten, welche du zur Wartung bzw. zur Reparatur gibst, alle Daten entfernt wurden.
- Falls du jemandem bei einer Wartung entfernten Zugriff auf ein Gerät gibst, beaufsichtige die Sitzung und beende sie sofort nach Abschluss der Wartung.
- Achte darauf, wem du bei einer Wartung/Reparatur Zutritt zu deiner Wohnung bzw. deinem Haus gewährst.
- Unterziehe jedes Gerät bei der Rückkehr von einer Wartung/Reparatur einer ausführlichen Überprüfung bzw. einem Test, bevor du es wieder regulär verwendest. Sofern es sich ohne weiteren Verschleiß machen lässt, unterziehe es einem Dauertest, um zu

überprüfen, ob der Fehler/das Problem wirklich beseitigt 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

Entwickle für dich selbst eine Richtlinie zum Umgang mit Datenträgern bzw. Medien, sei es digitaler oder nicht digitaler Art.

Dies betrifft die Erstellung, die Verwaltung sowie die Entsorgung bzw. Vernichtung derselben.

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 geschützt aufbewahren möchtest. Sehr sensible Inhalte auf Papier sind natürlich in einem Bankschließfach oder einem privaten Tresor am besten aufgehoben.

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

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

  Bei Papier ist an dieser Stelle eine Vernichtung mit einem Aktenvernichter mit Kreuzschnitt Pflicht.

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

  Bei Datenträgern gilt das bereits im vorhergehenden Punkt Beschriebene: Sofern der Datenträger mit starker Kryptographie komplett verschlüsselt ist, genügen bei der Entsorgung einfachere Maßnahmen, wie etwa das einfache Überschreiben bzw. Löschen.
  Wenn die Datenträger allerdings unverschlüsselt sind/waren, müssen, in Abhängigkeit zur Sensibilität der Daten, aufwändigere Maßnahmen ergriffen werden.

  Im Zweifel müssen magnetische Datenträger mit sehr sensiblen Daten durch anerkannte technische Methoden, wie zum Beispiel dem professionellen Degaussing komplett vernichtet werden.

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

- **Vorsicht bei Datenträgern mit Speicherzellen:** Durch die ausgeklügelte Technik, mit der die Speicherzellen von dem Controller auf dem Gerät

intern organisiert werden, ist es praktisch von extern nicht mehr möglich, alle Speicherinhalte verlässlich zu Löschen. Somit bleibt bei der Entsorgung im Falle von unverschlüsselten Inhalten praktisch ebenfalls nur mehr die Vernichtung als ausreichende Maßnahme.

- Kennzeichne Medien bzw. Informationen deutlich mit entsprechenden Vermerken zu Handhabung, Schutzbedürftigkeit bzw. Einschränkungen in der Verbreitung.
  Hier geht es darum, dass du selbst und eventuell auch andere die Medien bzw. Informationen sowie gegebenenfalls den Schutzbedarf derselben auf Anhieb eindeutig erkennen können.
  Das heißt jetzt nicht, dass du jedes Dokument nach den Sicherheitsklassen eines Geheimdienstes zuordnen musst, allerdings sollten bei Notwendigkeit zum Beispiel Familienmitglieder erkennen können, wenn sie ein besonders sensibles Dokument von dir in Händen halten oder du solltest, wenn du zum Beispiel mehrere Festplatten/Speichermedien besitzt, den Inhalt derselben durch die vorhandene Kennzeichnung von aussen zuordnen können.

- Bewahre den Überblick, wo du deine Medien verwahrst.

- Setze starke Kryptographie ein, um die auf den digitalen Medien gespeicherten Daten zu schützen. Starke Verschlüsselung schützt den Inhalt deiner Medien zuverlässig.

