Cybermonster

und

wie man sie zähmt

Die Gefahren im Internet

und wie man sich davor schützen kann

Jeff Valmorbida

7C11 – Ansemburg

LEM 2025-2026

Tutor: M. Jhang Majerus

Inhaltsverzeichnis

1. Einleitung 1
2. Darstellung digitaler Daten 2
   - 2.1 Taktfrequenz einer CPU 3
   - 2.2 Start eines Computers 3
3. Verschiedene Gefahren erklärt 5
   - 3.1 Identitätsmissbrauch 5
     - 3.1.1 Fake-Websites 5
     - 3.1.2 Abfangen von Daten 5
   - 3.2 Phishing-Arten 6
     - 3.2.1 Klassisches Phishing 6
     - 3.2.2 Spear-Phishing 7
     - 3.2.3 CEO-Fraud 7
     - 3.2.4 Smishing 8
     - 3.2.5 Vishing 8
     - 3.2.6 Tampering 9
   - 3.3 Datendiebstahl 10
     - 3.3.1 Persönlicher Daten 10
     - 3.3.2 Geschäftliche Daten 10
   - 3.4 Malware-Arten 10
     - 3.4.1 Viren 10
     - 3.4.2 Würmer 11
     - 3.4.3 Trojaner 11
     - 3.4.4 Ransomware 12
     - 3.4.5 Spyware 12
     - 3.4.6 Scareware 13
     - 3.4.7 Kryptominer 14
     - 3.4.8 Adware 14
   - 3.5 DLL-Dateien 15
4. Gefahren im Internet vermeiden 16
   - 4.1 Schutz vor Identitätsmissbrauch 16
   - 4.2 Schutz vor Phishing 16
   - 4.3 Schutz vor Datendiebstahl 16
   - 4.4 Schutz vor Malware 17

5. Technische Schutzmaßnahmen gegen Cybergefahren 18
5.1 Antivirus-Software 18
5.2 VPN 18
5.3 Firewall 19
6. Verhalten bei einer Malware-Warnung 20
6.1 Schritt 1 20
6.2 Schritt 2 20
6.3 Schritt 3 20
6.4 Schritt 4 20
7. Eigene Erfahrungen mit Gefahren im Internet 22
8. Schlussfolgerung 25
9. Quellenangaben 26

1. Einleitung

In diesem *Travail Personnel* beschäftige ich mich mit dem Thema „Gefahren im Internet und wie man sich davor schützen kann“. Ich habe dieses Thema gewählt, weil das Internet heute ein wichtiger Teil unseres Alltags ist und von sehr vielen Menschen täglich genutzt wird, besonders von Jugendlichen. Man kann damit kommunizieren, lernen, spielen oder Videos anschauen. Das Internet bietet viele Möglichkeiten und erleichtert viele Dinge im Alltag.

Trotzdem gibt es im Internet auch zahlreiche Gefahren, die man nicht immer sofort erkennt. Dazu gehören zum Beispiel Schadsoftware, Betrugsversuche oder gefälschte Nachrichten, mit denen Menschen getäuscht werden sollen. Viele Nutzer wissen nicht genau, worauf sie achten müssen, und geraten dadurch schnell in Schwierigkeiten.

Mit dieser Arbeit möchte ich erklären, welche Gefahren im Internet existieren und wie man sich davor schützen kann. Es ist wichtig, aufmerksam zu sein und die Risiken zu kennen, damit man das Internet sicher nutzen kann. Außerdem werde ich zeigen, wie man sich verhält, wenn man Opfer von Schadsoftware oder Betrug wird. Zum Schluss werde ich auch über meine eigenen Erfahrungen im Internet sprechen.

2. Darstellung digitaler Daten

Ein Computer benutzt **Bits** und **Bytes** um Informationen zu verarbeiten oder zu speichern. Dabei ist ein Bit die kleinste Informationseinheit eines Computers. Ein Bit ist eine Einheit zur Informationsdarstellung, die nur zwei Werte annehmen kann (0 und 1).

Beispiel:

https://www.pamono.at/schreibtischlampe

Lampe ein = **1 Bit**

https://www.handmadekultur.de/lampe_aus_rohren

Lampe aus = **0 Bit**

Ein **Byte** ist eine Einheit aus **8 Bits**.

Beispiel:

Es gibt **8 kleine Lampen**:

Jede Lampe kann **an** sein (**1**) oder **aus** (**0**).

Ein Byte ist also wie eine Reihe von 8 Lampen, die zusammen eine Information weitergeben, hier durch ein Lichtzeichen. Im oberen Beispiel mit den 8 Lampen entspricht das 8x1.

Diese Tabelle zeigt die Vielfach der Einheit Byte:

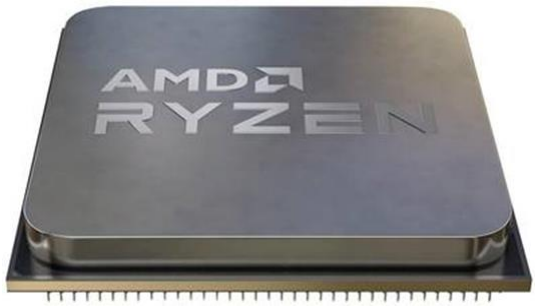
Bezeichnung	Bedeutung	Potenzschreibweise
1 Byte	= 8 Bit	= 10^0 Byte
1 Kilobyte (KB)	= 1000 Byte	= 10^3 Byte
1 Megabyte (MB)	= 1000 KB	= 10^6 Byte
1 Gigabyte (GB)	= 1000 MB	= 10^9 Byte
1 Terabyte (TB)	= 1000 GB	= 10^{12} Byte

Bildquelle: inf-schule | Binärdarstellung von Daten » Fachkonzept - Bit/Byte

2.1 Taktfrequenz einer CPU

Das Herzstück und "Gehirn" eines Computers ist die Central Processing Unit (kurz, die CPU).

Diese zentrale Recheneinheit ist der Haupt-Prozessor deines Computers und ist für die Verarbeitung von Daten, die Ausführung von Befehlen und die Steuerung anderer Computerkomponenten zuständig



AMD Ryzen 3 - 4300G - (3.8 GHz-4 Kerne-8 Threads)
https://asset.conrad.com/media10/isa/160267/c1/-/de/002851242PI00

Die CPU bestimmt, wie schnell Programme sich öffnen und durchführen lassen, aber auch, dass sie reibungslos laufen.

Es gibt heutzutage viele Methoden, um die CPU-Leistung zu messen. Die Taktfrequenz ist allerdings der wichtigste Wert. Also eine höhere Taktfrequenz bedeutet auch eine schnellere CPU. Eine CPU verarbeitet jede Sekunde Milliarden von Befehlen. Einige dieser Befehle umfassen eine einfache Rechenoperation, wobei andere umso komplizierter sind.

Die Taktfrequenz misst die Anzahl an Takten, die von der CPU pro Sekunde durchgeführt werden. Heute werden diese meist *in Gigahertz* (GHz) angegeben, also *in Milliarden Takten pro Sekunde*.

Beispiel:

Die hier abgebildete AMD-Ryzen CPU hat eine **Taktfrequenz von 3,8 GHz**.
Deshalb kann sie **3,8 Milliarden Takte pro Sekun**de ausführen.

2.2 Start eines Computers

Der Start eines Computers verläuft in mehreren Schritten. Direkt nach dem Einschalten wird ein einfaches kleines Programm aus einem Festwertspeicher (ROM, *Read-Only Memory*) gelesen.

