

IT Sicherheit - Grundlagen an einem Tag

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de
Version: 1.0

Folien: <https://delors.github.io/sec-schulung-grundlagen-ein-tag/folien.de.rst.html>
<https://delors.github.io/sec-schulung-grundlagen-ein-tag/folien.de.rst.html.pdf>
Fehler melden: <https://github.com/Delors/delors.github.io/issues>

Nachrichten aus der Welt der IT-Sicherheit

Paragon Spyware Tool Linked to Canadian Police

Researchers at the University of Toronto's Citizen Lab in Canada said Ontario Provincial Police appear to have deployed spyware from Israel's Paragon on computers under its control. Spyware victims were Android phone users who were added to a WhatsApp group, where a malicious PDF file was sent to compromise devices via "zero click" intrusion. The researchers said Paragon's Graphite spyware has been linked to users in Australia, Canada, Cyprus, Denmark, Israel, and Singapore.

—19.3.2025 - Bloomberg,

Paragon Spyware Tool mit kanadischer Polizei in Verbindung gebracht

Forscher des Citizen Lab der Universität Toronto in Kanada haben festgestellt, dass die Polizei der Provinz Ontario offenbar Spyware des israelischen Unternehmens Paragon auf den von ihr kontrollierten Computern eingesetzt hat. Bei den Spyware-Opfern handelte es sich um Nutzer von Android-Telefonen, die zu einer WhatsApp-Gruppe hinzugefügt wurden, in der eine bösartige PDF-Datei per „Zero-Click“-Einbruch an kompromittierte Geräte gesendet wurde. Den Forschern zufolge wurde die Graphite-Spyware von Paragon mit Nutzern in Australien, Kanada, Zypern, Dänemark, Israel und Singapur in Verbindung gebracht.

—19.3.2025 - Bloomberg (Übersetzt mit DeepL)

CISA Warns of Active Exploitation in GitHub Action Supply Chain Compromise

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday added a vulnerability linked to the supply chain compromise of the GitHub Action, tj-actions/changed-files, to its Known Exploited Vulnerabilities (KEV) catalog.

The high-severity flaw, tracked as CVE-2025-30066 (CVSS score: 8.6), involves the breach of the GitHub Action to inject malicious code that enables a remote attacker to access sensitive data via actions logs.

—19.3.2025 - The Hacker News

CISA warnt vor aktiver Ausnutzung einer Schwachstelle in der Lieferkette von GitHub-Aktion

Die US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) hat am Dienstag eine Schwachstelle im Zusammenhang mit der Kompromittierung der Lieferkette der GitHub-Aktion tj-actions/changed-files in ihren Katalog der bekannten ausgenutzten Schwachstellen (KEV) aufgenommen.

Die hochgradig gefährliche Schwachstelle, die als CVE-2025-30066 (CVSS-Score: 8.6) verfolgt wird, beinhaltet die Verletzung der GitHub-Aktion, um bösartigen Code einzuschleusen, der es einem entfernten Angreifer ermöglicht, über Aktionsprotokolle auf sensible Daten zuzugreifen.

—19.3.2025 - The Hacker News (Übersetzt mit DeepL)

Indonesia won't pay an \$8 million ransom after a cyberattack compromised its national data center

[...] The attackers have held data hostage and offered a key for access in return for the \$8 million ransom, said PT Telkom Indonesia's director of network & IT solutions, Herlan Wijanarko, without giving further details. Wijanarko said the company, in collaboration with authorities at home and abroad, is investigating and trying to break the encryption that made data inaccessible. [...]

—June 25th, 2024 - AP News

Crypto-Hackers Steal \$2.2bn as North Koreans Dominate

Threat actors stole \$2.2bn from cryptocurrency platforms in 2024, with the majority (61%) of illicit funds attributed to North Korean hackers, according to Chainalysis. [...]

Notably, attacks between \$50 and \$100m, and those above \$100m, occurred far more frequently in 2024 than they did in 2023, suggesting that the DPRK is getting better and faster at massive exploits[...].

This increase is unfortunately also being matched by “a growing density” of hacks which yielded lower amounts of around \$10,000 in value.[...]

Some of these events appear to be linked to North Korean IT workers, who have been increasingly infiltrating crypto and Web3 companies, and compromising their networks, operations, and integrity.

—19.12.2024 - **Infosecurity Magazine**

Hackers shut down heating in Ukrainian city with malware

For two days in mid-January, some Ukrainians in the city of Lviv had to live without central heating and suffer freezing temperatures because of a cyberattack against a municipal energy company [...]

[...], the cybersecurity company Dragos published a report with details about a new malware dubbed FrostyGoop, which the company says is designed to target industrial control systems [...]

—Juli 2024 - **Techcrunch**

US government tells officials, politicians to ditch regular calls and texts

The U.S. government [CISA] is urging senior government officials and politicians to ditch phone calls and text messages following intrusions at major American telecommunications companies blamed on Chinese hackers. [...]

The first recommendation: "Use only end-to-end encrypted communications." [...]

—18.12.2024 - **Reuters**

Want to Win a Bike Race? Hack Your Rival's Wireless Shifters

Relatively inexpensive hardware can be used to hack the Shimano Di2 wireless gear-shifting systems used by cyclists [...]. They tested the eavesdrop-and-replay attack with a \$1,500 USRP software-defined radio, an antenna, and a laptop but said the setup could be miniaturized. Attackers could spoof signals from up to 30 feet away, causing the target bike to shift gears unexpectedly or lock into the wrong gear.

—August 2024 - **summary provided by ACM; full article: Wired**

New RAMBO attack steals data using RAM in air-gapped computers

[...] A novel side-channel attack dubbed "RAMBO" (Radiation of Air-gapped Memory Bus for Offense) generates electromagnetic radiation from a device's RAM to send data from air-gapped computers.

[...] To conduct the Rambo attack, an attacker plants malware on the air-gapped computer to collect sensitive data and prepare it for transmission. It transmits the data by manipulating memory access patterns to generate controlled electromagnetic emissions from the device's RAM.

[...] The RAMBO attack achieves data transfer rates of up to 1,000 bits per second (bps) [at a distance of up to 7 meters], equating to 128 bytes per second, or 0.125 KB/s.

—September 2024 - **Bleepingcomputer**

Rambo Attack - weitere Details

The emitted data is encoded into "1" and "0", represented in the radio signals as "on" and "off." The researchers opted for using Manchester code to enhance error detection and ensure signal synchronization, reducing the chances for incorrect interpretations at the receiver's end.

The attacker may use a relatively inexpensive Software-Defined Radio (SDR) with an antenna to intercept the modulated electromagnetic emissions and convert them back into binary information.

SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript

[Side-Channel Attack to circumvent privacy.]

[...] The attack setup for SnailLoad. A victim downloads data from an attacker's HTTP server while it watches a video on a video-sharing platform, e.g., YouTube. Due to the network bottleneck on the victim's side, the attacker can infer the transmitted amount of data by measuring the packet round trip time. The round trip time traces are unique per video and can be used to classify the video watched by the victim. [...]

—28.6.2024 Snailload: **Paper**, **Web**

New PIXHELL Attack Exploits LCD Screen Noise to Exfiltrate Data from Air-Gapped Computers

A new side-channel attack dubbed PIXHELL could be abused to target air-gapped computers by breaching the "audio gap" and exfiltrating sensitive information by taking advantage of the noise generated by pixels on an LCD screen.

Malware in the air-gap and audio-gap computers generates crafted pixel patterns that produce noise in the frequency range of 0 - 22 kHz," Dr. Mordechai Guri, the head of the Offensive Cyber Research Lab in the Department of Software and Information Systems Engineering at the Ben Gurion University of the Negev in Israel, said in a newly published paper. [...]

—10. Sept. 2024 - **The Hacker News**

FAST 4.000 VERHAFTUNGEN: Interpol gelingt großer Schlag gegen Onlinebetrug

Die Einsatzkräfte haben nicht nur weltweit Tausende von Verdächtigen verhaftet, sondern auch Vermögenswerte im Umfang von 257 Millionen US-Dollar beschlagnahmt.

[...] Mit einem Gesamtwert von 135 Millionen US-Dollar besteht laut Interpol mehr als die Hälfte davon aus beschlagnahmten Fiat-Währungen wie US-Dollar, Euro oder Yen. Weitere zwei Millionen Dollar liegen in Form von Kryptowährungen vor. Hinzu kommen andere Vermögenswerte wie etwa Immobilien, Luxusfahrzeuge, teurer Schmuck und andere hochwertige Gegenstände und Sammlungen im Gesamtwert von 120 Millionen US-Dollar. [...]

—29. Juni 2024 - **Golem.de**

CEO VERHAFTET

Der Hersteller soll insgesamt 240.000 Geräte mit der DDoS-Funktion ausgestattet haben – teils ab Werk, teils erst nachträglich per Firmwareupdate.

[...] In Südkorea sind fünf Mitarbeiter sowie der CEO eines Unternehmens verhaftet worden. Dieses soll Satellitenreceiver [...] auf Wunsch eines Kunden mit einer DDoS-Funktion ausgestattet haben. [...] lieferte der Hersteller 98.000 Geräte ab Werk mit dieser Funktion aus. [...]

Dass Geräte ab Werk mit Schadsoftware ausgeliefert werden, ist gerade im unteren Preissegment keine Seltenheit. Sicherheitsforscher deckten erst im vergangenen Jahr eine Malware-Kampagne

auf, bei der vor allem billige Android-Geräte wie Smartphones, Tablets und TV-Boxen aus China vor ihrer Auslieferung an Endkunden mit einer Schadsoftware ausgestattet worden waren.

—3.12.2024 - **Golem.de**

U.S. charges 14 North Koreans in \$88 million identity theft and extortion case

The Department of Justice accused 14 North Koreans of conspiring to use false identities to get IT jobs with U.S. companies and siphon money back to their home country.

The indictment in Missouri federal court alleged that the conspiracy generated at least \$88 million.

The State Department said Thursday it is offering an up to \$5 million reward for information about the conspirators and others associated with the two "North Korean front companies."

—12.12.2024 - **CNBC**

UK cybersecurity agency warns over risk of quantum hackers

Organisations including energy and transport firms told to guard systems against powerful new computers

Guidance from the U.K.'s National Cyber Security Centre calls on large organizations, critical national infrastructure operators, and companies with bespoke IT systems to implement "post-quantum cryptography" to guard against future quantum hackers. These entities were urged to identify services in need of an upgrade by 2028. The guidance indicated that the most important upgrades should be completed by 2031, with migration to a new encryption system by 2035.

—20.3.2025 - **ACM Technews based on a report by The Guardian**

Britische Cybersicherheitsbehörde warnt vor der Gefahr von Quanten-Hackern

Organisationen, darunter Energie- und Transportunternehmen, sollen ihre Systeme gegen leistungsstarke neue Computer schützen

In einem Leitfaden [...] werden große Organisationen, Betreiber kritischer nationaler Infrastrukturen und Unternehmen mit maßgeschneiderten IT-Systemen aufgefordert, „Post-Quantum-Kryptografie“ zu implementieren, um sich gegen künftige Quanten-Hacker zu schützen. Diese Einrichtungen wurden aufgefordert, die Dienste zu identifizieren, die bis 2028 aufgerüstet werden müssen. Der Leitfaden besagt, dass die [...] die Migration auf ein neues Verschlüsselungssystem bis 2035 erfolgen sollte.

—20.3.2025 - **ACM Technews based on a report by The Guardian (Übersetzt mit DeepL)**

Jetzt updaten! Zero-Day-Sicherheitslücke in Chrome wird angegriffen

Google hat dem Webbrowser Chrome ein Update spendiert. Es schließt eine Zero-Day-Lücke, die bereits angegriffen wird.

Google hat in der Nacht zum Mittwoch eine Aktualisierung für den Webbrowser Chrome veröffentlicht. Sie stopft ein Zero-Day-Sicherheitsleck, das Angreifer bereits in freier Wildbahn missbrauchen. [...] "Google hat Kenntnis von Berichten, dass ein Exploit für CVE-2025-2783 im Netz existiert". [...] Demnach beginnt der Angriff mit einer Phishing-Mail, die vorgeblich zu einem Event des internationalen Wirtschafts- und Politikwissenschaftsforum einlädt und zu einem Programm sowie Anmeldeformular führt. Beide Links führen im Webbrowser Chrome unter Windows jedoch zu einer Malware-Infektion, ohne weitere Interaktion der Opfer.

—26.3.2025 - **Heise Security**

Cybersicherheit ist das Geschäftsrisiko Nr. 1

Cybervorfälle wie Ransomware-Angriffe, Datenschutzverletzungen und IT-Unterbrechungen sind laut dem Allianz Risk Barometer im Jahr 2024 die größte Sorge für Unternehmen weltweit. An zweiter Stelle steht die eng miteinander verknüpfte Gefahr der Betriebsunterbrechung. [...]

Cybervorfälle (36% der Gesamteinsätze) sind zum dritten Mal in Folge das weltweit gefürchtetste Risiko [...]. Eine Datenschutzverletzung wird von den Befragten des Allianz Risk Barometers (59%) als die besorgniserregendste Cyberbedrohung angesehen, gefolgt von Angriffen auf kritische Infrastrukturen und physische Vermögenswerte (53%). [...]

Cyberkriminelle suchen vermehrt nach Möglichkeiten, neue Technologien wie generative künstliche Intelligenz (KI) zu nutzen, um Angriffe zu automatisieren und zu beschleunigen und so effektivere Malware und Phishing zu schaffen. [...]

