Herzlich Willkommen:

NIS 2 Essentials: Grundlagen und Praxis der Cybersicherheit

DIH.02-24.AF.081-01
06.&07.11.2024

Ing. Christian Gubesch BSc

Der DIH SÜD wird unterstützt von

NIS 2 Essentials: Grundlagen und Praxis der Cybersicherheit

Schützen Sie Ihr Unternehmen vor den wachsenden Bedrohungen im Cyberspace!

Cyber Security Academy TU Graz

Fakten

- **Workshop Zeiten:**
  - Mittwoch 06.11.2024
    09:00 - 16:30
  - Donnerstag 07.11.2024
    09:00 - 16:30

- **Location:** Online TU-Graz Webex

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

Wer seid Ihr?

- **Hintergrund**
  - **Job / Aufgabenbereiche**
  - **Erfahrungen im Bereich der IT-Security?**
    (Privat als auch Unternehmen)
  - **Erfahrungen im IT-Operations Bereich oder anderen IT bezogenen Tätigkeiten?**
- **Vorstellungen & Erwartungen**
- **Nach diesem Workshop will ich in der Lage sein, …**

Workshop Überblick – Facts

Mir ist es wichtig das wir über aktuelle Themen sprechen und einen guten Überblick über die wichtigsten Sachen bekommen!

Ich habe auch daher vier Focus Areas mitgebracht:

FA01: Cybersicherheits-bedrohungen und ein ganzheitlicher Ansatz

FA02: EU x Cybersicherheit und das NIS 2 Gesetz

FA03: Praktische Sicherheits-maßnahmen anhand von NIS 2

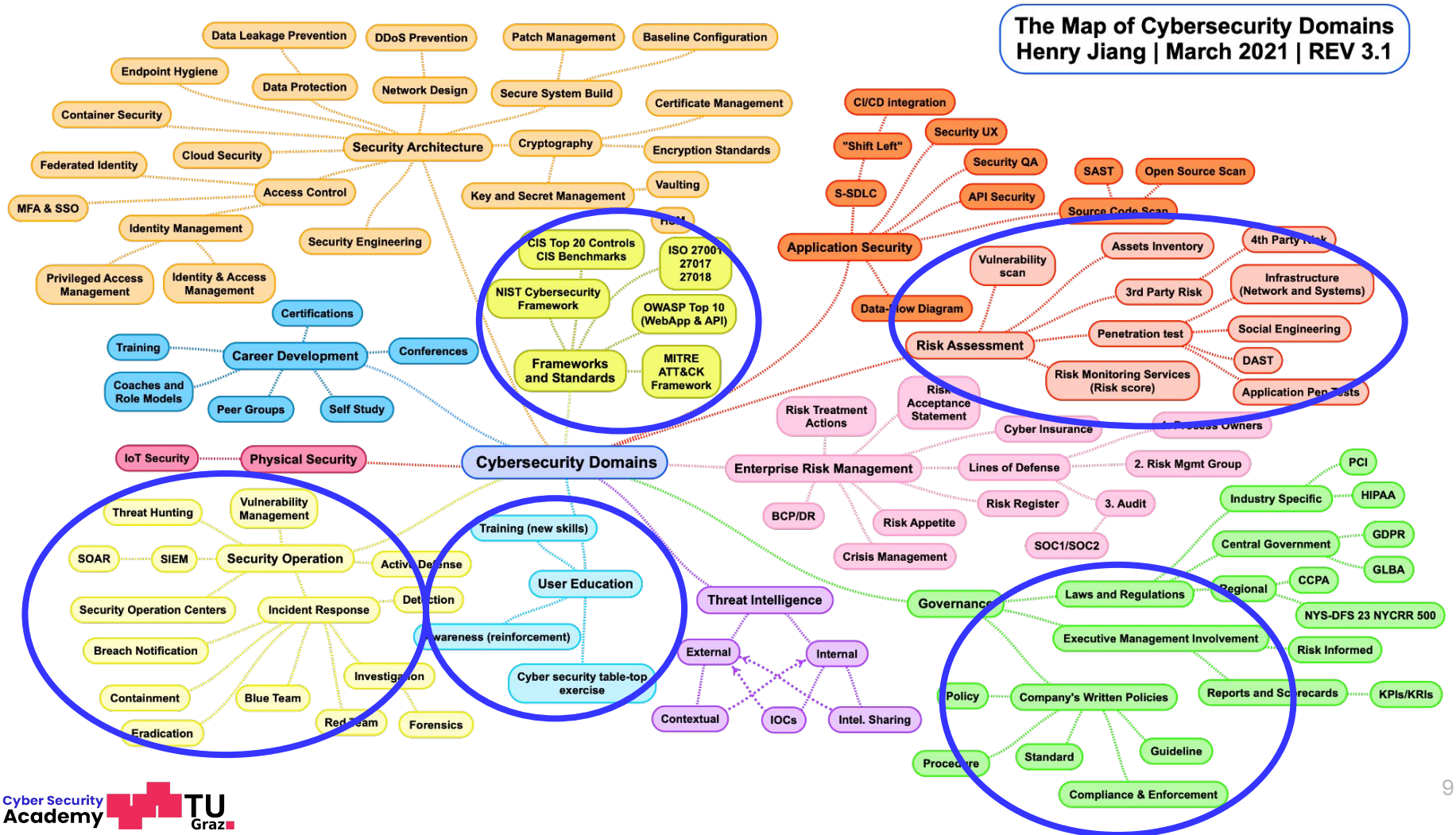
FA04: Compliance und kontinuierliche Verbesserung

