Guarding Your Gateways: Security Upgrade

Fakten

- **Workshop Zeiten:**
  - **Mittwoch 11.12.2024**

    08:00 - 12:00
  - **Donnerstag 12.12.2024**

    08:00 - 12:00
  - **Freitag 13.12.2024**

    08:00 - 12:00

- **Location:** Lakeside Science & Technology Park

Wer bin ich ?

- Christian Gubesch - sehr gerne per du 🚀
- Ausbildung
  - HTL Villach Schwerpunkt: Netzwerk- und Medientechnik
  - Bachelor - Business Informatics
  - Master - Digital Entrepreneurship & Business Development
- Laufbahn
  - Cyber Security Professional - BearingPoint GmbH
    - Operations - Network and Cloud Security
    - Consulting - Cloud, Application, and OT Security
    - Business Development and Employee Training
  - Coach and Trainer for IT and CyberSec
    - TU Graz, FH Campus 02 & Fern FH Porsche
    - Freelance for Companies
    - Cyber Security Academy

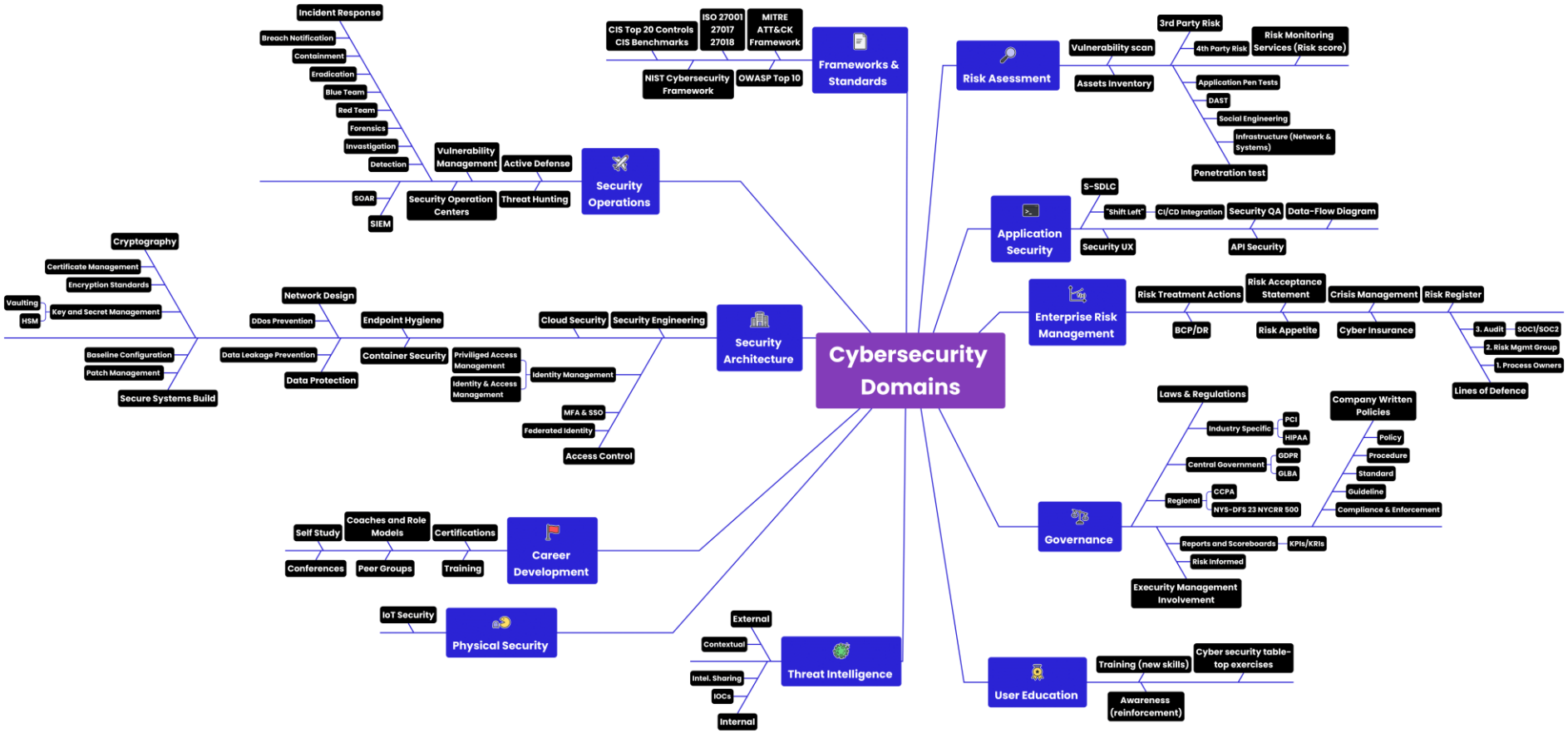
Cyber Security Academy

Wer seid ihr ?

- Hintergrund
  - Job / Aufgabenbereiche
  - Berührungspunkte im Bereich Cyber-Security?
    (Privat als auch Unternehmen)
- Vorstellungen & Erwartungen
- Nach diesem Workshop will ich in der Lage sein, …

Was bedeutet Cybersicherheit für euch?

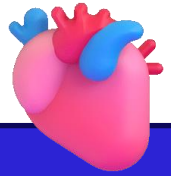
… nur mühsamer Overhead?



Quelle: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/

Wo könnte man bei euch im Unternehmen Security technisch ein Upgrade machen?

Motivation für Verbesserungen? 🔐



Worauf arbeitet ihr hin? Gibt es etwas spezielles?

Inhalte 📦

Cyberangriffe, Trends und Learnings

NIS 2 Richtlinie und die Lieferkette

Cyber Security 101 „Baseline“

Netzwerk, Infrastruktur, Cloud und Datensicherheit

Inhalte 📦

Cyberangriffe

NIS 2

Cyber Sec 101

Maßnahmen und Konzepte

Cyberangriffe 

Bekanntes, Trends und Learnings

Cyber Security Academy

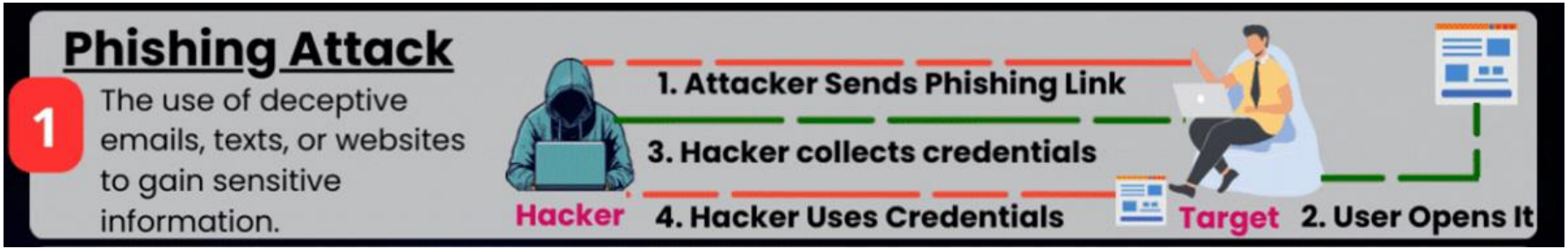
Lernziele 🚀

- Was sind gängige Arten von Cyberangriffen ?
- Welche Trends gibt es aktuell?
- Was lernen wir aus vergangenen Cyberangriffen?

Welche Cyber Angriffsarten oder Schwachstellen kennt Ihr?

Phishing Angriffe

- **Ziel:** Datenklau durch Täuschung.
- **Methoden:** E-Mail, SMS, soziale Medien, Anrufe.
- **Taktik:** Druck auf schnelle Handlungen.
- **Sicherheit:** Vorsicht bei verdächtigen Nachrichten, keine sensiblen Daten preisgeben.
- **Prävention:** Verhalten & Bewusstsein



Quelle: https://cybersecuritynews.com/

CEO Fraud

Methode?

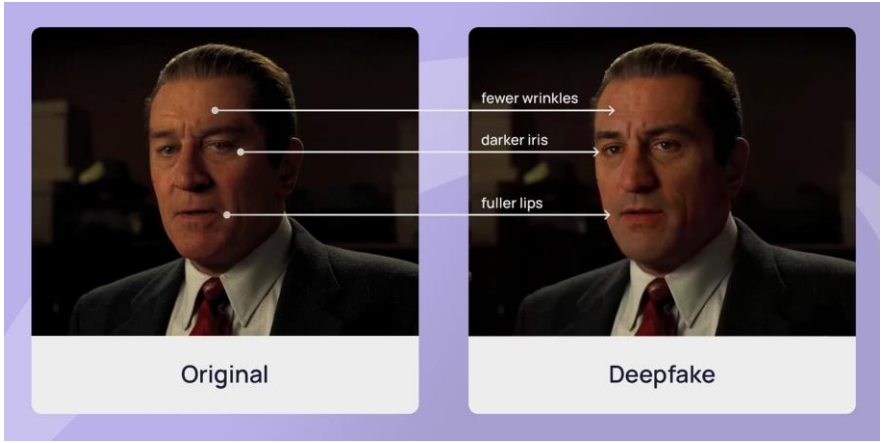
Taktik?

Schutz?

Ziel: Geld- oder Datenklau durch gefälschte Anweisungen von Führungskräften.

Quelle: https://sosafe-awareness.com/de/glossar/ceo-fraud/

AI & Deepfakes



Methode?

Taktik?

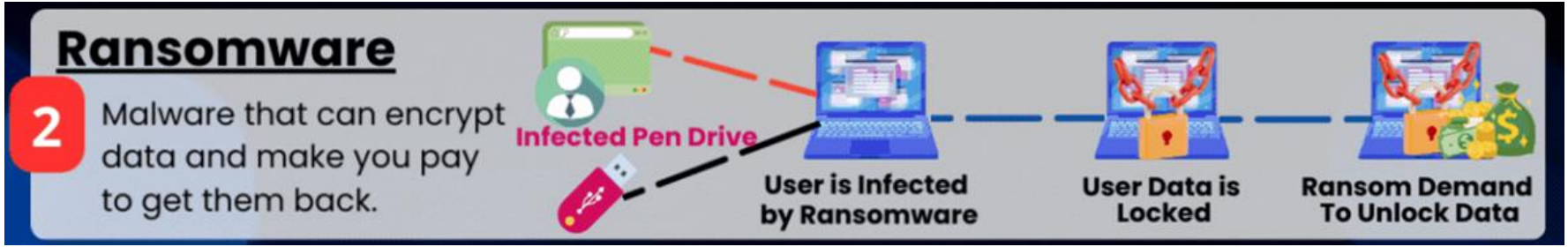
Schutz?

Ziel: Fälschung von Videos/Audio zur Täuschung.

Quelle: https://sosafe-awareness.com/blog/how-to-spot-a-deepfake/

Ransomware

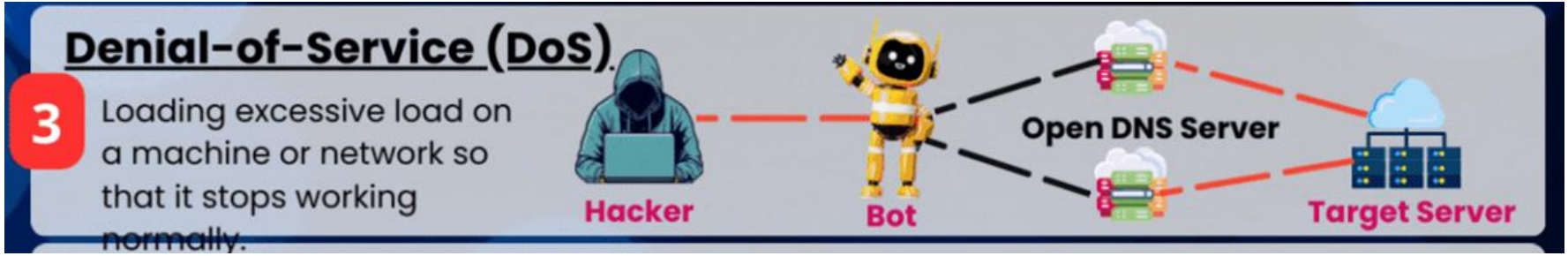
- **Ziel:** Erpressung von Geld durch Sperrung von Dateien/Systemen.
- **Schaden:** Datenverlust, Betriebsunterbrechungen.
- **Prävention:** Regelmäßige Backups, Aktualisierung von Software, Sicherheitsbewusstsein. → Antivirus & IPS
- **Reaktion:** Isolierung des betroffenen Systems, Kontakt mit Sicherheitsexperten.



Quelle: https://cybersecuritynews.com/

Denial-of-Service

- **Ziel:** Verhindern des normalen Betriebs, Beeinträchtigung der Verfügbarkeit.
- **Typen:** Verteilter DoS (DDoS), bei dem Angriffe von vielen verschiedenen Quellen ausgeführt werden.
- **Auswirkungen:** Dienstausfälle, finanzielle Verluste, Reputationsbeschädigung.
- **Prävention:** Verwendung von Load Balancern.
- **Verteidigung:** Einsatz von Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systems (IDS), und Traffic-Filtern.



Quelle: https://cybersecuritynews.com/

Man-in-the-Middle

- **Ziel:** Die Kommunikation zwischen den Parteien zu überwachen oder zu stören.
- **Typen:** Passiver MitM, bei dem nur Daten abgefangen werden; Aktiver MitM, bei dem Daten manipuliert werden.
- **Angriffsvektoren:** Öffentliche WLAN-Netzwerke, unsichere Verbindungen.
- **Prävention:** Verwendung von VPN Clients.
- **Verteidigung:** Verschlüsselte Verbindungen verwenden, Sicherheitsbewusstsein schärfen.

Quelle: https://cybersecuritynews.com/

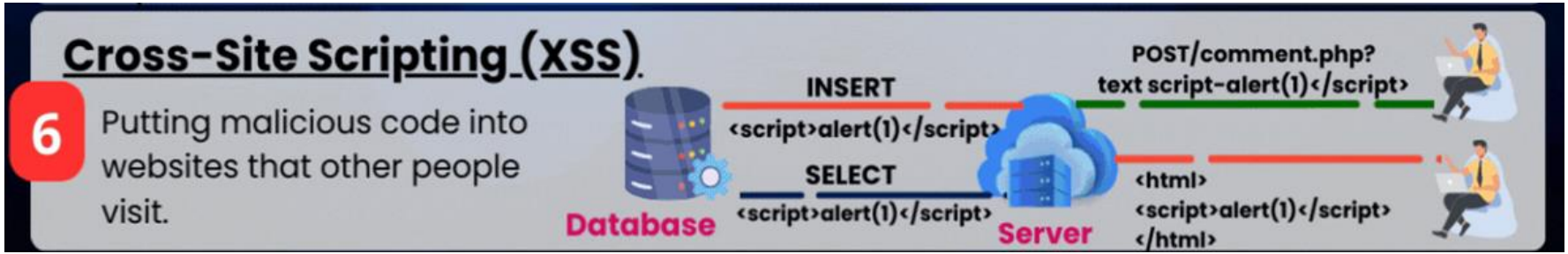
SQL Injection

- **Ziel:** Ausnutzung von Sicherheitslücken zur unbefugten Abfrage oder Manipulation der Datenbank.
- **Auswirkungen:** Datenlecks, unberechtigter Zugriff auf sensible Informationen.
- **Prävention:** Verwendung von Parametrisierung und Prepared Statements, regelmäßige Sicherheitsaudits.
- **Reaktion:** Schnelle Patching und Schließen von Sicherheitslücken, Überwachung auf verdächtige Aktivitäten.

Quelle: https://cybersecuritynews.com/

Cross-Site Scripting (XSS)

- **Ziel:** Ausnutzung von Sicherheitslücken zur Ausführung von Skripten im Browser anderer Benutzer.
- **Arten:** Reflektiertes XSS, gespeichertes XSS, DOM-basiertes XSS.
- **Auswirkungen:** Kompromittierung von Benutzerdaten, Session-Hijacking, Website-Defacement.
- **Prävention:** Eingabevalidierung, Escapen von benutzergeneriertem Inhalt, Content Security Policy (CSP).
- **Reaktion:** Schnelles Patchen von Sicherheitslücken, Überwachung auf verdächtige Aktivitäten.



Quelle: https://cybersecuritynews.com/

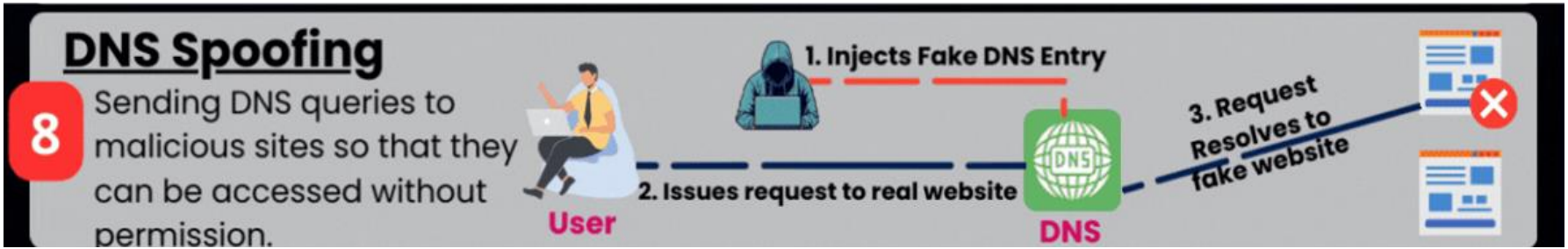
Zero-Day Exploits

- **Ziel:** Ausnutzung von Lücken, um Zugriff zu erhalten, Daten zu stehlen oder Schaden anzurichten.
- **Herausforderung:** Mangelnde Verteidigungsmöglichkeiten, da keine bekannten Fixes existieren.
- **Prävention:** Regelmäßiges Patchen von Software, Einsatz von Sicherheitslösungen zur Erkennung unbekannter Bedrohungen.
- **Reaktion:** Schnelles Erkennen und Eindämmen von Angriffen, Zusammenarbeit mit Herstellern zur Entwicklung von Patches.

Quelle: https://cybersecuritynews.com/

DNS Spoofing

- **Ziel:** Irreführung von Benutzern, um sie auf gefälschte Websites umzuleiten und ihre Daten zu stehlen.
- **Auswirkungen:** Phishing, Datenverlust, Malware-Infektionen.
- **Prävention:** Einsatz von DNSSEC (Domain Name System Security Extensions), regelmäßige Überprüfung der DNS-Einträge.
- **Reaktion:** Schnelles Erkennen und Beheben von gefälschten DNS-Einträgen, Überwachung auf verdächtige Aktivitäten.



Quelle: https://cybersecuritynews.com/

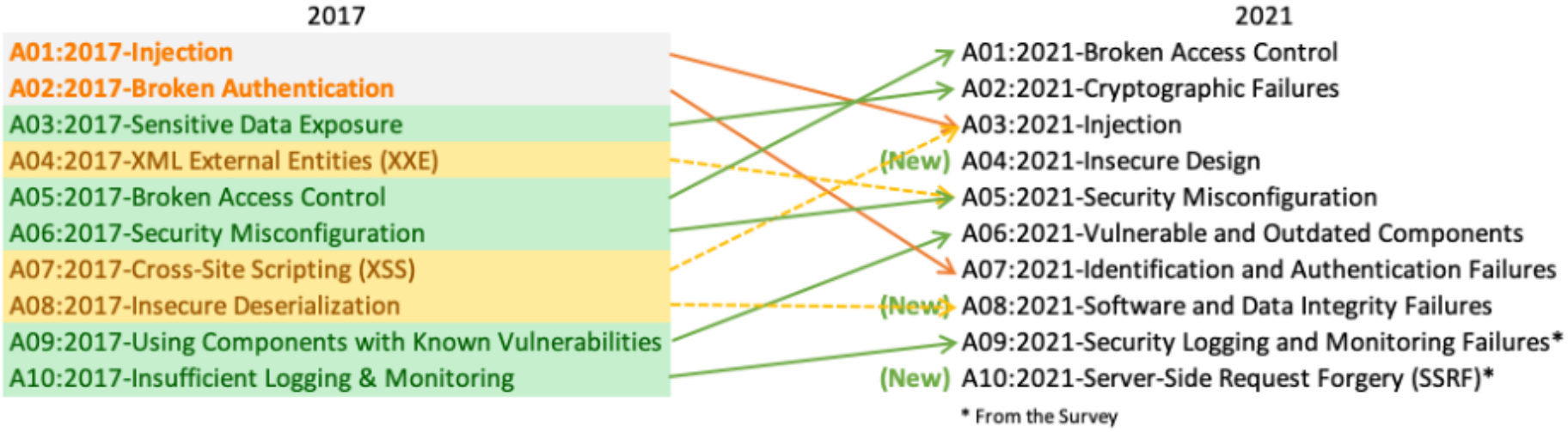
Zeit für ein Quiz! 

Risiken von Webapplikationen

Kennt ihr die “OWASP TOP 10” ?

