

Cybersecurity

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de
Version: 2.10

Folien: <https://delors.github.io/sec-cybersecurity/folien.de.rst.html>
<https://delors.github.io/sec-cybersecurity/folien.de.rst.html.pdf>
Kontrollfragen: <https://delors.github.io/sec-cybersecurity/kontrollfragen.de.rst.html>
Fehler melden: <https://github.com/Delors/delors.github.io/issues>

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

1. Neuigkeiten aus der Welt der IT-Security

Vorfälle, Forschung und Kampf gegen Cyberkriminalität

IT-Security Vorfälle

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***

UK government to ban public bodies from paying ransoms to hackers

The UK government is planning to ban public bodies from paying ransoms to computer hackers, and private companies will be required to inform authorities if they plan to cave into cash demands.

[...] The government could then provide those businesses with advice and support, including notifying them if any such payment would risk breaking the law by sending money to sanctioned cybercriminal groups, many of whom are based in Russia. [...]

*—July, 22nd, 2025 - **The Guardian***

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." [...]

Hijacked satellites and orbiting space weapons: In the 21st century, space is the new battlefield

[...] hackers backing the Kremlin hijacked an orbiting satellite that provides television service to Ukraine.

Instead of normal programing, Ukrainian viewers saw parade footage beamed in from Moscow: waves of tanks, soldiers and weaponry. The message was meant to intimidate and was an illustration that 21st-century war is waged not just on land, sea and air but also in cyberspace and the reaches of outer space. [...]

More than 12,000 operating satellites now orbit the planet, playing a critical role not just in broadcast communications but also in military operations, navigation systems like GPS, intelligence gathering and economic supply chains.[...]

GenAI Browserextensions verhalten sich unterschiedlich:

“Perplexity always prevents any collection of sensitive information. It was the most private assistant we found in our study.”

—April 24th, 2025 - **AP News**

Big Help or Big Brother? UC Davis Study Reveals Alarming Browser Tracking

[...] GenAI browser assistants use large language models to make browsing easier and more personalized, and act as your ride-along as you surf the web. [...] these assistants can pose a significant threat to user privacy. [They] often collect personal and sensitive information and share that information with both first-party servers and third-party trackers [...] one GenAI browser extension, collected form inputs as well. While filling out a form on the IRS website, [teh extension] exfiltrated the social security number that was provided in the form field.

—August 13th, 2025 - **UC Davis**

Chameleon Channels: Measuring YouTube Accounts Repurposed for Deception and Profit

[...] We explore this problem of repurposed channels, whereby a channel changes its identity and contents. [...] By observing YouTube channels (re)sold over these 6~months, we find that a substantial number (37%) are used to disseminate potentially harmful content, often without facing any penalty. Even more surprisingly, these channels seem to gain rather than lose subscribers. [...]

We confirm that these repurposed channels share several characteristics with sold channels -- mainly, the fact that they had a significantly high presence of potentially problematic content. Across repurposed channels, we find channels that became disinformation channels, as well as channels that link to web pages with financial scams.

—July 21st, 2025 - **arXiv**

Hackers Compromise Intelligence Website Used by CIA and Other Agencies

Unidentified hackers have successfully breached a critical intelligence website used by the CIA and other U.S. agencies to manage sensitive government contracts [...]

Sources familiar with the investigation confirmed that data from Digital Hammer, one of the CIA's most sensitive technology development programs, was among the information accessed by the hackers. Digital Hammer compiles cutting-edge technologies for human intelligence gathering, surveillance, and counterintelligence operations, with a particular

focus on countering Chinese intelligence and information operations.[...]

[...] The NNSA breach, exploited zero-day vulnerabilities in Microsoft SharePoint servers. Three Chinese threat groups Linen Typhoon, Violet Typhoon, and Storm-2603 were identified as the primary actors [...].

—<https://cybersecuritynews.com/cia-intelligence-website-compromised/>

Trump administration to spend \$1 billion on ‘offensive’ hacking operations

[...] Offensive cyber operations can describe a wide range of targeted hacks against U.S. adversaries, which include the use of zero-day exploits — unknown flaws in software that give their operators the ability to hack into a target’s device — or the deployment of spyware, which can be used to steal data from a person. [...]