Solltet ihr zu irgendeinem Thema Fragen haben: Bitte jederzeit Fragen!

Was bedeutet Cybersicherheit für euch?

...oder ist es nur mühsamer Overhead?

Kurzer Überblick und auf was wir uns konzentrieren werden 🔎🔐


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Container Security
Certificate Management
Cloud Security
Cryptography
Federated Identity
Encryption Standards
Access Control
Key and Secret Management
Vaulting
MFA & SSO
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Application Security
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Data Flow Diagram
Penetration test
Social Engineering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
Lines of Defense
2. Risk Mgmt Group
3. Audit
Risk Register
BCP/DR
Risk Appetite
Crisis Management
SOC1/SOC2
Governance
Laws and Regulations
PCI
Industry Specific
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Policy
Company's Written Policies
Reports and Scorecards
KPIs/KRIs
Procedure
Standard
Guideline
Compliance & Enforcement
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Detection
Security Operation Centers
Incident Response
Breach Notification
Containment
Blue Team
Investigation
Eradication
Red Team
Forensics
User Education
Training (new skills)
Awareness (reinforcement)
Cyber security table-top exercise
IoT Security
Physical Security

Cybersicherheits-bedrohungen und ein ganzheitlicher Ansatz

Was sind aktuelle Bedrohungen und was wäre ein guter Ansatz für Unternehmen?

Lernziele 🎯

- Was sind die wichtigsten Arten von Cyberangriffen?
- Wie schauen die Cyber Security Trends in Europa aus?
- Was ist ein ganzheitlicher Cyber Security Ansatz?