Überblick über die Top 10

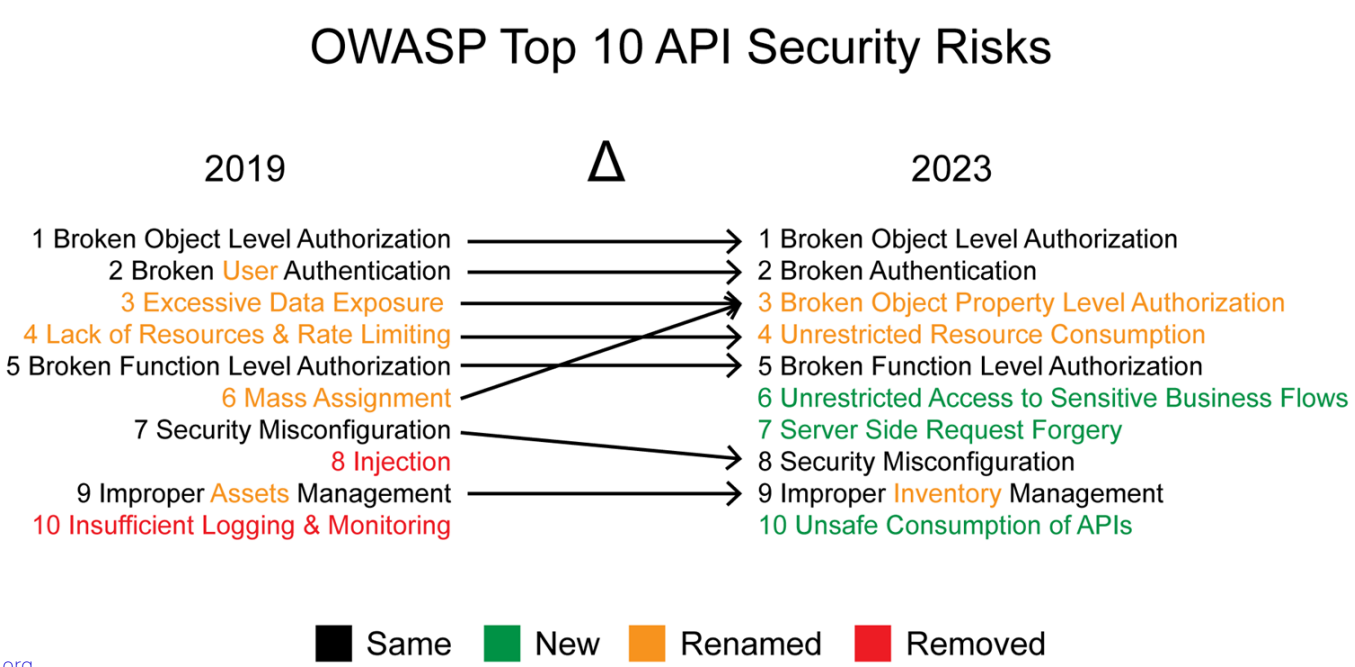
Webapplikationen



Quelle: https://www.owasp.org

Überblick über die Top 10

APIs



Quelle: https://www.owasp.org

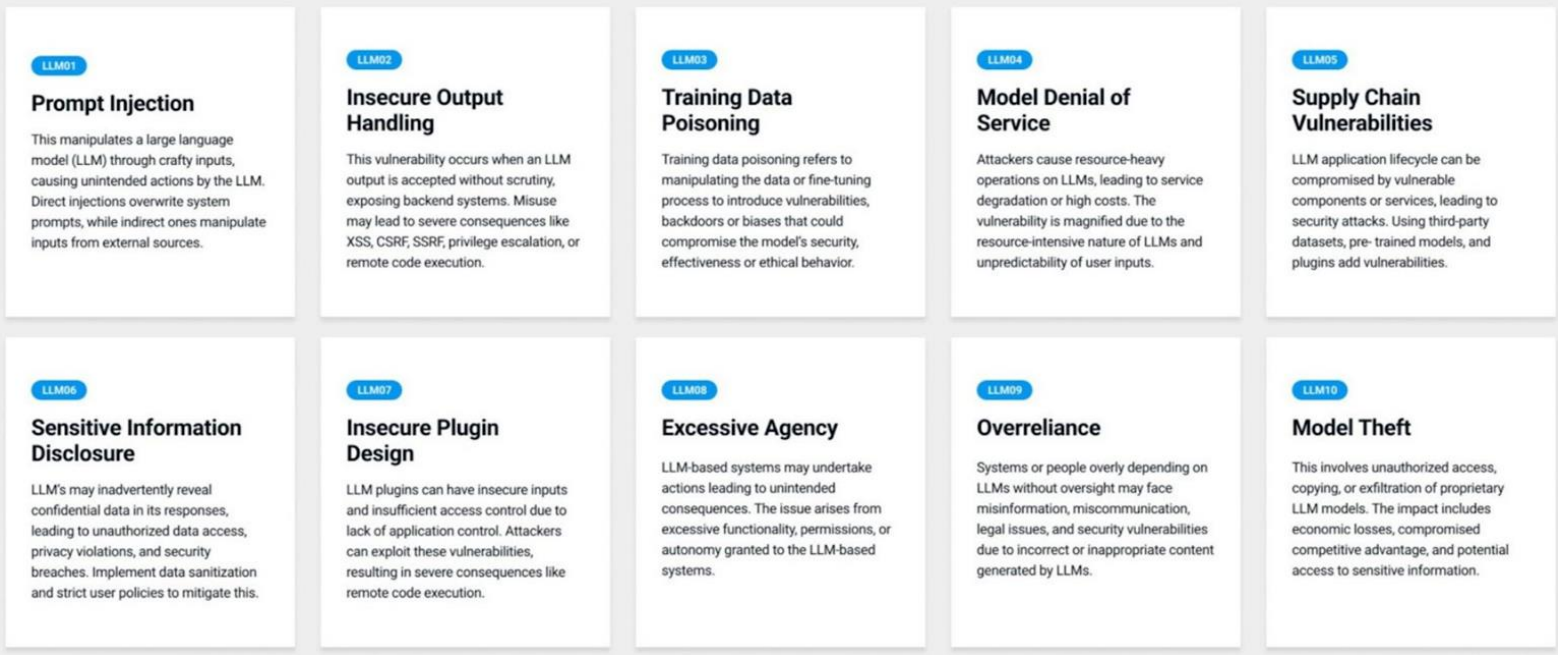
Überblick über die Top 10

Mobile

Quelle: https://www.owasp.org

Überblick über die Top 10

LLM - KI Entwicklung



Quelle: https://www.owasp.org

Praxisübung – Public Attack Surface

Ablauf ⏩

- Überlege dir welche öffentlichen Systeme deine Firma benutzt oder anbietet
- Werden diese Schnittstellen irgendwie geschützt?

Dokumentation 📄

- Auflistung aller öffentlich erreichbaren Firmenassets

Zeit & Format 🕛

- 10 min Recherche
- 10 min Diskussion

Live Demo 

Sample Firma und Schutz mit Cloudflare

Cyberbedrohungen 2030

Cyber Security Academy


FAKE
AI

SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES

1

WHAT IF...

State-sponsored actors insert a backdoor in a well-known and popular open-source library on online code repository. They use this to infiltrate information from most major European corporations and use the information to blackmail leaders, espionage, or otherwise initiate disruptions across the EU.

?

ADVANCED DISINFORMATION CAMPAIGNS

2

WHAT IF...

A state-sponsored actor may impersonate a political rival by using deepfakes and spoofing the candidate's digital identity, significantly impacting election results.

?

RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY

3

WHAT IF...

An authoritarian regime uses their power to retrieve databases of information about individuals who have visited their country, from both public and private entities. They track all those who participated in anti-government protests, put them on a watch list, and subsequently are able to manipulate those individuals' access to national services like voting, visits to their healthcare providers, or access to other online services.

?

HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBER-PHYSICAL ECOSYSTEMS

WHAT IF...

Manuals for all legacy OT equipment are available online and studied primarily by state-sponsored groups. Once a vulnerability is found, they target user devices or other IoT products used at the plant. Cyber criminals begin a new form of ransomware in which they bring down important infrastructure and demand payment, given that the operator likely lacks the resources to solve the issue themselves.

TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA

5

WHAT IF...

Cybercriminals may use the increased amount of available data from smart devices and analyse it with AI to create behavioral models of their victims for spear phishing campaigns or stalking.

?

LACK OF ANALYSIS AND CONTROL OF SPACE-BASED INFRASTRUCTURE AND OBJECTS

WHAT IF...

State-sponsored attackers access space infrastructure, build up their capabilities and knowledge of the technology, and secure their presence to execute attacks. Their aim may be to create infrastructure malfunctions as a statecraft tool to sabotage other governments or commercial space operations and systems during geopolitical conflicts.

RISE OF ADVANCED HYBRID THREATS

7

WHAT IF...

Hackers are hired by a corporation to investigate the new technology being developed by a competitor. In their quest, they are able to retrieve metadata, view code, and set up a machine learning algorithm that continuously collects changes to the code and then continuously accesses user account to prevent monitoring systems from recognising that the attacker is in the network. In parallel they obfuscate the activity by spreading fake news about insider trading and industrial espionage from a third competitor by dropping fake evidence of physical intrusion.

?

SKILL SHORTAGES

WHAT IF...

The skill shortage leads to an increase of online job advertisements that tell attackers the technologies that each organisation is using and the approximate number of empty positions. A state-sponsored actor may use this to their advantage as a part of a larger campaign to tamper with critical infrastructure in another country.

CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE

9

WHAT IF...

A state-sponsored actor aims to temporarily cripple a region during an active conflict by installing malware that disrupts all critical functions of the ICT provider. Without operational cities, roadways, and communication channels, the region is essentially crippled without the ability for civilians to go about their daily lives and the responsible parties limited in their ability to maintain defense monitoring systems and to collaborate to develop response options and methods for bringing the necessary systems back online.

?

ARTIFICIAL INTELLIGENCE ABUSE

10

WHAT IF...

A state-sponsored actor wants to sow discord in a population before an election and manipulates the learning data of a law enforcement algorithm to target specific populations, causing widespread protests and violence. They are also able to deduct information about the political opponents themselves by using an AI analysis of the individuals' whereabouts, health history, and voting history – the correlation of such personal data will likely only be feasible with the use of AI tools.

?

Was ist öffentlich zu meinem Unternehmen bekannt?

Was ist öffentlich zu meinem Unternehmen bekannt?

who.is

DNS Looking Glass

Info Sec Search Engine

Information Crawler

Open Source Project Web Check

';--have i been pwned?

Cyber Security Academy

Live Demo 

Reconnaissance

Jetzt seid Ihr dran! 

Praxisübung - Reconnaissance

Ablauf ⏩

- Was können angreifer direkt erkennen über dein Unternehmen?
- Lege den Fokus auf die „Public Attack Surface“ (z.B. VPN Endpoint, Server, etc.)

Dokumentation

- verwertbare Informationen & potentielle Angriffsvektoren

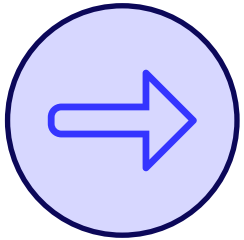
Zeit & Format 🕛

- 10 min Recherche
- 10 min Diskussion

Was ist ein Client VPN?

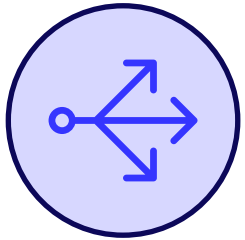
Kennt ihr hier Beispiele?

Technische Unterscheidung von Client VPNs



Tunnel All VPN

Gesamter Traffic wird durch den VPN geroutet



Split VPN

Nur spezielle Netze werden durch den VPN geroutet

Cyber Security Academy

Schaubild Tunnel All VPN

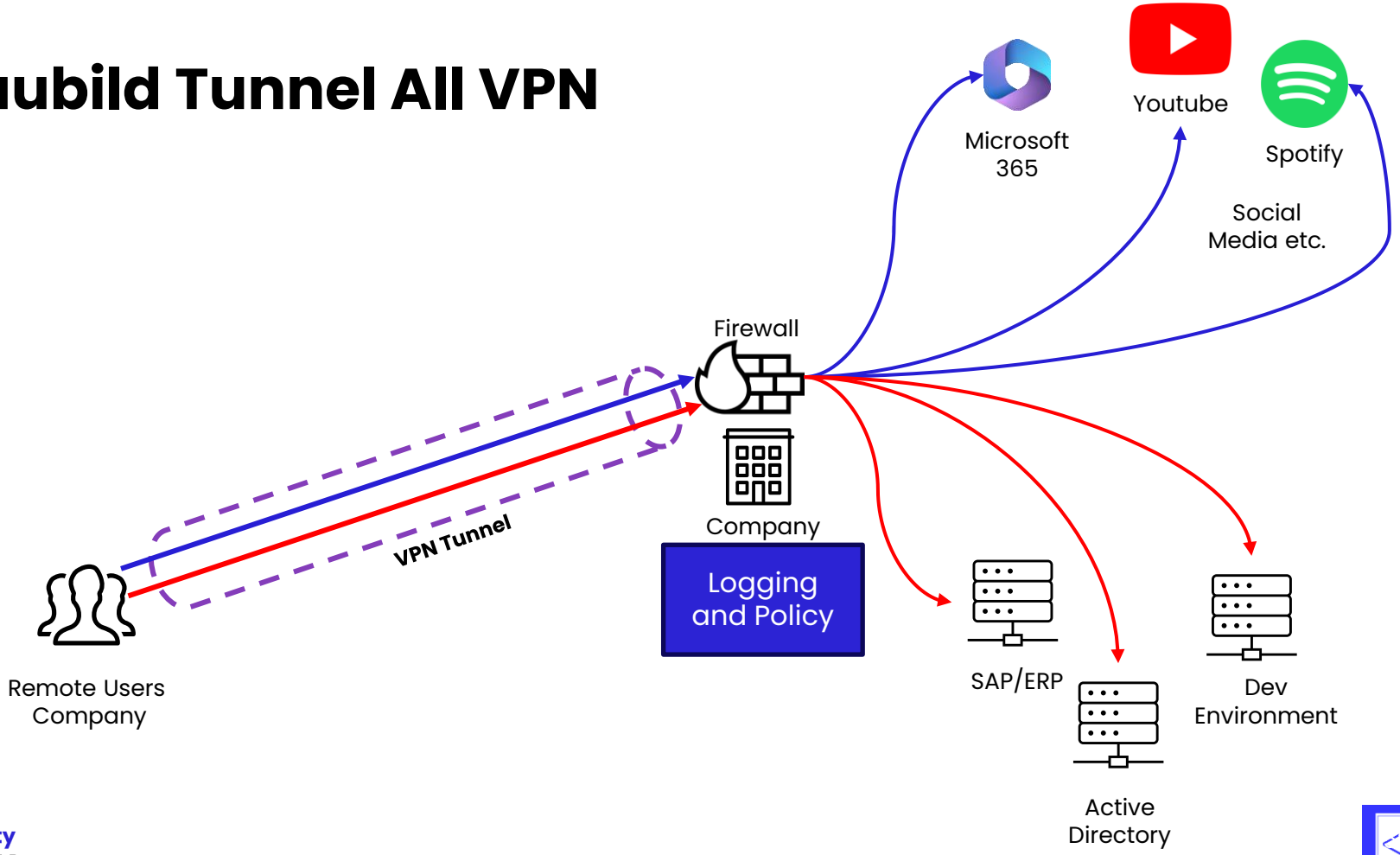
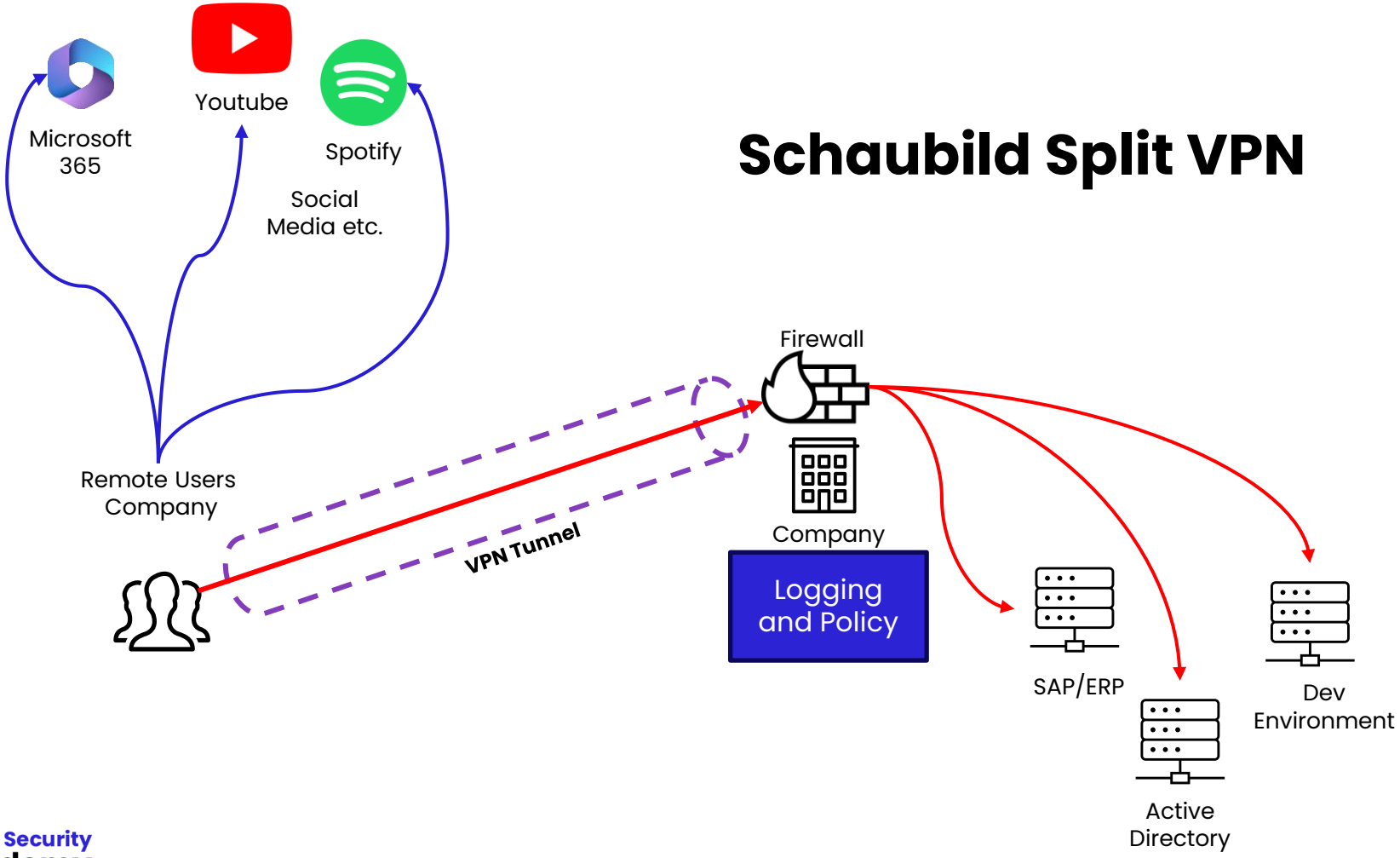
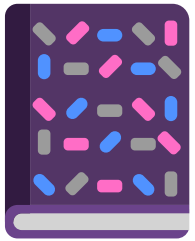


Schaubild Split VPN



Wichtige Begriffe in der Cyber Security



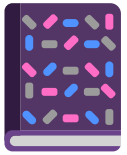
Wichtige Begriffe in der Cyber Security

Die Grundlage bzw. das Ziel!

Einhalten der Schutzziele - CIA-Triad:

- **Vertraulichkeit (Confidentiality):** Die Gewährleistung, dass sensible Informationen nur von autorisierten Personen eingesehen oder genutzt werden können und vor unbefugtem Zugriff geschützt sind.
- **Integrität (Integrity):** Die Sicherstellung, dass Daten genau und unverändert bleiben, während sie übertragen, gespeichert oder verarbeitet werden, und dass sie vor unbefugten Änderungen geschützt sind.
- **Verfügbarkeit (Availability):** Die Sicherstellung, dass Informationen und Ressourcen jederzeit und für autorisierte Benutzer verfügbar sind und vor Ausfällen oder Angriffen geschützt sind.

Wichtige Begriffe in der Cyber Security



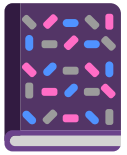
Cybersecurity: Der Schutz von Computersystemen, Netzwerken und Daten vor Diebstahl, Beschädigung oder unbefugtem Zugriff.

Awareness: Das Bewusstsein für Cybersecurity-Risiken und die Bedeutung sicherer Verhaltensweisen im digitalen Umfeld.

Angriffsvektoren: Die verschiedenen Methoden und Techniken, die von Angreifern verwendet werden, um in Computersysteme einzudringen oder sie zu kompromittieren.

Phishing: Eine betrügerische Methode, bei der Angreifer versuchen, sensible Informationen wie Benutzernamen, Passwörter und Kreditkarteninformationen durch gefälschte E-Mails, Websites oder Nachrichten zu stehlen.

Wichtige Begriffe in der Cyber Security

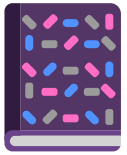


Malware: Schädliche Software, die dazu entwickelt wurde, in Computersysteme einzudringen und Schaden zu verursachen, wie z. B. Viren, Trojaner, Würmer und Ransomware.

Social Engineering: Eine Methode, bei der Angreifer menschliche Manipulationstechniken einsetzen, um Informationen zu erhalten oder Zugang zu Systemen zu erlangen, indem sie sich als vertrauenswürdige Personen ausgeben oder das Vertrauen der Opfer gewinnen.

Zero-Day-Exploits: Sicherheitslücken in Software oder Systemen, für die noch kein Patch oder Sicherheitsupdate verfügbar ist und die von Angreifern ausgenutzt werden können, um unbefugten Zugriff zu erhalten.

Wichtige Begriffe in der Cyber Security

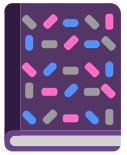


Firewall: Ein Sicherheitsmechanismus, der den Datenverkehr zwischen einem internen Netzwerk und externen Netzwerken überwacht und filtert, um unerwünschte Zugriffe zu verhindern.

Multi-Faktor-Authentifizierung (MFA): Ein Sicherheitsverfahren, das mehrere Identitätsnachweise erfordert, um auf ein Konto oder eine Anwendung zuzugreifen, wie z. B. die Kombination aus Passwort und einem einmaligen Code, der per SMS oder App gesendet wird.

Datenschutz: Die Praxis, personenbezogene Daten zu schützen und sicherzustellen, dass sie angemessen verwendet, gespeichert und übertragen werden, um die Privatsphäre und die Rechte der Personen zu wahren.

Wichtige Begriffe in der Cyber Security

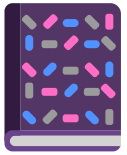


Verschlüsselung: Der Prozess der Umwandlung von lesbaren Informationen in eine nicht lesbare Form (Chiffre), um sie vor unbefugtem Zugriff zu schützen.

Penetrationstest (Pen-Test): Eine autorisierte Simulation eines Cyberangriffs, um Schwachstellen in einem Computersystem, einer Anwendung oder einem Netzwerk zu identifizieren.

Intrusion Detection System (IDS): Eine Sicherheitssoftware oder -gerät, das den Datenverkehr in einem Netzwerk überwacht und nach Anzeichen von ungewöhnlichem oder verdächtigem Verhalten sucht, um potenzielle Angriffe zu erkennen.

Wichtige Begriffe in der Cyber Security

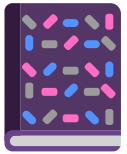


Intrusion Prevention System (IPS): Ein Sicherheitsmechanismus, der auf einem IDS aufbaut und aktiv Maßnahmen ergreift, um verdächtige Aktivitäten zu blockieren oder zu stoppen, bevor sie das Netzwerk erreichen.

Patch: Ein Software-Update, das entwickelt wurde, um eine Schwachstelle in einem Programm oder Betriebssystem zu beheben und Sicherheitslücken zu schließen.

Vulnerability Management: Der Prozess der Identifizierung, Bewertung und Behandlung von Sicherheitslücken in Computersystemen, Anwendungen oder Netzwerken, um das Risiko von Cyberangriffen zu minimieren.

Wichtige Begriffe in der Cyber Security

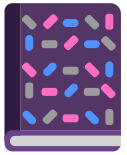


Advanced Persistent Threats: Advanced Persistent Threats (APTs) sind hochentwickelte und langfristig angelegte Cyberangriffe, die von gezielten Gegnern wie Nationen oder organisierten Kriminellen durchgeführt werden.

Data Breach: Ein Vorfall, bei dem sensible, vertrauliche oder geschützte Daten unbefugt offengelegt, kopiert, gestohlen oder kompromittiert werden.

Deepfake: Eine Art von synthetischen Medien, die mithilfe von künstlicher Intelligenz erstellt werden, um das Aussehen und Verhalten einer Person in Videos, Bildern oder Audioaufnahmen zu manipulieren.

Wichtige Begriffe in der Cyber Security



Endpoint Security: Die Sicherheitsmaßnahmen, die auf einzelnen Endgeräten wie Computern, Laptops, Tablets und Smartphones implementiert werden, um sie vor Bedrohungen und Angriffen zu schützen.

Cyberhygiene: Die Praxis der Einhaltung grundlegender Sicherheitsverfahren und -richtlinien, um das Risiko von Cyberangriffen zu reduzieren.

Incident Response Plan: Ein vordefinierter Satz von Verfahren und Maßnahmen, die ein Unternehmen ergreift, um auf einen Cyberangriff oder Sicherheitsvorfall zu reagieren, um die Auswirkungen zu minimieren und die Systeme wiederherzustellen.

Incident Response Prozess

Incident

Ruhe bewahren

Meldung an relevante Beteiligte

IT-Manager, GF, Dep., Stakeholder etc.

Logs von Servern, Apps und Devices

Sammeln und filtern von Infos

IT-Manager, GF

Entscheidung treffen

Hilfe anfordern

SOS

Expert:innen, Stakeholder?