*—July 14th, 2025 - **TechCrunch***

Hacker sneaks infostealer malware into early access Steam game

A threat actor called EncryptHub has compromised a game on Steam to distribute info-stealing malware to unsuspecting users downloading the title.

A few days ago, the hacker (also tracked as Larva-208), injected malicious binaries into the Chemia game files hosted on Steam.

[...] According to threat intelligence company Prodaft, the initial compromise occurred on July 22, when EncryptHub added to the game files the HijackLoader malware (CVKRUTNP.exe), which establishes persistence on the victim device and downloads the Vidar infostealer (v9d9d.exe). [...] It is unclear how EncryptHub managed to add the malicious files to the game project but one explanation could be an insider helping out.

[...] This is the third case of malware slipping into Steam this year. [...]

*—July 24th, 2025 - **BleepingComputer***

Internet-wide Vulnerability Enables Giant DDoS Attacks

Researchers have uncovered a distributed denial-of-service (DDoS) vulnerability in the HTTP/2 protocol that is more serious than anything seen in two years.

Hintergrund

In August 2023, unknown threat actors carried out the largest DDoS attack [...]. It worked thanks to a then-novel technique called "Rapid Reset," which took advantage of a fundamental flaw in implementations of HTTP/2.

Now, researchers from Tel Aviv University have identified a way around the Rapid Reset fix. They named the technique "MadeYouReset," and it's once again raising the possibility that attackers could enact colossal cyberattacks [...].

[...] but a large number of the vendors that were potentially exposed to this were informed about it, and they did whatever they believed they should do. [...]

—August, 18th, 2025 - **Dark Reading**

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. [...]

—Sept. 10th, 2024 - **The Hacker News**

Nvidia warns its GPUs – even Blackwells [Released in 2024] – need protection against Rowhammer attacks

Nvidia last week advised customers to ensure they employ mitigations against Rowhammer attacks, after researchers found one of its workstation-grade GPUs is susceptible to the exploit.

Rowhammer is a method of attempting to corrupt memory by repeatedly "hammering" rows of memory cells with a burst of read or write operations. The repeat operations can create electrical interference between rows of memory cells, potentially disrupting operations.[...]

—July 13th, 2025 - **The Register**

Kampf gegen Cyberkriminalität

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**

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 hergestellt und Hunderttausende davon auf Wunsch eines Kunden mit einer DDoS-Funktion ausgestattet haben. Wie [...] unter Verweis auf Angaben der südkoreanischen Polizei berichtet, 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: CEO verhaftet**

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**

VMware Hacked As \$150,000 Zero-Day Exploit Dropped

[...] Nguyen Hoang Thach of STARLabs SG used a single integer overflow to exploit #VMware ESXi - a first in Pwn2Own history. He earns \$150,000 [...]

—May 17, 2025 - **Davey Winder**

CISA open-sources Thorium platform for malware, forensic analysis

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) today announced the public availability of Thorium. Thorium was developed [...] as a scalable cybersecurity suite that automates many tasks involved in cyberattack investigations [...]

[...] teams can use Thorium for automating [...] various file analysis workflows [such as]:

- Easily import and export tools to facilitate sharing across cyber defense teams,
- Integrate command-line tools as Docker images, [...]
- Filter results using tags and full-text search,

- Control access to submissions, tools, and results with strict group-based permissions,
- Scale with Kubernetes and ScyllaDB to meet workload demands.

[...]

—August 24th, 2025 - **BleepingComputer**

Global crackdown hits pro-Russian cybercrime, 100+ systems taken down worldwide

In a major blow to pro-Russian cybercrime, authorities across Europe and the United States launched a sweeping international crackdown on the hacking group NoName057(16) between 14 and 17 July. The coordinated operation, led by Europol and Eurojust, targeted the group's members and infrastructure.

Law enforcement and judicial authorities from Czechia, France, Finland, Germany, Italy, Lithuania, Poland, Spain, Sweden, Switzerland, the Netherlands, and the United States took part in the simultaneous actions. The investigation was further supported by ENISA and authorities from Belgium, Canada, Estonia, Denmark, Latvia, Romania, and Ukraine.

The operation disrupted a global attack infrastructure [...].

—July 16th, 2025 - **HelpNet Security**

2. Cybersicherheitsvorfälle

Cybersicherheit ist das Geschäftsrisiko Nr. 1

Cyberfälle 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. [...]