—Jan. 24 - **Allianz Risk Barometer 2024**

Was ist Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

—July 4th, 2024 - **Cisco**

[...] The security precautions related to computer information and access address four major threats: **(1) theft of data**, such as that of military secrets from government computers; **(2) vandalism**, including the destruction of data by a computer virus; **(3) fraud**, such as employees at a bank channeling funds into their own accounts; and **(4) invasion of privacy**, such as the illegal accessing of protected personal financial or medical data from a large database. [...]

—July 4th, 2024 - **Britannica**

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit)

Artikel 2 Nummer 1

„Cybersicherheit“ bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen [...]

—**Verordnung (EU) 2019/881**

Das Ziel der IT-Sicherheit ist es Systeme vor:

- Ausfall
- Missbrauch
- Sabotage
- Spionage
- Betrug und Diebstahl zu schützen

Wichtige Kennzahlen bzgl. Cybersecurity-Vorfällen^[1]

Mean Time to Detection (MTTD):

Die mittlere Zeit, die benötigt wird, um einen Cyberangriff zu entdecken.

Mean Time to Identify (MTTI):

Die mittlere Zeit, die benötigt wird, um einen Cyberangriff zu identifizieren in der Hinsicht, dass die Schwachstelle erkannt wird bzw. die Art des Vorfalls erkannt wird und eine erste Idee entwickelt wird, wie gegen den Angriff vorgegangen werden kann.

Mean Time to Respond (MTTR):

Die mittlere Zeit, die benötigt wird, um auf einen Cyberangriff so zu reagieren, dass kein weiterer Schaden entsteht und der Weg zur Wiederherstellung der normalen Operationen eingeleitet werden kann.

Mean Time to Contain (MTTC):

Die mittlere Zeit, die benötigt wird, um einen Cyberangriff einzudämmen. D. h. die Zeit, die benötigt wird, um zu verhindern, dass sich der Angriff weiter ausbreitet.

$$MTTC = MTTD + MTTI + MTTR$$

Mean Time to Normal (MTTN) bzw. Mean Time to Recover/Restore/Resolve (MTTR):

Die mittlere Zeit, die benötigt wird, um die normalen Operationen wiederherzustellen.

Dies kann zum Beispiel auch die Zeit umfassen, die benötigt wird um etwaige Backups einzuspielen oder ggf. Firmware Patches einzuspielen.

Die MTTD kann häufig nur im Nachgang genau ermittelt werden, sollte aber natürlich nachgefasst werden, um die eigenen Prozesse zu kontrollieren und ggf. zu verbessern. Insbesondere im Zusammenhang mit APTs können vergleichsweise lange Zeiträume bis zur Entdeckung vergehen. Zum Beispiel kann es sein, dass man als erstes feststellt, dass es unerwartete Verbindungen zu einem externen Server gibt. Zu diesem Zeitpunkt ist aber noch unklar wie der Angreifer vorgegangen ist, welche Daten ggf. schon abgeflossen sind und was genau zu tun ist, um den Angreifer zu stoppen. Es ist insbesondere auch noch nicht klar auf welche Systeme er bereits Zugriff hat.

Die Zeit bis zum Beispiel erkannt wurde, dass ein bestimmter Account ausgenutzt wurde und dieser dann gesperrt wurde, oder zum Beispiel bestimmte Netzwerkverbindungen effektiv blockiert werden und begonnen werden kann mit der Wiederherstellung der Systeme, wird als MTTR bezeichnet.

Die MTTC misst somit nicht wie lange es dauert bis alle Auswirkungen des Angriffs beseitigt sind/die normale Operation wiederhergestellt ist, sondern „nur“ wie lange es dauert die weitere Verbreitung zu stoppen.

^[1] Die Begriffe sind nicht einheitlich definiert und ggf. ist es sinnvoll zu klären welcher Zeitraum genau gemeint ist.

1. Angriffe auf die Schutzziele der IT-Sicherheit

Ausgewählte Angriffe, Angriffsmethoden und Bedrohungsszenarien

- Backdoors (🚪 *Hintertüren*)
 - (Distributed-)Denial-of-service Angriffe
 - Direct-access Angriffe (d. h. physischer Angriff auf das System)
 - Eavesdropping (👂 *Abhören*)
 - Malware
 - Man-in-the-middle (MITM) Angriffe
 - Privilege escalation (unterschieden werden: horizontale und vertikale)
 - Side-Channel attacks (🗨️ *Seitenkanalangriffe*)
 - Spoofing (z. B. IP-Spoofing) (👤 *Vortäuschen*)
 - Social engineering (z. B. Phishing)
 - Advanced Persistent Threats (APT)
 - *Store-now, Decrypt-later* (📁 *Speichere jetzt, Entschlüssele später*)
-

Vertikale Privilege Escalation:

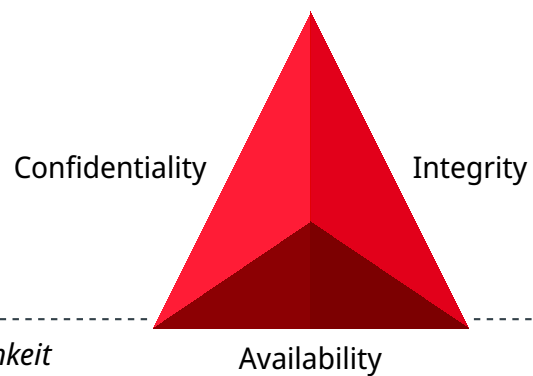
Der Angreifer erhält Zugriff auf höhere Rechte, die er vorher nicht hatte.


Horizontale Privilege Escalation:

Der Angreifer erhält Zugriff auf die Rechte einer anderen Person, die er vorher nicht hatte.

APT: Der Begriff *Advanced Persistent Threat* (≙ „fortgeschrittene, andauernde Bedrohung“) bezeichnet gezielte Cyberangriffe durch professionelle Gruppen (häufig *state sponsored*). Es werden in der Regel langfristige Ziele verfolgt. Diese dienen zum Beispiel der Spionage oder der Vorbereitung auf einen Cyberkrieg. Häufige Ziele sind Regierungen und Unternehmen sowie Organisationen, die über kritische Daten verfügen. Insbesondere in der Anfangsphase gehen die Angreifer sehr vorsichtig vor, um nicht entdeckt zu werden. Danach unterscheidet sich das Vorgehen je nach Zielsetzung. Häufig wird versucht den Zugriff auf das Zielsystem langfristig zu erhalten, um so an weitere Informationen zu gelangen.

Schutzziele der IT-Sicherheit: CIA-Triade



Confidentiality $\hat{=}$  *Vertraulichkeit*

Integrity $\hat{=}$  *Integrität*

Availability $\hat{=}$  *Verfügbarkeit*

Erweiterte Schutzziele

Neben den primären Schutzzielen, gibt es eine Reihe weiterer kontextabhängiger Schutzziele:

Verbindlichkeit/Nichtabstreitbarkeit (🇺🇸 *Accountability/Non-repudiation*):

Ein Akteur kann seine Handlungen nicht abstreiten.

Pseudo-/Anonymisierung:

Eine Person kann nicht (mehr) identifiziert werden.

Authentizität (🇺🇸 *Authenticity*):

Ist eine Information echt bzw. vertrauenswürdig?

2. Social-Engineering Angriffe

Weitergehende Informationen

Falls Sie als Shell Bash nutzen und Linux oder Mac OS x verwenden, dann kopieren Sie bitte den folgenden Befehl in die Konsole, für weitergehende Informationen:

```
curl https://github.com/Delors/delors.github.io/issues
```

Eigenschaften von Social-Engineering Angriffe

- **sind häufig die Ursache für erfolgreiche Angriffe**

(Der Hacker Kevin Mitnick war praktisch immer aufgrund von Social Engineering erfolgreich.)

- stellen die größte Bedrohung für die Sicherheit von IT-Systemen dar
- es wird angenommen, dass die betroffenen Personen es in vielen Fällen nicht merken
(Beispiel: Fake Bewerbungsgespräch)
- mittels OSINT kann die Vorbereitung von Social-Engineering Angriffen vereinfacht werden
- neue technische Möglichkeiten (z. B. KI generierte Stimmen) erweitern die Angriffsmöglichkeiten

Beispiel eines fortgeschrittenen Social-Engineering Angriffs

Ein vom Angreifer bewusst eingefädelt Bewerbungsgespräch für eine Position als Administrator könnte zum Beispiel dazu genutzt werden, um Informationen über das Zielsystem zu erhalten, die für einen Angriff nützlich sind (z. B. welche Software wird eingesetzt, wie sieht die Architektur aus, ...). In diesem Fall ist davon auszugehen, dass ein Bewerber zum Beispiel durch ein Headhunter eine gutes Angebot gemacht wird und er dann im Rahmen des Gesprächs gebeten wird eine Sicherheitsarchitektur darzustellen, die er einführen würde. Es ist dann davon auszugehen, dass er auf seine bisherige Erfahrung zurückgreift und diese darstellt und er somit die Architektur des Zielsystems offenlegt.

Neue Gefahren

Durch KI generierte Stimmen kann es Angreifern gelingen, z. B. durch das Vortäuschen einer Notlage einer nahestehenden Person, an Informationen zu gelangen.

One Question Saved Ferrari from a Deepfake Scam

With one question, an executive at Ferrari stopped an effort to use deepfake technology to scam the company. CEO Benedetto Vigna (pictured) was impersonated on a call by deepfake software that, using a convincing imitation of Vigna's southern Italian accent, said he needed to discuss something confidential that required an unspecified currency-hedge transaction to be carried out. The executive started to have suspicions and asked, for identification purposes, the title of the book Vigna had recently recommended to him. With that, the call ended.

—Juli, 2024 - Zusammenfassung: **ACM**; Original: **'I Need to Identify You': How One Question Saved Ferrari From a Deepfake Scam - Bloomberg**

Ausgewählte Social-Engineering Angriffe

Phishing and Spear Phishing:

Phishing nutzt elektr. Kommunikationswege um an Informationen zu gelangen (z. B. E-Mail oder SMS).

Spear phishing ist Phishing, bei der der Angreifer auf eine bestimmte Zielgruppe oder sogar eine einzelne Person abzielt.

Smishing: Phishing mit Hilfe von SMS.

Vishing: Phishing mit Hilfe von Telefonanrufen.
(Z. B. **Anrufe von Europol**)

Quishing/QR phishing:

Phishing mit Hilfe von QR Codes.

Whaling: Phishing, dass sich gegen hochrangige und sehr ausgewählte Personen richtet (z. B. den CEO eines Unternehmens).

Pharming: Manipulation des DNS-Servers, um den Nutzer auf eine gefälschte Webseite zu leiten, um dann sensitive Informationen zu erlangen.

Spam / Spam over Internet messaging (SPIM):

Unerwünschte und nicht angeforderte E-Mail-Nachrichten oder Nachrichten in sozialen Medien bzw. Instant Messaging-Diensten.

Dumpster Diving: Durchsuchen von „Müllcontainern“ nach Informationen, die für einen Angriff nützlich sein könnten.

Shoulder Surfing: Beobachten von Personen, die sich an einem Computer anmelden, um das Passwort zu erfahren oder die sensitive Informationen auf dem Schreibtisch liegen haben.

Tailgating: Ein Angreifer nutzt die Zugangsberechtigung einer Person, um sich Zugang zu einem Gebäude zu verschaffen ohne dass die Person dies bemerkt oder gar zustimmt.

Dies kann z. B. durch Zugangsschleusen verhindert werden, die immer nur einer Person den Zugang gewähren.

Identity Fraud: Identitätsdiebstahl. Der Angreifer gibt sich als jemand anderes aus, um an Informationen zu gelangen oder um eine Straftat zu begehen.

Invoice Scams: Versenden von Rechnungen, für Dienstleistungen und Produkte die man nicht gekauft hat (z. B. Rechnungen für Postzustellung.)

Credential Harvesting:

Sammlung von Zugangsdaten, die durch Sicherheitslücken in Systemen oder durch Phishing erlangt wurden.

Hoax: Eine bewusste Falschmeldung, die Menschen dazu veranlasst etwas falsches zu glauben.

Impersonation oder Pretexting:

Vorgabe einer falschen Identität (z. B. als Mitarbeiter des IT-Supports); d. h. der Angreifer gibt sich persönlich als jemand anderes aus, um an Informationen zu gelangen und nutzt dafür keine elektronischen Hilfsmittel.

Eavesdropping: Abhören von Gesprächen, um an relevante Informationen zu gelangen.

Eliciting Information:

Der Angreifer versucht durch geschicktes Fragen an Informationen zu gelangen, die für einen Angriff nützlich sein könnten.

Baiting ( **Ködern**):

Der Angreifer bietet etwas an, um an Informationen zu gelangen (z. B. ein USB-Stick mit einem Virus, der sich beim Einstecken des USB-Sticks auf dem Rechner installiert.)

Watering Hole Attack:

Der Angreifer infiziert eine Webseite, die von der Zielgruppe häufig besucht wird, um dann die Besucher der Webseite anzugreifen.

Typo Squatting:

Ausnutzen von Tippfehlern durch das Registrieren einer Domain, die der Domain eines Zielunternehmens ähnelt, um dann Besucher der Webseite auf eine gefälschte Webseite zu leiten. (z. B. *www.gooogle.com*)

Quishing/QR phishing:

D. h. der Angreifer erstellt einen QR Code, der auf eine gefälschte Webseite führt. Der QR Code wird dann z. B. auf einem Plakat angebracht oder zum Beispiel an einer Säule zum Kaufen von Fahrkarten, um möglichst viele Personen glaubhaft zu erreichen.