Bei kleineren Mengen an Information auf Papier kann es ebenfalls sinnvoll sein, diese verschlüsselt abzubilden, zum Beispiel 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
```

Sollte es nicht möglich sein, den gesamten Datenträger bzw. eine gesamte Partition komplett zu verschlüsseln, dann erstelle eine verschlüsselte Container-Datei mit der gewünschten Größe und speichere alle Daten darin. Achte dabei, dass keine Daten ausserhalb des Containers gespeichert werden und dass du auch hierbei starke Kryptographie verwendest.

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

- Kontrolliere bzw. **vermeide** das Benutzen von fremden externen Datenträgern, speziell wenn du den Besitzer nicht eindeutig zuordnen kannst.

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 sich darauf eine Schadsoftware befinden, welche die Software oder die Daten auf deinem Computer verändert oder löscht,

bzw. diese bei nächster Gelegenheit auch von deinem Computer nach aussen überträgt.

Wenn du die Notwendigkeit hast, dass du Datenträger von anderen (bekannten) Personen an dein Gerät anschließen musst, dann stelle sicher, dass dein Gerät ausreichend gegen Schadsoftware geschützt bzw. immun dagegen ist.

Überlege dir, ob du vielleicht ein weiteres, unkritisches Gerät besitzt, wo du den Datenträger anschließen könntest.

Thema: Backup

- Erstelle regelmäßig Backups.
- Achte darauf, dass deine Backups möglichst aktuell sind.
- Erstelle zwei oder mehr Sicherungen deiner Daten und halte sie an getrennten Orten vor.

  Ich habe für meine Backups den Grundsatz:

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

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

  “Vertraulichkeit, Integrität und Verfügbarkeit!”
- Schütze deine Backupdaten durch Verschlüsselung, speziell an externen Speicherorten.
  Sofern du starke kryptographische Methoden einsetzt, sind die Vertraulichkeit und die Integrität deiner Daten selbst eigentlich immer gewährleistet. Bedenke aber, dass beim Übertragen der Daten auch immer Meta-Daten

entstehen, die dann ihrerseits eventuell wieder sensibel sein können.

- Berücksichtige beim externen Speichern deiner Daten (Cloud) auch in welchem Land die Daten letztlich liegen, bzw. welche Gesetzgebung 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, möglichst gut ab, am besten durch starker Verschlüsselung.

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

Maßnahmen

- Verwende bevorzugt Software, welche bereits von Haus aus eine Rollen-Trennung von Benutzer und Administrator 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 dir, ob es möglich bzw. sinnvoll ist, verschiedene Geräte in unterschiedliche Netzwerke mit unterschiedlichem Sicherheitsniveau zu legen.

- 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 den getrennten Netzwerken aufbaut.

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

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

- Trenne Netzwerkverbindungen einer Kommunikationssitzung nach 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 Generierung, Verteilung, Speicherung und Löschung vorgehst.
  Bei der Erzeugung von GPG-Schlüsseln etwa, erstelle zeitgleich einen Rückrufschlüssel und bewahre deinen privaten Schlüssel sorgfältig auf.

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

- Achte darauf, dass niemand unbemerkt von aussen dein Geräte aktivieren bzw. benutzen kann.

Achte hier im Besonderen auf gegebenenfalls in dein Gerät integrierte Kameras oder Mikrofone.

Bei tragbaren Computern oder Tablets kannst du die Front- Kamera oft sehr einfach mit einem Stück matten und leicht haftenden Klebeband abdecken, sobald sie nicht gebraucht wird.

- Überwache und beschränke die Ausführung von mobilem Code bzw. die Technik/Produkte zum Ausführen von mobilem Code.
  Hiermit sind zum Beispiel Javascript und ähnliches, aber auch Postscript und PDF gemeint.
  Möglicherweise war dir bislang nicht bekannt, dass in PDF komplette Programme eingebettet bzw. über den Betrachter dann ausgeführt werden können ...