Incident lösen & Aufräumen

MA, GF, IT, Stakeholder

Cyber Security Academy

Jetzt seid Ihr dran! 

Praxisübung - Business Continuity - IT

Ablauf ⏩

- Überlegt euch, welche IT-Infrastruktur bzw. welche digitalen Systeme zwingend Notwendig sind für eure Firma.

Überlegung 💡

- Public Systeme & Interne Systeme
- Gibt es Sicherungen der Daten & Konfigurationen?

Dokumentation 📄

- Auflistung der Assets
- Klassifizierung nach Kritikalität

Zeit & Format 🕐

- 10 min
- 5 min Diskussion

Cyberangriff

Öffentliche Infos

Ursache

Recovery Prozess

LAND KÄRNTEN

Cyber Security Academy

Quelle: https://www.ktn.gv.at/Service/informationen-cyberangriff

Analyse

Maßnahmen

Meldung

Ausblick

LAND KÄRNTEN

Quelle: https://www.ktn.gv.at/Service/informationen-cyberangriff

Cyberangriff

Öffentliche Infos

Ursache

Recovery Prozess

Quelle: https://www.ktn.gv.at/Service/informationen-cyberangriff

Analyse

Maßnahmen

Meldung

Ausblick

Analyse

Maßnahmen

Meldung

Ausblick

Lessons Learned

UNI GRAZ

Cyber Security Academy

Quelle: https://www.ktn.gv.at/Service/informationen-cyberangriff

Weitere Angriffe in Österreich

Die meisten Angriffe werden verheimlicht!

Medienbeiträge zu dem Thema

Öffentliche Datenbank von Cyberangriffen

Die meisten Angriffe werden verheimlicht!

Wird sich in Zukunft ändern, dank NIS2!

Medienbeiträge zu dem Thema

Öffentliche Datenbank von Cyberangriffen

Zeit für ein Quiz! 

Inhalte 📦

Cyberangriffe, Trends und Learnings

NIS 2 Richtlinie und die Lieferkette

Cyber Security 101 „Baseline“

Netzwerk, Infrastruktur, Cloud und Datensicherheit

Inhalte 📦

Cyberangriffe

NIS 2

Cyber Sec 101

Maßnahmen und Konzepte

NIS 2 Richtlinie

und sonstige Cybersecurity Maßnahmen der EU.

Lernziele 🚀

- Was sind die Cyber Security Intentionen der EU?
- Wie ist die NIS 2 Richtlinie aufgebaut?
- Ist mein Unternehmen NIS 2 betroffen?

Welche Cybersecurity Maßnahmen der EU kennt ihr?

Rechtsgrundlagen der EU

Rechtsgrundlagen der EU

4.5.2016 DE Amtsblatt der Europäischen Union L 119/1

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

Rechtsgrundlagen der EU

DatenSchutz – Grund VerOrdnung

4.5.2016 DE Amtsblatt der Europäischen Union L 119/1

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

Rechtsgrundlagen der EU

DSGVO

4.5.2016 DE Amtsblatt der Europäischen Union L 119/1

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

Rechtsgrundlagen der EU

DSGVO

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Rechtsgrundlagen der EU

27.12.2022 DE Amtsblatt der Europäischen Union L 333/1

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32022R2554&qid=1732021267133

Rechtsgrundlagen der EU

Digital Operational Resilience Act

27.12.2022 DE Amtsblatt der Europäischen Union L 333/1

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

Cyber Security Academy

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32022R2554&qid=1732021267133

Rechtsgrundlagen der EU

DORA

27.12.2022 DE Amtsblatt der Europäischen Union L 333/1

VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32022R2554&qid=1732021267133

Rechtsgrundlagen der EU

DSGVO

DORA

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Rechtsgrundlagen der EU

7.6.2019 DE Amtsblatt der Europäischen Union L 151/15

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. April 2019

über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32019R0881&qid=1732021348618

Rechtsgrundlagen der EU

Cybersecurity Act

7.6.2019 DE Amtsblatt der Europäischen Union L 151/15

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. April 2019

über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32019R0881&qid=1732021348618

Rechtsgrundlagen der EU

DSGVO

DORA

Cybersecurity Act

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Rechtsgrundlagen der EU

27.12.2022 DE Amtsblatt der Europäischen Union L 333/80

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32022L2555&qid=1732021348618

Rechtsgrundlagen der EU

Netz & Informations Systeme 2

27.12.2022 DE Amtsblatt der Europäischen Union L 333/80

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32022L2555&qid=1732021348618

Rechtsgrundlagen der EU

NIS 2

27.12.2022 DE Amtsblatt der Europäischen Union L 333/80

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32022L2555&qid=1732021348618

Rechtsgrundlagen der EU

DSGVO

DORA

NIS 2

Cybersecurity Act

Cyber Security Academy

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Rechtsgrundlagen der EU

Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1689

12.7.2024

VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juni 2024

zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32024R1689&qid=1732021655487

Rechtsgrundlagen der EU

Artificial Inteligence Act

2024/1689 12.7.2024

VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juni 2024

zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32024R1689&qid=1732021655487

Rechtsgrundlagen der EU

AI Act

2024/1689 12.7.2024

VERORDNUNG (EU) 2024/1689 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juni 2024

zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

Quelle: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32024R1689&qid=1732021655487

Rechtsgrundlagen der EU

DSGVO

DORA

NIS 2

AI Act

Cybersecurity Act

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Rechtsgrundlagen der EU

EUROPÄISCHE KOMMISSION

Brüssel, den 15.9.2022

COM(2022) 454 final

2022/0272(COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454

Rechtsgrundlagen der EU

Cyber Resilience Act

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454

Rechtsgrundlagen der EU

CRA

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454

Rechtsgrundlagen der EU

DSGVO

DORA

NIS 2

Cybersecurity Act

AI Act

CRA

Cyber Security Academy

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Rechtsgrundlagen der EU

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7589/24 + ADD 1
No. Cion doc.:	8512/23 + ADD 1
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Letter sent to the European Parliament

Quelle: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8047_2024_INIT&qid=1732021470797

Rechtsgrundlagen der EU

Cyber Solidarity Act

INFORMATION NOTE	
From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7589/24 + ADD 1
No. Cion doc.:	8512/23 + ADD 1
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Letter sent to the European Parliament

Quelle: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8047_2024_INIT&qid=1732021470797

Rechtsgrundlagen der EU

Cyber Solidarity Act

befindet sich noch in der Testphase

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	7589/24 + ADD 1
No. Cion doc.:	8512/23 + ADD 1
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Letter sent to the European Parliament

Quelle: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8047_2024_INIT&qid=1732021470797

Was ist der Unteschied zwischen einer Verordnung und einer Richtlinie ?

Richtlinie

EU Recht

Interpretation

Nationales Recht

Gesetz

Unternehmen & Bürger

Verordnung

EU Recht

Gesetz

Unternehmen & Bürger

VS.

Richtlinie

EU Recht

Interpretation

Nationales Recht

Gesetz

Unternehmen & Bürger

Rechtsgrundlagen der EU

Verordnung

- CRA
- AI Act
- DSGVO
- DORA
- Cybersecurity Act

Richtlinie

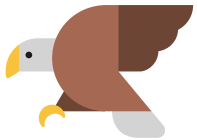
- NIS 2

Cyber Security Academy

Quelle: https://www.globalsign.com/en/blog/quick-guide-eu-cybersecurity-regulations

Den Überblick zu behalten ist schwierig.

Wo können wir aktuelle Informationen abgreifen?



Den Überblick zu behalten ist schwierig.

Wo können wir aktuelle Informationen abgreifen?

Cyber Risk GmbH

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Was ist euch zu dem Thema NIS2 bekannt ?

NIS2

Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU

Ist die NIS2 eigentlich schon scharf geschalten?

Cyber Security Academy

NIS 2 – Timeline

NIS 1
Regulierung:
06.07.2016

NIS 1
Umsetzung:
09.05.2018

NIS 2
Regulierung:
14.12.2022

NIS 2 nationale
Deadline:
17.10.2024

NIS 2 – Timeline

Trotzdem gibt es noch keine Umsetzung in Österreich.

NIS 2 – Timeline

$\frac{2}{3}$ **MEHRHEIT**

Nicht erreicht.

NIS 2 – Timeline

Ungewiss wird vermutlich 2025 kommen

NIS 2 – Timeline

NIS 1
Regulierung:
06.07.2016

NIS 1
Umsetzung:
09.05.2018

NIS 2
Regulierung:
14.12.2022

NIS 2 nationale
Deadline:
17.10.2024

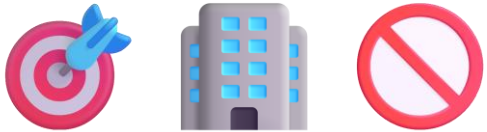
Ungewiss
wird vermutlich
2025 kommen

Was ist eigentlich der Unterschied zwischen NIS 1 und NIS 2?

NIS 1 vs. NIS 2

Unterscheidungsmerkmale

NIS 1 vs. NIS 2 – Unterscheidungsmerkmale



Betroffene Unternehmen

Lieferkette

Kleine & mittlere Unternehmen

Sanktionen

Sanktionen

NIS 1

99 (Kritis)
Nicht Betroffen
Nicht geregelt
max. 50/100k €*

NIS 2

5000
Betroffen
Zertifizierbar
max. 7/10m €**

*100k nur im Wiederholungsfall

**max. 7m € wichtige (o. 1,4% U. wenn höher)/10m € (o. 2% U. wenn höher) wesentliche Einrichtungen

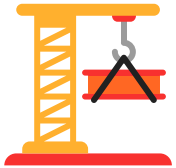
Cyber Security Academy

NIS 1 vs. NIS 2 – Unterschiede

Kriterien	NIS1	NIS2
Betroffene Unternehmen	99 (Kritis)	5000
Lieferkette	Nicht betroffen	Betroffen
KMU Regelung	Nicht geregelt	Zertifizierung
Sanktionen	max. 50/100K €*	Max. 7/10m €**

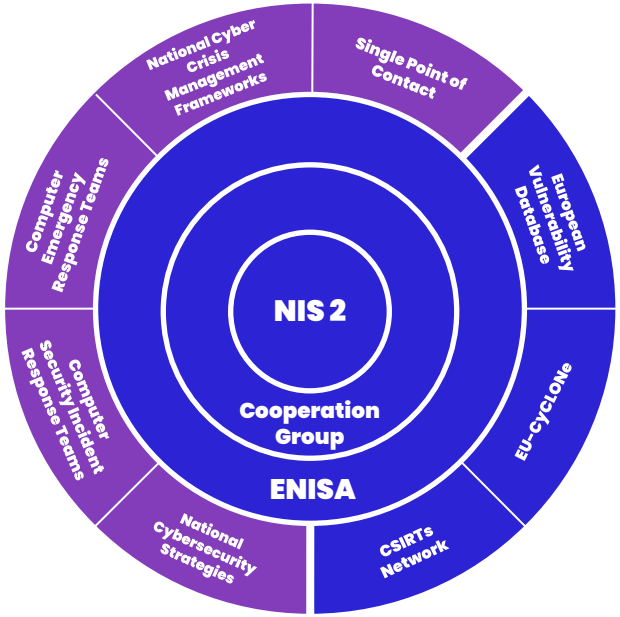
*100k nur im Wiederholungsfall

**max. 7m € wichtige (o. 1,4% U. wenn höher)/10m € (o. 2% U. wenn höher) wesentliche Einrichtungen



Was denkt ihr, wie ist die NIS2 Richtlinie aufgebaut ?

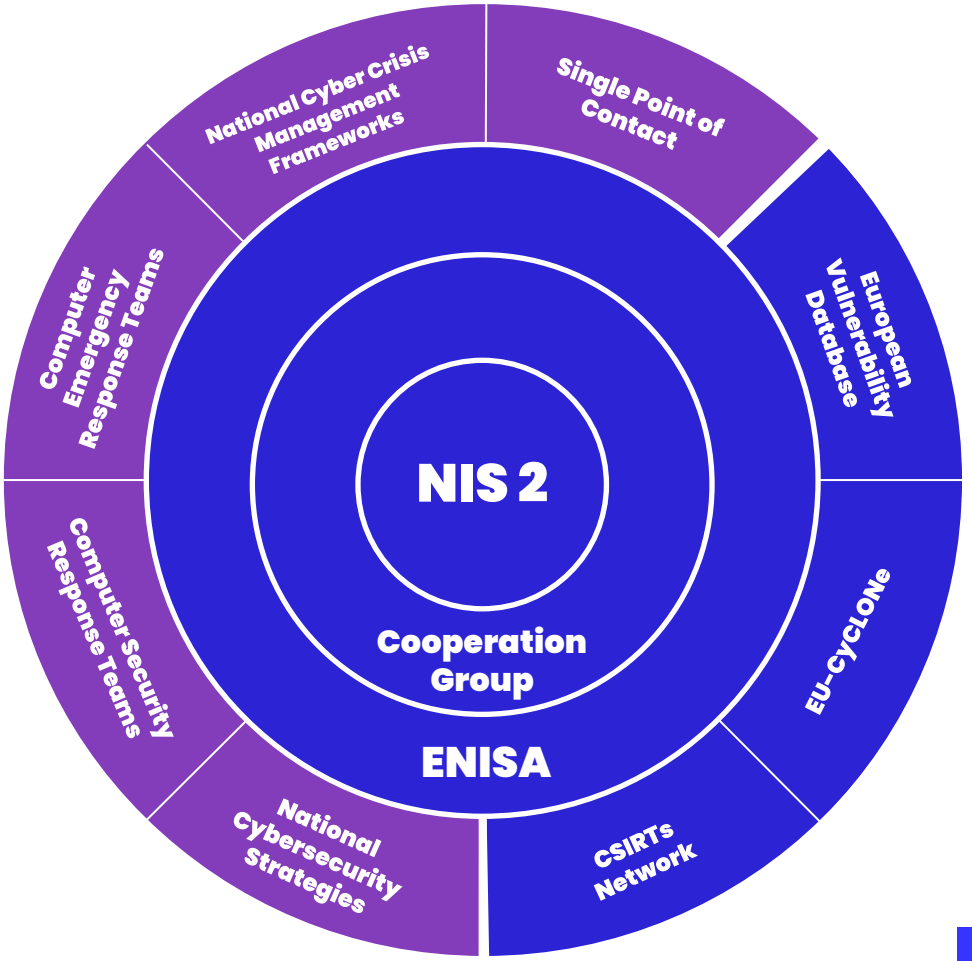
NIS2 – Aufbau/Akteure



EU

Cooperation Group
ENISA
EVD

CSIRTs Network
CyCLONe



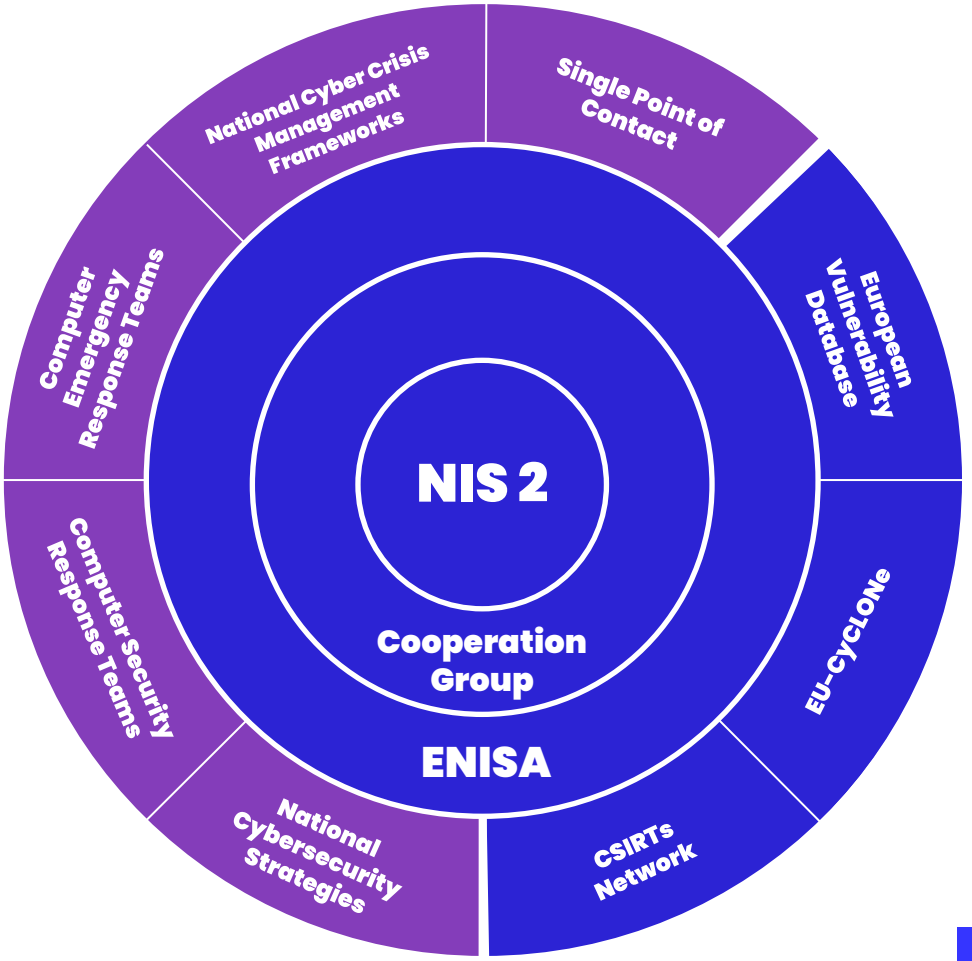
Cyber Security Academy

EU

1. Cooperation Group
2. ENISA
3. EVD
4. CSIRTs Network
5. CyCLONe

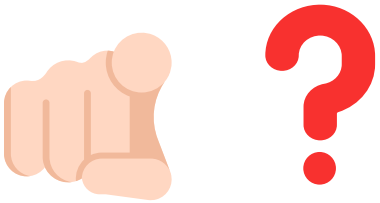
Österreich

1. CERT
2. CSIRTs
3. NCS
4. NCCMF
5. Single Point of Contact



Live Browsing 

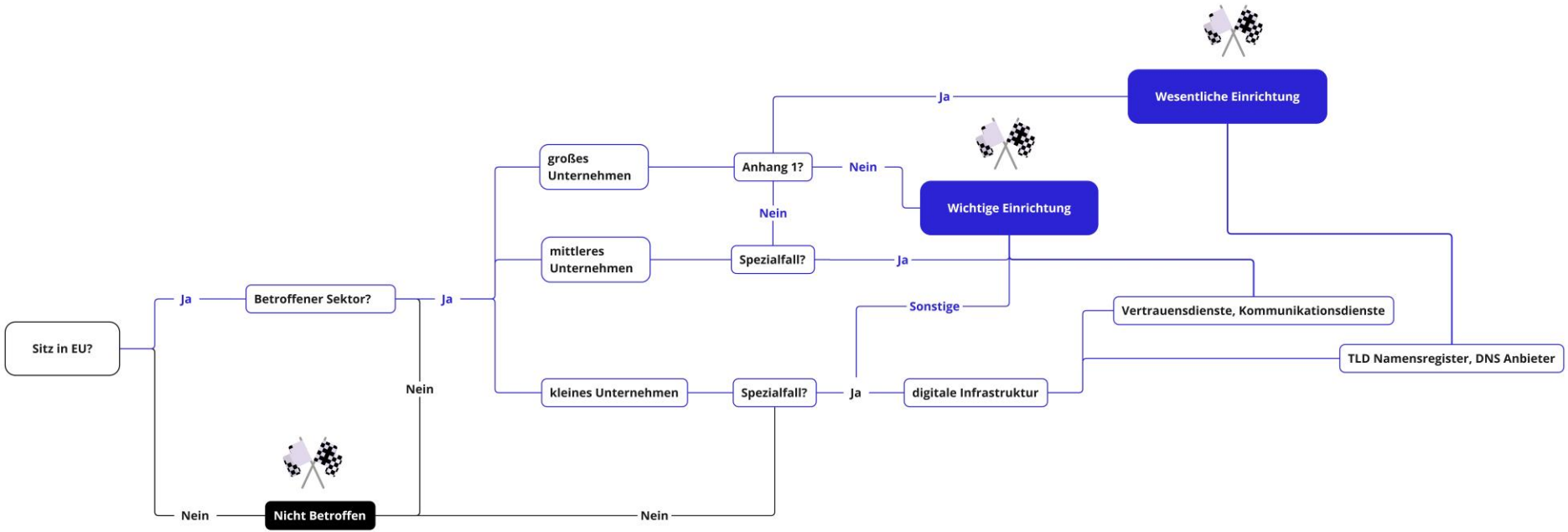
NIS 2 Informationen von ENISA



Wer denk ihr ist von der NIS 2 betroffen ?

Disclaimer – folgende Darstellungen basieren auf einem Gesetzesentwurf der sich noch ändern kann!

NIS 2 Betroffen?



Cyber Security Academy

NIS 2 Betroffen?

Nicht Betroffen

Wichtige Einrichtung

Wesentliche Einrichtung

Betroffene Sektoren

Anlage 1

- Energie
- Verkehr
- Bankwesen*
- Finanzmarktinfrastrukturen*
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten B2B
- öffentliche Verwaltung
- Weltraum

Anlage 2

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemie
- Lebensmittel
- verarbeitendes/herstellendes Gewerbe**
- Anbieter digitaler Dienste
- Forschung (fakultativ)

*Im Finanzsektor hat DORA Vorrang

**In bestimmen ÖNACE Klassen

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

Praxisübung – Sektoren NIS 2 

Ablauf ⏩

- Findet mehr über diese Betroffenen Sektoren in Anlage 1 & 2 heraus.

Tipps 💡

- Geht auf Seite des Öster. Parlament und sucht nach dem aktuellen Gesetzesentwurf.