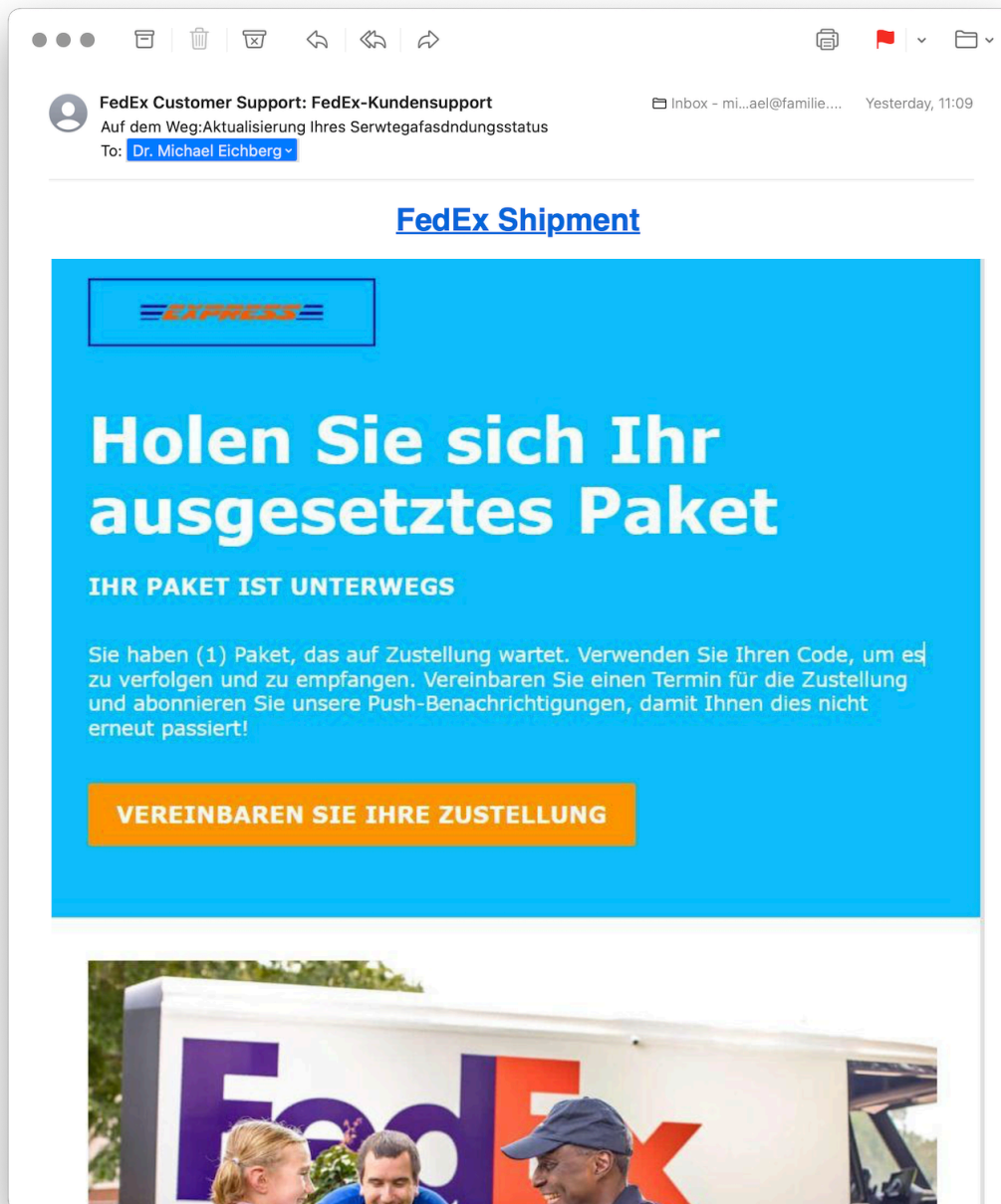
HOAX

Ein Beispiel eines nicht-harmlosen Streichs (Hoax) ist die Falschmeldung vom 1. April 2003, dass Bill Gates gestorben sei. Diese Falschmeldung wurde von vielen Menschen geglaubt und hatte relevanten Einfluss auf den Aktienmarkt.

Credential harvesting

In der Anfangszeit von Github und Bitbucket wurden häufig Zugangsdaten und Zertifikate in öffentlichen Repositories gefunden, da die Nutzer diese im Quellcode hinterlegt hatten oder sogar als Ressourcen direkt eingebunden hatten.

Typische Phishing E-Mail



„Motivationstechniken“ von Angreifern

- Autorität: Der Angreifer gibt sich z. B. als Mitarbeiter des IT-Supports aus.
- Einschüchterung (👊 *Intimidation*)
- Dringlichkeit („*In 10 Minuten verschlüssele ich den Rechner.*“)
- Konsens („*Alle machen das so.*“)
- Knappheit („*Es sind nur noch drei Rechner nicht infiziert.*“)
- Vertrautheit
- Vertrauen

3. Cybersicherheit stärken

Bug-Bounty-Programme

Microsoft to offer hackers millions in Zero Day Quest event

Microsoft on Tuesday unveiled Zero Day Quest, a bug bounty event offering up to \$4 million in rewards to security researchers.

"At the end of the day, we recognize that when it comes to security, it's fundamentally a team sport," Microsoft CEO Satya Nadella said during his Tuesday keynote. "And that's why we want to partner, and we're partnering broadly with the security community."

[...] Zero Day Quest is the "largest of its kind" and will offer a potential \$4 million in awards for research into cloud and AI, which he described as "high-impact areas."

*—19.11.2024 **Techtarget***

Bug-Bounty-Programme sind Initiativen, die Einzelpersonen oder Forschergruppen für das Finden und Melden von Softwarefehlern belohnen. Diese Programme werden häufig von Softwareanbietern initiiert, um die Sicherheit ihrer Produkte zu verbessern.

Post-Quantum Cryptography (PQC) Einführen

A joint statement from partners from 18 EU member states[...]

This threat to cryptography [i. e. established public-key cryptography is no longer secure] is posed by the development of a [...] quantum computer, which can break traditional public-key cryptographic schemes, [...] due to Shor's algorithm. While there are currently no such cryptographically relevant quantum computers (CRQC) available, their development is progressing rapidly [...] preparing for the quantum threat should be considered an integral aspect of cyber security risk management.

[...] we currently strongly recommend to deploy PQC in hybrid solutions for most use-cases, i.e. combining a deployed cryptographic scheme with PQC in such a way that the combination remains secure even if one of its components is broken.

[...] The transition should also consider cryptoagility, allowing to ensure a more resilient transition to PQC[...]

—27.11.2024 **Securing Tomorrow, Today: Transitioning to PQC**

Quantencomputer - Bedrohungsbewertung

[Bewertung der Bedrohung durch Quantencomputer]

[...] preparing for the quantum threat should be considered an integral aspect of cybersecurity risk management. In an attempt to quantify the risk, the 2023 issue of the Quantum Threat Timeline conducted a survey among 37 international leading experts from academia and industry. Out of these, 17 estimated the risk that a CRQC appears within a 10-year timeframe higher than 5%. Moreover, 10 of these respondents even indicated a likelihood of about 50% or more.

[...] To ensure an acceptable level of readiness, we recommend that these should be protected against "store now, decrypt later" attacks as soon as possible, latest by the end of 2030.

—27.11.2024 **Securing Tomorrow, Today: Transitioning to PQC**

Die NIS 2 Richtlinie

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

NIS 2 Richtlinie (NIS 2 Directive)

- Die NIS2-Richtlinie ist die zweite EU-Richtlinie zur Netz- und Informationssicherheit (NIS) in der EU.
- *seit 17. Oktober 2024 müss(t)en alle nationalstaaten entsprechende Regelungen in nationales Recht umgesetzt haben und ab 18. Oktober 2024 anwenden*
- Das Hauptziel ist die Verbesserung der Widerstandsfähigkeit gegen Cyberkriminalität und die Verbesserung des europäischen und nationalen Cybersecurity-Managements.

Die neue NIS-2-Richtlinie zielt darauf ab, die Widerstandsfähigkeit und Reaktionsfähigkeit des öffentlichen und privaten Sektors zu verbessern. Der Schwerpunkt der Richtlinie liegt auf der Bekämpfung der Cyberkriminalität.
- Die NIS-2-Richtlinie gilt für Organisationen, inkl. Unternehmen und Zulieferer, die durch Erbringung wesentlicher oder wichtiger Dienstleistungen eine entscheidende Rolle für die Aufrechterhaltung der europäischen Wirtschaft und Gesellschaft spielen.
- Die Führungskräfte von betroffenen Einrichtungen sind für die Überwachung der Umsetzung der NIS-2-Richtlinie verantwortlich und können für Verstöße gegen die NIS-2-Richtlinie haftbar gemacht werden (Artikel 20).

Artikel 20, Governance

1. *Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können. [...]*
2. *Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.*

—NIS 2 - KAPITEL IV **RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BE-
REICH DER CYBERSICHERHEIT**

NIS 2 - Berichtspflichten

- Wesentliche und wichtige Einrichtungen müssen unverzüglich (*in jeden Fall aber innerhalb von 24 Stunden*) über jeden Sicherheitsvorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat
- Ein Sicherheitsvorfall gilt als erheblich, wenn
 - a. er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
 - b. er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Von NIS2 betroffene öff. und priv. Einrichtungen[2]

Folgende Organisation mit mehr als 50 Mitarbeitern und einem Umsatz von mehr als 10 Millionen Euro müssen die NIS-2-Richtlinie einhalten (obligatorisch).

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemie
- Lebensmittel
- Herstellung medizinischer Geräten
- Computer und Elektronik
- Maschinen
- Kraftfahrzeuge
- Energie
- Verkehrswesen
- Bankwesen
- Finanzmarkt-Infrastrukturen
- Gesundheitswesen
- Trinkwasserversorgung und -verteilung
- Digitale Infrastrukturen
- Online-Marktplätze
- Online-Suchmaschinen
- Cloud Computing-Dienste

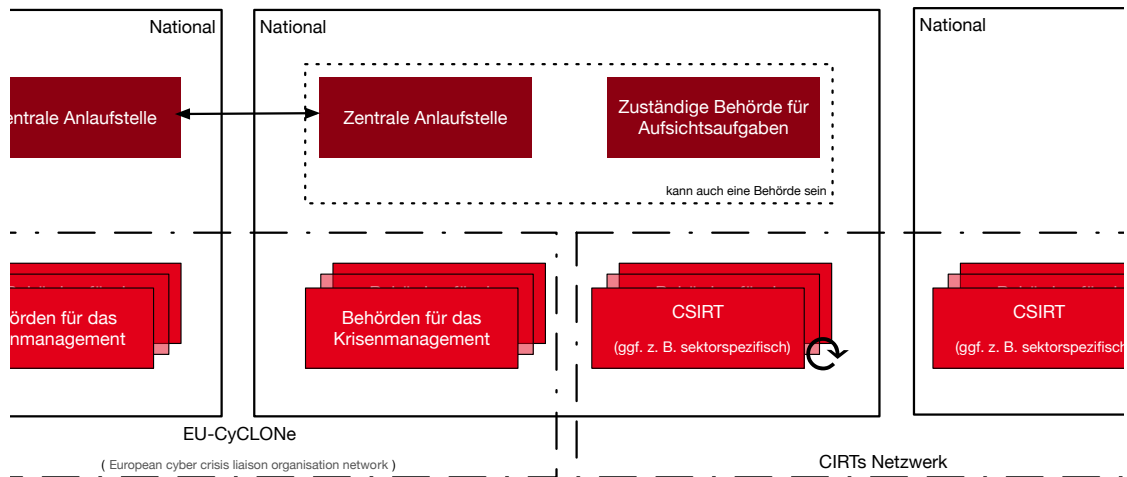
Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domännennamen-Registrierungsdienste erbringen und aktualisieren sie gegebenenfalls regelmäßig — spätestens alle 2 Jahre.

[2] Details siehe Anhang I und II der NIS 2 Richtlinie

Achtung!

Jeder Mitgliedstaat erlässt eine *nationale Cybersicherheitsstrategie*, die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält.

NIS 2 - zentrale Einrichtungen



Legende

CSIRT:

Computer Security Incident Response Team

Behörden für das Krisenmanagement:

Sollte es mehr als eine geben, so wird eine explizit benannt, die für die Koordination und das Management von *Cybersicherheitsvorfällen großen Ausmaßes und Krisen* zuständig ist

Ein zentraler Gedanke ist die Vernetzung der zuständigen Behörden sowohl auf nationaler als auch auf europäischer Ebene sicherzustellen.

4. Von der Bedeutung von Schwachstellen

CVSS, CVE, NVD, CVD, KEV, EPSS, VEP

Definition von Schwachstellen nach CVE

*"Eine Schwachstelle in der Berechnungslogik (z. B. Code), die in Software- und Hardwarekomponenten gefunden wird und die, wenn sie ausgenutzt wird, zu einer negativen Auswirkung auf die **Vertraulichkeit**, **Integrität** oder **Verfügbarkeit** führt. Die Behebung der Schwachstellen in diesem Zusammenhang umfasst in der Regel Änderungen am Code, kann aber auch Änderungen an der Spezifikation oder sogar die Ablehnung der Spezifikation (z. B. die vollständige Entfernung der betroffenen Protokolle oder Funktionen) beinhalten."*

—<https://nvd.nist.gov/vuln> (Übersetzt mit DeepL)

In der Praxis werden n-Day und 0-Day Schwachstellen unterschieden.