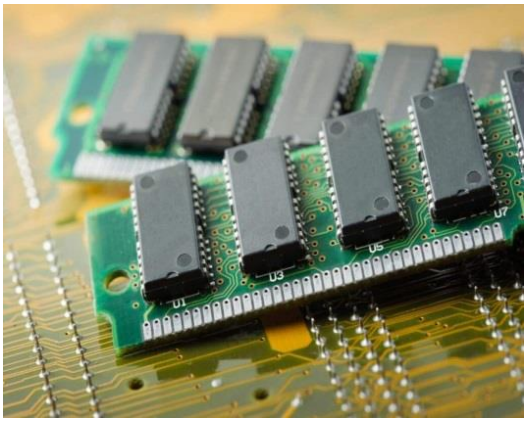


Foto eines Festwertspeichers
https://www.it-service24.com/lexikon/e/edo-dram

Dieses Programm erlaubt, dass ein komplexeres Programm aus dem ROM starten kann: das BIOS (*Basic Input/Output System*), bei älteren PCs oder das UEFI (*Unified Extensible Firmware Interface*) bei moderneren PCs. Beide bilden die Schnittstelle zwischen **Hardware**[1] und **Betriebssystem**[2].

Nach dem Start vom BIOS oder UEFI wird der POST (*Power-On Self-Test*) durchgeführt. Dieser prüft ob die Hardware und angeschlossene Medien wie Festplatten, USB, usw. richtig funktionieren.

Nach dieser Stufe fängt die Firmware an, nach startfähigen Medien zu suchen.

- Beim BIOS sucht die **Firmware**[3] nach einer speziellen Markierung (der Hexa-Signatur: (`0xAA55`). Wird sie gefunden, erkennt das BIOS einen *Master Boot Record*[4] (MBR) mit ausführbarem Code.
- Beim UEFI sucht die Firmware nach einer speziellen Partition (der ESP-EFI System Partition). Sie schaut dort im Ordner (/EFI/BOOT/) nach einer startfähigen Datei (z. B. `bootx64.efi`).

  ⟶ Wenn die Firmware den gültigen Boot-Code nun nicht findet erscheint eine Fehlermeldung (z.B.: *No bootable device found*).

  ⟶ Wird der Boot-Code aber erfolgreich gefunden, so wird die Suche abgebrochen und die Firmware übergibt die Kontrolle an den Bootloader. Ab hier beginnt das „*Chain-Loading*".

Nach diesem Schritt wird die Kontrolle an die CPU übergeben. Die CPU springt zum *Entry Point* (Startpunkt) des Codes. Ab diesem Moment hat nicht mehr BIOS/UEFI das Sagen, sondern das Programm, das sich in der Datei befindet.

Danach folgt die Hardware-Initialisierung, wobei der Bootloader UEFI-Dienste nutzt, um die Grafikkarte, die Tastatur und die Laufwerke anzusprechen.

Im zweitletzten Schritt wird der **Kernel**[5] geladen. Dies ist der entscheidende Schritt, da der Kernel das wichtigste Programm des Betriebssystems ist. Der *Bootloader* sucht dabei nach dem Betriebssystem-Kern und startet ihn. Sobald der Kernel läuft, übernimmt er die Kontrolle über die Hardware und lädt die benötigten Treiber, um Komponenten wie Grafikkarten, Drucker, Mäuse und Netzwerkkarten zu steuern. Zum Schluss erscheint der Startbildschirm.

Kurioses – *Fun facts*:

- Bei Computern vor den 1970er war oft kein Festwertspeicher verbaut. Dann musste man den ersten Schritt des Startens von Hand in den Speicher schreiben, sodass das System dann von externen Speichergeräten eingelesen werden konnte.
- Der Begriff Booten (Hochfahren) leitet sich von englischen Wort Bootstraps (Stiefelschlaufen) ab und beschreibt dem Prozess der Selbstaktivierung eines Computers. Da das System zum Starten bereits auf Funktionen angewiesen ist, die es erst im laufenden Betrieb vollständig bereitstellt, gleicht dieser Vorgang dem Sprichwörtlichen Versuch, sich an den eigenen Haaren aus einem Sumpf zu ziehen.

---

[1] Hardware sind Dinge im Computer die man berühren kann wie die CPU, Grafikkarte oder den Arbeitsspeicher.

[2] Ein Betriebssystem ist das Programm, das den Computer/Smartphone startet und es ermöglicht, ihn zu benutzen. (Windows, Android, IOS, Linux, ...).

[3] Eine Firmware ist ein fest eingebautes Programm, das ein Gerät startet und steuert.

[4] Der Master Boot Record sagt dem Computer beim Einschalten, wie er starten soll.

[5] Der Kernel ist das Herz des Betriebssystems, das beim Starten geladen wird und den Computer steuert.

3. Verschiedene Gefahren erklärt

Im Folgenden werde ich erklären, auf welche Gefahren man im Internet stoßen kann. Dazu zählen unter anderem Identitätsmissbrauch, Abfangen von Daten, Schadprogramme (Malware) sowie Betrugsmaschen wie Phishing, die Nutzerdaten gezielt ausnutzen.

3.1 Identitätsmissbrauch

Eine der häufigsten Gefahren im Internet ist der Identitätsmissbrauch. Dabei werden persönliche Daten unter anderem über gefälschte Webseiten oder durch das unbemerkte Abfangen von Daten gestohlen.

3.1.1 Fake-Websites

Mithilfe des Internets können Betrüger mit gefälschten Websites Leute betrügen. Für Betrüger ist es sehr leicht solche Fake-Websites zu erstellen. z. B. eine Bank-Webseite.

Beispiel:

Eine Frau möchte ihren Kontostand prüfen. Deshalb geht sie auf eine echt aussehende Bankwebseite. Sie gibt ihre Konto-Informationen an und ihr Passwort. Danach bekommt sie die Nachricht, dass es nicht funktioniert hat. Ab diesem Moment haben Betrüger Zugriff auf ihr Konto, weil sie ihre Daten gestohlen haben.

Dieses Bild zeigt eine Fake-Webseite an.

Bildquelle: https://cwatch.comodo.com/blog/website-security/how-to-spot-a-fake-fraudulent-or-scam-website

3.1.2 Abfangen von Daten

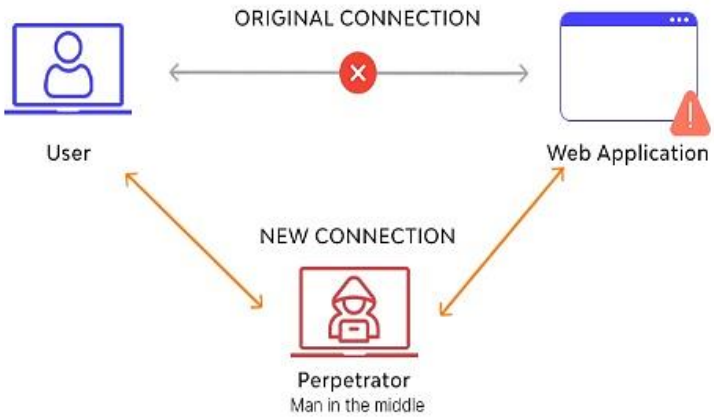
Schnappt ein Angreifer Daten während einer Übertragung, spricht man davon, dass sie abgefangen werden. Der Angreifer kann die Daten dann für seine Zwecke missbrauchen.

Diese Gefahr nennt man "*Man-in-the-Middle-Angriff*".

Beispiel:

Eine Person meldet sich in einem öffentlichen WLAN (z.B auf Bahnhöfen, Flughäfen, Restaurants) auf einer ungesicherten Webseite an. Ein Angreifer im selben Netzwerk liest den Datenverkehr mit. Benutzername und Passwort werden dabei abgefangen. Der Angreifer nutzt die Daten später für einen Kontozugriff.

Dieses Bild zeigt, wie ein Angreifer sich zwischen einen Benutzer und eine Web Anwendung schaltet und die Verbindung abfängt.



Bildquelle: https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attackz

3.2 Phishing-Arten

Phishing setzt sich vom englischen Wort „fishing“ (fischen) ab und bedeutet sinngemäß, dass Kriminelle „nach Daten angeln“.

Phishing ist eine weitverbreitete Form des Internetbetrugs, bei der Nutzer gezielt manipuliert werden, um vertrauliche Daten preiszugeben. Es gibt verschiedene Methoden wie klassisches Phishing, Spear Phishing, CEO Fraud sowie Varianten wie Smishing, Vishing und Tampering.