Cyberfälle (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**

More Than 25% of U.K. Businesses Hit by Cyberattack in Last Year

A survey by the U.K.'s Royal Institution of Chartered Surveyors found an increase in the share of U.K. businesses experiencing a cyberattack in the last year from 16% in 2024 to around 27%. Nearly three-quarters (73%) of respondents to the survey expect a cybersecurity incident to impact their operations in the next one to two years. Risk areas identified by the survey include building management systems, CCTV networks, Internet of Things devices, access control systems, and other operational technologies.

—2 Juli 2025 - **Summary provided by ACM; Full article: Guardian**

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 abgefließen 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.

Beispielszenario

MTTD:

Es kommt zu einer starken Häufung von gesperrten (z.B. Exchange-) Accounts aufgrund von zu vielen fehlschlagenden Anmeldeversuchen durch die vermeintlichen Nutzer. Aufgrund der hohen Zahl muss jedoch von einem Cyberangriff ausgegangen werden. *Durch eine Analyse der Log-Dateien kann festgestellt werden wann der Angriff begonnen hat und die MTTD ermittelt werden.*

MTTI:

Nach einer Analyse des Netzwerkverkehrs wird festgestellt, dass alle Anfragen von externen Rechnern aus einem definierten IP-Addressbereich erfolgen. (Eine Alternative wäre, dass die Anfragen von einem oder mehreren internen Rechner ausgehen.) Dies ist die MTTI.

MTTR:

Durch eine Rekonfiguration der Firewallregeln können die Anfragen blockiert werden und somit der Angriff eingedämmt werden. Dies ist die MTTR.

MTTN:

Als letzter Schritt muss untersucht werden welche Credentials ggf. erfolgreich gestohlen wurden und ob diese bereits genutzt wurden/werden. Nach dem Abschluss dieser Schritte kann ggf. die MTTN ermittelt werden.

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

3. 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
 - Person-in-the-middle 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:

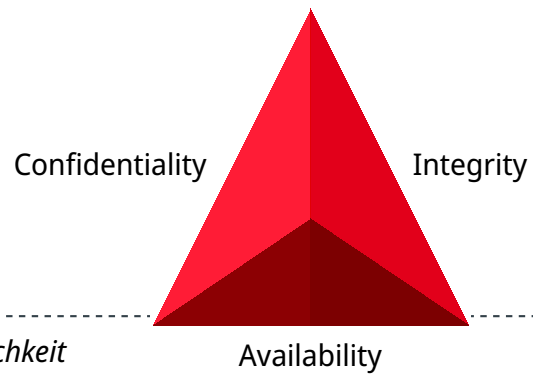
Der Angreifer erhält Zugriff auf höhere Rechte, die er vorher nicht hatte.


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?

4. 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.