Das Common Vulnerability Scoring System (CVSS)^[3]





CVSS 4.0 stellt einen Rahmen bereit für die Beschreibung und Bewertung des Schweregrads von Software-/Hardware-/Firmwareschwachstellen.

Die Bewertung der Basiskennzahlen ergibt eine Punktzahl zwischen 0,0 und 10,0. Wobei 0 bedeutet, dass die Schwachstelle (bisher) harmlos ist und 10,0 bedeutet, dass die Schwachstelle sehr gravierend ist.

Harmlos ist im Prinzip damit gleichzusetzen, dass die Schwachstelle nicht ausgenutzt werden kann oder dass die Auswirkungen nicht weiter relevant sind.






[3] CVSS 4.0

CVSS umfasst vier Gruppen von Metriken


- 01** Basis-Metriken ( *Base Metrics*) erfassen die inhärenten Eigenschaften einer Schwachstelle, die sich nicht ändern, wenn sich die Umgebung ändert.
- 02** Bedrohungs-Metriken ( *Threat Metric Group*) spiegelt die Merkmale einer Schwachstelle wieder, die sich im Laufe der Zeit verändern.
- 03** Umgebungs-Metriken ( *Environmental Metric Group*) erfassen die Eigenschaften einer Schwachstelle, die sich ändern, wenn sich die Umgebung ändert.
- 04** Ergänzende-Metriken ( *Supplemental*) liefern zusätzliche Informationen, die für die Bewertung einer Schwachstelle nützlich sein können, aber den Schweregrad nicht direkt beeinflussen.




CVSS - Basis-Metriken (*Base Metric Group*)


Bewertung der Ausnutzbarkeit (*Exploitability Metrics*)




- Angriffsvektor ( *Attack Vector*)
- Angriffskomplexität ( *Attack Complexity*)
- Angriffsanforderungen ( *Attack Requirements*)
- Benötigte Privilegien ( *Privileges Required*)
- Erforderliche Benutzerinteraktion ( *User Interaction*)

Bewertung der Auswirkungen (*Impact Metrics*)

bzgl. des betroffenen Systems ( *Vulnerable System*)

- Vertraulichkeit ( *Confidentiality Impact*)
- Integrität ( *Integrity Impact*)
- Verfügbarkeit ( *Availability Impact*)

bzgl. nachgelagerter Systeme ( *Subsequent System*)

- Vertraulichkeit ( *Confidentiality Impact*)
- Integrität ( *Integrity Impact*)
- Verfügbarkeit ( *Availability Impact*)

CVSS - Bedrohungs-Metriken (*Threat Metric Group*)[4]

■ Reifegrad des Exploits ( *Exploit Maturity*)

Gibt es bisher nur die Beschreibung der Schwachstelle oder gibt es bereits einen Proof-of-Concept (PoC) Exploit?

[4] Die Namen und der Gruppenzuschnitt (hier:  *Temporal Metric Group*) waren unter **CVSS 3.0** anders.

CVSS - Bewertung der Ausnutzbarkeit (*Exploitability Metrics*)

Attack Vector (AV): Network, Adjacent, Local, Physical

Attack Complexity (AC):

Low, High

Attack Requirements (AT):

None, Present

Privileges Required (PR):

None, Low, High

User Interaction (UI):

None, Passive, Active

Attack Vector

Network

Schwachstellen, die häufig "aus der Ferne ausnutzbar" sind und als ein Angriff betrachtet werden können, der auf Protokollebene über einen oder mehrere Netzknoten hinweg (z. B. über einen oder mehrere Router) ausgenutzt werden kann.

Adjacent

Der Angriff ist auf eine logisch benachbarte Topologie beschränkt. Dies kann z. B. bedeuten, dass ein Angriff aus demselben gemeinsamen Nahbereich (z. B. Bluetooth, NFC oder IEEE 802.11) oder logischen Netz (z. B. lokales IP-Subnetz) gestartet werden muss.


Local

Der Angreifer nutzt die Schwachstelle aus, indem er lokal auf das Zielsystem zugreift (z. B. Tastatur, Konsole) oder über eine Terminalemulation (z. B. SSH); oder der Angreifer verlässt sich auf die Interaktion des Benutzers, um die zum Ausnutzen der Schwachstelle erforderlichen Aktionen durchzuführen (z. B. mithilfe von Social-Engineering-Techniken, um einen legitimen Benutzer zum Öffnen eines bösartigen Dokuments zu verleiten).

Physical

Der Angreifer muss physisch Zugriff auf das Zielsystem haben, um die Schwachstelle auszunutzen.

Attack Complexity

Wie aufwendig ist es explizite Schutzmaßnahmen ((K)ASLR, Stack Canaries, ...) zu umgehen. Wie wahrscheinlich ist es, dass ein Angriff erfolgreich ist. Im Falle von  *Race Conditions* können ggf. sehr viele Ausführungen notwendig sein bevor die Race Condition erfüllt ist.

Attack Requirements

Welcher Vorbedingungen (unabhängig von den expliziten Sicherungsmaßnahmen) müssen erfüllt sein, damit die Schwachstelle ausgenutzt werden kann. (z. B. der Nutzer muss sich an seinem Smartphone mindestens einmal seit dem Boot angemeldet haben (*After-First-Use* vs. *Before-First-Use*)).

Privileges Required

Welche Privilegien muss der Angreifer mindestens haben, um die Schwachstelle auszunutzen (Sind Administratorrechte erforderlich oder reichen normale Benutzerrechte).

User Interaction

Passiv bedeutet hier, dass der Nutzer unfreiwillig die Schwachstelle ausnutzt ohne bewusst Schutzmechanismen zu unterlaufen. Aktiv bedeutet, dass der Nutzer aktiv Interaktionen unternimmt, um die Schutzmechanismen des Systems auszuhebeln (z. B. durch das Installieren einer nicht-signierten Anwendung aus dem Internet).

CVSS - Bewertung der Auswirkung auf das betroffene System/Vulnerable System Impact Metrics

Confidentiality Impact (C):

None, Low, High

Integrity Impact (I):

None, Low, High

Availability Impact (A):

None, Low, High

CVSS - Bewertung der Auswirkung auf das nachgelagerte System/Vulnerable System Impact Metrics

Confidentiality Impact (C):

None, Low, High

Integrity Impact (I):

None, Low, High

Availability Impact (A):

None, Low, High

Diskussion: Schwachstellen und Ihre Bewertung

Ihnen liegt eine externe Festplatte vor, die Hardwareverschlüsselung unterstützt. D. h. wenn diese Festplatte an einen Computer angeschlossen wird, dann muss ein Passwort eingegeben werden, bevor auf die Daten zugegriffen werden kann. Dieses entsperren der Festplatte geschieht mit Hilfe eines speziellen Programms, dass ggf. vorher installiert werden muss. Die Festplatte ist mit AES-256-XTX verschlüsselt.

Das Clientprogramm *hasht* erst das Passwort clientseitig, bevor es den *Hash* an den Controller der Festplatte überträgt. Die Firmware des Controllers validiert das Passwort in dem es den gesendeten Hash direkt mit dem bei der Einrichtung übermittelten Hash vergleicht; d. h. es finden keine weiteren sicherheitsrelevanten Operationen außer dem direkten Vergleich statt. Zum Entsperren der Festplatte ist es demzufolge ausreichend, den Hash aus der Hardware auszulesen und diesen an den Controller zu senden, um die Festplatte zu entsperren. Danach kann auf die Daten frei zugegriffen werden.

? Frage

Wie sieht der **CVSS 4.0 Score** für diese Schwachstelle aus? (**CVSS Rechner**)

5. Common Vulnerabilities and Exposures (CVE)


Zweck von CVEs

- Schwachstellen eindeutig identifizieren und bestimmten Versionen eines Codes (z. B. Software und gemeinsam genutzte Bibliotheken) mit diesen Schwachstellen verknüpfen.
- Kommunikationsgrundlage bilden, damit mehrere Parteien über eine eindeutig identifizierte Sicherheitslücke diskutieren können. **National Vulnerabilities Database - NIST**

1. Jan. 2024 - zuletzt bewertete CVEs

- **CVE-2024-20672** - .NET Denial of Service Vulnerability
V3.1: 7.5 HIGH
- **CVE-2024-20666** - BitLocker Security Feature Bypass Vulnerability
V3.1: 6.6 MEDIUM
- **CVE-2024-20680** - Windows Message Queuing Client (MSMQC) Information Disclosure
V3.1: 6.5 MEDIUM
- **CVE-2024-20676** - Azure Storage Mover Remote Code Execution Vulnerability
V3.1: 8.0 HIGH
- **CVE-2024-20674** - Windows Kerberos Security Feature Bypass Vulnerability
- **CVE-2024-20682** - Windows Cryptographic Services Remote Code Execution Vulnerability
V3.1: 7.8 HIGH
- **CVE-2024-20683** - Win32k Elevation of Privilege Vulnerability
V3.1: 7.8 HIGH
- **CVE-2024-20681** - Windows Subsystem for Linux Elevation of Privilege Vulnerability
V3.1: 7.8 HIGH
- ...

National Vulnerability Database (NVD)[5]

- Auflistung aller CVEs und deren Bewertung
 - Alle Schwachstellen in der NVD sind mit einer CVE-Kennung versehen
 - Die NVD ist ein Produkt der NIST Computer Security Division, Information Technology Laboratory
 - Verlinkt häufig weiterführend Seiten, die Lösungshinweise und Tools bereitstellen, um die Schwachstelle zu beheben
 - Verweist auf entsprechende Schwachstellen gemäß **CWEs**
 - Verlinkt gelegentlich *PoC Exploits* ( *Proof-of-Concept Exploits*)
-


[5] Die NIS 2 Richtlinie der EU sieht auch den Aufbau einer europäischen Schwachstellen-Datenbank vor. Aktuell ist die NVD die zentrale Anlaufstelle bzgl. Schwachstellen.

Common Weakness Enumeration (CWE)

- eine kollaborativ entwickelte, vollständig durchsuchbare, kategorisierte Liste von Typen von Software- und Hardware-Schwachstellen und deren Beschreibung, dient als:
 - gemeinsame Sprache,
 - Messlatte für Sicherheitstools,
 - als Grundlage für die Identifizierung von Schwachstellen sowie für Maßnahmen zur Abschwächung und Prävention.

CWE - Schwachstellenkatalog TOP 25 in 2023

Rank	ID	Name	Rank Change vs. 2022
1	CWE-787	Out-of-bounds Write	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation (" <i>Cross-site Scripting</i> ")	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command (" <i>SQL Injection</i> ")	0
4	CWE-416	Use After Free	+3
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command (" <i>OS Command Injection</i> ")	+1
6	CWE-20	Improper Input Validation	-2
7	CWE-125	Out-of-bounds Read	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory (" <i>Path Traversal</i> ")	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	0
11	CWE-862	Missing Authorization	+5
12	CWE-476	NULL Pointer Dereference	-1
13	CWE-287	Improper Authentication	+1
14	CWE-190	Integer Overflow or Wraparound	-1
15	CWE-502	Deserialization of Untrusted Data	-3
16	CWE-77	Improper Neutralization of Special Elements used in a Command (" <i>Command Injection</i> ")	+1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	+2
18	CWE-798	Use of Hard-coded Credentials	-3
19	CWE-918	Server-Side Request Forgery (SSRF)	+2
20	CWE-306	Missing Authentication for Critical Function	-2
21	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization (" <i>Race Condition</i> ")	+1
22	CWE-269	Improper Privilege Management	+7
23	CWE-94	Improper Control of Generation of Code (" <i>Code Injection</i> ")	+2
24	CWE-863	Incorrect Authorization	+4
25	CWE-276	Incorrect Default Permissions	-5

Request Forgery =  *Anfragefälschung*

Fest codierte Cloud-Zugangsdaten in populären Apps entdeckt

Betroffen sind mehrere Apps mit teils Millionen von Downloads. Den Entdeckern zufolge gefährdet dies nicht nur Backend-Dienste, sondern auch Nutzerdaten.

Sicherheitsforscher von Symantec haben Anwendungen aus dem Google Play Store und dem Apple App Store untersucht und dabei festgestellt, dass mehrere Apps mit teils Millionen von Downloads fest codierte und unverschlüsselte Anmeldedaten für verschiedene Clouddienste enthalten. Entdeckt wurden sowohl Schlüssel für den Zugang zu AWS-Ressourcen als auch solche für Microsoft Azure. [...]

—23.10.2024 **Golem.de**

CVE-2023-51034 - Arbitrary Code Execution

TOTOLink EX1200L V9.3.5u.6146_B20201023 is vulnerable to arbitrary command execution via the cste cgi UploadFirmwareFile interface.

—Published: December 22, 2023; Last modified: January 2, 2024

Bewertung: CVSS V3.1: 9.8 Critical

PoC Exploit: [815yang.github.io](https://github.com/815yang)

Weakness Enumeration:

CWE-434 Unrestricted Upload of File with Dangerous Type

Bei TOTOLink EX1200L handelt es sich um einen Wifi Range Expander.

PoC ≙ Proof-of-Concept

CWE-434 Unrestricted Upload of File with Dangerous Type^[6]

■ **Beschreibung**

Das Produkt ermöglicht es dem Angreifer, Dateien gefährlicher Typen hochzuladen oder zu übertragen, die in der Produktumgebung automatisch verarbeitet werden können.

■ **Art der Einführung**

Diese Schwäche wird durch das Fehlen einer Sicherheitstaktik während der Architektur- und Entwurfsphase verursacht.