3.2.1 Klassisches Phishing

Phishing ist ein Betrugsversuch, bei dem Kriminelle sich als echte Unternehmen oder Personen ausgeben, um Passwörter, Daten oder Geld zu stehlen.

Meist passiert das über gefälschte E-Mails, Nachrichten oder Webseiten. Ziel ist es, dass man auf einen Link klickt oder Daten eingibt, ohne es zu merken.

Dieses Bild zeigt ein Phishing-Beispiel, bei dem sich jemand als Netflix-Mitarbeiter ausgibt und nach sensiblen Daten fragt.

Bildquelle: https://blog.usecure.io/de/the-most-common-examples-of-a-phishing-email

3.2.2 Spear-Phishing

Spear-Phishing sind Phishing-Angriffe auf bestimmte Personen, Unternehmen oder Organisationen.

Beispiel:

So kann so eine Mail aussehen:

> **Absender:** IT-Support <it-support@schule-intern.com>
> **Betreff:** Dringend: Zugriff auf dein Schul-Konto
>
> Hallo lieber Leser,
>
> uns ist aufgefallen, dass es gestern einen ungewöhnlichen Login-Versuch in deinem Schul-Konto gab.
>
> Bitte bestätige **bis heute 18:00 Uhr** deine Zugangsdaten, damit dein Konto nicht gesperrt wird:
>
> http://schule-intern-verify[.]com
>
> Vielen Dank für deine schnelle Mithilfe.
>
> Freundliche Grüße
> IT-Administration
> Deine Schule

3.2.3 CEO-Fraud

Beim CEO-Fraud gibt sich eine Person auch als jemand anderen aus aber hier als Geschäftsführer (CEO) oder Angestellter eines Unternehmens.

Beispiel:

Tom arbeitet in der Buchhaltung und erhält eine dringende Mail vom „CEO“, der ihn zu einer vertraulichen Überweisung auffordert. Die Nachricht wirkt echt und setzt ihn unter Druck. Erst später merkt Tom, dass Betrüger hinter der Mail steckten und das Geld verloren ist.

Dieses Bild zeigt eine Person, die Opfer von CEO-Fraud wird und Geld an Betrüger überweist.

Bildquelle: @ Jeff - ChatGPT (Self-made)

3.2.4 Smishing

Das Smishing ist eine Phishing-Masche, wo die Betrüger NICHT über E-Mail ihre Nachrichten verschicken, sondern über SMS. Dabei ist es das Ziel, Benutzernamen, Passwörter oder eine Schadsoftware auf einem Gerät zu installieren.

Beispiel:

Lisa bekommt eine SMS von ihrer „Bank“, dass ihr Konto gesperrt wurde. In Panik klickt sie sofort auf den Link in der Nachricht. Dort gibt sie ihre Zugangsdaten ein, um alles zu „bestätigen“. Kurz darauf ist Geld von ihrem Konto verschwunden.

Dieses Bild zeigt einen Smishing-Betrug, bei dem eine gefälschte SMS den Empfänger dazu auffordern soll, persönliche Daten oder Passwörter einzugeben

Bildquelle: @ Jeff - ChatGPT (Self-made)

3.2.5 Vishing

Beim Vishing rufen Betrüger für ihre Betrugsmaschen über ein Telefon an. Oft werden gezielt ältere Menschen ausgewählt.

Beispiel:

Bei einer alten Dame wird angerufen und gefordert einem Betrüger 30.000 € zu zahlen, sodass ihrem „entfürten“ Sohn nichts passiert, obwohl ihr Sohn gar nicht entführt wurde.

Dieses Foto zeigt einen Telefonbetrug, bei dem eine ältere Person mit einer falschen Drohung unter Druck gesetzt wird, um Geld zu überweisen.

Bildquelle: @ Jeff - ChatGPT (Self-made)

3.2.6 Tampering

Tampering bezeichnet das absichtliche Verändern von Daten, Systemen oder Software durch Angreifer. Dabei werden Informationen manipuliert, gelöscht oder verfälscht.

Ziel ist oft, den Betrieb eines Unternehmens zu stören und daraus finanziellen Vorteil zu ziehen. Dadurch können falsche Daten entstehen, die Geldverluste oder Sicherheitsprobleme verursachen.

Beispiel:

Ein Beispiel für Tampering ist die Firma „Firma X“, die Online-Bestellungen verarbeitet. Ein Angreifer greift das System an und verändert Daten in der Datenbank: Aus einer Bestellung über 100 € macht er 10 €.

Die Buchhaltung von Firma X sieht dadurch falsche Beträge und überweist zu wenig Geld oder berechnet falsche Rechnungen. Das führt zu finanziellen Verlusten und Problemen in der Abrechnung.

3.3 Datendiebstahl

Datendiebstahl bezeichnet das unbefugte Erlangen persönlicher oder geschäftlicher Daten. Die in den vorherigen Kapiteln beschriebenen Methoden wie Identitätsmissbrauch oder Phishing dienen häufig dazu, solche Daten zu stehlen und wirtschaftlich zu nutzen.

3.3.1 Persönlicher Daten

Kriminelle stehlen persönliche Daten, weil sie darin Informationen suchen, die sich zu Geld machen lassen.

Beispiel:

Jemand gibt einer fremden Person vertrauliche Informationen weiter. Diese speichert die Daten und gibt sie später heimlich an andere weiter oder verkauft sie. So werden persönliche Daten gestohlen und missbraucht.

3.3.2 Geschäftliche Daten

Kriminelle können auch gestohlene Daten von Unternehmen für viele üble Zwecke nutzen.

Diese Methode ist ähnlich wie die erste nur mit einem Unternehmen.

3.4 Malware-Arten

Im folgenden Abschnitt werden verschiedene Arten von Schadsoftware (Malware) erklärt, die Computern und Netzwerken schaden können.

Diese Programme verfolgen unterschiedliche Ziele, zum Beispiel das Ausspähen von Daten, das Erpressen von Geld oder das Stören von Systemen. Zu jeder Malware-Art wird eine einfache Erklärung und ein alltagsnahes Beispiel gegeben. So lassen sich die Gefahren und Funktionsweisen besser verstehen.

3.4.1 Viren

Ein Computervirus ist eine Schadsoftware, die sich bei der Verwendung verbreitet in dem sie ihren eigenen Code in Computersysteme einschleust.

Beispiel:

Ein Nutzer lädt ein kostenloses Programm aus dem Internet herunter, ohne die Quelle zu prüfen. In der Datei ist ein Computervirus versteckt. Sobald das Programm gestartet wird, installiert sich der Virus unbemerkt auf dem Computer und verbreitet sich auf weitere Dateien. Dadurch können Programme beschädigt oder Daten gelöscht werden.

Dieses Prinzip lässt sich mit der Biologie vergleichen: Ein Tier ist krank, wirkt aber äußerlich gesund. Ein anderes Tier kommt in Kontakt mit ihm und steckt sich an. Das infizierte Tier kann die Krankheit anschließend weiter verbreiten.

3.4.2 Würmer

Computerwürmer sind eine eigenständige Schadsoftware. Würmer breiten sich oft über Verbindungen wie WLAN zu den Zielcomputern/Netzwerken aus, indem sie ihre Sicherheitslücken ausnutzen. Würmer können Netzwerkverbindung-interne und externe- verlangsamen.

Beispiel: *Der Wurm im Schulnetzwerk*

In einer Schule sind alle Computer schlecht geschützt. Unabsichtlich wird ein Computer-Wurm installiert, der sich selbst kopiert und andere Geräte im selben Netzwerk infiziert. Kurz darauf sind alle Computer betroffen.

Dies ist der Code eines alten Wurms aus den Jahren 1998-2002 für Windows 95/98.
Heute würde er nicht mehr funktionieren.

Bildquelle: https://de.wikipedia.org/wiki/Computerwurm

3.4.3 Trojaner

Trojaner (benannt nach dem *Trojanischen Pferd* [6] aus der griechischen Mythologie) sind Schadprogramme, die sich als harmlose Software tarnen oder in scheinbar seriösen Anwendungen bzw. Dateien versteckt sind.