- Wähle die Nutzung von VoIP-Technologien (FaceTime, WhatsApp, Skype/Teams, Zoom usw.) mit Bedacht und setze hier möglichst solche ein, die eine Ende-zu-Ende-Verschlüsselung integriert haben.

- Schütze die Authentizität von Kommunikationssitzungen. Vergewissere dich, dass dich dein Browser zuverlässig warnt, wenn das Zertifikat einer Webseite und deren Name nicht überein stimmen.

- 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 dabei, deine Daten vertraulich und integer zu halten.
Aber was ist starke Verschlüsselung?
Unter starker Verschlüsselung versteht man Algorithmen und Methoden, die Inhalte nach dem aktuellen Stand der Technik derart gut schützen, dass sie vor kryptografischer Analyse und Entschlüsselung sicher sind.

Generell wird bei 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, welches einen öffentlichen Schlüssel zum Verschlüsseln und einen privaten Schlüssel zum Entschlüsseln umfasst. Dabei kann der öffentliche Schlüssel, wie der Name schon sagt, problemlos offen gelegt werden, der private Schlüssel muss hingegen geheim gehalten werden. 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 bzw. die technischen Hintergründe wissen 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, welche in Bit angegeben wird. Je länger dieser Schlüssel, um so mehr mögliche Schlüssel bzw. Variationen gibt es.

Thema: Verschlüsselung Fortsetzung

Empfehlungen für symmetrische Verschlüsselung

Twofish oder AES

- **Twofish** ist ein von dem Crypto-Experten Bruce Schneier bereits im Jahre 1998 veröffentlichter Verschlüsselungsalgorithmus, welcher Schlüsselgrößen von 128, 192 und 256 Bit unterstützt.

  Obwohl der Algorithmus bereits viele Jahre öffentlich ist und vielfach analysiert wurde, existieren bislang nur theoretische Angriffsszenarien.

- **AES** (Advanced Encryption Standard) ist der aktuell weltweit am häufigsten benutzte Verschlüsselungsalgorithmus. Er ging im Jahr 2000 als Sieger aus einem Wettbewerb hervor, welcher vom NIST (National Institute of Standards and Technology) ausgerufen wurde um einen Nachfolger für den geknackten Algorithmus DES zu finden.

  Auch für AES existieren praktisch bislang nur theoretische Angriffsszenarien.

  Allerdings wird oft kritisiert, dass der Wettbewerb von einer Bundesbehörde der USA veranstaltet wurde und es eine Beeinflussung

durch die NSA (National Security Agency = Auslandsgeheimdienst der Vereinigten Staaten) gegeben haben könnte.

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

Betriebsmodus

Wenn mit einer Blockchiffre (symmetrische Verschlüsselung) eine Nachricht verschlüsselt werden soll, welche länger als ein Block ist, muss dafür ein entsprechendes Verfahren festgelegt werden. Dies bedeutet, es wird festgelegt, wie der Schlüssel für die Verschlüsselung weiterer Blöcke verwendet werden soll. Würde man immer den gleichen Schlüssel verwenden, würden sich bei gleichen Daten auch immer die gleichen chiffrierten Daten ergeben.

 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 der stetig wachsender Rechenleistung von Computerclustern immer mehr Angriffsfläche. Um mit einiger Reserve für die nächsten Jahre zu verschlüsseln, müsstest du heute schon eine Schlüssellänge von 15360 Bit verwenden.
Dies wiederum würde eine Verlangsamung der Ver-/Entschlüsselung um ca. den Faktor 500 mit sich bringen.

Deshalb solltest du einen Blick auf ECC (Elliptic Curve Cryptography) werfen. Auch wenn das Verfahren schon seit einigen Jahren standardisiert und in GPG integriert ist, ist es aber noch nicht überall umgesetzt und die Nutzung deshalb manchmal inkompatibel zu anderen Benutzern/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, welche über ei- ne beliebige Menge von Daten berechnet werden können und sozusagen den Fingerabdruck derselben darstellen.

An für Kryptographie geeignete Hashverfahren werden diverse Anforderungen gestellt, unter anderem, dass sie nicht reversibel sind und dass sie resistent gegen Kollisionen sind. Letzteres bedeutet, dass unterschiedliche Daten nicht denselben Hash haben können.