■ **Scope**

Willkürliche Codeausführung ist möglich, wenn eine hochgeladene Datei vom Empfänger als Code interpretiert und ausgeführt wird. [...] Somit ist ggf. die Integrität, Vertraulichkeit und Verfügbarkeit betroffen.

[6] [Mitre.org](#) (2023; übersetzt mit DeepL)

CVE-2023-51034 - PoC (gekürzt)

Initiale Anfrage

```
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 [...]
3 {
4   "FileName":
5     ";ls../>/www/yf.txt;",
6   "topicurl":
7     "UploadFirmwareFile"
8 }
```

Abfrage der Datei (hier: yf.txt)

```
1 GET /yf.txt HTTP/1.1
2 [...]
3 Connection: close
```

Das Ergebnis ist eine Datei mit der Auflistung der Dateien im Verzeichnis (. .).

CVE-2023-51034 - zugrundeliegende Schwachstelle

```
1 Var = (const char *)websGetVar(a1, "FileName", &byte_42FE28);
2 v3 = (const char *)websGetVar(a1, "FullName", &byte_42FE28);
3 v4 = (const char *)websGetVar(a1, "ContentLength", &word_42DD4C);
4 v5 = websGetVar(a1, "flags", &word_42DD4C);
5 v6 = atoi(v5);
6 Object = cJSON_CreateObject();
7 v8 = fopen("/dev/console", "a");
8 v9 = v8;
9 if ( v8 )
10 {
11     fprintf(v8, "[%s:%d] FileName=%s,FullName=%s,ContentLength=%s\n",
12             "UploadFirmwareFile", 751, Var, v3, v4);
13     fclose(v9);
14 }
15 v10 = strtol(v4, 0, 10) + 1;
16 strcpy(v52, "/tmp/myImage.img");
17 doSystem("mv %s %s", Var, v52);
```

Die Lücke ist auf die folgenden Zeilen zurückzuführen:

```
1 Var = (const char *)websGetVar(a1, "FileName", &byte_42FE28);
2 ...
3 doSystem("mv %s %s", Var, v52);
```

Der Aufruf von doSystem ermöglicht die Ausführung von beliebigem Code. Der Angreifer kann den Wert von Var so manipulieren, dass er quasi beliebigen Code ausführen kann.

Ausgenutzte Schwachstellen

Der **Known Exploited Vulnerabilities (KEV) Katalog der CISA** umfasst Produkte deren Schwachstellen ausgenutzt wurden oder aktiv ausgenutzt werden.

■ Kriterien für die Aufnahme in den KEV Katalog:

1. Eine CVE-Id liegt vor.
2. Die Schwachstelle wird aktiv ausgenutzt (🇺🇸 *Active Exploitation*) (ggf. reicht es jedoch wenn „nur“ ein *Honeypot* aktiv angegriffen wurde) - ein PoC reicht nicht aus.
3. Eine Handlungsempfehlung liegt vor (z. B. Patch, Workaround oder vollständige Abschaltung).

■ Firmen sollten die KEV *Schwachstellen priorisieren*, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu verringern.

CISA = *Cybersecurity and Infrastructure Security Agency* (oder *America's Cyber Defense Agency*)

Ausgewählte Amerikanische Behörden sind sogar verpflichtet innerhalb vorgegebener Zeiträume zu reagieren.

2023 CWE Top 10 KEV Weaknesses

Schwachstelle	CWE ID	# CVE Mappings in KEV	Avg. CVSS
Use After Free	416	44	8.54
Heap-based Buffer Overflow	122	32	8.79
Out-of-bounds Write	787	34	8.19
Improper Input Validation	20	33	8.27
Improper Neutralization of Special Elements used in an OS Command (" <i>OS Command Injection</i> ")	78	25	9.36
Deserialization of Untrusted Data	502	16	9.06
Server-Side Request Forgery (SSRF)	918	16	8.72
Access of Resource Using Incompatible Type (" <i>Type Confusion</i> ")	843	16	8.61
Improper Limitation of a Pathname to a Restricted Directory (" <i>Path Traversal</i> ")	22	14	8.09
Missing Authentication for Critical Function	306	8	8.86

Schwachstellen, die auf Fehler beim Speicherzugriff zurückzuführen sind, sind nicht (mehr) notwendig!

Google hails move to Rust for huge drop in memory vulnerabilities

[...] Memory access vulnerabilities often occur in programming languages that are not memory safe. In 2019, memory safety issues accounted for 76% of all Android vulnerabilities.

[...] the transition to memory safe languages through the gradual use of memory safe code in new projects and developments over a five year period. The results showed that despite a gradual rise in code [still] being written in memory unsafe languages, memory safety vulnerabilities dropped significantly.

[...] there has been a significant drop in the number of memory-related vulnerabilities, with memory safe vulnerabilities down to 24% in 2024 [...]

—26. September 2024 - **Techradar.com**

Offenlegung von Sicherheitslücken nach CISA [7]

Coordinated Vulnerability Disclosure (CVD)

1. Sammlung von Schwachstellenmeldungen:
 - Eigene Schwachstellenanalysen
 - Überwachung öffentlicher Quellen
 - Direkte Meldungen von Herstellern, Forschern und Nutzern
2. Analyse der Schwachstellenmeldungen zusammen mit den Herstellern, um die Sicherheitsauswirkungen zu verstehen.
3. Entwicklung von Strategien zur Eindämmung der Schwachstellen; insbesondere Entwicklung von notwendigen Patches.
4. Anwendung der Strategien zur Eindämmung der Schwachstellen in Zusammenarbeit mit dem Hersteller und ggf. betroffenen Nutzern.
5. Veröffentlichung der Schwachstellenmeldung in Abstimmung mit der Quelle des Schwachstellenberichts und dem Hersteller.

CISA (America's Cybersecurity and Infrastructure Security Agency/Cyber Defense Agency).

[7] Das BSI verfährt ähnlich; **tut sich aber sehr schwer**.

Zeitlicher Rahmen für die Offenlegung von Sicherheitslücken

Der Zeitrahmen für die Offenlegung von Sicherheitslücken wird durch folgende Faktoren bestimmt:

- Aktive Ausnutzung der Schwachstelle
- besonders kritische Schwachstellen
- Auswirkungen auf Standards
- bereits öffentlich bekannt (zum Beispiel durch einen „naïven“ Forscher)
- Auswirkungen auf die kritische Infrastruktur, öffentliche Gesundheit und Sicherheit
- die Verfügbarkeit von effektiven Eindämmungsmaßnahmen
- das Verhalten des Herstellers und die Möglichkeit der Entwicklung eines Patches
- Schätzung des Herstellers wie lange es dauert einen Patch zu entwickeln, zu testen und auszurollen.

Welche neuen Schwachstellen werden in absehbarer Zeit ausgenutzt?



Beobachtung

Am 1. Oktober 2023 hat die NVD 139.473 CVEs veröffentlicht. In den folgenden 30 Tagen wurden 3.852 CVEs beobachtet, die ausgenutzt (🚩 *exploited*) wurden.

Ca. 5-6% aller Schwachstellen werden „irgendwann“ ausgenutzt. [8]



Frage

Wie stelle ich sicher, dass ich meine Bemühungen zum Beseitigen der Schwachstellen auf diejenigen konzentriere, die am wahrscheinlichsten zeitnahe ausgenutzt werden?

[8] Fortinet, [Threat Landscape Report Q2 2018](#)

Nutzung des CVSS als Grundlage für die Schätzung?

Annahme: Schwachstellen mit einem CVSS Score ≥ 7 (d. h. mit einer Bewertung von Hoch oder kritisch) werden ausgenutzt.

- 80.024 Schwachstellen haben einen CVSS Score ≥ 7

Ausgenutzt wurden: 3.166

- 59.449 Schwachstellen haben eine CVSS < 7

Ausgenutzt wurden: 686

Zusammenfassung

Die Strategie „Priorisierung von Schwachstellen mit einem bestimmten CVSS Score“ (hier ≥ 7) ist keine geeignete Strategie, da sie nicht alle relevanten Schwachstellen erfasst (686 *False Negatives*) und - ganz insbesondere - zu viele Schwachstellen (76.858 *False Positives*) erfasst, die nicht ausgenutzt werden.

Exploit Prediction Scoring System (EPSS)

- EPSS ist eine Methode zur *Bewertung der Wahrscheinlichkeit*, dass eine Schwachstelle in den nächsten 30 Tagen ausgenutzt wird.
- EPSS basiert auf der Analyse von Schwachstellen, die in den letzten 12 Monaten ausgenutzt wurden.
- EPSS nutzt KI basierend auf folgenden Informationen (Stand Jan. 2024):
 - Hersteller
 - Alter der Schwachstelle (Tage seit der Veröffentlichung des CVEs)
 - die Beschreibung der Schwachstelle
 - betroffene CWEs
 - CVSS Bewertungen der Schwachstellen
 - Wird der CVE auf bekannten Listen diskutiert bzw. aufgelistet?
 - Gibt es öffentliche verfügbare Exploits?

Nutzung des EPSS für die Schätzung? [9]

Annahme: Schwachstellen mit EPSS 10% und größer sind werden ausgenutzt werden.

- 3.735 Schwachstellen haben ein Wahrscheinlichkeit von EPSS 10% und größer

Ausgenutzt wurden: 2.435

- 135.738 Schwachstellen haben ein EPSS < 10%

Ausgenutzt wurden: 1.417

Zusammenfassung

Die Strategie „Priorisierung von Schwachstellen mit einem EPSS von 10% und höher“ ist eine geeignetere Strategie, da sehr viele relevante Schwachstellen erfasst werden und - ganz insbesondere - die Anzahl der zu beachtenden Schwachstellen ganz massiv reduziert wird ohne die Gesamtqualität *zu stark* zu beeinflussen.

[9] Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights

Vulnerabilities Equities Process (VEP) (USA) [10]

[...] Der Vulnerability-Equity-Process (VEP) wägt ab, ob Informationen über Schwachstellen an den Hersteller/Lieferanten weitergegeben werden sollen, in der Erwartung, dass sie gepatcht werden, oder ob die Kenntnis der Schwachstelle vorübergehend auf die US-Regierung und möglicherweise andere Partner beschränkt werden soll, damit sie für Zwecke der nationalen Sicherheit und der Strafverfolgung, wie z. B. nachrichtendienstliche Erfassung, militärische Operationen und/oder Spionageabwehr, genutzt werden können. [...]

—Übersetzung: DeepL

Insbesondere durch die föderale Struktur in Deutschland kann es ggf. dazu kommen, dass bezüglich der Handhabung von Schwachstellen unterschiedliche rechtliche Regelungen gelten werden - je nachdem ob die Behörde eine Bundes- oder Landesbehörde ist.

[10] Die rechtlichen Rahmenbedingungen bzgl. eines effektiven Schwachstellenmanagement sind in Deutschland gerade in der Diskussion. (Stand Jul. 2024); Schwachstellen, die direkt an das BSI gemeldet werden, unterliegen dem vorher diskutierten CVD.

Vulnerabilities Equities Process (VEP) (USA)

[...] Die Entscheidung der US-Regierung, ob eine Schwachstelle veröffentlicht oder eingeschränkt werden soll, ist nur ein Element des Prozesses zur Bewertung der Schwachstellen und ist nicht immer eine binäre Entscheidung. Andere Optionen, die in Betracht gezogen werden können, sind die Verbreitung von Informationen zur Schadensbegrenzung an bestimmte Stellen, ohne die jeweilige Schwachstelle offenzulegen, die Einschränkung der Nutzung der Schwachstelle durch die US-Regierung in irgendeiner Weise, die Information von Regierungsstellen der USA und verbündeter Staaten über die Schwachstelle [...].

—Übersetzung: DeepL

Vulnerabilities Equities Process (VEP) (USA)

[...] Alle diese Entscheidungen müssen auf der Grundlage des Verständnisses der Risiken einer Verbreitung, des potenziellen Nutzens von Schwachstellen durch die Regierung sowie der Risiken und Vorteile aller dazwischen liegenden Optionen getroffen werden. [...]

—Übersetzung: DeepL

Schwachstellenmanagement in Deutschland - Quo Vadis?

~~[...] Die Ausnutzung von Schwachstellen von IT-Systemen steht in einem hochproblematischen Spannungsverhältnis zur IT-Sicherheit und den Bürgerrechten. Der Staat wird daher keine Sicherheitslücken ankaufen oder offenhalten, sondern sich in einem Schwachstellenmanagement unter Federführung eines unabhängigeren Bundesamtes für Sicherheit in der Informationstechnik immer um die schnellstmögliche Schließung bemühen.[...]~~

~~—KOALITIONSVERTRAG 2021—2025 (SPD, BÜNDNIS 90/DIE GRÜNEN, FDP)~~

Definitionen

Klartext:

 *Plaintext*


Die Originalnachricht, die verschlüsselt werden soll.

Geheimtext oder Chiffretext oder **Kryptogramm:**

 *Ciphertext*


Die kodierte/verschlüsselte Nachricht.

Verschlüsselung:

 *Encryption*

Der Prozess der Umwandlung von Klartext in Geheimtext.

Entschlüsselung:

 *Decryption*

Der Prozess der Wiederherstellung des Klartextes aus dem Geheimtext.

Sicherheit von Verschlüsselungsschemata

Bedingungslos Sicher (🚩 *Unconditionally Secure*)

- Unabhängig davon wie viel Zeit ein Gegner hat, ist es ihm unmöglich, den Geheimtext zu entschlüsseln, weil die erforderlichen Informationen nicht vorhanden sind.

Rechnerisch Sicher (🚩 *Computationally Secure*)

- Die Kosten für das Brechen der Chiffre übersteigen den Wert der verschlüsselten Informationen.
- Die zum Knacken der Chiffre benötigte Zeit übersteigt die Lebensdauer der Informationen.