Lernpfad

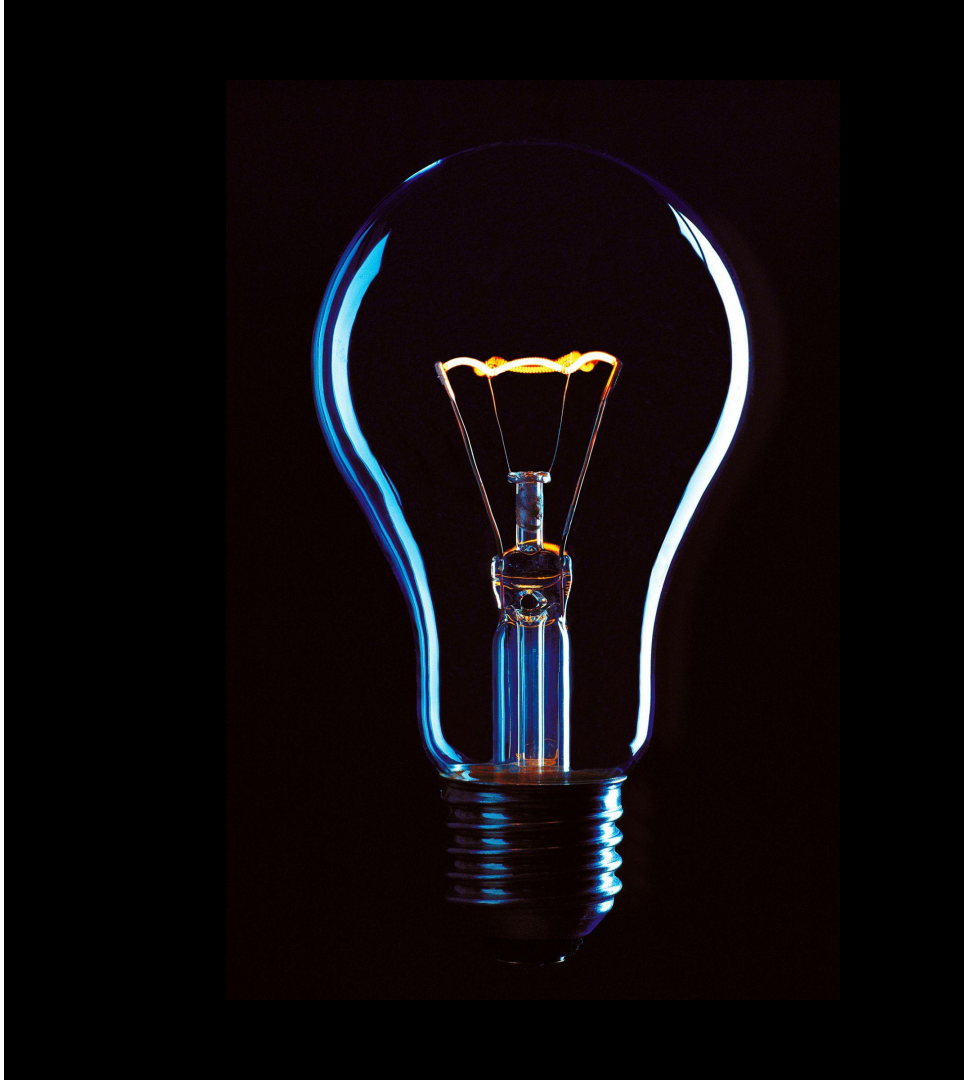
FA01: Cybersicherheits-bedrohungen und ganzheitlicher Ansatz

FA02: EU x Cybersicherheit und das NIS 2 Gesetz

FA03: Praktische Sicherheits-maßnahmen anhand von NIS 2

FA04: Compliance und kontinuierliche Verbesserung

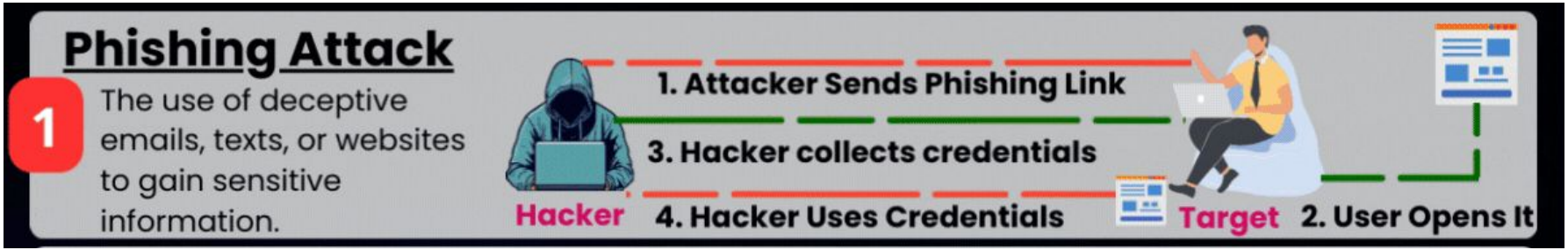
Welche Cyber Angriffsarten kennst du?