Sie verbreiten sich meist durch Verhaltensmanipulation: Nutzer werden dazu gebracht, einen Link zu öffnen, eine App zu installieren oder einen E-Mail-Anhang zu öffnen. Ein Trojaner tarnt sich also als etwas Nützliches oder Harmloses, enthält aber versteckte schädliche Funktionen.

Beispiel:

Jemand lädt aus dem Internet ein angeblich kostenloses Spiel („PremiumGame.exe“) herunter. Die Datei sieht echt aus und hat vielleicht sogar ein professionelles Logo. Nachdem das Spiel gestartet wird, funktioniert es zunächst ganz normal, sodass der Benutzer keinen Verdacht schöpft. Während der Spieler spielt, arbeitet jedoch im Hintergrund der Trojaner. Er installiert heimlich weitere Schadsoftware auf dem Computer und kann persönliche Daten wie Passwörter, Fotos oder gespeicherte Bankdaten ausspionieren. Diese Informationen werden anschließend über das Internet an Kriminelle geschickt.

[6] Das trojanische Pferd war ein großes Holzpferd, in dem sich Soldaten versteckten. Die Bewohner Trojas hielten es für ein Geschenk und holten es in die Stadt. So konnten die Soldaten eindringen und Troja erobern.

Darstellung des Trojanischen Pferdes.

Bildquelle: https://wtig.org/knowledge-database/security/datensicherheit/attachment/trojanisches-pferd-2

3.4.4 Ransomware

Ransomware ist Malware, die jemanden verlangt Geld an eine kriminelle Organisation zu zahlen im Gegensatz soll Ihnen keinen Schaden entstehen. Häufig verschlüsselt Ransomware die Dateien des Benutzers und droht ihm damit, den Schlüssel zu löschen, wenn nicht innerhalb einer kurzen Zeitspanne Geld gezahlt wird.

Einfaches Beispiel:

Bei einer Person wurde eingebrochen und es wurden wichtige Dokumente geklaut. Plötzlich bekommt diese Person eine Nachricht, wo steht, dass sie innerhalb von 24 Stunden Geld an eine Organisation zahlen muss um die wichtigen Dokumente zu retten.

Dieses Bild zeigt die verschiedenen Gefahren von Ransomware.

Bildquelle:.https://www.miniorange.com/blog/about-ransomware-attack (auf Deutsch übersetzt mit „Copilot“)

3.4.5 Spyware

Spyware ist Software die heimlich im Hintergrund Informationen über ihr Gerät sammelt. Spyware kann beispielsweise Software sein, die alle Anschläge auf der Tastatur protokoliert und auch Videos von der Kamera oder Ton vom Mikrofon mitschneidet und ihren Bildschirm aufnimmt usw.

Einfaches Beispiel:

Ein reicher Mann stellt jemanden als Reinigungskraft ein. Die Person macht ihre Arbeit ganz normal, aber währenddessen öffnet sie seine Schubladen, liest seine Notizen, fotografiert Dokumente und merkt sich alles, was sie interessant findet.

Dieses Bild zeigt eine Frau, die an einem infizierten Gerät arbeitet. Dabei wird sie unbemerkt gefilmt und abgehört, außerdem wird ihr Bildschirm aufgezeichnet.

Bildquelle: @ Jeff - Copilot (Self-made)

3.4.6 Scareware

Scareware ist eine Art von Schadsoftware oder Betrug, bei der Menschen durch Angst, Schock oder Druck manipuliert werden. Die Täter wollen erreichen, dass die Opfer schnell und unüberlegt handeln, ohne die Warnung zu überprüfen.

Dabei werden oft gefälschte Fehlermeldungen oder Warnungen angezeigt, die so aussehen, als kämen sie vom Betriebssystem oder von einer bekannten Sicherheitsfirma.

Häufigste Beispiele:

Eine Person sitzt zuhause am Computer und plötzlich erscheint ein großes Warnfenster. Zusätzlich ertönen laute Alarmgeräusch, ein Countdown läuft ab oder der Browser lässt sich scheinbar nicht mehr schließen:

„***ACHTUNG*!** **Ihr Computer ist mit mehreren Viren infiziert!** “
„Ihre Dateien und Passwörter sind in Gefahr!“

Die Meldung fordert die Person auf, sofort ein „Sicherheitsprogramm“ herunterzuladen oder Geld zu bezahlen, um den Computer zu schützen. Aus Angst und unter Zeitdruck klickt die Person auf den Link. Das angebliche Schutzprogramm ist jedoch selbst Schadsoftware oder dient dazu, Geld oder persönliche Daten zu stehlen.

Oder:

„***WARNUNG*! Ihr Computer wurde gehackt!“
„Rufen Sie sofort den technischen Support an!“

Die angezeigte Telefonnummer gehört jedoch Betrügern. Diese versuchen, die Person dazu zu bringen, Geld zu bezahlen oder ihnen Zugriff auf den Computer zu geben.

3.4.7 Kryptominer

Kryptominer sind Malware, die die Rechenkraft des infizierten Geräts übernehmen, um damit neue Einheiten einer bestimmten Krypto-Währung zu generieren. Die Währung wird dann von der Malware an den Gauner übermittelt. Bei diesem Mining dem Schürfen der Währung werden komplexe mathematische Berechnungen angestellt, für deren Lösung eine hohe Rechenleistung erforderlich ist.

Einfaches Beispiel:

Ein Handwerker geht in eine Wohnung, weil er angeblich etwas reparieren soll. Während er arbeitet, schließt er heimlich mehrere seiner eigenen Geräte an den Strom an und nutzt es aus um Strom zu sparen.

Dieser Handwerker profitiert von gratis Strom anstelle, dass er etwas repariert.

Bildquelle: @ Jeff - Copilot (Self-made)

3.4.8 Adware

Adware ist eine Schadsoftware, bei der verschiedene Malware-Technologien in einem Angriff kombiniert werden (Viren, Würmer und Trojaner).

Dieses Bild zeigt anschaulich, wie mehrere Malware-Technologien zusammenarbeiten.

Bildquelle: https://www.bitdefender.de/consumer/support/answer/12223/

Die besondere Gefahr liegt in der Kombination mehrerer Angriffsarten, wodurch gleichzeitig unterschiedliche schädliche Aktionen möglich sind, wie das Ausspähen von Daten, das Nachladen weiterer Schadsoftware oder eine starke Beeinträchtigung der Systemleistung.

Zusätzlich wird Adware häufig unauffällig mit kostenloser Software installiert, sodass Nutzer sie nicht sofort bemerken. Während sie scheinbar nur Werbung anzeigt, kann im Hintergrund bereits ein viel größerer Schaden entstehen. Besonders gefährlich ist daher die Kombination aus Tarnung und vielfältigen Angriffsmöglichkeiten.

3.5 DLL-Dateien

DLL-Dateien (*Dynamic Link Libraries*) sind ein wichtiger Bestandteil des Betriebssystems Microsoft-Windows. Sie enthalten Funktionen und Programmelemente, die von mehreren Programmen gleichzeitig verwendet werden können. Dadurch müssen diese Funktionen nicht mehrfach gespeichert werden, was Speicherplatz spart und die Leistung des Systems verbessert. Viele Prozesse des Betriebssystems sowie von Programmen basieren auf diesen Dateien.

Diese Struktur bringt jedoch auch Sicherheitsrisiken mit sich, da Programme oft externe DLL-Dateien laden. Angreifer können diese Eigenschaft ausnutzen, indem sie manipulierte Dateien einschleusen – ein bekanntes Beispiel ist das sogenannte DLL-Hijacking.

Dabei platziert ein Angreifer eine schädliche DLL-Datei in einem Ordner, den ein Programm durchsucht. Wird das Programm gestartet, lädt es versehentlich die falsche Datei statt der echten, wodurch Schadsoftware unbemerkt ausgeführt werden kann. So können Daten ausspioniert, weitere Schadprogramme nachgeladen oder sogar Systeme übernommen werden.