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 eingesetzten Geräte bzw. 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 am Mailserver.

Lass dich regelmäßig von externen Angeboten über aktuelle Sicherheitswarnungen und Empfehlungen zu den von dir verwendeten Geräten bzw. zu der eingesetzten Software informieren und ergreife zeitnahe (!) die notwendigen Aktionen.

Maßnahmen

- Installiere alle für die von dir eingesetzte Software verfügbaren Updates, speziell Sicherheitsupdates, zeitnahe - beziehungsweise je nach Bedrohungslage - innerhalb von wenigen Tagen.
- Falls du einen Virenscanner einsetzt, aktualisiere ihn regelmäßig.

- Falls du einen Virenscanner einsetzt, lasse alle Dateien auf deinem Gerät periodisch und heruntergeladene, geöffnete oder ausgeführte Dateien in Echtzeit prüfen.

- 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 zur Erkennung von unrechtmäßiger Nutzung deiner Geräte.
  Dazu kannst du beispielsweise die Systemlogs auf fehlgeschlagene Anmeldeversuche untersuchen.

- Überwache auch die von dir genutzten externen IT-Systeme, wie etwa Webdienste auf unrechtmäßige Nutzung.
  Bei den meisten Webdiensten kannst du dir anzeigen lassen, von welchem Standort bzw. welcher IP-Adresse aus die letzten Zugriffe getätigt wurden, bzw. wieviele Benutzersitzungen aktuell aktiv sind.

   Bei einigen (Web-)Diensten ist es an dieser Stelle auch möglich, dass du dir offene Sitzungen von

anderen Geräten anzeigen lässt. 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 Pläne, um Schwachstellen zu erkennen, zu reduzieren oder zu beseitigen.

14 Wurdest du gehackt?

Überlege dir im Vorfeld, was du machen würdest, wenn eines deiner Geräte wirklich gehackt würde bzw. Daten von dir kompromittiert, entwendet, manipuliert oder gelöscht würden.

Teste regelmäßig deine Fähigkeit auf einen etwaigen Sicherheitsvorfall reagieren zu können.

Grundsätzlich gibt es zwei Arten von Hackerangriffen:

I) Irgendjemand hackt irgendjemand, und in diesem Falle hat es eben (auch) dich getroffen

Der Angriff war nicht individuell auf dich als Opfer zugeschnitten, sondern auf die breite Masse ausgerichtet, du warst einer von vielen. Diese Art von Hackerangriffen werden oft sogar mit öffentlich verfügbaren Werkzeugen durchgeführt und ließen sich meistens vermeiden.

- Wenn du die Ratschläge in diesem Buch befolgt bzw. umgesetzt hast, wird es dich vermutlich kaum treffen können.
- Falls du doch betroffen bist, wirst du mittels der Backups von deinen Daten schnell wieder ein funktionierendes System hergestellt 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, das heißt jemand will dir Schaden zufügen, oder du besitzt etwas, was für dein Gegenüber sehr wertvoll ist und er/sie unbedingt haben will.

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

Generelles Vorgehen

- Wenn du etwas Verdächtiges entdeckst bzw. Spuren findest, nimm möglichst alle deine Geräte sofort vom Netz, das heißt, trenne sie sowohl vom Internet als auch vom lokalen Netzwerk.
- Sobald die Geräte vom Netzwerk getrennt sind, beginne vorsichtig damit, alle Daten und Zustände zu sichern bzw. darauf zu achten, dass sie nicht weiter verändert werden.
- Oberstes Ziel muss es sein, herauszufinden, über welchen Weg der Angreifer eindringen konnte. **Nur so kannst du verhindern, dass es in Zukunft wieder passiert.**

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

  Falls ein erheblicher Schaden verursacht wurde, oder dir der Angreifer noch nicht bekannt ist, und du die Hoffnung hast, dass du mit Hilfe von anderen den oder die Täter ausfindig machen kannst, ziehe in Betracht, den Vorfall der Polizei oder einer anderen geeigneten, offiziellen Behörde zu melden.

Prinzipiell kannst du im Zusammenhang mit individuellen Angriffen im Weiteren zwei mögliche Annahmen treffen.

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, er hätte sein Ziel bereits vollständig erreicht.
