

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. [...]

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:

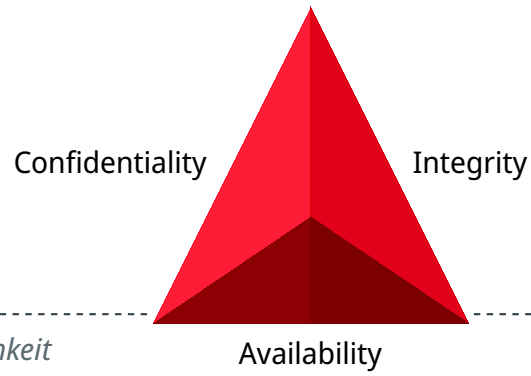
Der Angreifer erhält Zugriff auf höhere Rechte, die er vorher nicht hatte.

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.google.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.

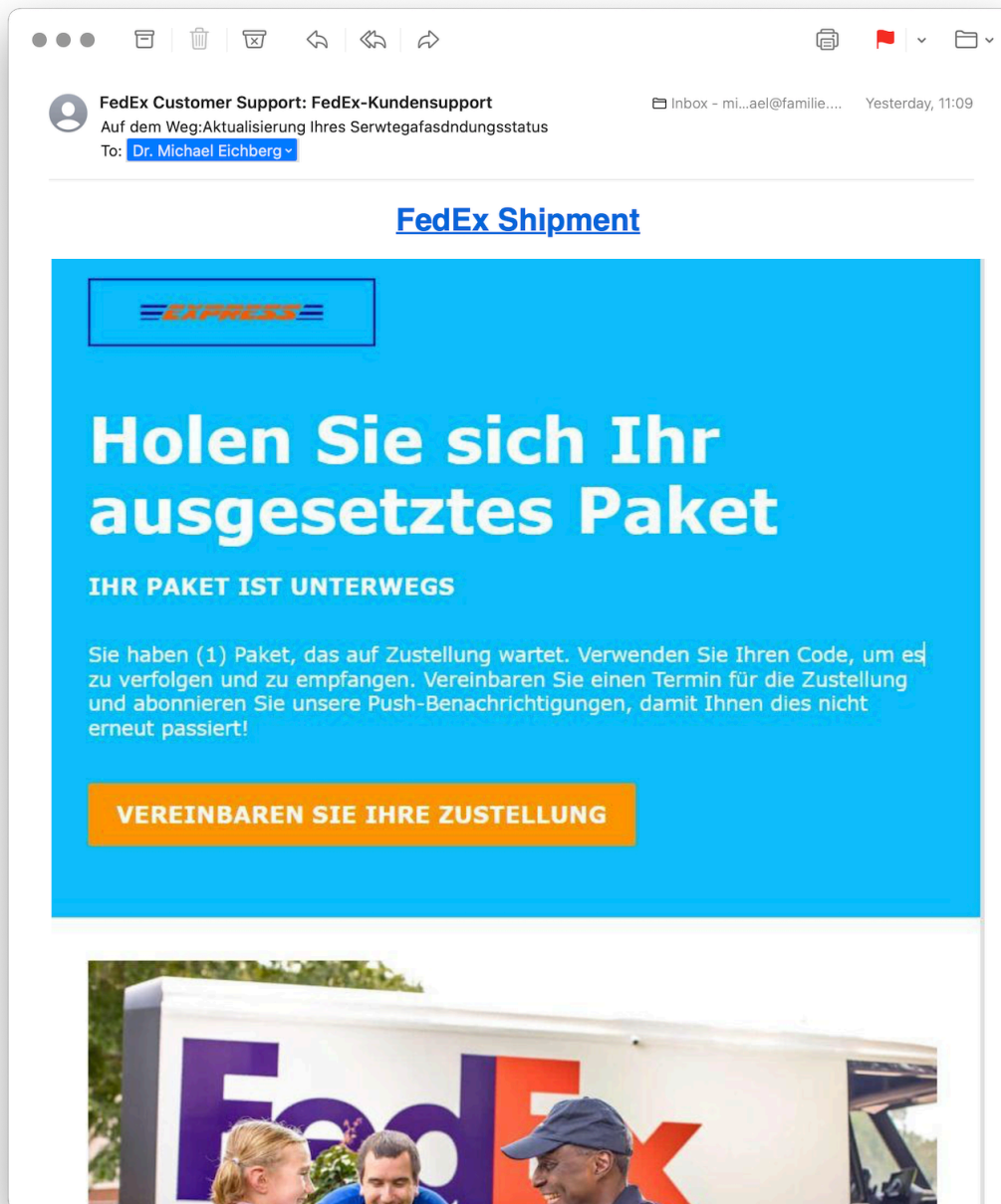
HOAX

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 muss(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

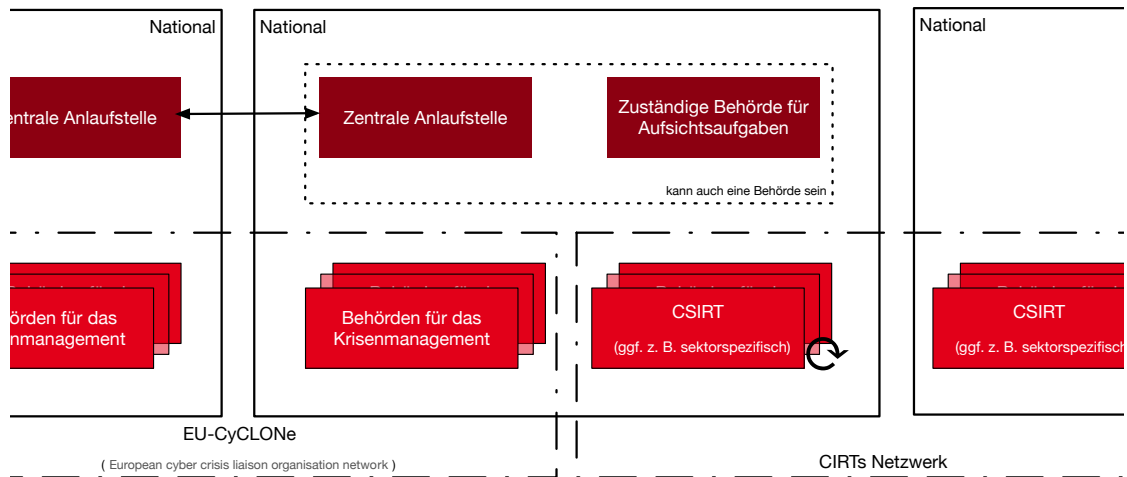
Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domännennamen-Registrierungsdienste erbringen und aktualisieren sie gegebenenfalls regelmäßig — spätestens alle 2 Jahre.

[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 böartigen 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 Sicherheitsmaßnahmen) 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

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