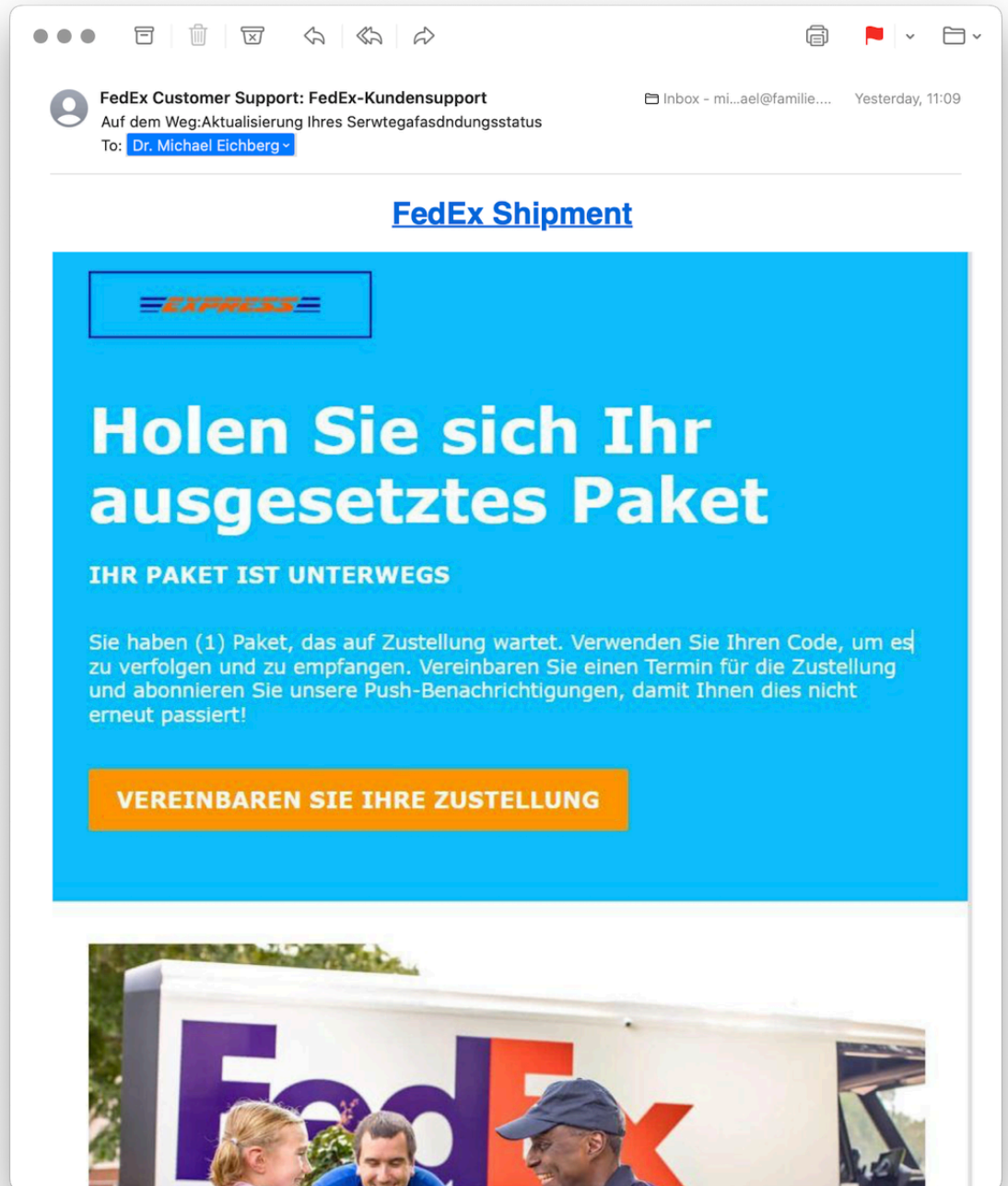
—Juli, 2024 - Zusammenfassung: **ACM**; Original: **'I Need to Identify You': How One Question Saved Ferrari From a Deepfake Scam - Bloomberg**

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.

(heise.de - Aug. 2025 - Vishing: So gelingt der Angriff per Telefon selbst auf Großunternehmen)

(Z. B. Anrufe von Europol)

Quishing/QR phishing:

Phishing mit Hilfe von QR Codes.

Beim Quishing/QR Phishing erstellt der Angreifer 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.

- 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.

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

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

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.

- 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)

Juice Jacking/Choice Jacking:

Angriffe auf Smartphones über manipulierte Ladegeräte. Beim Laden wird gleichzeitig Malware auf die Handys gespielt.

Klassisches Juice Jacking spielt (Stand 2025) auf aktuellen Smartphones von Apple und Google keine relevante Rolle mehr.

Choice Jacking war zum Beispiel bis iOS 18.4 möglich. Hierbei wird auf Fehler in den USB Implementierungen gesetzt. Insbesondere darauf, dass manche Geräte gleichzeitig USB Host und USB Device sein können - wider der Spezifikation. Dies wird dann ausgenutzt um zum Beispiel gleichzeitig eine Tastatur ein Ladegerät und eine Tastatur zu simulieren. Alternativ ist es ggf. möglich eine Bluetooth Tastatur zu simulieren. Beides wird dazu benötigt um die Dialoge, die vom Betriebssystem bei Geräteverbindungen aufgehen und als Schutz dienen sollen, unmittelbar abzunicken.

Links

<https://www.derstandard.at/story/3000000266075/choice-jacking-grazer-forscher-zeigen-wie-man-daten-vom-handy-abzapft>

bzw.