Beispiel:

Ein Nutzer startet ein seriöses Programm, das zum Beispiel eine Bildbearbeitung öffnet. Beim Start sucht das Programm automatisch nach einer bestimmten DLL-Datei, um eine Funktion zu laden. Ein Angreifer hat zuvor eine manipulierte DLL-Datei mit genau diesem Namen in denselben Ordner gelegt wie das Programm.

Beim Start lädt das Programm nicht die echte System-Datei, sondern die schädliche Version aus dem Ordner. Dadurch wird unbemerkt Schadcode ausgeführt, der zum Beispiel Daten ausliest oder weitere Malware installiert.

Ein weiteres Problem sind veraltete oder unsichere DLL-Dateien. Diese können Sicherheitslücken enthalten. Werden Programme oder das Betriebssystem nicht regelmäßig aktualisiert, können Angreifer bekannte Schwachstellen ausnutzen. Besonders gefährlich ist dies bei Programmen mit Administratorrechten, weil Schadsoftware dadurch umfangreichen Zugriff auf den Computer erhalten kann.

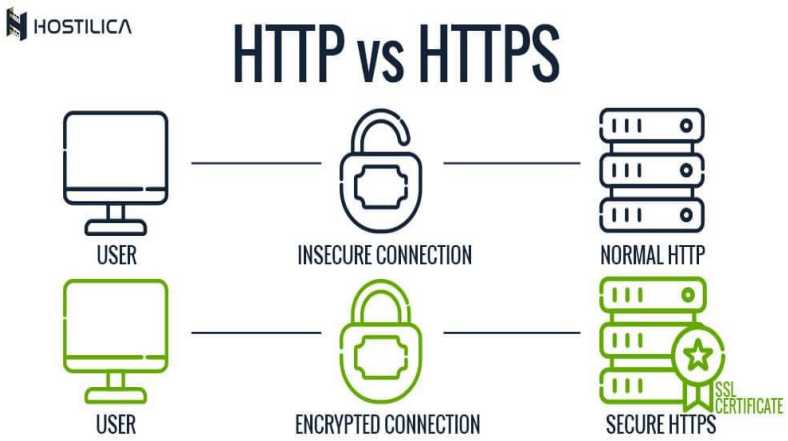
DLL-Dateien sind also ein wichtiger Bestandteil moderner Betriebssysteme, können aber auch ein großes Sicherheitsrisiko darstellen, wenn sie von Angreifern missbraucht werden.

4. Gefahren im Internet vermeiden

Um sich vor Gefahren im Internet zu schützen, ist ein vorsichtiges und bewusstes Verhalten wichtig. Viele Risiken entstehen durch unsichere Websites oder unachtsames Klicken auf Links. Deshalb gibt es verschiedene Maßnahmen, um sich vor Identitätsdiebstahl, Phishing und Malware zu schützen. Im Folgenden werden wichtige Schutzmethoden kurz vorgestellt.

4.1 Schutz vor Identitätsmissbrauch

Wenn man z. B. die Website einer Bank (oder anderer sensiblen Online-Dienste) besucht, sollte man drauf achten, dass die Internetadresse mit „https“ anfängt. Dabei steht „HTTPS“ für *„Hypertext Transfer Protocol Secure“* und kennzeichnet eine verschlüsselte sowie authentifizierte Verbindung, also eine geprüfte Web-Seite.



Bildquelle: https://hostilica.com/blog/http-vs-https

Darüber hinaus sollten vertrauliche Daten möglichst nur in sicheren Netzwerken übertragen werden. Öffentliche oder stark frequentierte WLAN-Netzwerke, beispielsweise in Cafés, Bahnhöfen oder Einkaufszentren, bergen ein erhöhtes Sicherheitsrisiko und sollten für sensible Transaktionen vermieden werden.

4.2 Schutz vor Phishing

Man soll Nachrichten von fremden Nummern immer ignorieren und löschen und niemals einen Link öffnen, dasselbe gilt auch bei Anrufen. Man kann sich auch einen Spam-Filter installieren.

4.3 Schutz vor Datendiebstahl

Man soll immer ein sicheres Passwort für seine Geräte und Programme verwenden. Beispiel

LeM-2013_LuXEmBurg_¢Jeff

Tipps für ein sicheres Passwort:

Minimum 12 Zeichen
Persönliche Infos, Interessen, Name, usw.
Zahlen und Sonderzeichen

4.4 Schutz vor Malware

Um sich vor Malware zu schützen, sollte man einige wichtige Sicherheitsmaßnahmen beachten.

Zunächst sollte man darauf achten, nur vertrauenswürdige Webseiten zu besuchen. Sichere Webseiten beginnen meist mit **„https“**. Das „s“ steht wie schon gesagt für „secure“ und bedeutet, dass die Verbindung verschlüsselt ist. Trotzdem können auch HTTPS-Webseiten gefährlich sein, daher sollte man immer vorsichtig bleiben.

Außerdem ist es wichtig, das Betriebssystem und Programme regelmäßig zu aktualisieren. Updates schließen Sicherheitslücken, die von Schadsoftware ausgenutzt werden könnten.

Man sollte außerdem:

- keine unbekannten Links oder Anhänge öffnen,
- starke Passwörter verwenden, und
- Downloads nur aus sicheren Quellen durchführen.

Wichtige Anmerkung:

Der **Inkognito-Modus**[7] im Browser speichert keinen Verlauf, keine Cookies und keine Suchdaten auf dem eigenen Gerät. Er schützt jedoch nicht vor Malware, Hackerangriffen oder der Überwachung durch Webseiten und Internetanbieter. Diese können trotzdem weiterhin Daten erfassen.

Inkognito erhöht daher eher die Privatsphäre, aber nicht die Sicherheit vor Angriffen.

[7] Der Inkognito-Modus ist ein spezieller Browsermodus, bei dem lokale Browserdaten nach dem Schließen der Sitzung automatisch gelöscht werden.

5. Technische Schutzmaßnahmen gegen Cybergefahren

Neben vorsichtigem Verhalten im Internet gibt es auch technische Schutzmaßnahmen, die Computer und persönliche Daten zusätzlich absichern können. Diese Programme und Systeme arbeiten im Hintergrund und helfen dabei, Schadsoftware zu erkennen, Angriffe zu verhindern und die Privatsphäre im Internet zu verbessern.

Zu den wichtigsten technischen Schutzmaßnahmen gehören Antivirus-Programme, VPN-Dienste und Firewalls. Während Antivirus-Programme schädliche Software erkennen und entfernen, schützt ein VPN die Privatsphäre und die Daten im Internet, indem es die Internetverbindung verschlüsselt. Firewalls greifen direkt in die Netzwerkverbindung ein, da sie unerlaubte oder verdächtige Verbindungen blockieren.

Im Folgenden werden diese Schutzmaßnahmen und ihre Funktionsweise genauer erklärt.

5.1 Antivirus-Software

Eine *Antivirus-Software* ist sehr hilfreich beim Schutz eines Gerätes. Leistungsstarke Antiviren-programme können verhindern, dass schädliche Software oder gefährliche Dateien auf einem Gerät installiert werden. Außerdem können sie Schadsoftware beseitigen, die bereits durch andere Schutzmaßnahmen geschlüpft ist.

Die Software scannt das System und dessen Ordner regelmäßig nach bösartiger Software. Wird eine Bedrohung erkannt, wird diese gesperrt und der Benutzer erhält eine Warnung. Manche Antivirenprogramme können die schädliche Datei automatisch löschen, häufig muss sie jedoch manuell entfernt werden.

Zusätzlich überwachen viele Programme ein- und ausgehende Verbindungen und suchen nach ungewöhnlichen Aktivitäten. Einige Antivirus-Programme prüfen außerdem besuchte Webseiten. Ist bekannt, dass eine Website gefährlich ist, wird der Benutzer gewarnt oder der Zugriff auf die Seite blockiert.