Dokumentation 📃

- Sektor v. euren Unternehmen
- Lieferkette u. Teilsektoren

Zeit & Format 🕛

- 10 min
- 5 min Diskussion

kleines, mittleres und Großes Unternehmen

Größenklasse	Beschäftigte	Jahresumsatz	Jahresbilanz
Kleines Unternehmen (KU)	< 50 und	≤ 10 Mio. € oder	≤ 10 Mio. €
Mittleres Unternehmen (MU)	< 250 und	≤ 50 Mio. € oder	≤ 43 Mio. €
Großes Unternehmen (GU)	≥ 250 oder	> 50 Mio. € und	> 43Mio. €

NIS 2 – Spezialfälle

Sonstige

- **Verbundene und Partner Unternehmen (Ausnahme Holdings)**
- **Lieferkette (auch indirekt über Kunden Betroffen)**
- **Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essenziell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.**

Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht

NIS 2 – Spezialfälle

Sonstige

- **Verbundene und Partner Unternehmen (Ausnahme Holdings)**
- **Lieferkette (auch indirekt über Kunden Betroffen)**
- **Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essentiell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.**

Digitale Infrastruktur

- **Vertrauensdienste Anbieter**
- **Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste**
- **TLD-Namenregister und DNS-Diensteanbieter (ausgenommen Betreiber von Root-Namenservern)**

Cyber Security Academy

Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht

kleines Unternehmen

Wesentliche Einrichtung

Wichtige Einrichtung

Sonstige

Vertrauensdienste, Kommunikationsdienste

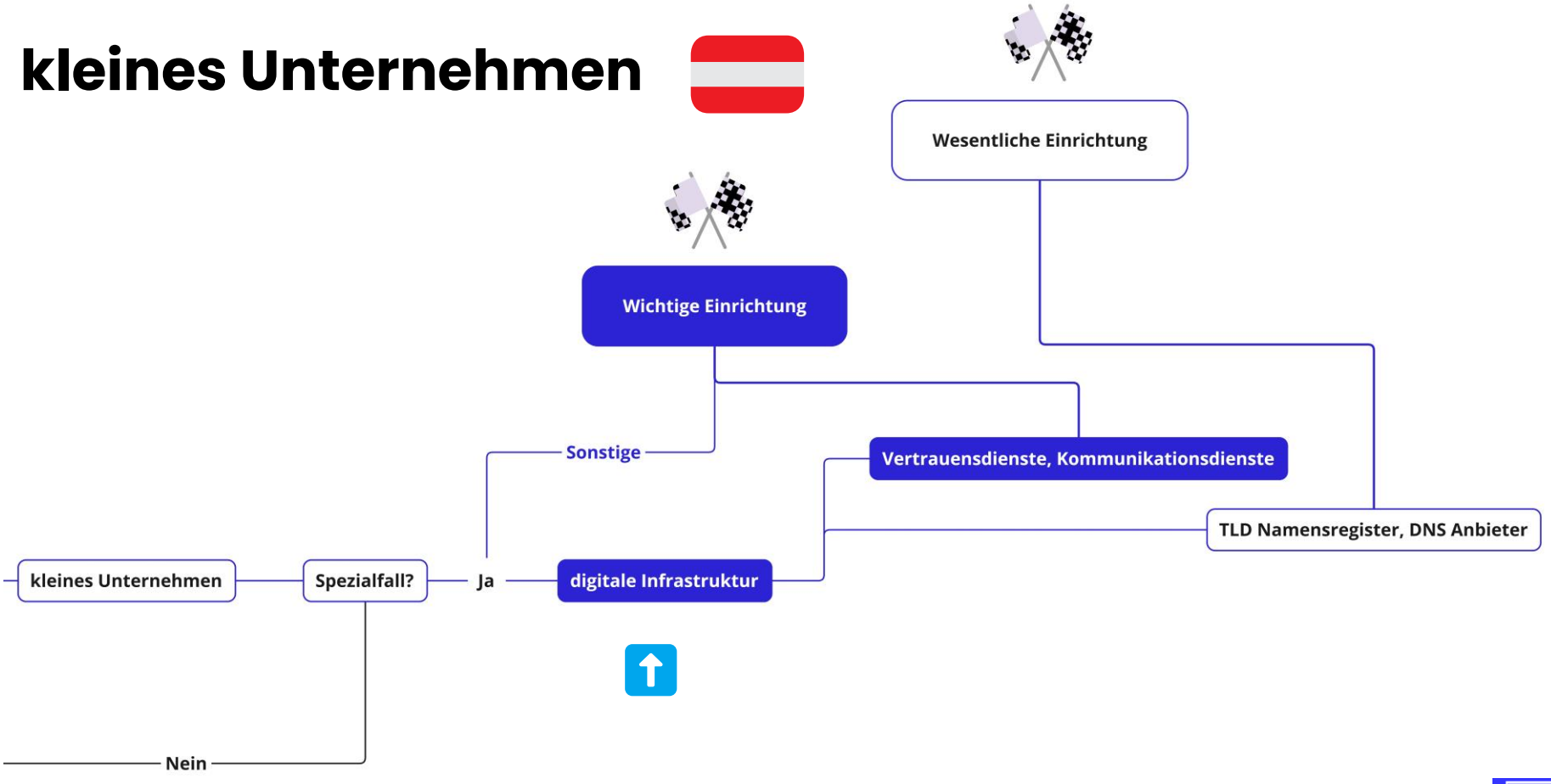
TLD Namensregister, DNS Anbieter

kleines Unternehmen — Spezialfall? — Ja — digitale Infrastruktur

Nein

Cyber Security Academy

kleines Unternehmen



Cyber Security Academy

kleines Unternehmen

Wesentliche Einrichtung

Wichtige Einrichtung

Sonstige

Vertrauensdienste, Kommunikationsdienste

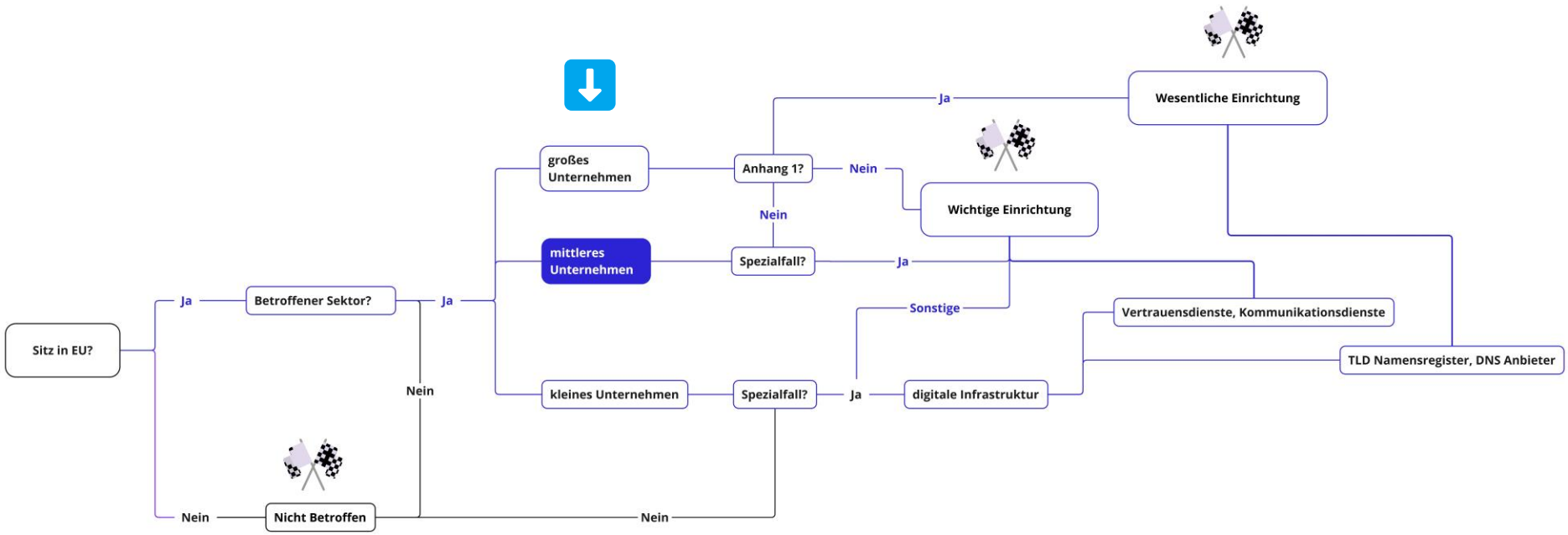
TLD Namensregister, DNS Anbieter

kleines Unternehmen — Spezialfall? — Ja — digitale Infrastruktur

Nein

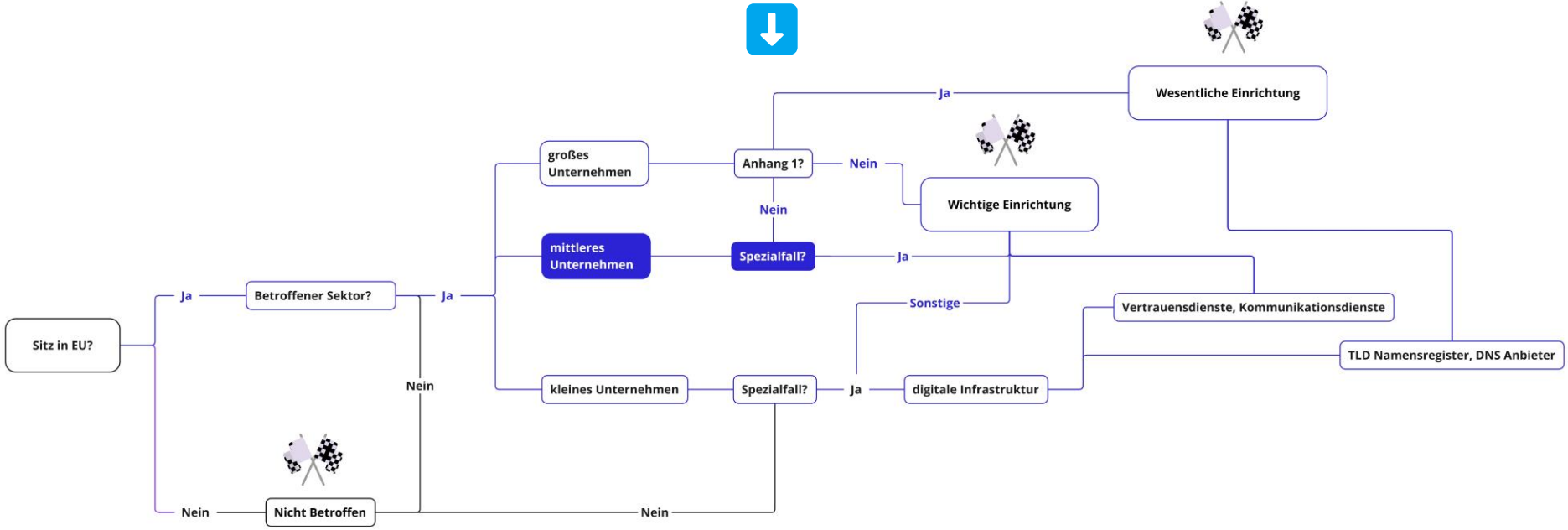
Cyber Security Academy

mittleres Unternehmen



Cyber Security Academy

mittleres Unternehmen



Cyber Security Academy

NIS 2 – Spezialfälle

Sonstige

- **Verbundene und Partner Unternehmen (Ausnahme Holdings)**
- **Lieferkette (auch indirekt über Kunden Betroffen)**
- **Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essentiell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.**

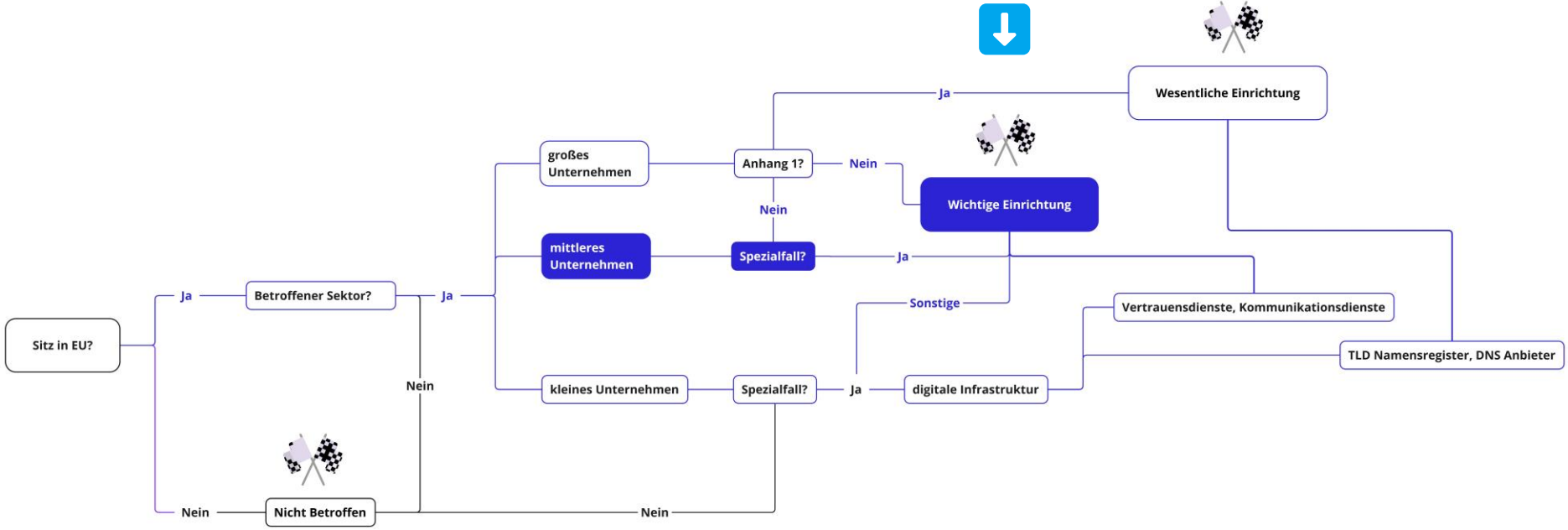
Digitale Infrastruktur

- **Vertrauensdienste Anbieter**
- **Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste**
- **TLD-Namenregister und DNS-Diensteanbieter (ausgenommen Betreiber von Root-Namenservern)**

Cyber Security Academy

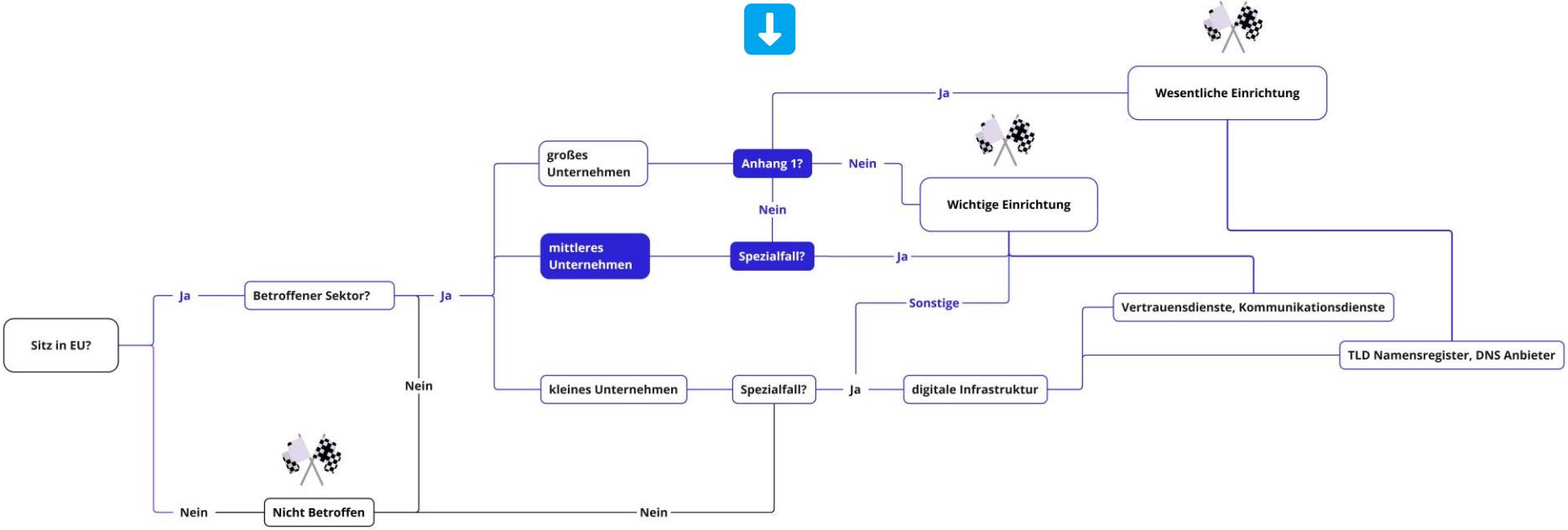
Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht

mittleres Unternehmen



Cyber Security Academy

mittleres Unternehmen



Cyber Security Academy

Betroffene Sektoren

Anhang 1

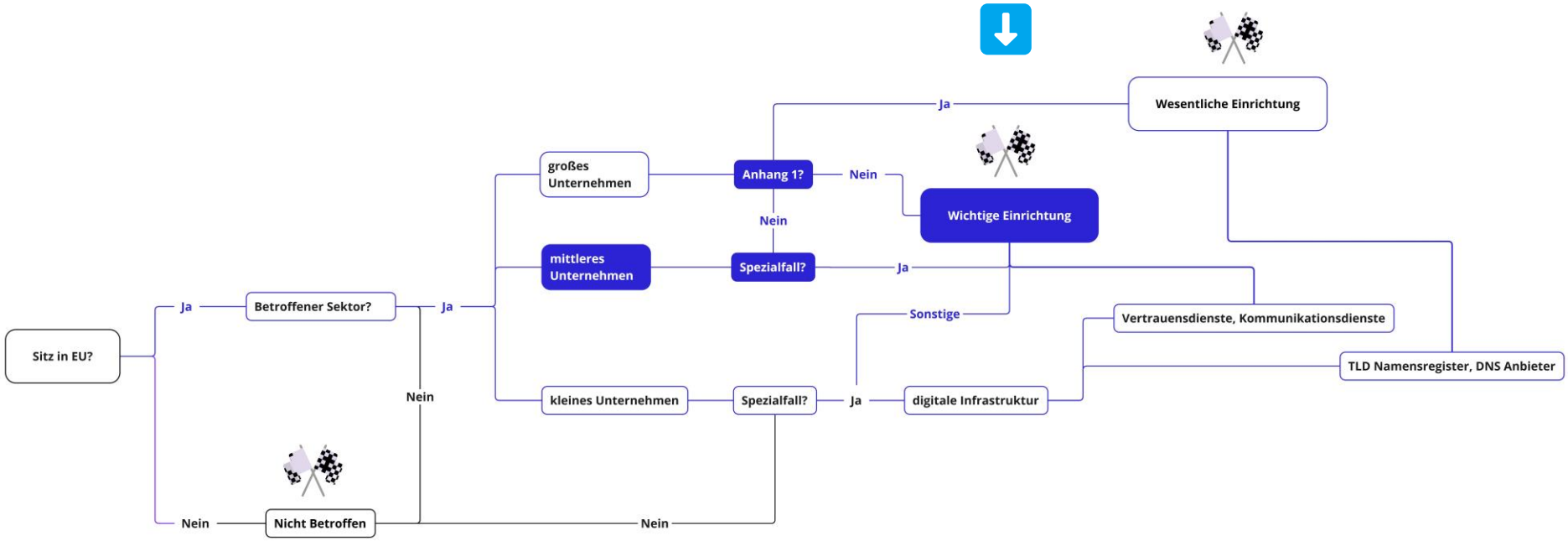
- Energie
- Verkehr
- Bankwesen*
- Finanzmarktinfrastrukturen*
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten B2B
- öffentliche Verwaltung
- Weltraum