? Frage

Wie lange könnte der Nutzen einer bestimmten Information andauern?

Eines der ersten Verschlüsselungsverfahren: Caesar Cipher

- Einfachste und früheste bekannte Verwendung einer Substitutions-Chiffre; verwendet von Julius Cäsar.
- Dabei wird jeder Buchstabe des Alphabets durch einen Buchstaben ersetzt, der drei Stellen weiter hinten im Alphabet steht.
- Am Ende des Alphabets wird wieder am Anfang begonnen. Somit folgt auf den Buchstabe Z der Buchstabe A.

```
unverschlüsselt:  meet me after the toga party
verschlüsselt:    PHHW PH DIWHU WKH WRJD SDUWB
```

Das Verfahren ist aus mehrfacher Sicht komplett unsicher und verletzt allg. Sicherheitsprinzipien.
Es ist jedoch ein einfaches Beispiel für eine Substitutions-Chiffre.

Brute-Force Angriff

- Es werden alle möglichen Schlüssel ausprobiert, bis eine verständliche Übersetzung des Chiffriertextes in Klartext erreicht wird.
- Im Durchschnitt muss die Hälfte aller möglichen Schlüssel ausprobiert werden, um Erfolg zu haben.
- Zur Durchführung des Brute-Force-Ansatzes ist ein gewisses Maß an Wissen über den zu erwartenden Klartext erforderlich. Es werden Mittel zur automatischen Unterscheidung von Klartext und „Müll“ benötigt.

Frage

Was bedeutet somit *bis eine verständliche Übersetzung des Chiffriertextes in Klartext erreicht wird*? Wenn der Klartext zum Beispiel ein Bild, ein Video oder ein Computerprogramm ist?

Hashfunktionen

- Eine Hashfunktion H akzeptiert eine beliebig lange Nachricht M als Eingabe und gibt einen Wert fixer Größe zurück: $h = H(M)$.
- Eine Änderung eines beliebigen Bits in M sollte mit hoher Wahrscheinlichkeit zu einer Änderung des Hashes h führen.
- Kryptographische Hashfunktionen werden für das Signieren von Nachrichten, die Erstellung von digitalen Signaturen, die Überprüfung von Nachrichtenintegrität und bei der Speicherung von Passwörtern verwendet.

Kollisionen bei Hashes

Wenn ein Passwort „nur“ als Hash gespeichert wird, dann gibt es zwangsläufig Kollisionen und es kann theoretisch passieren, dass ein Angreifer (zufällig) ein völlig anderes Passwort findet, dass bei der Überprüfung des Passworts akzeptiert wird. Die Konstruktion kryptografischer Hashfunktionen stellt jedoch sicher, dass dies in der Praxis nicht auftritt. Sollte jedoch eine „normale Hashfunktion“ genommen werden, dann ist dieses Szenario durchaus realistisch.

SHA256 Hashfunktion - Beispiele

ok: 2689367b205c16ce32ed4200942b8b8b1e262dfc70d9bc9fbc77c49699a4f1df

password:

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

Password:

e7cf3ef4f17c3999a94f2c6f612e8a888e5b1026878e4e19398b23bd38ec221a

12345678:

ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f

12345679:

b759803bc6037a05e6564b6447a755b7f3862ba4d0d746785dbe133dcb6c8f4d

"this is a very, very long password that would be absolutely safe for all purposes until the END of tIME!":

b915b962df3b0d49b6c7995164a0a1756885d749af214e561aa8125a9186b26d

Sicherheit - Verschlüsselung und Signaturen

Es geht im Wesentlichen um das Ver- und Entschlüsseln von Daten (X) mit Hilfe von Schlüsseln.

$E(K, X)$ bedeutet, dass wir die Nachricht X mit dem Schlüssel K verschlüsseln (🔒 *encryption*).

$D(K, X)$ bezeichnet die Umkehrfunktion, die die Daten wieder entschlüsselt (🔓 *decryption*).

Symmetrische Verschlüsselung

Der Schlüssel zur Verschlüsselung ist identisch mit dem Schlüssel zur Entschlüsselung (🔒 *decryption* (D)).

$$X = D(K, E(K, X))$$

Asymmetrische Verschlüsselung

Wir unterscheiden zwischen privaten (PR) und öffentlichen Schlüsseln (PU) ($PU \neq PR$). Ein privater und ein öffentlicher Schlüssel bilden immer ein Paar. Der private Schlüssel ist immer geheim zu halten.

Verschlüsselung von Nachrichten

Alice sendet eine Nachricht an Bob mit Hilfe des öffentlichen Schlüssels von Bob.

$$\begin{aligned} Y &= E(PU_{Bob}, X) \\ X &= D(PR_{Bob}, Y) \end{aligned}$$

Signierung von Nachrichten

Alice „signiert“ (S) eine Nachricht mit ihrem privaten Schlüssel.

$$\begin{aligned} Y &= E(PR_{Alice}, X) \\ X &= D(PU_{Alice}, Y) \end{aligned}$$

Signierung von Nachrichten mit sicheren Hashfunktionen

Alice signiert eine Nachricht X mit ihrem privaten Schlüssel.

$$Alice : [E(PR_{Alice}, H = Digest(X)), X]$$

Bob prüft die Nachricht X auf Authentizität:

$$Bob : D(PU_{Alice}, H) \stackrel{?}{=} Digest(X)$$

Verwendung von Passwörtern



Beobachtung

Klassische Passwörter werden (noch immer) in zahlreichen Bereichen verwendet.

Beispiele

- Smartphones
- Cryptosticks
- Logins für Computer und Serversysteme
- verschlüsselte Dateien und Datenträger
- "als Backup"

Hintergrund

Obwohl an vielen Stellen versucht wird Passwörter aus vielen Gründen zurück zu drängen, so ist die Verwendung noch allgegenwärtig und in machen Bereichen ist auch nicht unmittelbar eine Ablösung zu erkennen.

Biometrie ist zum Beispiel in machen Bereichen kein Ersatz für Passwörter und wird - wenn überhaupt - nur ergänzend genommen. So ist es zum Beispiel im deutschen Recht erlaubt/möglich einem Beschuldigten sein Smartphone bei Bedarf vor das Gesicht zu halten, um es zu entsperren (Stand 2023). Je nach Qualität des Fingerabdrucksensors können ggf. auch genommene Fingerabdrücke verwendet werden. Möchte der Beschuldigte jedoch das Passwort nicht freiwillige nennen, dann besteht keine direkte weitere Handhabe.

Passwortbasierte Angriffe auf Unternehmen

Microsoft said hackers working for the Russian government breached its corporate networks recently and stole email from executives and some employees to find out what the company knew about them. The tech company said the breach was not due to any flaw in its software, but rather began with a “password spraying.” The technique worked on what Microsoft said was an old test account, and the hackers then used the account’s privileges to get access to multiple streams of email.

—19. Januar 2024: The Washington Post; Joseph Menn

Ist Passwortwiederherstellung nicht „trivial“?

59 Prozent aller Passwörter in unter 60 Minuten knackbar

Forscher haben per Brute-Force-Methode mit einer Nvidia GeForce RTX 4090 Millionen von Passwörtern aus dem Darknet geknackt.

[...] Sicherheitsforscher von Kaspersky haben untersucht, wie schnell sich gängige Passwörter mit einer modernen GPU vom Typ Nvidia GeForce RTX 4090 knacken lassen. Durchgeführt wurde die Untersuchung anhand einer Datenbank mit 193 Millionen echten Nutzerpasswörtern, die die Forscher aus dem Darknet bezogen. Sämtliche Passwörter lagen dabei in Form von gesalzenen MD5-Hashes vor. [...]

—21. Juni 2024: ***golem.de***

An AI cracked your password. Time It Takes Using AI to Crack Your Password.^[11]

# OF CHARACTER	Numbers Only	Lowercase Letters	Lower- & Uppercase Letters	Numbers, Upper- & Lowercase Letters	Numbers, Upper- & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	4 Seconds
7	Instantly	Instantly	22 Seconds	42 Seconds	6 Minutes
8	Instantly	3 Seconds	19 Minutes	48 Minutes	7 Hours
9	Instantly	1 Minutes	11 Hours	2 Days	2 Weeks
10	Instantly	1 Hours	4 Weeks	6 Months	5 Years
11	Instantly	23 Hours	4 Years	38 Years	356 Years
12	25 Seconds	3 Weeks	289 Years	2K Years	30K Years
13	3 Minutes	11 Months	16K Years	91K Years	2M Years
14	36 Minutes	49 Years	827K Years	9M Years	187M Years
15	5 Hours	890 Years	47M Years	613M Years	14Bn Years
16	2 Days	23K Years	2Bn Years	26Bn Years	1Tn Years
17	3 Weeks	812K Years	539.72M Years	2Tn Years	95Tn Years
18	10 Months	22M Years	7.23Bn Years	96Tn Years	6Qn Years

Aus dem "Paper":

We used [...] PassGAN to run through a list of 15,680,000 passwords. [...]

[11] Home Security Heroes

Check Your Accounts: 10 Billion Passwords Exposed in Largest Leak Ever

The 'RockYou2024' database includes almost 10 billion passwords pulled from 'a mix of old and new data breaches.' Here's how to check if yours are at risk.

[...]Researchers at Cybernews have uncovered a massive trove of nearly 10 billion passwords on a popular hacking forum in what they're calling "largest password compilation" ever.

The file, titled `rockyou2024.txt`, was posted on July 4 by someone going by the name ObamaCare and contains a mind-boggling 9,948,575,739 unique plaintext passwords. The user only joined the forum in late May, but they've posted data from other breaches, too. [...]

—6. Juli 2024: **PCMag**

Raum der Passwortkandidaten

vierstellige PIN: 10.000 Kombinationen

Passwort mit 8 Zeichen und 70 Zeichen im Zeichensatz (a-z, A-Z, 0-9 und ausgewählte Sonderzeichen):
 $70^8 = 576.480.100.000.000 \approx 5,7 \times 10^{14}$ Kombinationen

Passphrase mit 6 Wörtern aus einem Wörterbuch mit 2.000 Wörtern:
 $2.000^6 = 6,4 \times 10^{19}$ Kombinationen

Passphrase mit 4 Wörtern aus einem Wörterbuch mit 100.000 Wörtern:
 $100.000^4 = 1 \times 10^{20}$ Kombinationen

Passwort mit 16 Zeichen und 84 Zeichen im Zeichensatz (a-z, A-Z, 0-9 und die meisten Sonderzeichen):
 $84^{16} = 6,14 \times 10^{30}$ Kombinationen

Eine vierstellige PIN kann niemals als sicher angesehen werden. Selbst wenn ein Bruteforce nur auf 4 oder 5 Versuche pro Stunde kommt, so ist es dennoch in wenigen Monaten möglich die PIN zu ermitteln.

Quellen für Passwortkandidaten

- Wörterbücher
- Verzeichnisse (z. B. Postleitzahlen, Städte, Straßennamen)
- Leaks

(Sammlungen von realen Passwörtern, die meist von Hackern veröffentlicht wurden.)

- Rockyou
- LinkedIn
- Sony
- etc.

Qualität von Passworten

Wie ist die Qualität der folgenden Passwörter zu bewerten in Hinblick darauf wie aufwändig es ist das Passwort ggf. wiederherzustellen:

1. Donaudampfschiffahrt
2. Passwort
3. ME01703138541
4. 2wsx3edc4rfv
5. Haus Maus
6. iluvu
7. Emily18
8. MuenchenHamburg2023!!!!
9. hjA223dn4fw"üäKßß k`≤~ajsdk
10. Baum Lampe Haus Steak Eis Berg
11. password123

8. Kryptografische Hashfunktionen und Passwörter

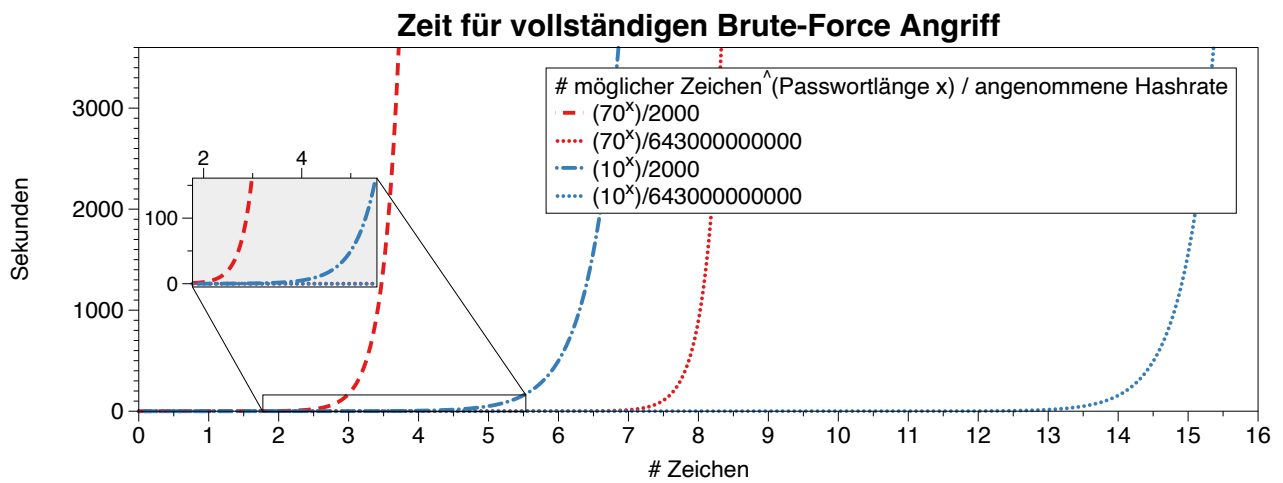
Hashraten in MH/s auf aktueller Hardware

Hashcat Mode (Hashcat 6.2.6)	Hash	RTX 1080Ti (250 W)	RTX 2080TI (260 W)	RTX 3090 (350 W)	RTX 4090 (450 W)
25700	Murmur				643700.0 (643 GH/s)
23	Skype	21330.1	27843.1	37300.7	84654.8
1400	SHA2-256	4459.7	7154.8	9713.2	21975.5
10500	PDF1.4-1.6	24.9	29.8	76.8	122.0
1800	SHA 512 Unix (5000 Iterations)	0.2	0.3	0.5	1.2
13723	Veracrypt SHA2- 512 + XTX 1536Bit	0.0004	0.0006	0.0009	0.002 (2000 H/s)

Quellen:

- 4090: <https://gist.github.com/Chick3nman/e4fcee00cb6d82874dace72106d73fef>
- 3090: <https://gist.github.com/Chick3nman/e4fcee00cb6d82874dace72106d73fef>
- 1080Ti: <https://www.onlinehashcrack.com/tools-benchmark-hashcat-nvidia-gtx-1080-ti.php>
- 2080Ti: <https://gist.github.com/binary1985/c8153c8ec44595fdabbf03157562763e>

Brute-Force Angriff auf lange Passworte



Kryptografische Hashfunktionen für Passworte

Warnung

Bekannte kryptografische Hash-Funktionen wie MD4, MD5, SHA-256, SHA-512 oder auch RIPEMD sind für das Hashen von Passwörtern nicht geeignet.