5.2 VPN

Ein VPN (*Virtual Private Network*) wurde entwickelt, um den Online-Verkehr zu verschlüsseln, die IP-Adresse zu verbergen und Daten vor Hackern zu schützen. Besonders wichtig ist der Schutz bei der Nutzung öffentlicher Netzwerke, aber auch zu Hause oder am Arbeitsplatz kann ein VPN sinnvoll sein.

Ohne VPN können Kriminelle unter bestimmten Umständen Online-Aktivitäten eines Nutzers verfolgen oder Daten abfangen. Solche Informationen können anschließend missbraucht oder im Darknet[8] verkauft werden.

Ein VPN funktioniert, indem die Internetverbindung über einen speziell konfigurierten Remoteserver geleitet wird, der vom VPN-Anbieter betrieben wird. Dadurch wird der VPN-Server zum Ursprung der Datenverbindung. Internetanbieter oder andere Dritte können somit nur noch sehr eingeschränkt erkennen, welche Webseiten besucht wurden oder welche Daten übertragen werden.

[8] Das Darknet ist ein Teil des Internets, der nur mit spezieller Software zugänglich ist und genutzt wird, um weitgehend anonym zu kommunizieren und Inhalte bereitzustellen, die teilweise illegal sind.

5.3 Firewall

Eine Firewall ist ein Sicherheitssystem, das den Netzwerkverkehr eines Computers oder Netzwerks überwacht und kontrolliert. Sie schützt Geräte davor, dass unerlaubte oder gefährliche Verbindungen hergestellt werden.

Dabei wird zwischen zwei Arten unterschieden: der *Hardware-Firewall* und der *Software-Firewall*.

- Eine ***Hardware-Firewall*** ist direkt in den **Router**[9] integriert. Sie kontrolliert den gesamten Datenverkehr, der zwischen dem heimischen Netzwerk und dem Internet stattfindet. Dadurch schützt sie alle Geräte im Netzwerk gleichzeitig, bevor die Daten überhaupt auf den einzelnen Computer gelangen. Sie bietet somit einen grundlegenden, zentralen Schutz für das gesamte Netzwerk.
- Eine ***Software-Firewall*** hingegen ist direkt auf dem Computer oder Gerät installiert. Sie überwacht den Datenverkehr auf diesem einzelnen Gerät und kann sehr genau steuern, welche Programme auf das Internet zugreifen dürfen und welche nicht. Dadurch bietet sie einen detaillierteren Schutz auf Anwendungsebene.

Die Firewall überprüft dabei ein- und ausgehende Datenpakete anhand festgelegter Sicherheitsregeln. Verdächtige oder nicht erlaubte Verbindungen werden blockiert, während sichere Verbindungen zugelassen werden. Dadurch kann verhindert werden, dass Hacker oder Schadsoftware auf ein Gerät zugreifen.

Viele Betriebssysteme besitzen bereits eine integrierte Software-Firewall. Zusätzlich verwenden Unternehmen oft leistungsstärkere Firewalls, um ganze Netzwerke vor Angriffen aus dem Internet zu schützen. In Kombination mit der Hardware-Firewall im Router entsteht so ein mehrstufiger Schutz, der die Sicherheit im Netzwerk deutlich erhöht.

[9] Ein Router ist ein Anschlussgerät zwischen dem heimischen Netzwerk und dem Netzbetreiber (z. B. die Post). Er stellt die Verbindung zum Internet her und leitet Daten zwischen Internet und den verbundenen Geräten im Haushalt weiter.

6. Verhalten bei einer Malware-Warnung

Wenn eine Malware-Warnung erscheint, ist schnelles und richtiges Handeln sehr wichtig. Viele Menschen reagieren in solchen Situationen unsicher oder machen Fehler. Deshalb sollte man einige grundlegende Schritte kennen, um sich und seine Daten zu schützen.

Im Folgenden wird erklärt, wie man sich bei einer Malware-Warnung richtig verhält.

6.1 Schritt 1

Am wichtigsten ist es Ruhe zu bewahren, auch wenn die Meldung ein Schock ist.

Die Täter versuchen, sich oft die Überraschung auszunutzen. Mit Erpressungstrojanern versuchen sie dann die Orientierungslosigkeit der Opfer möglichst effektiv auszunutzen. Dabei bauen die Täter eine Drohkulisse und erzeugen Zeitdruck. Die Opfer sollen dabei schnell die gewollte Handlung machen (Zahlung eines Lösegeldes).

Wie man sich verhalten soll, hängt immer ab, welche Malware man eingefangen hat.

6.2 Schritt 2

Um die richtigen Schritte für die Entfernung der Schadsoftware einzuleiten, muss man zunächst wissen, welche Art von Malware es sich handelt und welche Gefahren das Schadprogramm hat. Ein Antivirusprogramm kann oft eine erste Einschätzung dazu geben, um welche Malware es sich handelt.

6.3 Schritt 3

Nach dieser Meldung, das Gerät nicht mehr nutzten, es vom Internet trennen und ausschalten. So kann die Malware sich nicht mehr weiterverbreiten.

Das Gerät bleibt so lange ausgeschaltet bis, dass bekannt ist wie man die Malware entfernt. Man sollte sich später von Fachleuten beraten lassen, wie man die Malware entfernen kann. Man sollte die Malware dann von Computerfachleuten beseitigen lassen.

Man sollte dann Anzeige erstatten und das betroffene Gerät bei der Polizei lassen.

Dann ändert man von einem sicheren Gerät aus allen Passwörtern und sperrt betroffene Kreditkarten.

Wenn diese Malware auch noch Zugriff auf Konten bekommen hat, informiert man am besten auch noch Freunde, Verwandte und Bekannte aus sozialen Medien, um zu fragen ob sie in letzter Zeit verdächtige Nachrichten bekommen haben.

6.4 Schritt 4

Damit man in Zukunft besser vor Malwaregeschützt bleibt sollte man nach der Entfernung der Malware einige grundlegende Sicherheitsvorkehrungen treffen. Dabei sollte man sich informieren, wie man keine eine Malware mehr bekommen kann. Malware kann über viele Wege in ein Gerät eindringen. Meistens wird Malware über eine Datei auf ein Gerät installiert. Dabei müssen die Opfer selber die Malware auf das Gerät installieren. Betrüger haben einige Maschen entwickelt um Leute Dateien installieren zu lassen.

Meistens sind das E-Mails mit irreführenden Dateinamen, E-Mails von Anhängenden Freunden oder Links, die zu einem Dateidownload führen.

Man sollte dabei immer drauf Achten keine Dateien von unbekannten Quellen zu installieren.

Ab jetzt sollte man sich auch eine Antivirussoftware installieren, sodass man das System regelmäßig nach Malware scannen kann, eine Datensicherung einrichten und Apps, Software und Programme regelmäßig aktualisieren, denn durch Updates werden häufig Sicherheitslücken geschlossen.

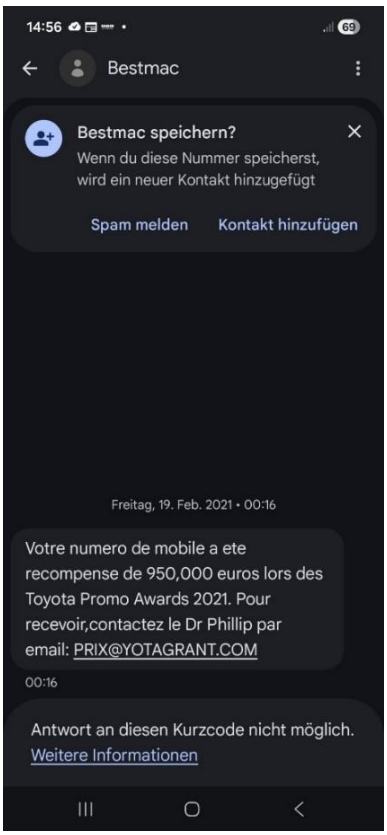
7. Eigene Erfahrungen mit Gefahren im Internet