Cyber Security Academy

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

Wenn nein ->

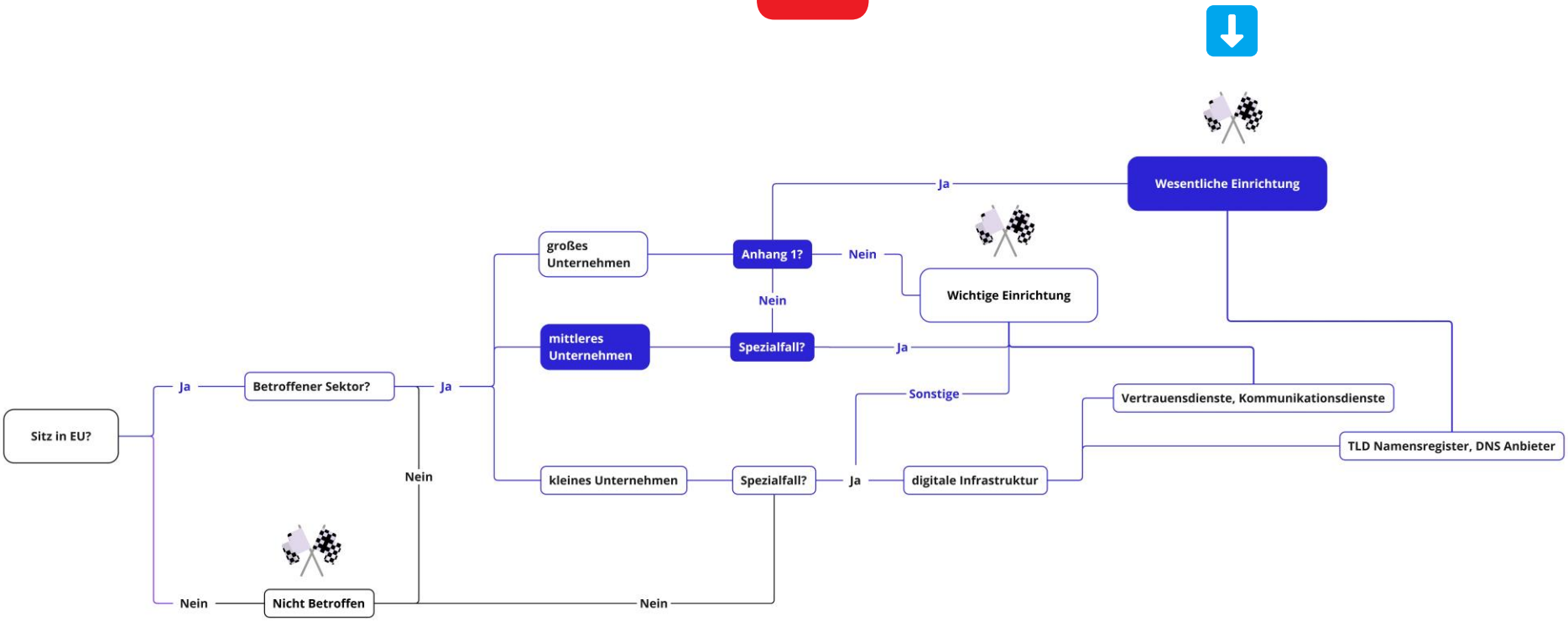
mittleres Unternehmen



Cyber Security Academy

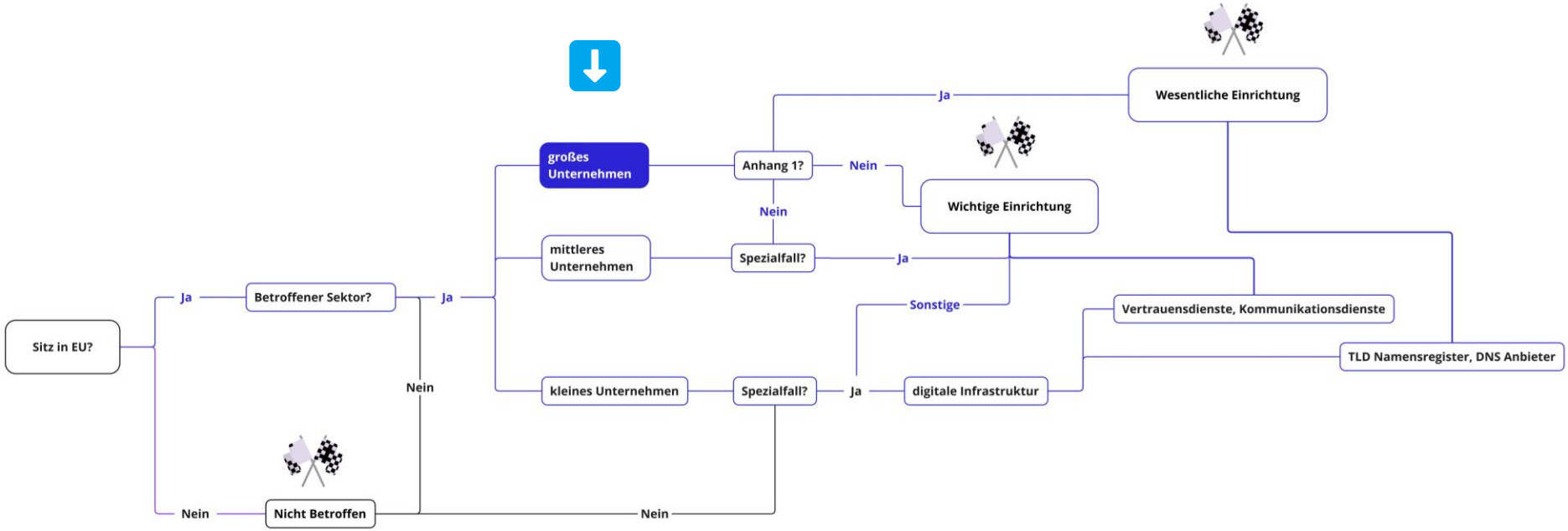
Wenn ja ->

mittleres Unternehmen

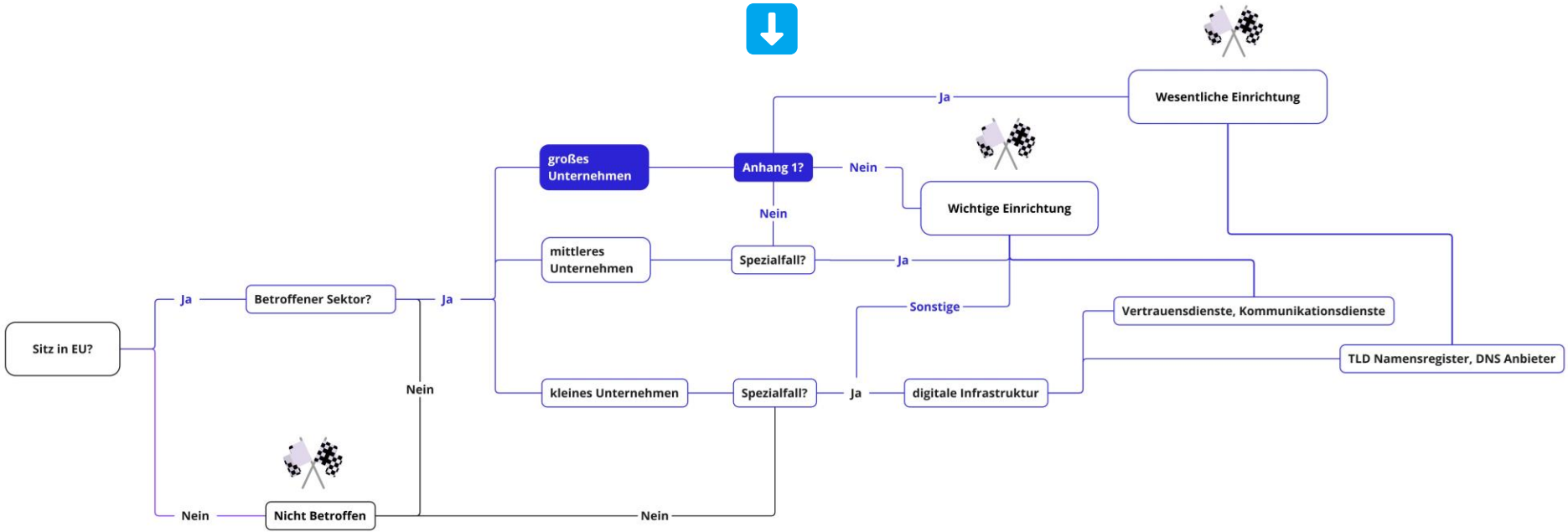


Cyber Security Academy

großes Unternehmen



großes Unternehmen



Betroffene Sektoren

Anhang 1

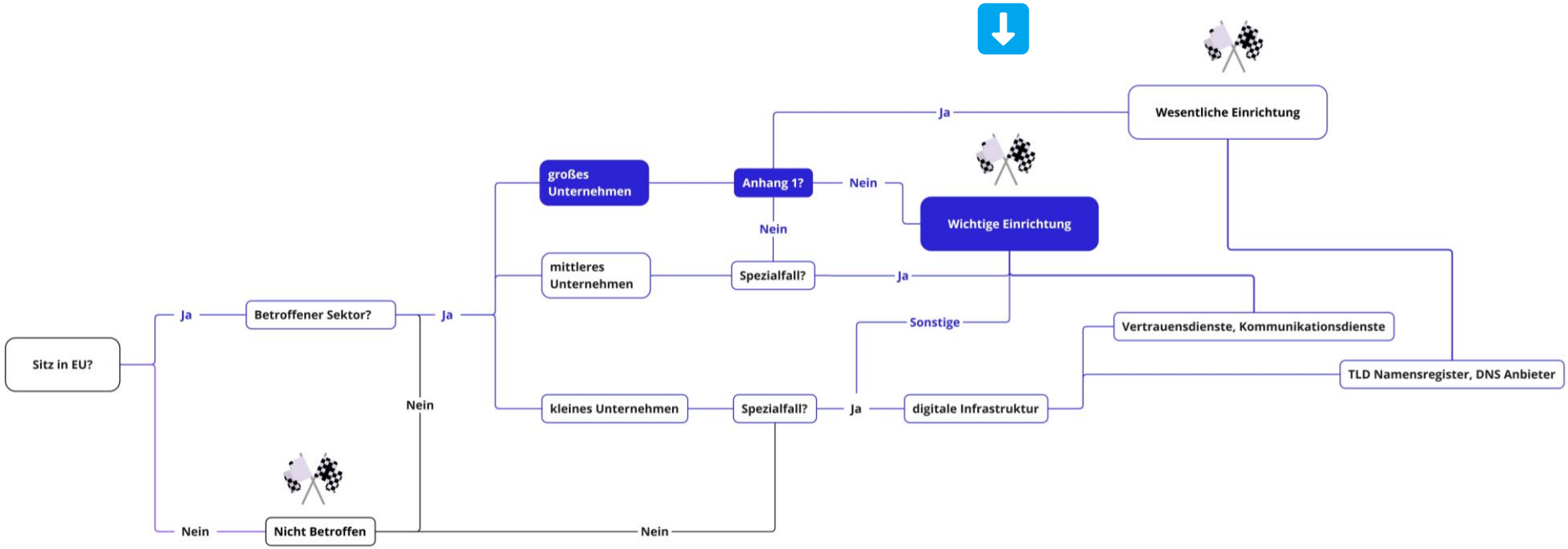
- Energie
- Verkehr
- Bankwesen*
- Finanzmarktinfrastrukturen*
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten B2B
- öffentliche Verwaltung
- Weltraum

Cyber Security Academy

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

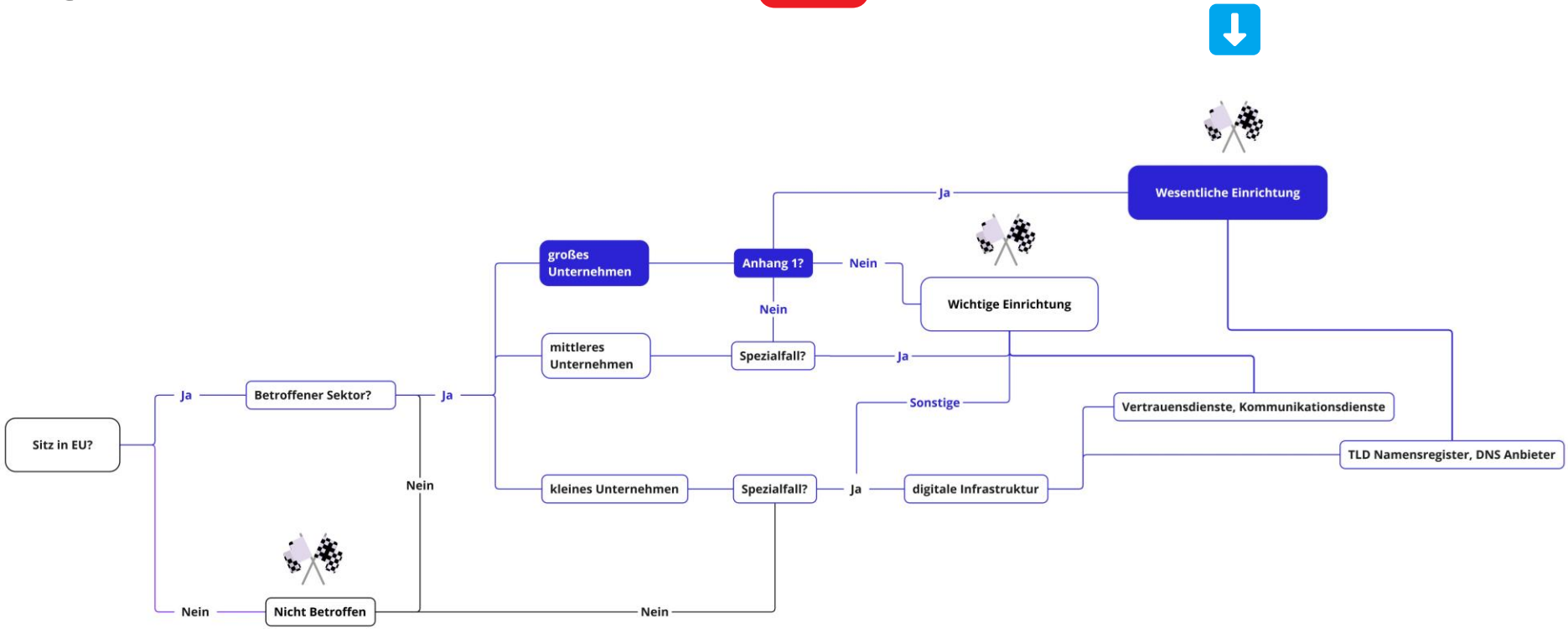
Wenn nein ->

großes Unternehmen



Wenn ja ->

großes Unternehmen



Ist das Vorgehen für euch verständlich?

Zeit für ein Quiz! 

Überprüfung und Rechtskraft zum Thema NIS 2

Warten auf finales Gesetz ⏩

- **Es gibt wahrscheinlich keine Bescheide mehr**
- **Einstufung ist selbst zu erfolgen**
- **Das ist dann dementsprechend zu Melden.**
  Könnte über USP passieren oder eigene Schnittstelle.
- **Überprüft ob eure Kunden betroffen sind.**

Was erwartet mich wenn ich betroffen bin ?

NIS 2 Auflagen

Wesentliche Einrichtungen

ex-ante & ex-post Aufsicht

regelmäßige und gezielte Sicherheitsprüfungen

Wichtige Einrichtungen

ex-post Aufsicht

nur bei begründetem Verdacht

Cyber Security Academy

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

NIS 2 Auflagen

Wesentliche Einrichtungen

ex-ante & ex-post Aufsicht

regelmäßige und gezielte Sicherheitsprüfungen

Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, Stichprobenkontrollen

Wichtige Einrichtungen

ex-post Aufsicht

nur bei begründetem Verdacht

Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

NIS 2 Auflagen

Wesentliche Einrichtungen	Wichtige Einrichtungen
ex-ante & ex-post Aufsicht	**ex-post Aufsicht**
regelmäßige und gezielte Sicherheitsprüfungen	nur bei begründetem Verdacht
Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, Stichprobenkontrollen	Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen
Bußgeldrahmen 10 Mio € oder 2 % des Weltweiten Jahresumsatzes (higher wins)	7 Mio € oder 1.4 % des Weltweiten Jahresumsatzes (higher wins)

Cyber Security Academy

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

Praxisübung – NIS 2 Selfcheck

Ablauf ⏩

- Überprüft, ob euer Unternehmen von der NIS 2 betroffen ist.
- Überprüft ob eure Kunden betroffen sind.

Tipps 💡

- Ruft den Ratgeber der WKO auf.
  [WKO Online Ratgeber NIS 2]

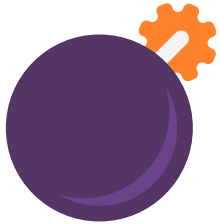
Dokumentation 📃

- Betroffen – JA/NEIN?
- „Wichtige“ oder „Wesentliche“ Einrichtung?

Zeit & Format 🕐

- 10 min
- 5 min Diskussion

Cyber Security Academy



Was denkt ihr, ist bei einem Incident zu tun, wenn ihr NIS 2 betroffen seit ?

Kurzer Recap
Incident Prozess

Incident Response Prozess

Incident

Ruhe bewahren

Meldung an relevante Beteiligte

IT-Manager, GF, Dep., Stakeholder etc.

Logs von Servern, Apps und Devices

Sammeln und filtern von Infos

Hilfe anfordern

SOS

Expert:innen, Stakeholder?

IT-Manager, GF

Entscheidung treffen

Incident lösen & Aufräumen

MA, GF, IT, Stakeholder

Cyber Security Academy

Mit der NIS 2 kommen weitere Aufgaben dazu.

Meldefristen – NIS 2

24h

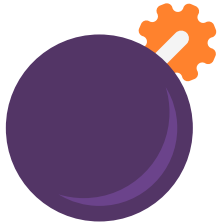
Frühwarnung

72h

Ordentliche Meldung

1 Monat

Endbericht



Aber was für Incidents müssen eigentlich überhaupt gemeldet werden laut NIS 2?

Jegliche Vorfälle, die unter die Kategorie „erheblich“ fallen.

Meldepflichtige Vorfälle – NIS 2

§ 35. (1) Ein Cybersicherheitsvorfall gilt als erheblich, wenn er

1. schwerwiegende Betriebsstörungen der erbrachten Dienste der Einrichtung oder schwerwiegende finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;

2. er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Quelle: https://www.parlament.gv.at/dokument/XXVII/A/4129/fname_1635702.pdf

Meldepflichtige Vorfälle – NIS 2

Vereinfacht gesagt:

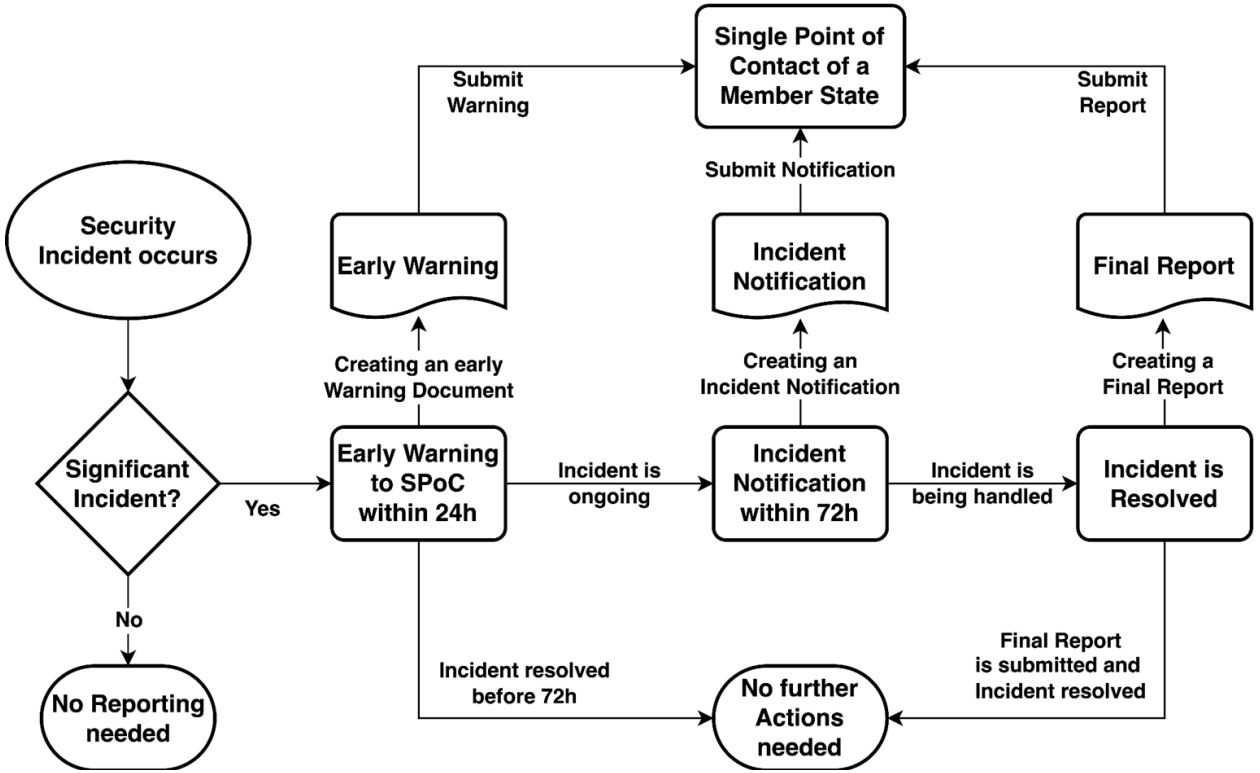
Ein Cybersicherheitsvorfall liegt vor bei..

schwerwiegender Betriebsstörung

erheblichem Schaden

Quelle: https://www.parlament.gv.at/dokument/XXVII/A/4129/fname_1635702.pdf

Meldeprozess – NIS 2



Quelle: https://www.parlament.gv.at/dokument/XXVII/A/4129/fname_1635702.pdf

Meldeprozess – NIS 2

Meldungen erfolgen über das nationale CERT.

Welche Institutionen, mit NIS 2 Bezug sind euch bekannt ?

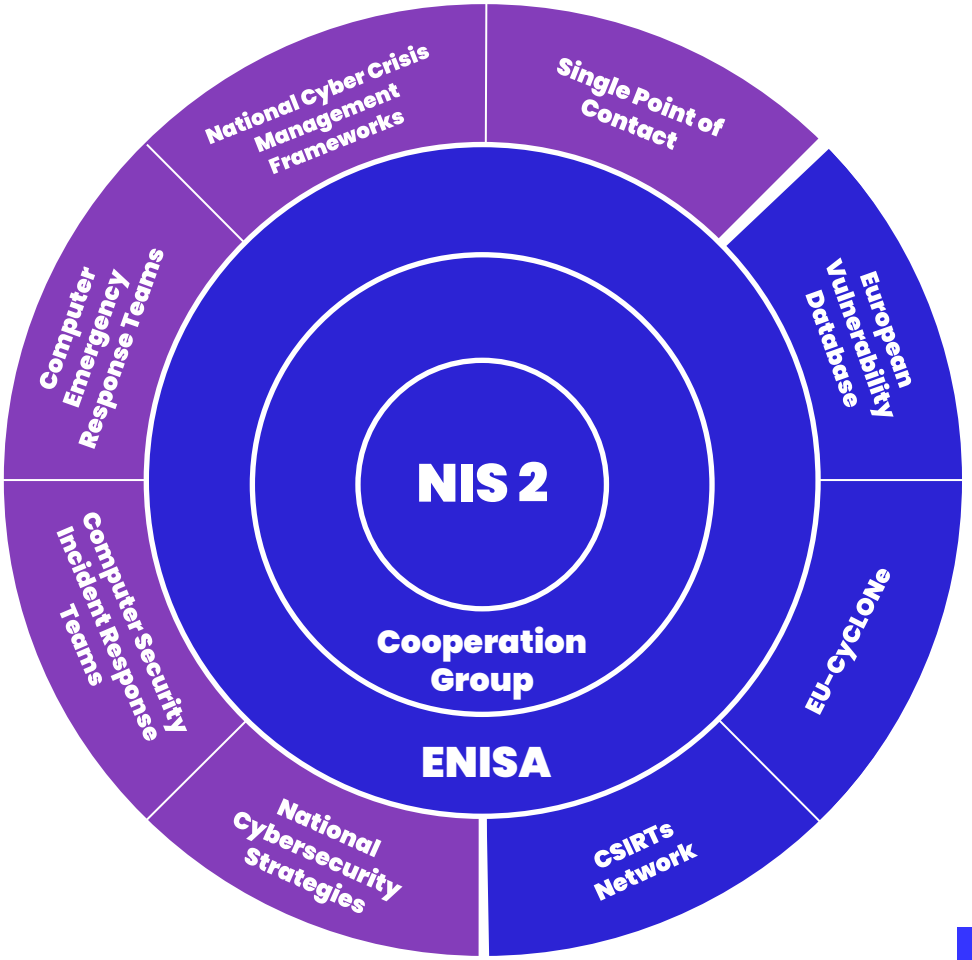
Als kurze Erinnerung, hier nochmal der vorgegebene Aufbau.

EU

1. Cooperation Group
2. ENISA
3. EVD
4. CSIRTs Network
5. CyCLONe

Österreich

1. CERT
2. CSIRTs
3. NCS
4. NCCMF
5. Single Point of Contact



CSIRT – in Österreich gibt es dafür 3 Teams

CSIRT

Quelle: https://www.nis.gv.at/fragen-und-antworten/computer-notfallteams.html

CERT – gibt es in Österreich viele, da schon vor NIS 2 relevantes Thema

CERT (Auszug)

A1-CERT	CERT.at	IKT Linz CERT	sCERT
ACOnet-CERT	CERT-Verbund Österreich	MilCERT	SV-CERT
Austrian Energy CERT	FREQUENTIS SIRT	Post CSIRT	WienCERT
BRZ-CERT	GovCERT Austria	Raiffeisen Informatik CSIRT	WILICERT

Quelle: https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/CERTs.html

Was ist jetzt eigentlich der Unterschied zwischen CERT und CSIRT?

CERT vs. CSIRT

CERT

regionale/nationale Ebene

Reaktion und Koordination bei einem Vorfall.

CSIRT

innerhalb der Organisation

Identifikation, Analyse und Melden von Sicherheitsvorfällen.

Cyber Security Academy

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

CERT vs. CSIRT

CERT

regionale/nationale Ebene

Reaktion und Koordination bei einem Vorfall.

Fokus auf Erkennung, Reaktion, Behebung und Prävention von Vorfällen.

CSIRT

innerhalb der Organisation

Identifikation, Analyse und Melden von Sicherheitsvorfällen.

Fokus auf die Implementierung von Maßnahmen zur Verbesserung der Sicherheit in der Organisation.

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

CERT vs. CSIRT

CERT

regionale/nationale Ebene

- Reaktion und Koordination bei einem Vorfall.
- Fokus auf Erkennung, Reaktion, Behebung und Prävention von Vorfällen.
- Verbunden mit Regierungsbehörden, Bildungseinrichtungen oder Unternehmen.

CSIRT

innerhalb der Organisation

- Identifikation, Analyse und Melden von Sicherheitsvorfällen.
- Fokus auf die Implementierung von Maßnahmen zur Verbesserung der Sicherheit in der Organisation.
- Haben spezialisierte Kenntnisse in forensischer Analyse und Incident-Response-Techniken.

Cyber Security Academy

Quelle: https://www.parlament.gv.at/gegenstand/XXVII/A/4129

Praxisübung – Cyber Strategien 🔍

Ablauf ⏩

- Versucht herauszufinden, welche Cybersicherheitsstrategie Österreich verfolgt.

Dokumentation 📄

- Notiert die relevantesten Informationen und zugehörigen Quellen

Zeit & Format 🕐

- 10 min Recherche
- 5 min Diskussion

Zum Abschluss des Kapitels, hier nochmal die wichtigsten Ressourcen rund um das Thema NIS 2

NIS 2 – Nützliche Links

CSIRT Network

NIS Meldung

EU-CyCLONe

Watchlist Internet AT

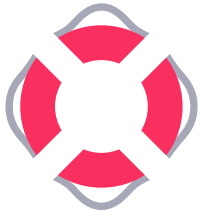
NIS Cooperation Group

WKO NIS Übersicht

Data Breach Meldung

Basissicherheit KMUs

Risikomanagament maßnahmen



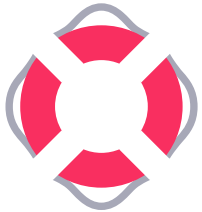
Welche Anforderungen müssen aufgrund der NIS 2 in Organisationen erfüllt werden ?

Das hängt stark von der Organisation ab.

Es gibt jedoch Maßnahmen, die jede Organisation treffen sollte!

Das hängt stark von der Organisation ab.