- Zur Schlüsselableitung bzw. zum Hashen von Passwörtern wurden spezialisierte Funktionen entwickelt. Zum Beispiel: PBKDF2, Scrypt, Bcrypt und die Argon2 Familie. Diese widerstehen gängigen Angriffen.
PBKDF2 verwendet zum Beispiel beim Hashing von Passwörtern klassische Basisalgorithmen (z. B. SHA-256) und wiederholt diese mehrfach (ggf. viele hunderttausend Male), um die Laufzeit zu verlängern und es für Angreifer schwieriger zu machen.
- Diese Algorithmen sind parametrisierbar, um sie an verschiedene Zwecke anpassen zu können. Je nach Parametrisierung sind diese so rechenintensiv, dass sie z. B. nicht für Webanwendungen mit vielen Nutzern geeignet sind.

Parametrisierungen, die die Laufzeit und den Speicherbedarf so stark erhöhen, dass eine Verwendung in Webanwendungen nicht mehr sinnvoll ist, können z. B. ideal sein zum Schutz von Dateien, Containern oder lokaler Festplatten.

Vom Salzen (🇺🇸 Salt) ...

Beobachtung/Problem

Werden Passwörter direkt mit Hilfe einer kryptografischen Hashfunktion gehasht, dann haben zwei Nutzer, die das gleiche Passwort verwenden, den gleichen Hash.

User	Hash
Alice	sha256_crypt.hash('DHBWMannheim',salt='',rounds=1000) = \$5\$rounds=1000\$1b/CwYgN/xR9dqYuYxYVtWkxMEh.VK.QOC9IKmy9DP/
Bob	sha256_crypt.hash('DHBWMannheim',salt='',rounds=1000) = \$5\$rounds=1000\$1b/CwYgN/xR9dqYuYxYVtWkxMEh.VK.QOC9IKmy9DP/

Lösung

Passwörter sollten immer mit einem einzigartigen und zufälligen „Salt“ gespeichert werden, um Angriffe mittels Regenbogentabellen zu verhindern.

User	Hash
Alice	sha256_crypt.hash('DHBWMannheim',salt='0123456',rounds=1000) = \$5\$rounds=1000\$0123456\$66x8MB.qev25coq9OVrD1lr1ZGJJelAzOVlCDZykrY0
Bob	sha256_crypt.hash('DHBWMannheim',salt='1234567',rounds=1000) = \$5\$rounds=1000\$1234567\$LxD/hg29N9KYpNdFMW69Kk65BLkVL1z1SEJvqhCmFU9

Rainbow Tables

Eine *Rainbow Table* (🇺🇸 Regenbogentabelle - Verwendung jedoch nicht gängig) bezeichnet eine vorberechnete Tabelle, die konzeptionell zum einem Hash ein jeweilig dazugehöriges Passwort speichert und einen effizienten Lookup ermöglicht. Dies kann ggf. die Angriffsgeschwindigkeit sehr signifikant beschleunigen, auch wenn die Tabellen sehr groß sind und ggf. in die Terabytes gehen.

Aufgrund der allgemeinen Verwendung von Salts sind Angriffe mit Hilfe von Regenbogentabellen heute (fast nur noch) von historischer Bedeutung.

Verwendung sicherer Hash- bzw. Schlüsselableitungsfunktionen für Passworte

Argon2:	z. B. verwendete von LUKS2
bcrypt:	basierend auf Blowfish; z. B. verwendet in OpenBSD
scrypt:	z. B. (ergänzend) verwendet für das Hashing von Passwörtern auf Smartphones
yescrypt:	z. B. moderne Linux Distributionen
PBKDF2-HMAC-SHA256:	Ethereum Wallets

Bemerkung

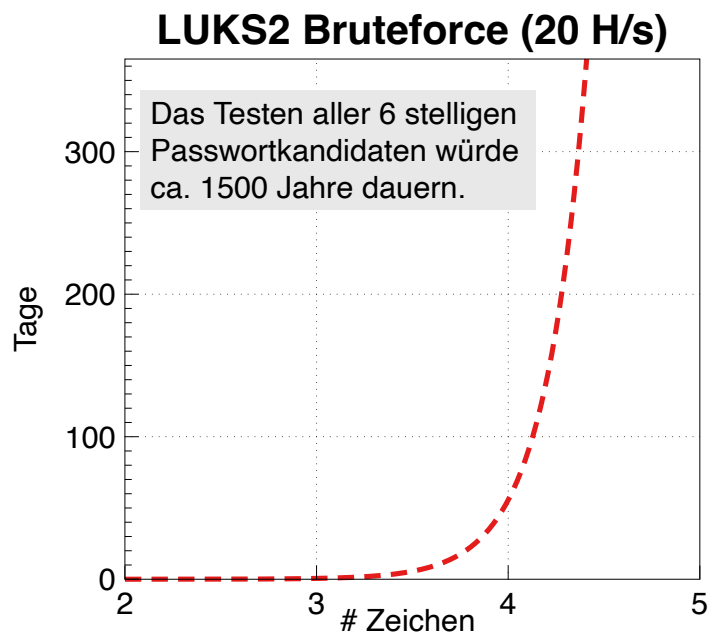
Häufig werden die „Hashwerte“ von Passwörtern in Datenbanken oder Dateien als Base64 kodierter String gespeichert.

Angriff auf LUKS2 mit Argon2

[...] The choice of Argon2 as a KDF makes GPU acceleration impossible. As a result, you'll be restricted to CPU-only attacks, which may be very slow or extremely slow depending on your CPU. To give an idea, you can try 2 (that's right, two) passwords per second on a single Intel(R) Core(TM) i7-9700K CPU @ 3.60GHz. Modern CPUs will deliver a slightly better performance, but don't expect a miracle: LUKS2 default KDF is deliberately made to resist attacks. [...]

—Elcomsoft **LUKS2 with Argon2**

Effizienz eines Brute-Force Angriffs auf LUKS2



9. Passworte Verstehen

Aufbau von Passwörtern

Von Menschen vergebene Passwörter basieren häufig auf Kombinationen von Wörtern aus den folgenden Kategorien:

- Pins: 1111, 1234, 123456, ...
 - Tastaturwanderungen (👉 *keyboard walks*): asdfg, q2w3e4r5t, ...
 - Patterns: aaaaa, ababab, abcabcabc, ...
 - Reguläre Wörter aus Wörterbüchern: Duden, Webster, ...
 - Kontextinformationen:
 - szenetypisch: acab, 1888, 1488[12], oder bestimmte Marken (z. B. Gucci, Ferrari), ...
 - privates Umfeld: Namen von Kindern, Eltern, Hunden, Geburtsort, Adresse, ...
-

[12] 14 oder 1488 ist ein numerischer Code für die vierzehn Worte des David Eden Lane. (Er war ein Mitbegründer der Terrororganisation *The Order*, die für die Vorherrschaft der weißen Rasse in den USA kämpfte.)

Häufige Passworte

Eine gute Quelle für das Studium von Passwörtern sind sogenannte *Leaks* oder auch Listen mit gängigen Passwörtern. Zum Beispiel **Becker's Health IT 2023**:

123456	abc123	princess
password	1234	letmein
123456789	password1	654321
12345	iloveyou	monkey
12345678	1q2w3e4r	27653
qwerty	000000	1qaz2wsx
1234567	qwerty123	123321
111111	zaq12wsx	qwertyuiop
1234567890	dragon	superman
123123	sunshine	asdfghjkl

Hinweise

- Die Listen ändern sich in der Regel von Jahr zu Jahr nicht wesentlich.
- Die konkrete Methodik ist oft fragwürdig; in der Gesamtheit aber dennoch aussagekräftig.

Die Struktur von Passwörtern in Rockyou

Hier haben wir alle **Kleinbuchstaben auf l**, **Großbuchstaben auf u**, **Ziffern auf d** und **Sonderzeichen auf s** abgebildet.

llllllll	4,8037%	llllllldd	1,4869%	ddddddddddddd	0,2683%	ddddddll	0,1631%
llllll	4,1978%	llllld	1,3474%	llldddd	0,2625%	llllls	0,1615%
lllllll	4,0849%	llllldd	1,3246%	llllllllldd	0,2511%	dddlll	0,1613%
lllllllll	3,6086%	llllllllll	1,3223%	llllllllllll	0,2340%	dllllll	0,1583%
ddddddd	3,4003%	llldddd	1,2439%	llldddd	0,2322%	dlllll	0,1575%
dddddddddd	3,3359%	llllldddd	1,2109%	lldddd	0,2270%	llldddd	0,1560%
ddddddddd	2,9878%	llllldddd	1,1204%	uuuuuudd	0,2189%	dddddddl	0,1557%
llllldd	2,9326%	llllllld	1,1168%	dddll	0,2169%	uuuudd	0,1551%
lllllllll	2,9110%	llllldd	1,0633%	ldddd	0,2064%	llllldddd	0,1395%
dddddd	2,7243%	llllldd	0,9225%	ddddddddddddd	0,2017%	ddl	0,1391%
ddddddddd	2,1453%	llllllld	0,9059%	ullllld	0,1930%	ullll	0,1379%
llllldd	2,0395%	lllll	0,8793%	dddllll	0,1905%	uuuuuuuuuu	0,1378%
llllllldd	1,9092%	llllllllll	0,8334%	uuuuuuuuu	0,1886%	llllls	0,1374%
lllllllll	1,8697%	llllld	0,8005%	uuuuudd	0,1815%	llllllld	0,1345%
llldddd	1,6420%	llldd	0,7759%	llllllldd	0,1808%	llllllldd	0,1344%
llldd	1,5009%	dddddddddd	0,7524%	llllllldd	0,1725%

Analyse auf Grundlage des „berühmten“ Rockyou-Lecks.

Die Zusammensetzung von Passwörtern verstehen

Analyse des ersten/original *Rockyou* Leaks.

Σ Passworte	14.334.851	100%
Pins	2.346.591	16,37%
Passworte mit Buchstaben	11.905.977	83,34%

Analyse der Passworte mit Buchstaben:

Kategorie	Absolut	Prozentual	Beispiele		
E-Mails	26.749	0,22%	me@me.com		
Zahlen gerahmt von Buchstaben	35696	0,30%	a123456a		
Leetspeak	64.672	0,54%	G3tm0n3y		
Patterns	124.347	1,04%	lalala		
Reguläre oder Populäre Wörter	4.911.647	41,25%	princess	iloveu	
Sequenzen	5.290	0,04%	abcdefghijklmnopqrstuvwxyz		
keyboard walks (de/en)	14.662	0,12%	q2w3e4r		
Einfache Wortkombinationen	535.037	4,49%	pinkpink	sexy4u	te amo
Komplexe Wortkombinationen	5.983.259	50,25%	Inparadise	kelseylovesbarry	
<Rest>	204.618	1,72%	j4**9c+p	i(L)you	p@55w0rd

Hinweise

Die Sprachen, die bei der Identifizierung der Wörter berücksichtigt wurden, waren: "de, en, fr, es, pt, nl".

Populäre Wörter sind Wörter, die auf Twitter oder Facebook verwendet wurden, z. B. "iloveu", "iluvu",

Gedankenexperiment

9.1. Kosten und Aufwand für Passwortwiederherstellung

Sie wollen einen *SHA-256* angreifen und sie haben 100 Nvidia 4090 GPUs. Jede GPU hat eine Hash-Rate von $\sim 22\text{GH/s}$ (mit Hashcat 6.2.6) und benötigt ~ 500 Watt pro Stunde (Wh). Der verwendete Zeichensatz besteht aus 84 verschiedenen Zeichen (z. B. a-z, A-Z, 0-9, <einige Sonderzeichen>).

1. Wie lange dauert es, ein 10-stelliges Passwort zu ermitteln (Worst Case)?
2. Wie viel Geld wird es Sie kosten, ein 10-stelliges Passwort zu knacken (Worst Case), wenn 1kWh 25ct kostet?
3. Werden Sie im Laufe Ihres Lebens in der Lage sein, ein Passwort mit 12 Zeichen Länge zu ermitteln?