Falls er dir Schaden zufügen wollten, könntest du beispielsweise, deine Computer bzw. IT im verborgenen weiterführen 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 dir immer wenn Daten entstehen, ob diese wirklich notwendig oder hilfreich sind.

Obwohl es in der Datenschutz-Grundverordnung der Europäischen Union einen Artikel zur Datenminimierung, und speziell in Deutschland im Paragraphen 71 des Bundesdatenschutzgesetzes das Gebot der Datensparsamkeit gibt, sind Dienste, Programme und mobile Applikationen dennoch oft so nicht so gestaltet, dass sie generell bzw. die Voreinstellungen datenschutzfreundlich sind.

Maßnahmen

- Wenn du bei der Nutzung eines Dienstes oder einer Anwendung aufgefordert wirst, persönliche Daten anzugeben, gibt nur die absolut 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 Verwendung alle Einstellungsmöglichkeiten, speziell jene welche die verarbeiteten Daten bzw. den Datenschutz betreffen.

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

 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 Benutzung des Internets, aber auch sonst im täglichen Leben Datenspuren.
Vielen von uns ist gar nicht bewusst, in welchen Situationen im Alltag wir Datenspuren erzeugen.
Deshalb geht es auch hier in erster Linie darum, dass du ein Bewusstsein dafür entwickelst.

- Überlege dir, 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 bzw. einen bestimmten Kontext haben, andere eventuell aber erst in Zukunft in einen bestimmten Kontext gestellt werden.

Sich im Internet oder auch im Alltag komplett oder weitgehendst anonym zu bewegen ist sehr schwer bis fast unmöglich. Dennoch kannst du einige Vorkehrungen bzw. Verhaltensweisen ergreifen, um

deine Datenspuren wo weit wie möglich zu reduzieren.

Vermeidung von Datenspuren im Alltag

Jeder Mensch hinterlässt im Alltag Datenspuren, bewusst oder unbewusst. Oft erlauben wir sogar selbst das Entstehen von Daten, weil wir im Gegenzug einen (vermeintlichen?) Vorteil sehen oder einen solchen suggeriert bekommen. Sehr häufig sind es auch Annehmlichkeiten gegen die wir unsere Daten eintauschen.

 In der folgenden Aufzählung liefere ich dir (ohne Anspruch auf Vollständigkeit) eine Liste von Alltagssituationen, bei welchen du wahrscheinlich schon Daten generiert bzw. hinterlassen hast.

Aufnahmen durch Überwachungskameras

- Praktisch auf Schritt und Tritt werden wir heutzutage gefilmt und somit überwacht. Ob auf öffentlichen Plätzen, auf Straßen und Autobahnen, an Bahnhöfen, auf Flughäfen, in Banken, beim Juwelier oder in anderen Geschäften und auch durch (falsch angebrachte) private Überwachungskameras.
- Neuerdings werden wir auch auch durch die Body-Cams von Polizisten erfasst.

Telefonieren mit Mobiltelefon

- Die Gespräche könnten von staatlichen Behörden, Geheimdiensten, Telekommunikationsunternehmen oder auch

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

Bezahlung mit EC-Karte, Kreditkarte

- Wenn du häufiger bzw. ständig mit der selben Karte bezahlst, hinterlässt du praktisch eine komplette Route deines Alltags.

Sammeln von Payback Punkten

- Auch beim Sammeln von Payback Punkten gilt wie bei dem Bezahlen mit Karte, du hinterlässt praktisch eine komplette Route deines Alltags. Hierbei kommt noch hinzu, dass man auch online Payback-Punkte sammeln kann und so die Offline- und Online-Aktivitäten verknüpfte werden können.

Diverse andere Kundenkarten

- Für Kundenkarten gilt dasselbe, wie oben bei 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 Zugtickets kannst du die Erfassung deines Namens eventuell noch verhindern, indem du sie am Schalter kaufst.
- Für Flugtickets ist es praktisch auch bei Inlandsflügen nicht mehr möglich, ohne die Angabe des Namens zu fliegen.

Autos mit Blackbox

Bereits heutzutage haben die meisten Autos eine Blackbox. Sofern diese nicht bereits als dediziertes Gerät im Auto verbaut ist, zeichnet in älteren Autos unter Umständen bereits die Airbag-Steuerung (seit in Etwa dem Jahr 2015) fast in gleichem Maße Daten auf.

Im einzelnen sind dies:

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

Bei modernen Fahrzeugen werden aber noch viele weitere Ereignisse zu Fahrzeugfunktionen erfasst, zum Beispiel:

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

- Betätigung der Differentialsperre

Dateien mit Metadaten
Diverse Programme hinterlassen in den von ihnen erstellten oder bearbeiteten Dateien entweder sogar Daten von dem Benutzer oder aber andere Metadaten, wie zum Beispiel am Computer angeschlossene Drucker oder die Seriennummer des Programmes.

Digitale Bilddateien mit Metadaten
In Digitalen Fotos sind meistens diverse Metadaten abgespeichert:

- 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 oder aber das Internet sein.

Die IP-Adresse zur Teilnahme am Internet wird in der Regel vom Provider (Internetanbieter) zugewiesen und kann dauerhaft (statisch) oder temporär (dynamisch, für einen bestimmten Zeitraum) benutzt sein. Diese IP-Adresse wird auch oft öffentliche IP-Adresse genannt.

Bei der Kommunikation mit Gegenstellen bzw. Diensten im Netzwerk wird immer die öffentliche IP-Adresse übertragen. Über eine entsprechende Protokollierung und einer Zuordnung mit Hilfe des Internetanbieters kann so der Anschlussinhaber des verwendeten Internetzuganges ermittelt werden.

Erklärung: Was sind Cookies?

Cookies sind kleine Mengen von Daten, welche von einem Server bzw. einem Dienst im Internet über den Browser des Benutzers temporär oder dauerhaft auf dessen Gerät abgelegt werden.

Der Zweck ist meist um bestimmte Daten bei der nächsten Nutzung bereits vorliegen zu haben oder den Benutzer wieder zu erkennen.

Dies ermöglicht natürlich auch ein Tracking ein und desselben Benutzers.

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

- Du stellst deinen Browser so ein, dass er überhaupt keine Cookies annimmt (diverse Dienste, welche zwingend Cookies erfordern, werden allerdings nicht mehr funktionieren).
- Du löschst die Cookies nach einem in sich abgeschlossenen Surf-Vorgang (Besuch **einer** Website).
- Du verwendest für jeden Surf-Vorgang eine neue virtuelle Maschine bzw. einen Docker-Container.

Erklärung: Was ist der Referrer?

Ein Browser gibt bei jedem Aufruf einer Webseite mit, über welchen Link er dort hin gelangt ist. Dies ist der sogenannte Referrer. Das heißt, sofern du eine Website nicht direkt aufrufst, oder der Link

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

Auch die Weitergabe des Referrer kannst du, ebenso wie die Annahme von Cookies, in deinem Browser einschränken.

Erklärung: Was ist VPN?

VPN steht für „Virtual Private Network“ und bezeichnet eine meist verschlüsselt hergestellte Verbindung zwischen Netzwerken, die an unterschiedlichen Orten liegen. So kann zum Beispiel von einem mobilen Gerät aus eine Verbindung zu dem Heimnetzwerk oder zum internen Netzwerk einer Firma hergestellt werden.

Von dort aus ist es dann oft auch möglich, auf das Internet zuzugreifen.
Bei einem derartigen Zugriff auf das Internet sieht dann der Ziel-Server/-Dienst nicht mehr die IP-Adresse des ursprünglichen Gerätes, sondern jene des ausgehenden Netzwerkes.

Zu Erhöhung der Sicherheit kannst du von einem mobilen Gerät aus eine verschlüsselte VPN-Verbindung zu dem Router in deinem Heimnetzwerk herstellen und dann von dort aus auf das Internet zugreifen.

 Es gibt im Internet zahlreiche Anbieter von sogenannten VPN-Diensten, über welche es dann möglich ist, etwa mit einer einem anderen Land zugeordneten IP-Adresse auf das Internet zuzugreifen.

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

Sei dir aber bewusst, dass du dies nicht verifizieren kannst oder der Anbieter von Behörden verdeckt zu einer solchen Erfassung gezwungen werden könnte.

Erklärung: Was ist Tor?

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

Tor bzw. das Tor-Netzwerk wird durch eine Reihe von Relais, auch Knoten genannt, realisiert, über welche die Zugriffe verschlüsselt weitergeleitet werden, bis sie zu dem „Exit Node“ gelangen, welcher letztlich auf das Ziel zugreift.
Der Ziel-Server erhält also nur die IP-Adresse des „Exit Node“ und nicht jene des Benutzers. Auch jedes Relais

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