Risikomanagament maßnahmen

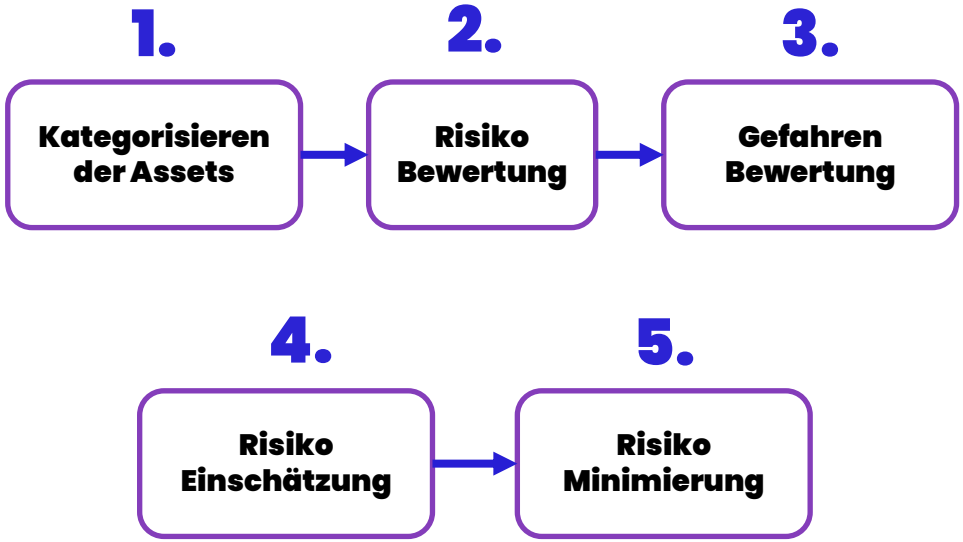


Maßnahmen, die jede Organisation treffen sollte!

1. Risikoanalyse und Sicherheitskonzept

1. Risikoanalyse und Sicherheitskonzept

- IT Asset Management
- Gefahrenidentifikation
- Ist es für mich für mein Unternehmen relevant?
- Welche Maßnahmen gehe ich in welcher Reihenfolge an?



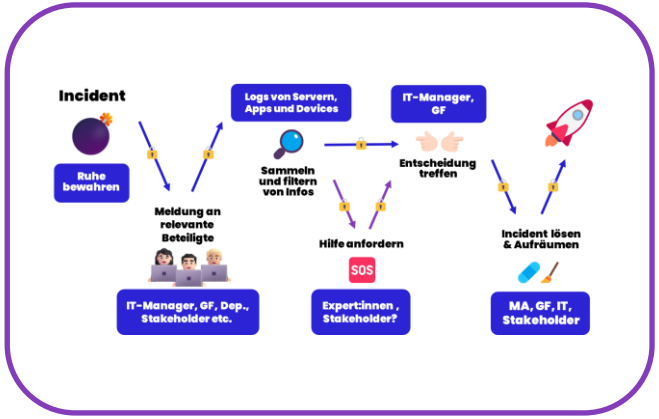
Quelle: https://searchinform.com/

Risikomanagementmaßnahmen

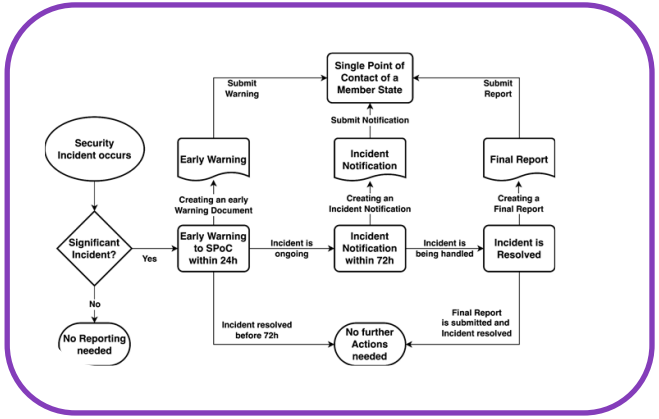
1. **Risikoanalyse und Sicherheitskonzept:** Die Risiken identifizieren, bewerten und dokumentieren.

2. Sicherheitsvorfälle und Meldepflicht

2. Sicherheitsvorfälle und Meldepflicht



Interner Incident Response Plan



NIS 2 Meldeverhalten

Quelle: https://axaxl.com/fast-fast-forward/articles/the-cyber-incident-response-lifecycle

Risikomanagementmaßnahmen

1. **Risikoanalyse und Sicherheitskonzept:** Die Risiken identifizieren, bewerten und dokumentieren.

2. **Sicherheitsvorfälle und Meldepflicht:** Verhaltensregeln und Prozesse für Sicherheitsvorfälle.

3. Backups, Continuity & Notfallmanagement

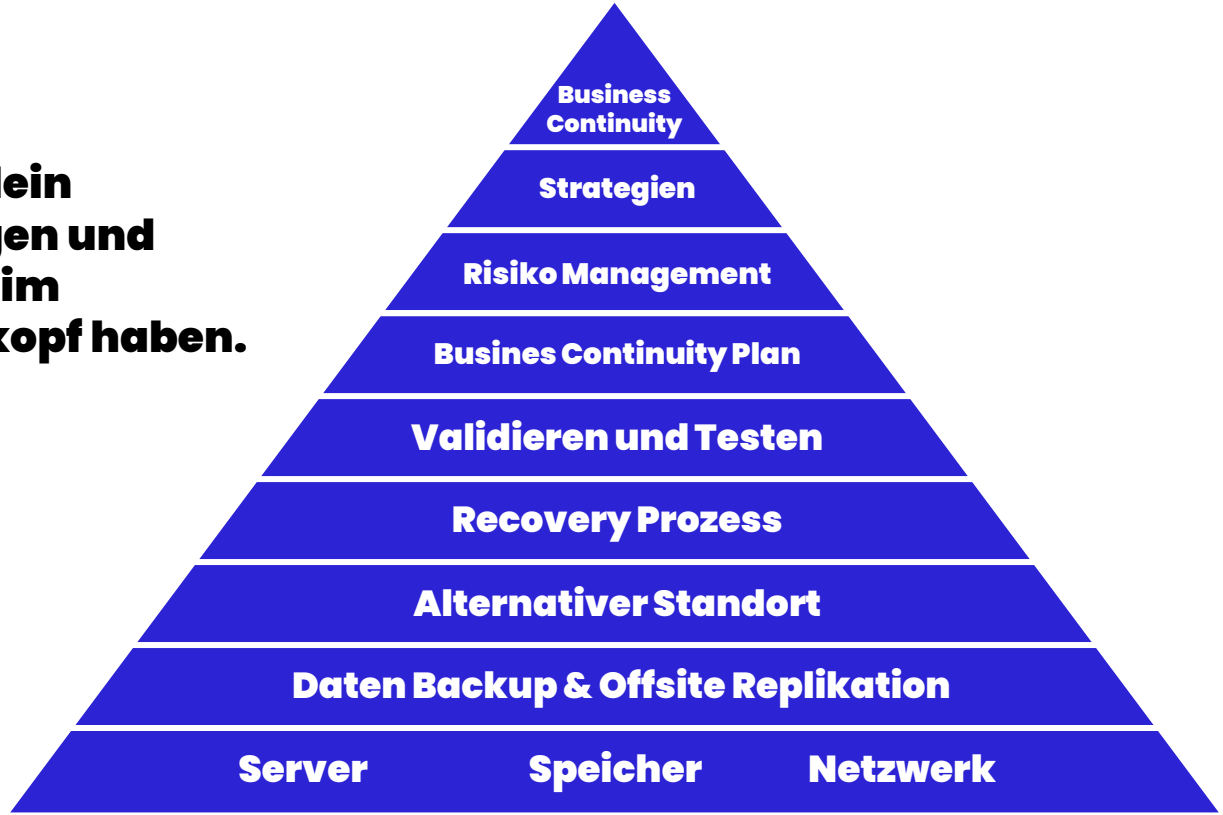
3. Backups, Continuity & Notfallmanagement

Tipp: klein anfangen und immer im Hinterkopf haben.

Quelle: https://www.boxuk.com/insight/business-continuity-disaster-recovery-why-should-you-care/

3. Backups, Continuity & Notfallmanagement

Tipp: klein anfangen und immer im Hinterkopf haben.



Quelle: https://www.boxuk.com/insight/business-continuity-disaster-recovery-why-should-you-care/

Risikomanagementmaßnahmen

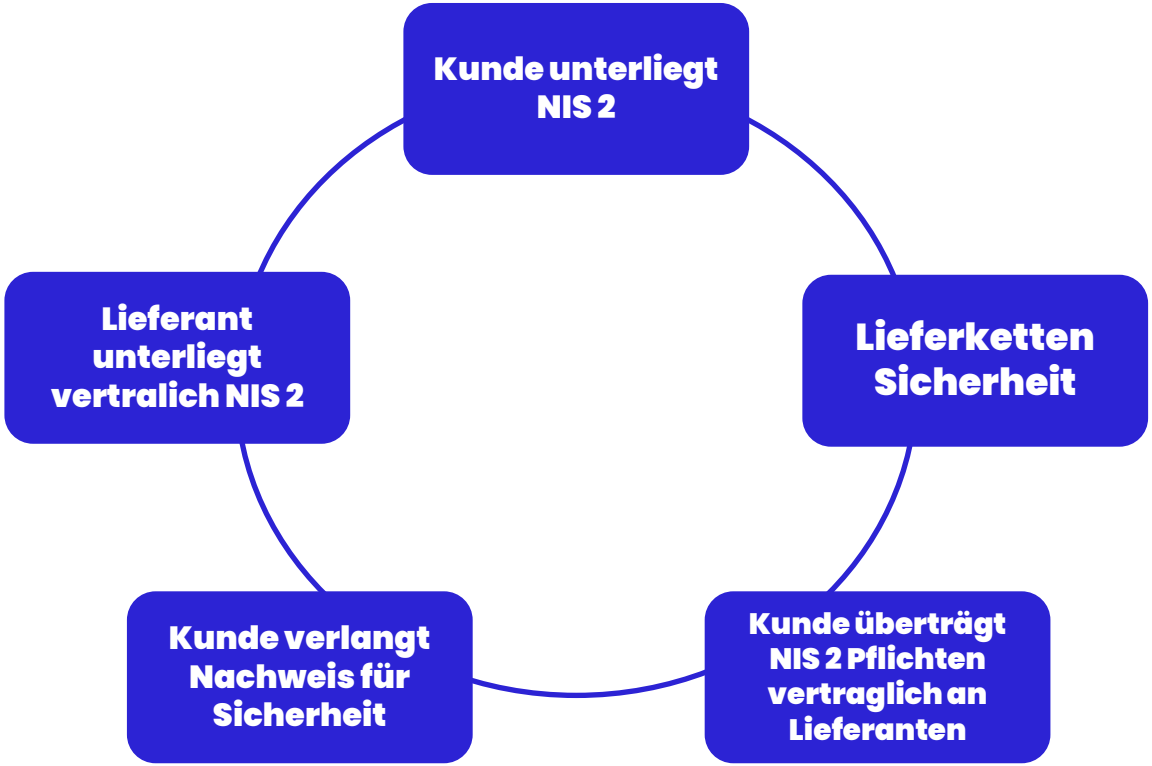
1. **Risikoanalyse und Sicherheitskonzept:** Die Risiken identifizieren, bewerten und dokumentieren.

2. **Sicherheitsvorfälle und Meldepflicht:** Verhaltensregeln und Prozesse für Sicherheitsvorfälle.

3. **Backups, Continuity und Notfallmanagement :** Notfallhandbuch und verschiedene Szenarien, wie der Betrieb wiederaufgenommen werden kann.

4. Sicherheit der Lieferkette

4. Sicherheit in der Lieferkette



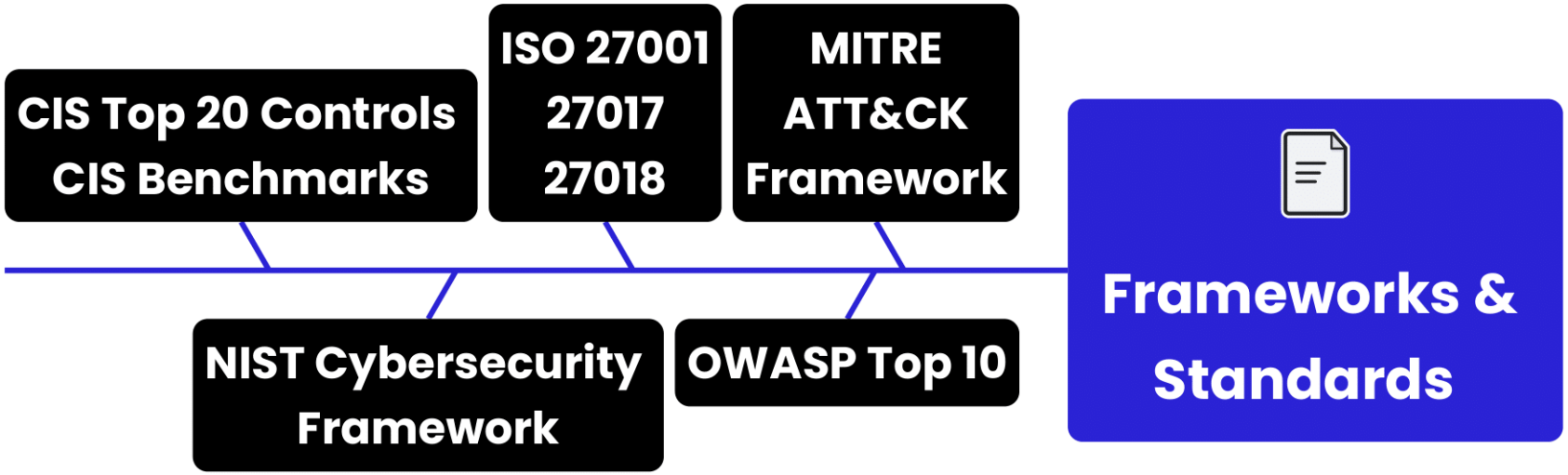
Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht - Webinar

Risikomanagementmaßnahmen

4. Sicherheit der Lieferkette:
Wer hat Zugriff auf Systeme, welche Daten und Produkte gelangen in die sichere Zone des eigenen Unternehmens?

5. Erwerb, Entwicklung und Wartung von IKT

5. Erwerb, Entwicklung und Wartung von ITK



Risikomanagementmaßnahmen

4. Sicherheit der Lieferkette:
Wer hat Zugriff auf Systeme, welche Daten und Produkte gelangen in die sichere Zone des eigenen Unternehmens?

5. Erwerb, Entwicklung und Wartung von IKT:
Patch Management System und Update Plan.

6. Planung und Bewertung von Maßnahmen

6. Planung und Bewertung von Maßnahmen

C A R E

Consistent **Adequate** **Reasonable** **Effective**

Quelle: https://www.gartner.com/en/articles/4-metrics-that-prove-your-cybersecurity-program-works

6. Planung und Bewertung von Maßnahmen

Diese Fragen solltet ihr euch stellen:

- **Was sind meine Risiken?**
- **Wie kann ich die Maßnahmen messen?**
- **Wie definiere ich die richtigen Metriken?**
- **Wo wird das Dokumentiert?**
- **Wann verändere ich die Metriken?**

CARE

Adequate **E**ffective

Consistent **R**easonable

Cyber Security Academy

Quelle: https://www.gartner.com/en/articles/4-metrics-that-prove-your-cybersecurity-program-works

Risikomanagementmaßnahmen

4. Sicherheit der Lieferkette:
Wer hat Zugriff auf Systeme, welche Daten und Produkte gelangen in die sichere Zone des eigenen Unternehmens?

5. Erwerb, Entwicklung und Wartung von IKT:
Patch Management System und Update Plan.

6. Planung und Bewertung von Maßnahmen:
Überprüfen, ob gesetzte Maßnahmen auch gewünschte Wirkung entfalten.

7. Awareness und Cyber-Hygiene

7. Awareness und Cyber-Hygiene

Klassische Security Schulungen sind meistens sehr altmodisch und nicht am aktuellen Stand!

Quelle: https://digitaleneuordnung.de/blog/why-how-what/

7. Awareness und Cyber-Hygiene

WHY

Warum und wofür ist es wichtig ?

Quelle: https://digitaleneuordnung.de/blog/why-how-what/

7. Awareness und Cyber-Hygiene

HOW

Wie willst du dein Ziel erreichen?

Quelle: https://digitaleneuordnung.de/blog/why-how-what/

7. Awareness und Cyber-Hygiene

WHAT

was machst du um dein Ziel zu erreichen?

Quelle: https://digitaleneuordnung.de/blog/why-how-what/

Risikomanagementmaßnahmen

7. Awareness und Cyber-Hygiene:
Alle technischen oder organisatorischen Maßnahmen sind nur dann wirkungsvoll, wenn alle Mitarbeiter*innen sie kennen und umsetzen.

8. Konzepte und -verfahren für Kryptografie

8. Konzepte und -verfahren für Kryptografie

Confidentiality

Integrity

Availability

Quelle: https://www.idstrong.com/sentinel/what-is-cia-triad/

Risikomanagementmaßnahmen

7. Awareness und Cyber-Hygiene:
Alle technischen oder organisatorischen Maßnahmen sind nur dann wirkungsvoll, wenn alle Mitarbeiter*innen sie kennen und umsetzen.

8. Konzepte und -verfahren für Kryptografie:
Jegliche Kommunikation sollte durch Kryptographische Verschlüsselung abgesichert werden.

9. Personal, Zugriffskontrolle und Anlagenmanagement

9. Personal, Zugriffskontrolle und Anlagenmanagement

- **Least Privilege Principle**
- **Regelmäßige Überprüfung (Auditing)**
- **Schulung von Mitarbeiter:innen**

Quelle: https://www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf

Risikomanagementmaßnahmen

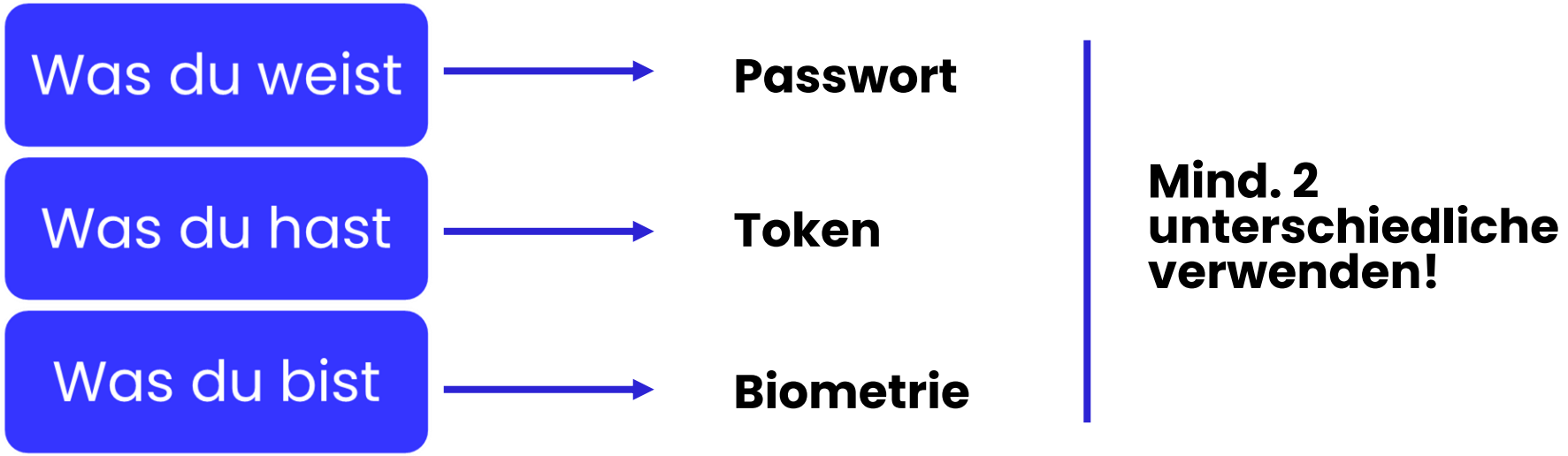
7. Awareness und Cyber-Hygiene:
Alle technischen oder organisatorischen Maßnahmen sind nur dann wirkungsvoll, wenn alle Mitarbeiter*innen sie kennen und umsetzen.

8. Konzepte und -verfahren für Kryptografie:
Jegliche Kommunikation sollte durch Kryptographische Verschlüsselung abgesichert werden.

9. Personal, Zugriffskontrolle und Anlagenmanagement:
Risiken bestehen nicht nur da, wo Firewalls versagen – sondern auch dort, wo Unbefugte ohne Weiteres Zugriff auf Dokumente, Maschinen oder IT haben.

10. Multifaktor-Authentifizierung und gesicherte Kommunikation

10. Multi Faktor Authentifizierung



Quelle: https://blog.lastpass.com/de/posts/2023/10/tracing-the-evolution-of-multi-factor-authentication

Risikomanagementmaßnahmen

7. Awareness und Cyber-Hygiene:
Alle technischen oder organisatorischen Maßnahmen sind nur dann wirkungsvoll, wenn alle Mitarbeiter*innen sie kennen und umsetzen.

8. Konzepte und -verfahren für Kryptografie:
Jegliche Kommunikation sollte durch Kryptographische Verschlüsselung abgesichert werden.

9. Personal, Zugriffskontrolle und Anlagenmanagement:
Risiken bestehen nicht nur da, wo Firewalls versagen – sondern auch dort, wo Unbefugte ohne Weiteres Zugriff auf Dokumente, Maschinen oder IT haben.

10. Multifaktor-Authentifizierung und gesicherte Kommunikation:
Zweistufige Authentifizierung macht unberechtigte Zugriffe unwahrscheinlicher, aber nicht unmöglich. Deshalb sieht NIS-2 auch funktionierende Kommunikationskanäle für den Notfall vor.

Risikomanagementmaßnahmen

1. Risikoanalyse und Sicherheitskonzept
2. Sicherheitsvorfälle und Meldepflicht
3. Backups, Continuity und Notfallmanagement
4. Sicherheit der Lieferkette
5. Erwerb, Entwicklung und Wartung von IKT
6. Planung und Bewertung von Maßnahmen
7. Awareness und Cyber-Hygiene
8. Konzepte und -verfahren für Kryptografie
9. Personal, Zugriffskontrolle und Anlagenmanagement
10. Multifaktor-Authentifizierung und gesicherte Kommunikation

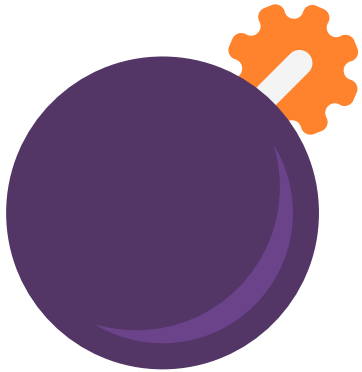
Zeit für ein Quiz! 

Wie können wir diese Maßnahmen nun umsetzen ?

Ein kleiner Appell an euch

Auch wenn ihr nicht betroffen seid!

- Verliert auf keinen Fall Zeit!
- Wartet nicht auf das Gesetz!
- Die wesentlichen Grundlagen zur Informationssicherheit sind längst etabliert, hinlänglich bekannt und allgemein zugänglich - packt es direkt an! Am besten noch in dieser Woche!



Security Timer

Ausgangspunkt für alle Maßnahmen ist unser Risikomanagement.

Risikomanagement Prozess

Ziele der Organisation

- Was ist das aktuelle Unternehmensziel?
- Was ist unsere Vision/Mission?
- Wie ist die Arbeitsweise/Kultur?
- Wie werden diese Ziele kommuniziert?