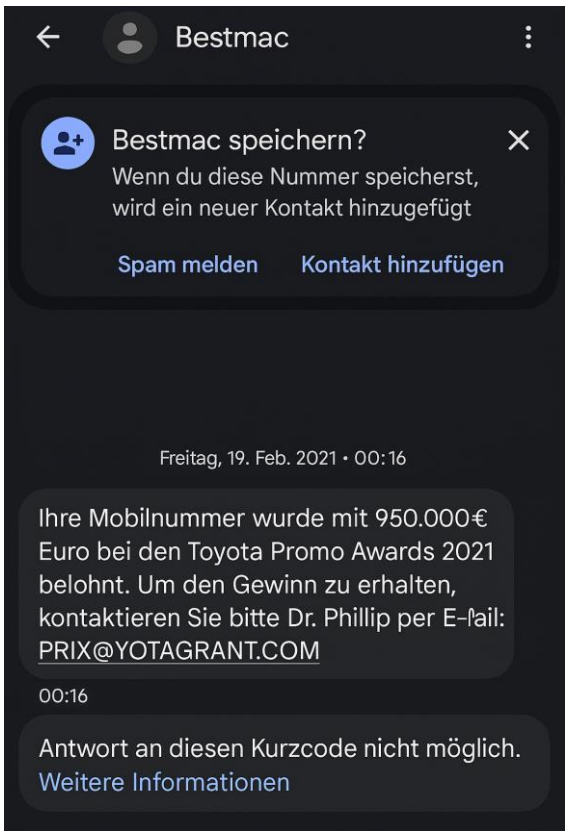
In diesem letzten Abschnitt beschreibe ich meine persönlichen Erfahrungen mit Gefahren im Internet. Dabei gehe ich auf Erlebnisse mit Phishing sowie auf verschiedene Schutzmaßnahmen ein. Außerdem erkläre ich, wie ich mein Gerät vor Malware abgesichert habe. So wird deutlich, welche Maßnahmen im Alltag wirklich sinnvoll und hilfreich sind.

Bis jetzt hatte ich noch keine schwerwiegenden Erfahrungen mit Malware. Allerdings habe ich bereits Bekanntschaft mit *Smishing* gemacht, also Phishing über SMS. Dabei erhielt ich verdächtige Nachrichten, in denen ich aufgefordert wurde, auf unsichere Links ohne geschütztes „https“ zu klicken.

Leider habe ich keine echten Screenshots oder Fotos mehr davon, da ich solche Nachrichten sofort lösche und nicht darauf antworte.

Screenshot vom Handy meiner Mutter, der einen Phishing-Betrug aus dem Jahr 2021 zeigt.



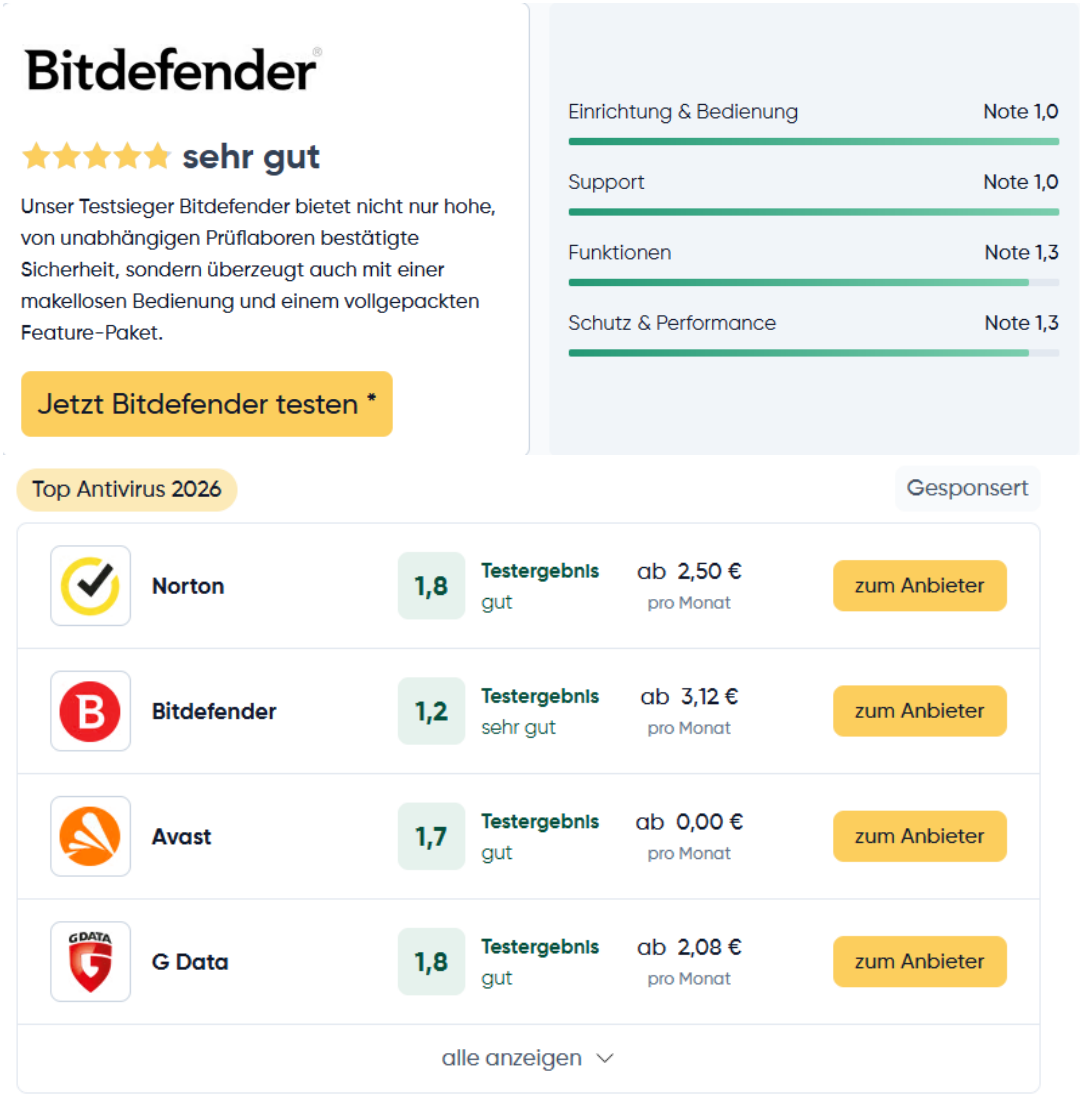


Bildquelle: Handy meiner Mutter (mit Copilot übersetzt)

Um sicherer im Internet zu sein, nutze ich eine *Antiviren-Software* namens **Bitdefender**. Es handelt sich um eine leistungsstarke Software, die Geräte vor Malware und anderen Gefahren schützt.

Bildquelle: https://laptoplemur.com/product/bitdefender-anti-virus1-device1-yearpc/

Hier sind Bilder einer Webseite, die zeigt, dass Bitdefender als sehr leistungsstark bewertet wird.



Bildquelle: https://www.experte.de/antivirus/bitdefender

Bitdefender scannt jede paar Stunden mein Gerät und sucht nach Malware. Auch wenn eine neue App installiert wird, wird diese sofort gescannt. Auch nach einem Neustart wird ein Scann durchgeführt.

Bitdefender scannt sogar alle meine Chats (Whatsapp, SMS) und sperrt Betrüger die schlechten Absichten haben. Die Anti-Viren Software schaut auch bevor ich eine Webseite besuche ob sie vertrauenswürdig ist. Sie scannt auch im Darknet nach Datenpannen[10].