Gedankenexperiment

9.2. Verstehen des Suchraums

Sie haben „ganz viele“ Grafikkarten und einen sehr schnellen Hash. Sie kommen auf eine Hashrate von 1 THash/Sekunde (1×10^{12}). Sie haben einen Monat Zeit für das Knacken des Passworts. Gehen Sie vereinfacht davon aus, dass Ihr Zeichensatz 100 Zeichen umfasst.

Berechnen Sie den Anteil des Suchraums, den Sie abgesucht haben, wenn das Passwort 32 Zeichen lang sein sollte und Sie dies wissen. Drücken Sie den Anteil des abgesuchten Raums in Relation zu der Anzahl der Sandkörner der Sahara aus. Gehen Sie davon aus, dass die Sahara ca. 70 Trilliarden (70×10^{21}) Sandkörner hat.[13]

[13] [Astronom widerlegt die Sandkorn These \(Welt.de\)](#)

Effekte von Passwortrichtlinien

Moderne Passwortrichtlinien (📄 *Password Policies*) machen es unmöglich, ältere Leaks *direkt* zu nutzen.

Beispiele:

- Mindestanzahl von Zeichen (maximale Anzahl von Zeichen)
- Anforderungen an die Anzahl der Ziffern, Sonderzeichen, Groß- und Kleinbuchstaben
- Anforderungen an die Vielfalt der verwendeten Zeichen
- einige Passwörter (z. B. aus bekannten Leaks und Wörterbüchern) sind verboten
- ...

Passwortrichtlinien extrem: **Password Game**

Die wichtigsten **NIST-Richtlinien** für Passwörter:

- Mindestlänge von 8 Zeichen.
- Keine Komplexitätsanforderung. Benutzer sollten auch die Möglichkeit haben, Leerzeichen einzufügen, um die Verwendung von Phrasen zu ermöglichen. Für die Benutzerfreundlichkeit [...] kann es von Vorteil sein, wiederholte Leerzeichen in getippten Passwörtern vor der Überprüfung zu entfernen.

Der Effekt von Passwortrichtlinien auf Passwörter

Reale Passwortrichtlinie:

Nutze 1 Großbuchstabe, 1 Kleinbuchstabe, 2 Symbole, 2 Ziffern, 4 Buchstaben, 4 Nicht-Buchstaben

Exemplarisch beobachteter Effekt wenn die Passwörter vorher einfacher waren und der Benutzer gezwungen wurde diese zu erweitern:

Password11##

Password12!!

d. h. die Passworte werden mit möglichst geringem Aufwand erweitert.

Aufbau von Passwörtern - Zusammenfassung

- Passwörter, die häufig eingegeben werden müssen, basieren in den allermeisten Fällen auf „echten“ Wörtern.
- Echte Wörter werden oft nicht unverändert verwendet, sondern nach einfachen Regeln umgewandelt, z. B. durch Anhängen einer Zahl oder eines Sonderzeichens, Veränderung der Groß-/Kleinschreibung, etc.

Frage

Wie können wir gute Passwortkandidaten identifizieren/generieren, wenn ein *Leak* nicht ausreicht oder nur eine kleine Anzahl von Passwörtern getestet werden kann?

Zum Beispiel dauert das Testen aller Passwörter von Rockyou...:

~13.000.000 Passworte / 5 Hashes/Sekunde \approx 1 Monat

~13.000.000 Passworte / 5 Hashes/Stunde \approx ~297 Jahre

Bewertung von Passwörtern

- **Donaudampfschiffahrt:** Ist weder in Rockyou noch im Duden und auch nicht in den Corpora von Twitter und Facebook von 2022 zu finden.
- **Password:** Nr. 93968 in Rockyou.
- **password123:** Nr. 1348 in Rockyou.
- **2wsx3edc4rfv:** So nicht in Rockyou, aber 1qaz2wsx3edc4rfv ist Nr. 143611 in Rockyou.
- **Haus Maus:** In Rockyou ist lediglich hausmaus zu finden.
- **iluvu:** Nr. 1472 in Rockyou.
- **Emily060218:** Emily ist Nr. 35567 in Rockyou. Die Zahl ist ganz offensichtlich ein Datum: 6. Feb. 2018 und könnte ein Geburtsdatum, Hochzeitsdatum, oder ein für die Person vergleichbar bedeutends Datum sein.
- **MuenchenHamburg2023!!!!*:** Das Passwort ist zwar sehr lang aber es handelt sich vermutlich um zwei - für die entsprechende Person - bedeutende Orte. Die Zahl und die Sonderzeichen sind vermutlich auf eine Passwortrichtlinie zurückzuführen.
- **hjA223dn4fw"üäKßß k`≤~ajsdk:** 28 Stellen basierend auf einem Zeichensatz, der vermutlich ca. 192 Zeichen pro Stelle umfasst.
- **Baum Lampe Haus Steak Eis Berg:** Es handelt sich um ein Passwort mit 30 Stellen, das vermutlich mit Hilfe von Diceware generiert wurde und 6 Worte umfasst.
- **ME01703138541:** Namenskürzel und Telefonnummer.

Diceware

Auch wenn dem Angreifer (a) bekannt ist, dass das Passwort mit Hilfe von Diceware generiert wurde, (b) die zugrundeliegende Wortliste vorliegt und (c) auch die Länge (hier 6 Worte) bekannt sein sollte, dann umfasst der Suchraum: $(6^5)^6 \approx 2,21 \times 10^{23}$ Passwortkandidaten. Sollte man also mit einer Geschwindigkeit von 1 Billion Hashes pro Sekunde angreifen können, dann braucht man noch immer über 7000 Jahre für das Absuchen des vollständigen Suchraums.

Beim klassischen Dicewareansatz umfasst das Wörterbuch 6^5 Worte, da man mit einem normalen Würfel fünfmal würfelt und dann das entsprechende Wort nachschlägt. Würde man zum Beispiel die folgenden Zahlen würfeln: 1,4,2,5,2. Dann würde man das Wort zur Zahl: 14252 nachschlagen.

Schwachstellen in Passwort-Managern

Das Bundesamt für Informationssicherheit (BSI) hat zusammen mit der Münchner Firma MGM Security Partners zwei Passwort-Manager im Rahmen des Projekts zur Codeanalyse von Open-Source-Software (Caos 3.0) auf mögliche Mängel überprüft. Die Tester wurden dabei vor allem bei Vaultwarden fündig.

[...] "Vaultwarden sieht keinen Offboarding-Prozess für Mitglieder vor" [...] "Das bedeutet, dass die für den Datenzugriff notwendigen Master-Schlüssel in diesem Fall nicht ausgetauscht werden." Folglich besitze die ausscheidende Person, der eigentlich der Zugang entzogen werden sollte, weiterhin den kryptografischen Schlüssel zu den Daten der Organisation. [...]

"Das Admin-Dashboard ist anfällig für HTML-Injection-Angriffe", haben die Prüfer zudem entdeckt (CVE-2024-39926, Risiko mittel).[...]

*—15.10.2024 - Heise.de **BSI: Forscher finden Schwachstellen in Passwort-Managern***

Password Sniffing

In der Anfangszeit: unverschlüsselte Übertragung von Passwörtern (telnet, ftp, ...)

In der Übergangszeit:

Verwendung von Einmal-Passwörtern (S/Key, ...)

Heute:

Passwörter werden verschlüsselt übertragen (ssh, https, ...)

Zusätzliche Absicherung durch Zwei-Faktor-Authentifizierung (basierend auf Einmalpassworten: TOTP, ...)

Unverschlüsselte Passwörter können leicht mittels eines Sniffers, der den Netzwerkverkehr mitschneidet (z. B. Wireshark), abgefangen werden.

Einmal-Passwörter

Die Idee ist, dass Passwörter nur genau einmal gültig sind und nicht wiederverwendbar sind.

- Tokens (z. B. RSA SecurID)
- Codebuch: Liste von Einmal-Passwörtern, die das gemeinsame Geheimnis sind.
- S/Key: Passwort „wird mit einem Zähler kombiniert“ und dann gehasht.

Das S/Key Verfahren

Einmal-Passwort-System nach Codebuch-Verfahren.

Initialisierung

1. Der Nutzer gibt sein Passwort W ein; dies ist der geheime Schlüssel.
(Sollte W bekannt werden, dann ist die Sicherheit des Verfahrens nicht mehr gewährleistet.)
2. Eine kryptografische Hash-Funktion H wird n -mal auf W angewandt, wodurch eine Hash-Kette von n einmaligen Passwörtern entsteht. $H(W), H(H(W)), \dots, H^n(W)$
3. Das initiale Passwort wird verworfen.
4. Der Benutzer erhält die n Passwörter, die in umgekehrter Reihenfolge ausgedruckt werden:
 $H^n(W), H^{n-1}(W), \dots, H(H(W)), H(W)$.
5. Nur das Passwort $H^n(W)$, das an erster Stelle der Liste des Benutzers steht, der Wert von n und ggf. ein Salt, wird auf dem Server gespeichert.

Anmeldung

Identifiziere das letzte verwendete Passwort n .

- Der Server fragt den Nutzer nach dem Passwort $n - 1$ (d. h. $H^{n-1}(W)$) und übermittelt ggf. auch den Salt.
- Der Server hasht das Passwort und vergleicht es dann mit dem gespeicherten Passwort $H^n(W)$.
- Ist das Passwort korrekt, dann wird der Nutzer angemeldet und der Server speichert das Passwort $H^{n-1}(W)$ als neues Passwort $H^n(W)$ und dekrementiert n .

Im Original basiert S/Key auf der kryptographischen Hashfunktion MD4. Ein Austausch wäre aber selbstverständlich möglich!

Intern verwendet S/KEY 64-bit Zahlen. Für die Benutzbarkeit werden diese Zahlen auf sechs kurze Wörter, von ein bis vier Zeichen, aus einem öffentlich zugänglichen 2048-Wörter-Wörterbuch ($2048 = 2^{11}$) abgebildet. Zum Beispiel wird eine 64-Bit-Zahl auf "ROY HURT SKI FAIL GRIM KNEE" abgebildet.

HMAC-based one-time password (HOTP)[14]

- ermöglicht die Erzeugung von Einmal-Passwörtern auf Basis eines geheimen Schlüssels und eines Zählers; Parameter:
 - Ein kryptografisches Hash-Verfahren H (Standard ist SHA-1)
 - einen geheimen Schlüssel K , der eine beliebige Bytefolge ist
 - Ein Zähler C , der die Anzahl der Iterationen zählt
 - Länge des Passworts: d (6-10, Standardwert ist 6, empfohlen werden 6-8)
- Zur Authentifizierung berechnen beide das Einmalpasswort (HOTP) und dann vergleicht der Server den Wert mit dem vom Client übermittelten Wert:

Berechnung aus dem Schlüssel K und dem Zähler C :

$$HOTP(K, C) = truncate(HMAC_H(K, C))$$

$$truncate(MAC) = extract31(MAC, MAC[(19 \times 8 + 4) : (19 \times 8 + 7)])$$

$$HOTP\ value = HOTP(K, C) \bmod 10^d \quad (\text{führende Nullen behalten!})$$

truncate verwendet die 4 niederwertigsten Bits des MAC als Byte-Offset i in den MAC. Der Wert 19 kommt daher, dass ein SHA-1 160 Bit hat und $160/8 = 20$ Byte.

extract31 extrahiert 31 Bit aus dem MAC. Das höchstwertig Bit wird (wenn es nicht 0 ist) entsprechend maskiert. Eine Schwäche des Algorithmus ist, dass beide Seiten den Zähler erhöhen müssen und, falls die Zähler aus dem Tritt geraten, ggf. eine Resynchronisation notwendig ist.

[14] <https://www.rfc-editor.org/rfc/rfc4226>

Time-based one-time password (TOTP)[15]

- Erzeugung von zeitlich limitierten Einmal-Passwörtern (z. B. 30 Sekunden)
- Basierend auf einem vorher ausgetauschten geheimen Schlüssel und der aktuellen Zeit
Z. B. Unix-Zeit in Sekunden (ganzzahlig) und danach gerundet auf 30 Sekunden.
- Es wird das HOTP Verfahren mit der Zeit als Zähler verwendet und entweder SHA-256 oder SHA-512 als Hashverfahren, d. h. $\text{TOTP value}(K) = \text{HOTP value}(K, C_T)$, wobei T die „aktuelle Zeit“ ist.

$$C_T = \lfloor \frac{T - T_0}{T_X} \rfloor$$

T_X ist die Länge eines Zeitintervalls (z. B. 30 Sekunden)

T ist die aktuelle Zeit in Sekunden seit einer bestimmten Epoche

T_0 ist bei Verwendung der Unix-Zeit 0

C_T ist somit die Anzahl der Dauern T_X zwischen T_0 und T

Das Verfahren verlangt somit, dass die Uhren von Server und Client (hinreichend) synchronisiert sind.

[15] <https://www.rfc-editor.org/rfc/rfc6238>

Why Government Workers, Military Planners Use Signal Now

This week's revelation that U.S. officials planned a recent military attack in Yemen on Signal highlights increasing use of the messaging app by U.S. government workers to communicate with colleagues, journalists, and family members without fear of monitoring or retaliation. The switch to Signal among federal workers and top government officials has raised concerns about transparency and the preservation of government correspondence and internal communications.

—25.3.2025 - ACM Technews based on The Washington Post; Shira Ovide; Danielle Abril; Hannah Natanson; et al.