Risikomanagement Prozess

Ziele der Organisation

Vision/Mission

Risikomanagement Prozess

Wertschöpfungs-kette

- **Wie passiert die Wertschöpfung?**
- **Wie viele Produkte/Dienstleistungen gibt es?**
- **Wie kommen diese an die Kunden?**

Risikomanagement Prozess

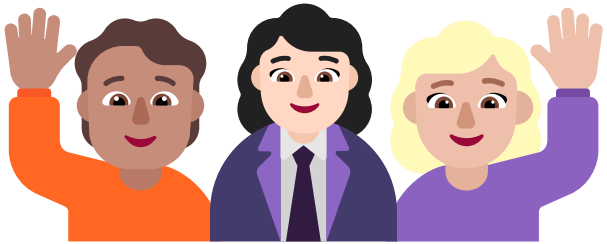
Ziele der Organisation

Vision/Mission

Wertschöpfungskette

Produkte/ Dienstleistung

Risikomanagement Prozess



Abteilungen &Teams

- **Welche Teams und Abteilungen gibt es?**
- **Wie arbeiten diese Teams?**
- **Was brauchen diese Teams täglich zum Arbeiten?**
- **Wer ist für die IT-Security verantwortlich?**

Risikomanagement Prozess

Ziele der Organisation

Vision/Mission

Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Wertschöpfungs kette

Produkte/ Dienstleistung

Cyber Security Academy

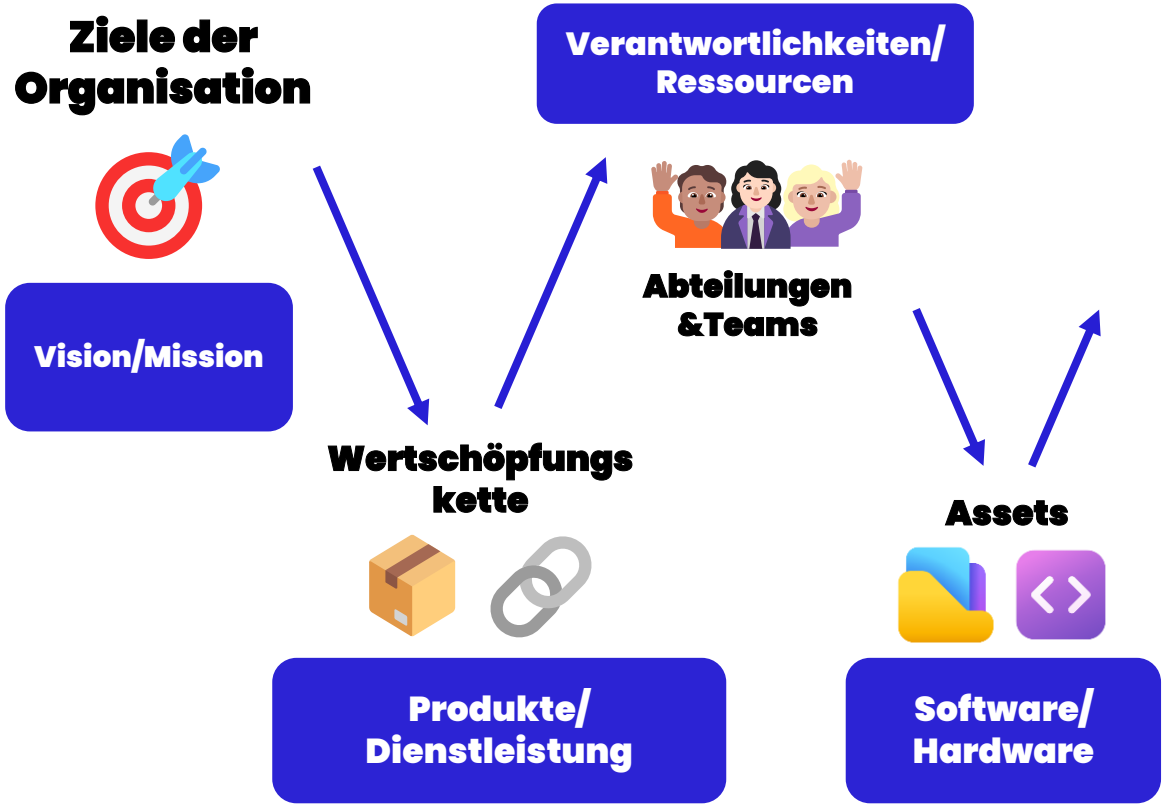
Risikomanagement Prozess

Assets

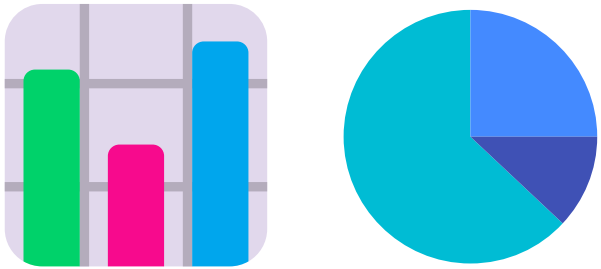
Welche Assets benötigt man für was?

- Software
- Hardware
- Daten
- Services
- Lieferanten

Risikomanagement Prozess



Risikomanagement Prozess



Assets Kritikalität zuweisen

Wie kritisch ist ein Asset für mein Ziel?

Leicht

Mittel

Stark

Risikomanagement Prozess

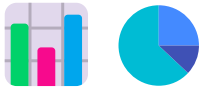
Ziele der Organisation

Vision/Mission

Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Leicht, Mittel, Stark



Kritikalität zuweisen

Wertschöpfungs kette

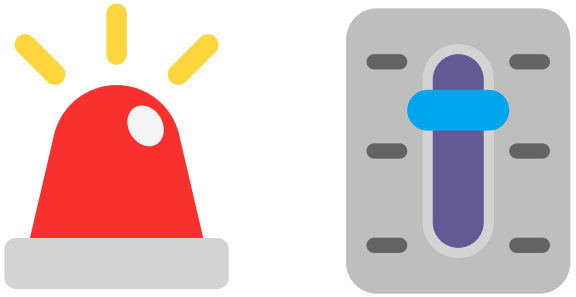
Produkte/ Dienstleistung

Assets

Software/ Hardware

Cyber Security Academy

Risikomanagement Prozess



Maßnahmen setzen

- **Adäquat zu den zugewiesenen Einstufungen.**

Leicht **Mittel** **Stark**

Risikomanagement Prozess

Ziele der Organisation

Vision/Mission

Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Leicht, Mittel, Stark

Kritikalität zuweisen

Wertschöpfungs kette

Produkte/ Dienstleistung

Assets

Software/ Hardware

Maßnahmen setzen

Entsprechend Kritikalität

Cyber Security Academy

Risikomanagement Prozess

KVP

- Der Prozess sollte kontinuierlich verbessert werden.
- Das ist ein lebendes Projekt.
- Ein minimaler Prozess ist viel besser als gar kein Prozess!

Risikomanagement Prozess

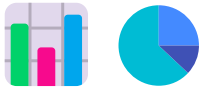
Ziele der Organisation

Vision/Mission

Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Leicht, Mittel, Stark



Kritikalität zuweisen

Wertschöpfungs kette

Produkte/ Dienstleistung

Assets

Software/ Hardware

Maßnahmen setzen

Entsprechend Kritikalität

Cyber Security Academy

Blick hinter die Kulissen 🖥️

Anhang 3 und NIS Fact Sheets

Praxisübung – Status Quo

Ablauf ⏩

- Wie funktioniert euer Unternehmen?
- Welche Assets sind im Einsatz?
- Wie kritisch sind diese?

Dokumentation 📃

- Assets die in deiner Rolle von Bedeutung sind

Zeit & Format ⏲️

- 30 min selbständige Ausarbeitung
- 10 min Diskussion

Zeit für ein Quiz! 

Habt ihr noch Fragen zu dem Thema NIS 2?

Lernziele 🚀

- Was sind die Cyber Security Intentionen der EU?
- Wie ist die NIS 2 Richtlinie aufgebaut?
- Ist mein Unternehmen NIS 2 betroffen?



Inhalte 📦

Cyberangriffe, Trends und Learnings

NIS 2 Richtlinie un die Lieferkette

Cyber Security 101 „Baseline“

Netzwerk, Infrastruktur, Cloud und Datensicherheit

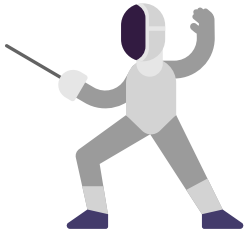
Inhalte 📦

Cyberangriffe

NIS 2

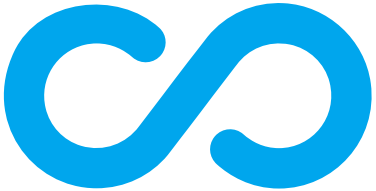
Cyber Sec 101

Maßnahmen und Konzepte



Wie können wir uns schützen?

Ganzheitliches Bild von Cybersecurity



Security is Everywhere

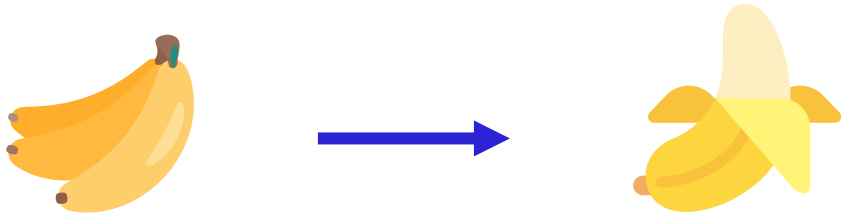
Ganzheitliches Bild von Cybersecurity

Security is Everywhere: Security sollte immer ganzheitlich betrachtet werden und nicht nur punktuell.

Die Bananenschale

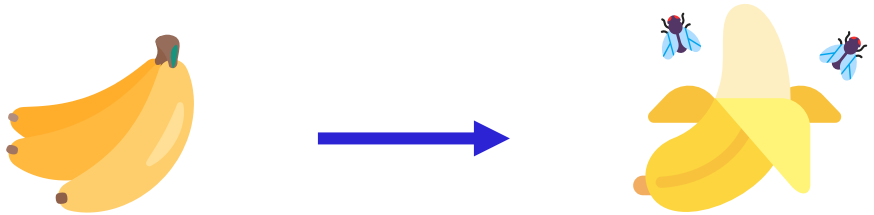
Ganzheitliches Bild von Cybersecurity

Die Bananenschale



Ganzheitliches Bild von Cybersecurity

Die Bananenschale



Ganzheitliches Bild von Cybersecurity

Security is Everywhere: Security sollte immer ganzheitlich betrachtet werden und nicht nur punktuell.

Die Bananenschale: Security ist wie die Schale einer Banane 🍌 , wenn die Schale wegfällt, hält die Frucht nicht lange.

Hausverstand

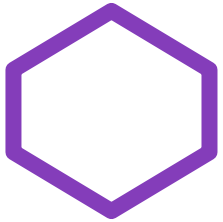
Ganzheitliches Bild von Cybersecurity

Security is Everywhere: Security sollte immer ganzheitlich betrachtet werden und nicht nur punktuell.

Die Bananenschale: Security ist wie die Schale einer Banane 🍌, wenn die Schale wegfällt, hält die Frucht nicht lange.

Hausverstand : Sicherheitsbewusstsein sollte bei jeder Person Teil davon sein.

Wie funktioniert das in der Praxis?



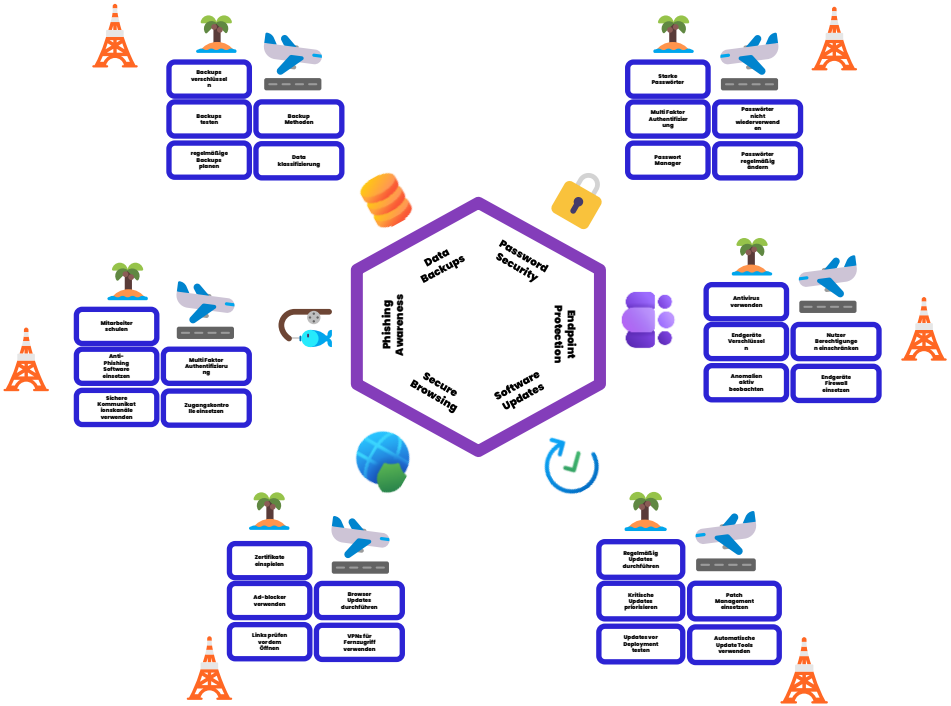
Cybersecurity 101

Cybersecurity 101

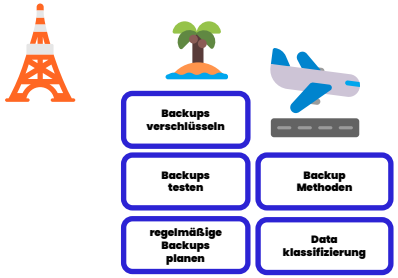
Überblick der wichtigsten Cybersecurity Maßnahmen

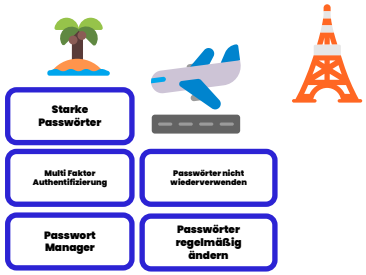
Cyber Security Academy

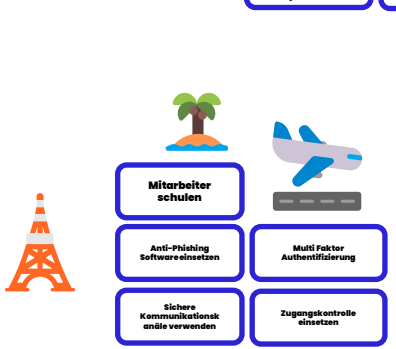
Cybersecurity 101

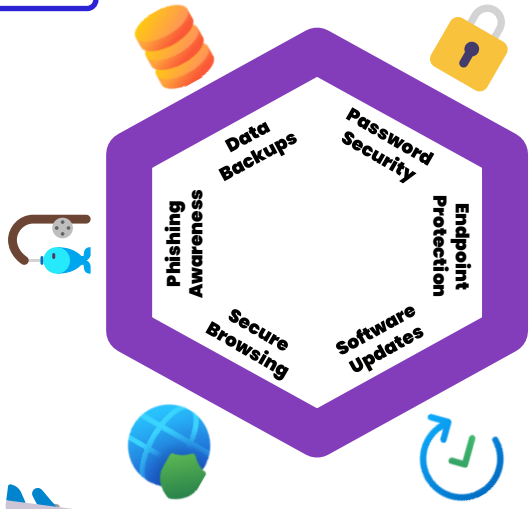


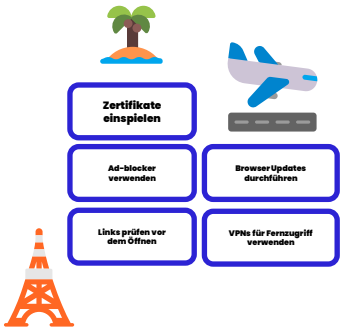
Quelle:https://linkedin.com/Gruppe: Information Security Network

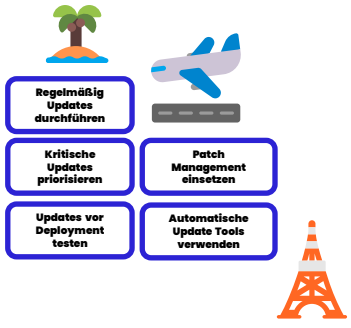




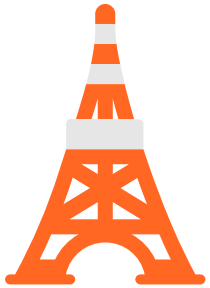








Cyber Security Academy



Backups verschlüsseln

Backups testen

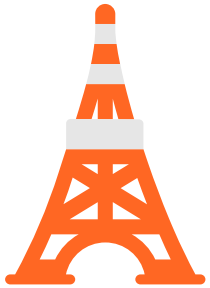
Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups

Cyber Security Academy



Backups verschlüsseln

Backups testen

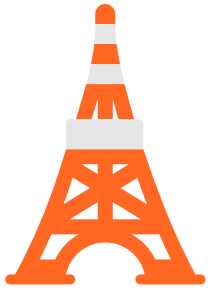
Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups

Cyber Security Academy



Backups verschlüsseln

Backups testen

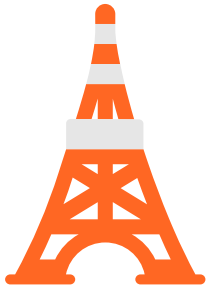
Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups

Cyber Security Academy



Backups verschlüsseln

Backups testen

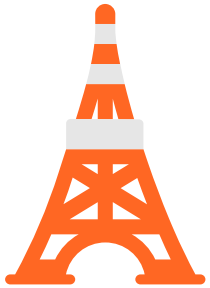
Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups

Cyber Security Academy



Backups verschlüsseln

Backups testen

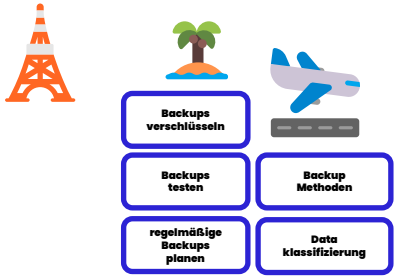
Backup Methoden

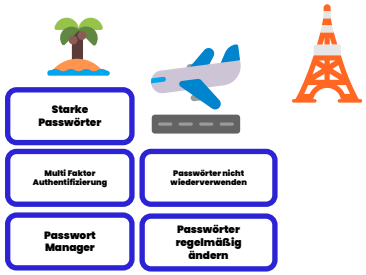
regelmäßige Backups planen

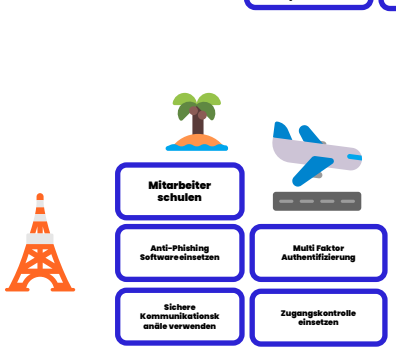
Daten Klassifizierung

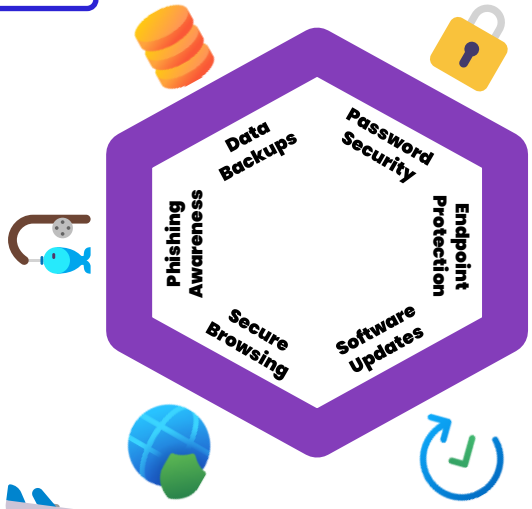
Data Backups

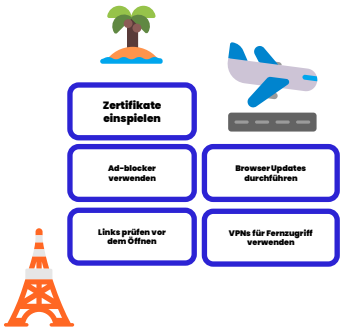
Cyber Security Academy

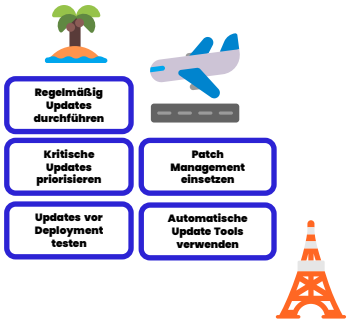






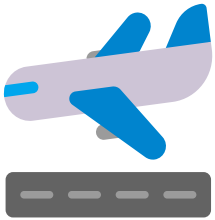


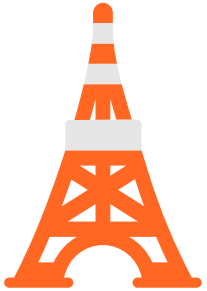




Cyber Security Academy

Passwort Security





Starke Passwörter

Multi Faktor Authentifizierung

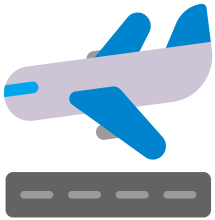
Passwörter nicht wiederverwenden

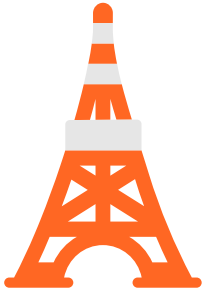
Passwort Manager

Passwörter regelmäßig ändern

Cyber Security Academy

Passwort Security





Starke Passwörter

Multi Faktor Authentifizierung

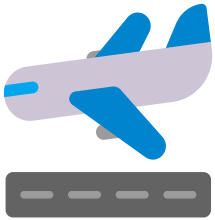
Passwörter nicht wiederverwenden

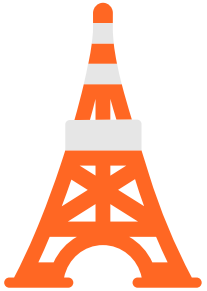
Passwort Manager

Passwörter regelmäßig ändern

Cyber Security Academy

Passwort Security





Starke Passwörter

Multi Faktor Authentifizierung

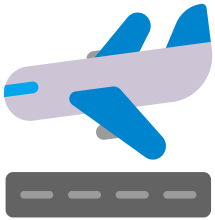
Passwörter nicht wiederverwenden

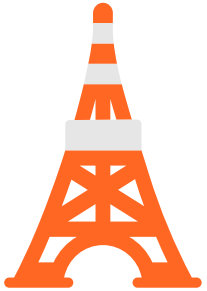
Passwort Manager

Passwörter regelmäßig ändern

Cyber Security Academy

Passwort Security

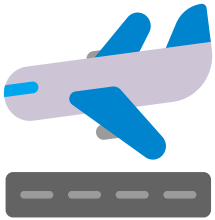


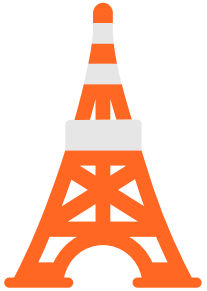


- Starke Passwörter
- Multi Faktor Authentifizierung
- Passwort Manager
- **Passwörter nicht wiederverwenden**
- Passwörter regelmäßig ändern