Gängigste Cyberangriffe im Jahr 2024

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.



Quelle: https://cybersecuritynews.com/

CEO Fraud

Methode?

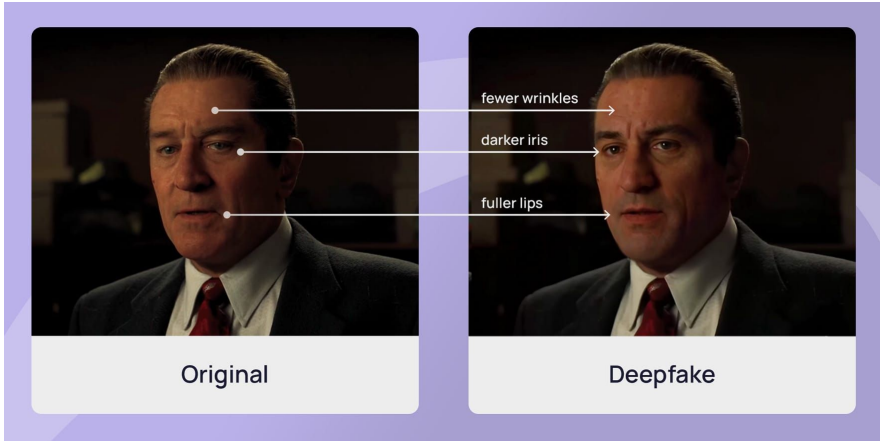
Taktik?

Schutz?

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

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

AI & Deepfakes



Methode?

Taktik?

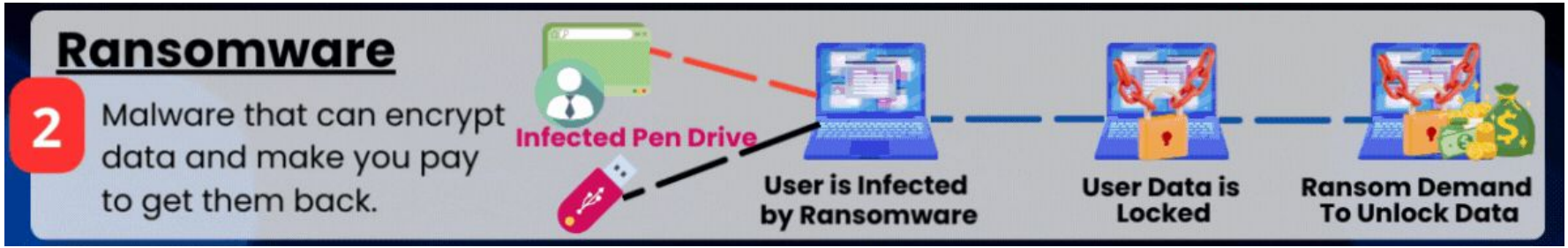
Schutz?

Ziel: Fälschung von Videos/Audio zur Täuschung.

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

Ransomware

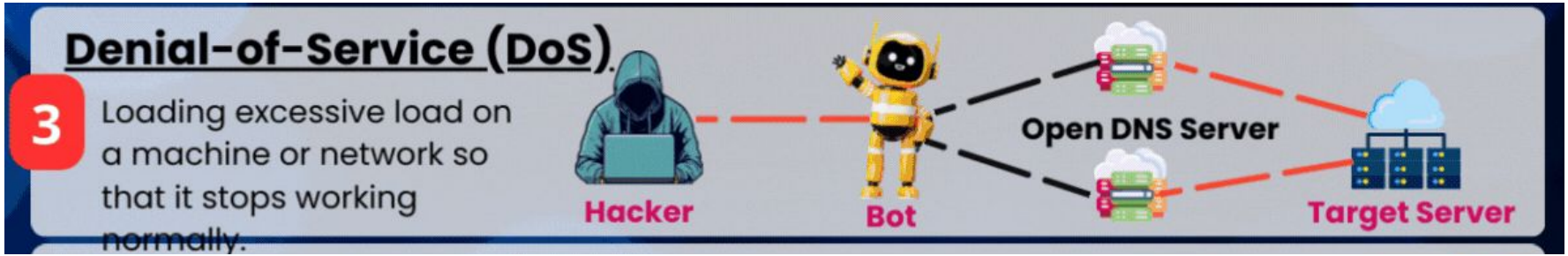
- **Ziel:** Erpressung von Geld durch Sperrung von Dateien/Systemen.
- **Schaden:** Datenverlust, Betriebsunterbrechungen.
- **Prävention:** Regelmäßige Backups, Aktualisierung von Software, Sicherheitsbewusstsein.
- **Reaktion:** Isolierung des betroffenen Systems, Kontakt mit Sicherheitsexperten.