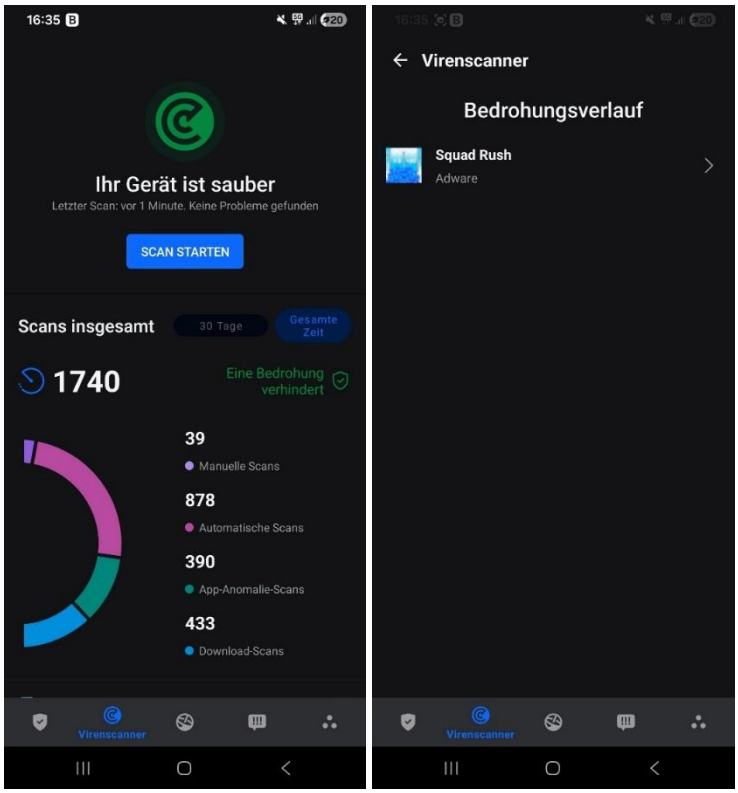
Leider hat man im Standard Abo nur 200 MB[11] VPN-Datenverkehr pro Tag verfügbar. Für unendlich viel Datenverkehr braucht man ein extra Abo.

[10] Datenpannen sind Sicherheitsvorfälle, bei denen persönliche oder vertrauliche Daten unbeabsichtigt verloren gehen, gestohlen werden oder für Unbefugte zugänglich sind (z. B. durch Hackerangriffe oder Fehlversände).

[11] 1 MB = 1 Mega Byte = eine Million Bytes (weiter gilt: 1000 Mega Bytes = 1 Giga Byte = 1 GB)

Trotzdem kann ich Bitdefender nur empfehlen. Mein Smartphone wurde damit sogar schon vor einer Adware namens **Squad Rush** geschützt.

Auf diesen Fotos sieht man, wie Bitdefender mich bereits davor geschützt hat.



Bildquelle: @Jeff Valmorbida (mein Handy)

Weitere Informationen zu Bitdefender stehen auf dieser Webseite:

Bitdefender - Weltspitze in Cybersicherheit https://www.bitdefender.com/de-de/

Schützen Sie sich mit der bestbewerteten Virenschutzlösung der letzten 10 Jahre
(und wir sind noch lange nicht fertig)
Wir haben die richtige Lösung für Ihre Anforderungen.
https://www.bitdefender.com/pages/consumer/de/new/cl-offer-premium-fam?locale=de

Um noch sicherer zu sein, installiere ich neue Systemupdates immer direkt, sobald sie verfügbar sind.

Außerdem aktualisiere ich meine Apps regelmäßig – etwa einmal pro Woche –, damit sie sicher bleiben und *Sicherheitslücken*[12] geschlossen werden.

Wenn möglich, habe ich außerdem immer die Zwei-Faktor-Authentifizierung[13] (2FA) aktiviert.

---

[12] Sicherheitslücken sind Schwachstellen in Software, Hardware oder Systemen, die von Angreifern ausgenutzt werden können, um Schaden anzurichten oder Daten zu stehlen.

[13] Zwei-Faktor-Authentifizierung (2FA) ist ein Sicherheitsverfahren, bei dem man sich mit zwei verschiedenen Faktoren anmeldet, zum Beispiel mit einem Passwort und einem einmaligen Code, der aufs Handy gesendet wird.

8. Schlussfolgerung

In diesem *Travail Personnel* wurde deutlich, dass das Internet viele Vorteile, aber auch zahlreiche Gefahren mit sich bringt. Da das Internet täglich von vielen Menschen genutzt wird, ist es besonders wichtig, diese Risiken zu kennen. Gefahren wie Phishing, Identitätsmissbrauch, Datendiebstahl oder Malware können großen Schaden anrichten, vor allem wenn man unvorsichtig ist oder sich unter Druck setzen lässt.

Die Arbeit zeigt aber auch, dass man sich gut schützen kann, wenn man aufmerksam bleibt und bestimmte Regeln beachtet. Dazu gehören sichere Passwörter, das Meiden unbekannter Links, regelmäßige Updates und das vorsichtige Weitergeben persönlicher Daten. Zusätzlich können technische Hilfsmittel wie Antivirus-Programme, VPNs und die Zwei-Faktor-Authentifizierung die Sicherheit deutlich erhöhen.

Zusammenfassend kann man sagen, dass das Internet sicher genutzt werden kann, wenn man informiert ist und verantwortungsvoll handelt. Wer die Gefahren kennt und weiß, wie man sich schützt, kann die vielen Vorteile des Internets ohne große Risiken nutzen.

9. Quellenangaben

1. Seite 2: „Binärdarstellung von Daten und Tabelle“,
   inf-schule | Binärdarstellung von Daten » Fachkonzept - Bit/Byte
   (Abgerufen am: 12.05.2026 um 15:08)

2. Seite 3: Intel, „CPU-Taktfrequenz erklärt“,
   https://www.intel.de/content/www/de/de/gaming/resources/cpu-clock-speed.html
   (Abgerufen am: 12.05.2026 um 15:09)

3. Seite 3-4: „Der Start eines Computers”,
   + UEFI Forum – Specifications
   (Abgerufen am: 12.5.2026 um 15:10)
   + Microsoft Learn - Boot and UEFI
   (Abgerufen am: 12.5.2026 um 15:11)
   + Linux Kernel Boot Protocol
   (Abgerufen am: 12.5.2026 um 15:12)
   + ArchWiki - Boot Process
   https://wiki.archlinux.org/title/Arch_boot_process
   (Abgerufen am: 12.5.2026 um 15:13)

4. Seite 4: „Kurioses“,
   https://de.wikipedia.org/w/index.php?title=Booten&veaction=edit&section=2
   (Abgerufen am: 12.5.2026 um 15:14)

5. Seite 5-17: „Cybersicherheit“,
   Verlag: Wissen für Dummies®
   Autor: Jospeh Steinberg

6. Seite 6-9: Mahr-EDV, „Phishing-Angriff in 4 Schritten“,
   https://www.mahr-edv.de/phishing-attacke
   (Abgerufen am: 12.5.2026 um 15:15)

7. Seite 13: „Was ist Scareware“,
   https://www.zenarmor.com/docs/network-security-tutorials/what-is-scareware
   (Abgerufen am: 12.5.2026 um 15:14)

8. Seite 15: „DLL-Hijacking“,
   https://www.okta.com/de-de/identity-101/dll-hijacking
   (Abgerufen am: 12.5.2026 um 15:15)

9. Seite 10 und 18: „Viren und Antivirus“,
   https://www.avast.com/de-de/c-computer-virus
   (Abgerufen am: 12.5.2026 um 15:15)

10. Seite 16-17: „Tipps zum Sicheren Internet-Surfen“,
    https://www.emsisoft.com/de/blog/28810/sicher-internet-surfen-tipps
    (Abgerufen am: 12.5.2026 um 15:16)

11. Seite 18: „Was ist ein Antivirus-Programm“,
    https://nordpass.com/de/blog/what-is-antivirus-software
    (Abgerufen am: 12.5.2026 um 15:16)

12. Seite 18: „Was ist ein VPN“,
    https://www.kaspersky.de/resource-center/definitions/what-is-a-vpn
    (Abgerufen am: 12.5.2026 um 15:16)

13. Seite 18: „Warum und Wann ein VPN“,
https://nordvpn.com/de/blog/vpn-notwendig
(Abgerufen am: 12.5.2026 um 15:16)

14. Seiten 20-21: „Virus! Was tun in 4 Schritten“,
https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/virus-auf-dem-geraet-das-muessen-sie-jetzt-tun-in-4-schritten-70198
(Abgerufen am: 12.5.2026 um 15:16)