Cyber Security Academy

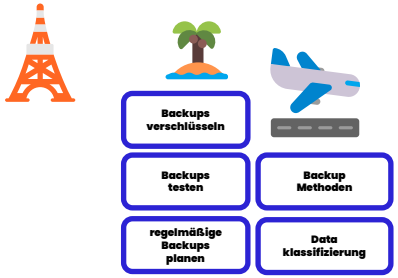
Passwort Security

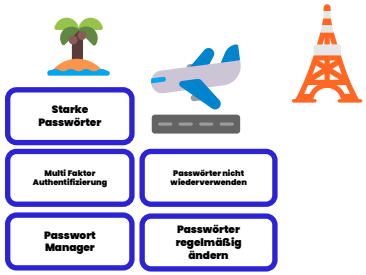


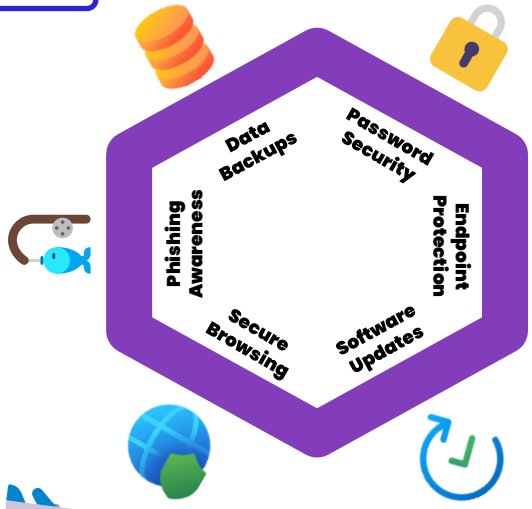


- Starke Passwörter
- Multi Faktor Authentifizierung
- Passwörter nicht wiederverwenden
- Passwort Manager
- **Passwörter regelmäßig ändern**

Cyber Security Academy

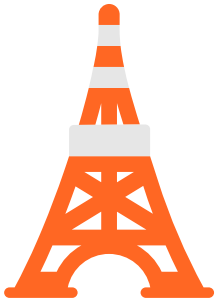






Cyber Security Academy

Endpoint Protection



Antivirus verwenden

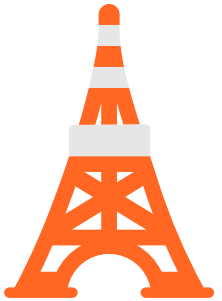
Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Endpoint Protection



Antivirus verwenden

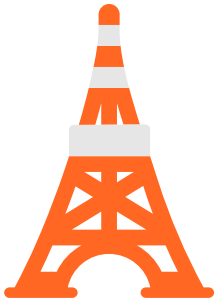
Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Endpoint Protection



Antivirus verwenden

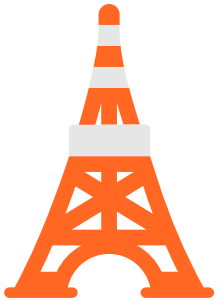
Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

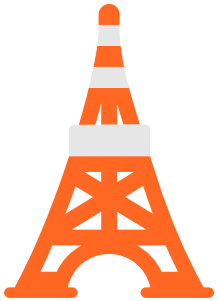
Endgeräte Firewall einsetzen

Endpoint Protection



- Antivirus verwenden
- Endgeräte Verschlüsseln
- Anomalien aktiv beobachten
- **Nutzer Berechtigungen einschränken**
- Endgeräte Firewall einsetzen

Endpoint Protection



- Antivirus verwenden
- Endgeräte Verschlüsseln
- Nutzer Berechtigungen einschränken
- Anomalien aktiv beobachten
- Endgeräte Firewall einsetzen

Backups verschlüsseln

Backups testen

Backup Methoden

regelmäßige Backups planen

Data klassifizierung

Starke Passwörter

Multi Faktor Authentifizierung

Passwörter nicht wiederverwenden

Passwort Manager

Passwörter regelmäßig ändern

Mitarbeiter schulen

Anti-Phishing Software einsetzen

Multi Faktor Authentifizierung

Sichere Kommunikationskanäle verwenden

Zugangskontrolle einsetzen

Data Backups

Password Security

Phishing Awareness

Endpoint Protection

Secure Browsing

Software Updates

Antivirus verwenden

Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

Links prüfen vor dem Öffnen

VPNs für Fernzugriff verwenden

Regelmäßig Updates durchführen

Kritische Updates priorisieren

Patch Management einsetzen

Updates vor Deployment testen

Automatische Update Tools verwenden

Cyber Security Academy

Software Updates

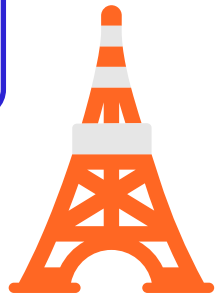
Regelmäßig Updates durchführen

kritische Updates priorisieren

Patch Management einsetzen

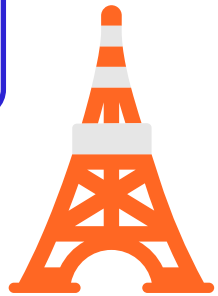
Updates vor Deployment testen

Automatische Update Tools verwenden



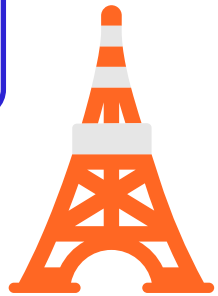
Software Updates

- Regelmäßig Updates durchführen
- kritische Updates priorisieren
- Patch Management einsetzen
- Updates vor Deployment testen
- Automatische Update Tools verwenden



Software Updates

- Regelmäßig Updates durchführen
- kritische Updates priorisieren
- Patch Management einsetzen
- Updates vor Deployment testen
- Automatische Update Tools verwenden



Software Updates

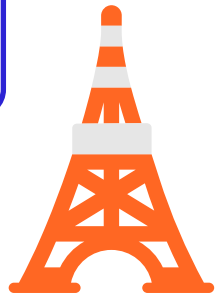
Regelmäßig Updates durchführen

kritische Updates priorisieren

Patch Management einsetzen

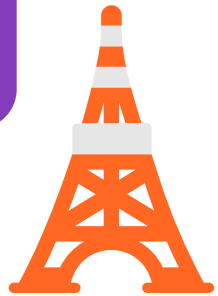
Updates vor Deployment testen

Automatische Update Tools verwenden



Software Updates

- Regelmäßig Updates durchführen
- kritische Updates priorisieren
- Patch Management einsetzen
- Updates vor Deployment testen
- **Automatische Update Tools verwenden**



Backups verschlüsseln

Backups testen

Backup Methoden

regelmäßige Backups planen

Data klassifizierung

Starke Passwörter

Multi Faktor Authentifizierung

Passwörter nicht wiederverwenden

Passwort Manager

Passwörter regelmäßig ändern

Mitarbeiter schulen

Anti-Phishing Software einsetzen

Multi Faktor Authentifizierung

Sichere Kommunikationskanäle verwenden

Zugangskontrolle einsetzen

Data Backups

Password Security

Phishing Awareness

Endpoint Protection

Secure Browsing

Software Updates

Antivirus verwenden

Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

Links prüfen vor dem Öffnen

VPNs für Fernzugriff verwenden

Regelmäßig Updates durchführen

Kritische Updates priorisieren

Patch Management einsetzen

Updates vor Deployment testen

Automatische Update Tools verwenden

Cyber Security Academy

Secure Browsing

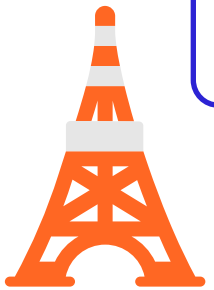
Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

Links prüfen vor dem Öffnen

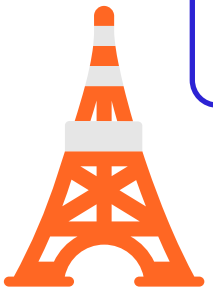
VPNs für Fernzugriff verwenden



Cyber Security Academy

Secure Browsing

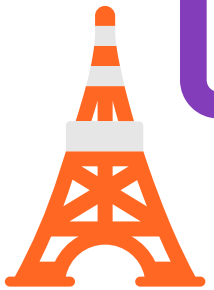
- Zertifikate einspielen
- Ad-blocker verwenden
- Browser Updates durchführen
- Links prüfen vor dem Öffnen
- VPNs für Fernzugriff verwenden



Cyber Security Academy

Secure Browsing

- Zertifikate einspielen
- Ad-blocker verwenden
- Browser Updates durchführen
- Links prüfen vor dem Öffnen
- VPNs für Fernzugriff verwenden



Secure Browsing

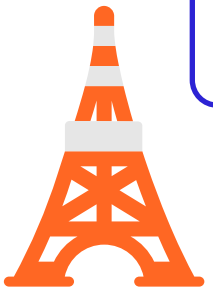
Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

Links prüfen vor dem Öffnen

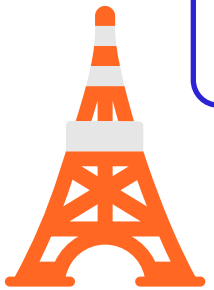
VPNs für Fernzugriff verwenden



Cyber Security Academy

Secure Browsing

- Zertifikate einspielen
- Ad-blocker verwenden
- Browser Updates durchführen
- Links prüfen vor dem Öffnen
- VPNs für Fernzugriff verwenden



Backups verschlüsseln

Backups testen

Backup Methoden

regelmäßige Backups planen

Data klassifizierung

Starke Passwörter

Multi Faktor Authentifizierung

Passwörter nicht wiederverwenden

Passwort Manager

Passwörter regelmäßig ändern

Mitarbeiter schulen

Anti-Phishing Software einsetzen

Multi Faktor Authentifizierung

Sichere Kommunikationskanäle verwenden

Zugangskontrolle einsetzen

Data Backups

Password Security

Phishing Awareness

Endpoint Protection

Secure Browsing

Software Updates

Antivirus verwenden

Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

Links prüfen vor dem Öffnen

VPNs für Fernzugriff verwenden

Regelmäßig Updates durchführen

Kritische Updates priorisieren

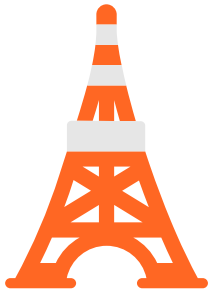
Patch Management einsetzen

Updates vor Deployment testen

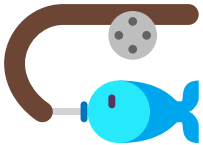
Automatische Update Tools verwenden

Cyber Security Academy

Phishing Awareness

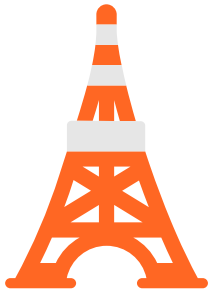


- **Mitarbeiter schulen**
- **Anti-Phishing Software einsetzen**
- **Multi Faktor Authentifizierung**
- **Sichere Kommunikationskanäle verwenden**
- **Zugangskontrolle einsetzen**

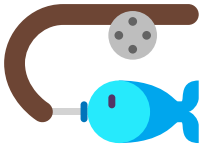


Cyber Security Academy

Phishing Awareness

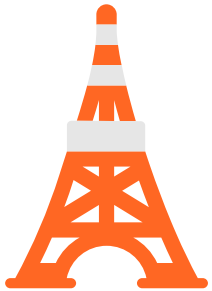


- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- Multi Faktor Authentifizierung
- Sichere Kommunikationskanäle verwenden
- Zugangskontrolle einsetzen

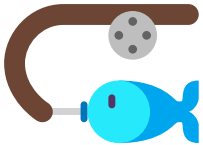


Cyber Security Academy

Phishing Awareness

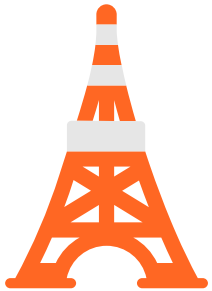


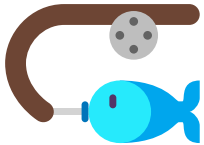
- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- Multi Faktor Authentifizierung
- Sichere Kommunikationskanäle verwenden
- Zugangskontrolle einsetzen



Cyber Security Academy

Phishing Awareness

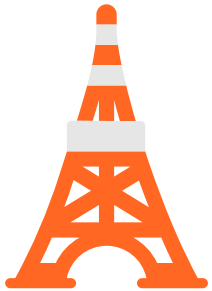


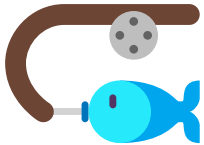


- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- **Multi Faktor Authentifizierung**
- Sichere Kommunikationskanäle verwenden
- Zugangskontrolle einsetzen

Cyber Security Academy

Phishing Awareness





- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- Multi Faktor Authentifizierung
- Sichere Kommunikationskanäle verwenden
- **Zugangskontrolle einsetzen**

Backups verschlüsseln

Backups testen

Backup Methoden

regelmäßige Backups planen

Data klassifizierung

Starke Passwörter

Multi Faktor Authentifizierung

Passwörter nicht wiederverwenden

Passwort Manager

Passwörter regelmäßig ändern

Mitarbeiter schulen

Anti-Phishing Software einsetzen

Multi Faktor Authentifizierung

Sichere Kommunikationskanäle verwenden

Zugangskontrolle einsetzen

Antivirus verwenden

Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

Links prüfen vor dem Öffnen

VPNs für Fernzugriff verwenden

Regelmäßig Updates durchführen

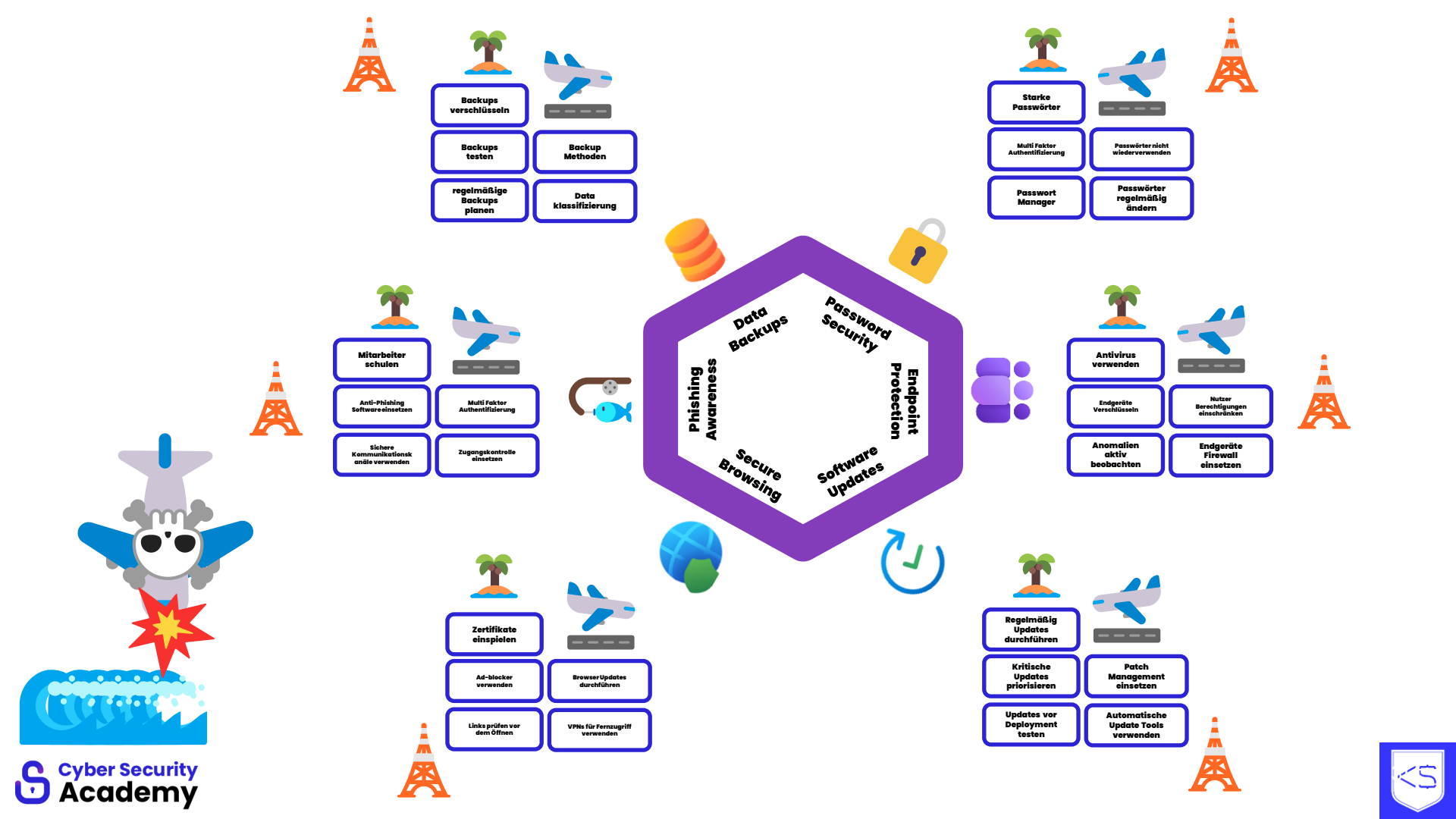
Kritische Updates priorisieren

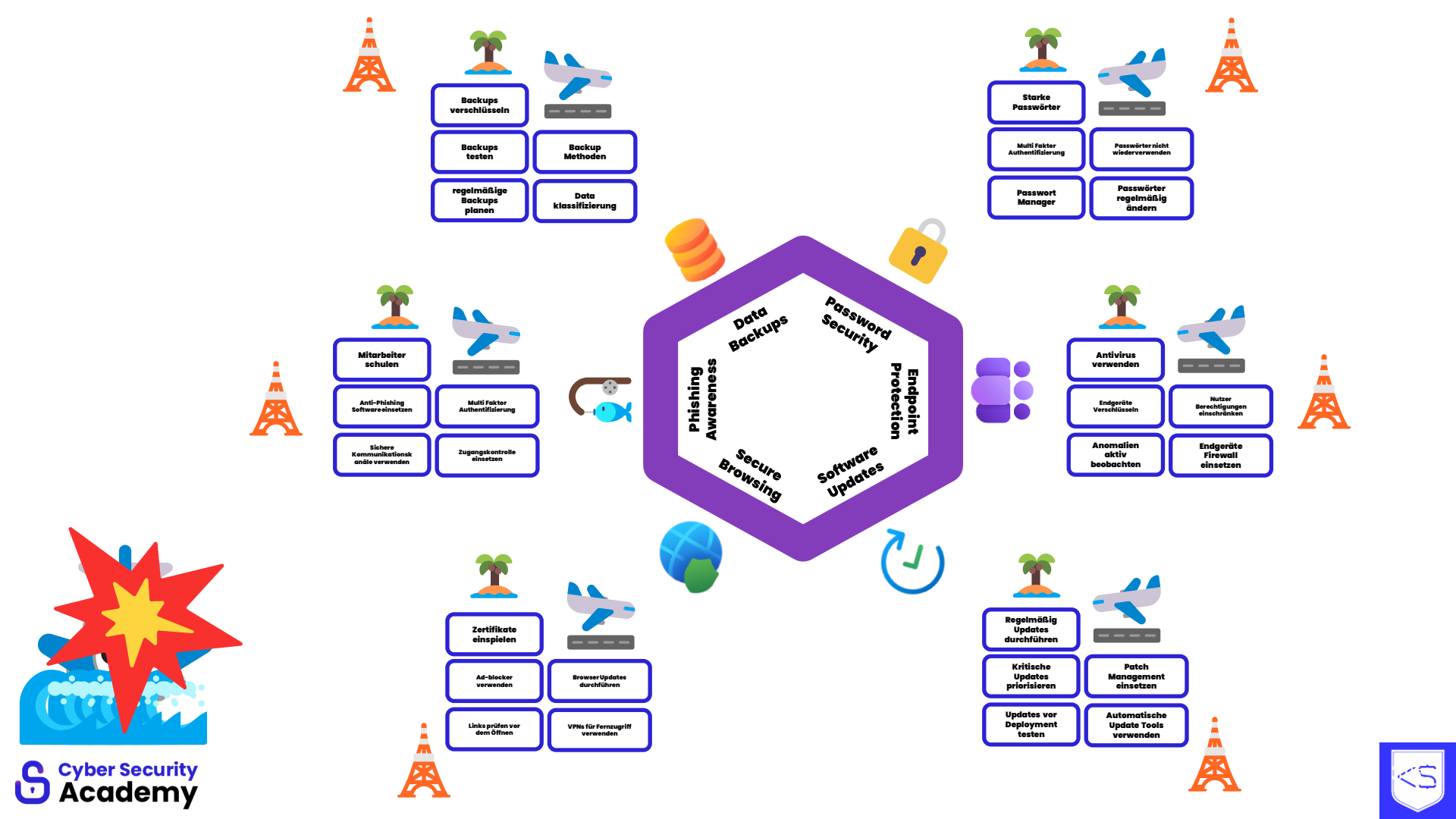
Patch Management einsetzen

Updates vor Deployment testen

Automatische Update Tools verwenden

Cyber Security Academy


Data Backups
Password Security
Endpoint Protection
Software Updates
Secure Browsing
Phishing Awareness
Backups verschlüsseln
Backups testen
Backup Methoden
regelmäßige Backups planen
Data klassifizierung
Starke Passwörter
Multi Faktor Authentifizierung
Passwörter nicht wiederverwenden
Passwort Manager
Passwörter regelmäßig ändern
Mitarbeiter schulen
Anti-Phishing Software einsetzen
Multi Faktor Authentifizierung
Sichere Kommunikationskanäle verwenden
Zugangskontrolle einsetzen
Antivirus verwenden
Endgeräte Verschlüsseln
Nutzer Berechtigungen einschränken
Anomalien aktiv beobachten
Endgeräte Firewall einsetzen
Zertifikate einspielen
Ad-blocker verwenden
Browser Updates durchführen
Links prüfen vor dem Öffnen
VPNs für Fernzugriff verwenden
Regelmäßig Updates durchführen
Kritische Updates priorisieren
Patch Management einsetzen
Updates vor Deployment testen
Automatische Update Tools verwenden
Cyber Security Academy


Backups verschlüsseln
Backups testen
Backup Methoden
regelmäßige Backups planen
Data klassifizierung
Starke Passwörter
Multi Faktor Authentifizierung
Passwörter nicht wiederverwenden
Passwort Manager
Passwörter regelmäßig ändern
Mitarbeiter schulen
Anti-Phishing Software einsetzen
Multi Faktor Authentifizierung
Sichere Kommunikationskanäle verwenden
Zugangskontrolle einsetzen
Data Backups
Password Security
Endpoint Protection
Software Updates
Secure Browsing
Phishing Awareness
Antivirus verwenden
Endgeräte Verschlüsseln
Nutzer Berechtigungen einschränken
Anomalien aktiv beobachten
Endgeräte Firewall einsetzen
Zertifikate einspielen
Ad-blocker verwenden
Browser Updates durchführen
Links prüfen vor dem Öffnen
VPNs für Fernzugriff verwenden
Regelmäßig Updates durchführen
Kritische Updates priorisieren
Patch Management einsetzen
Updates vor Deployment testen
Automatische Update Tools verwenden
Cyber Security Academy

Inhalte 📦

Cyberangriffe, Trends und Learnings

NIS 2 Richtlinie un die Lieferkette

Cyber Security 101 „Baseline“

Netzwerk, Infrastruktur, Cloud und Datensicherheit

Habt ihr noch Fragen? 🚀