<https://www.blackhat.com/asia-25/briefings/schedule/index.html#watch-your-phone-novel-usb-based-file-access-attacks-against-mobile-devices-43262>

Dangling DNS/Subdomain Takeover:

Angreifer registrieren alte Domains, die von Firmen (temporär genutzt) wurden, in der Hoffnung, dass es noch (relevanten) Datenverkehr mit diesen Domains gibt, da möglicherweise nicht aller Code/alle Konfigurationen entsprechend umgestellt wurden. Zum Beispiel auch im Zusammenhang mit Subdomains bei Diensten wie AWS oder GitHub.


Slopsquatting:

Implementation von Softwarepaketen/-bibliotheken, die es (bisher) *nicht* gibt, die jedoch von bestimmten LLMs häufig im generierten Code eingebunden werden. Die Pakete werden dann implementiert inkl. von den Nutzern ungewünschter Funktionalität.

Slopsquatting ist (Stand Anfang 2025) deswegen möglich, da LLMs beim Generieren von Code häufiger auf nicht-existierende Pakete verweisen und diese im generierten Code importieren. Welche Paket importiert werden ist pro LLM relativ stabil aber über LLM-Grenzen hinweg sehr unterschiedlich.

Noch zu benennen: Wie an den letzten Einträgen zu erkennen ist, darf diese Liste nicht als abschließend betrachtet werden! Neue Technologien (insbesondere KI) werden (vermutlich) zu neuen Angriffen führen.

„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

5. 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**

Ergänzende Quellen

Podcasts

- [Passwort - Der Podcast von heise security](#)
- [Nachgehackt – Der IT-Security Podcast](#)
- [Spiegel Vulkan Files](#)

(Es gibt sowohl einen Podcast als auch Artikel (frei/zu bezahlen))

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

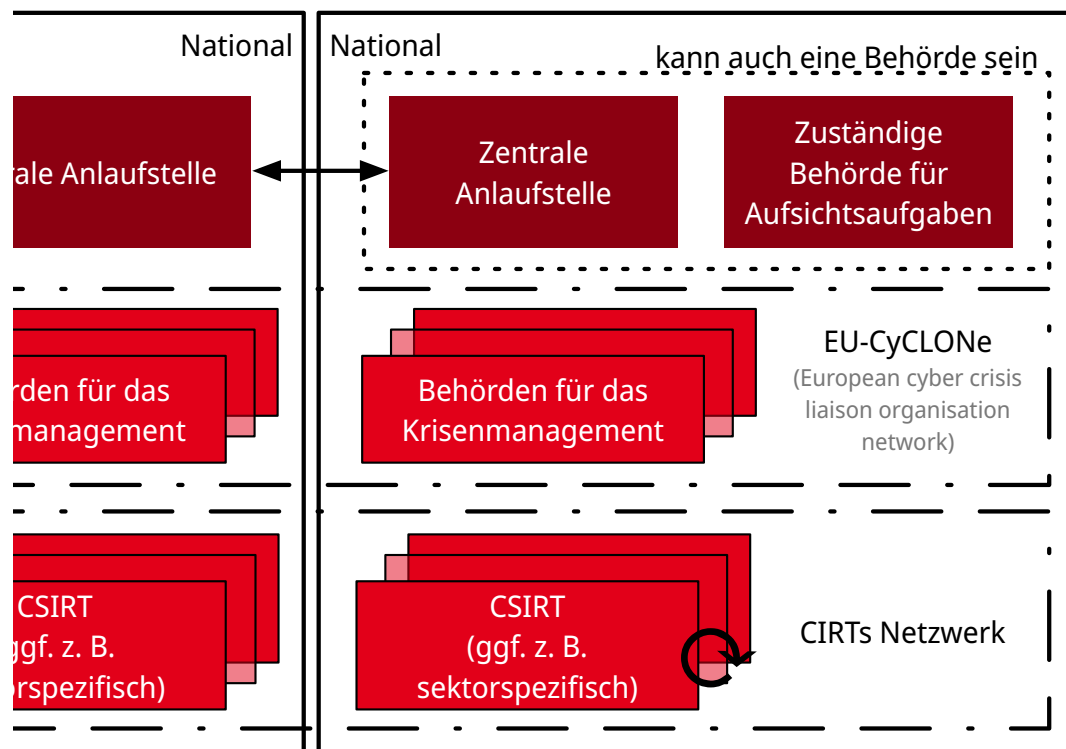
Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen und aktualisieren sie gegebenenfalls regelmäßig — spätestens alle 2 Jahre.

^[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.