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.
- **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.
- **Verteidigung:** Verschlüsselte Verbindungen verwenden, Sicherheitsbewusstsein schärfen.

Quelle: https://cybersecuritynews.com/

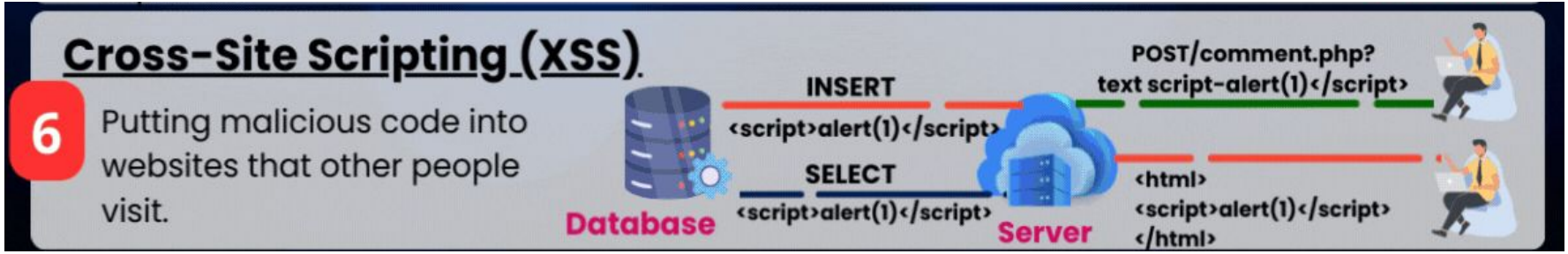
SQL Injection

- **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/

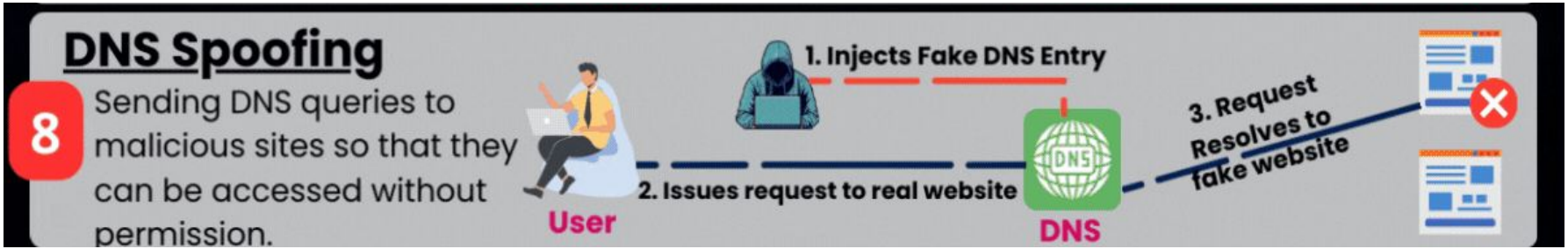
Zero-Day Exploits

- **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! 

Cyber Security Threats von ENISA for 2030

Cyber Security Threats for 2030

Ein Blick in die Zukunft

Stand 27. März 2024

Cyber Security Academy TU Graz

Überblick (1)

1. Kompromittierung der Lieferkette
2. Fachkräftemangel
3. Human Error und Legacy Systeme
4. Ungepatchte Systeme
5. Anstieg der digitalen Überwachung und Verlust der Privatsphäre

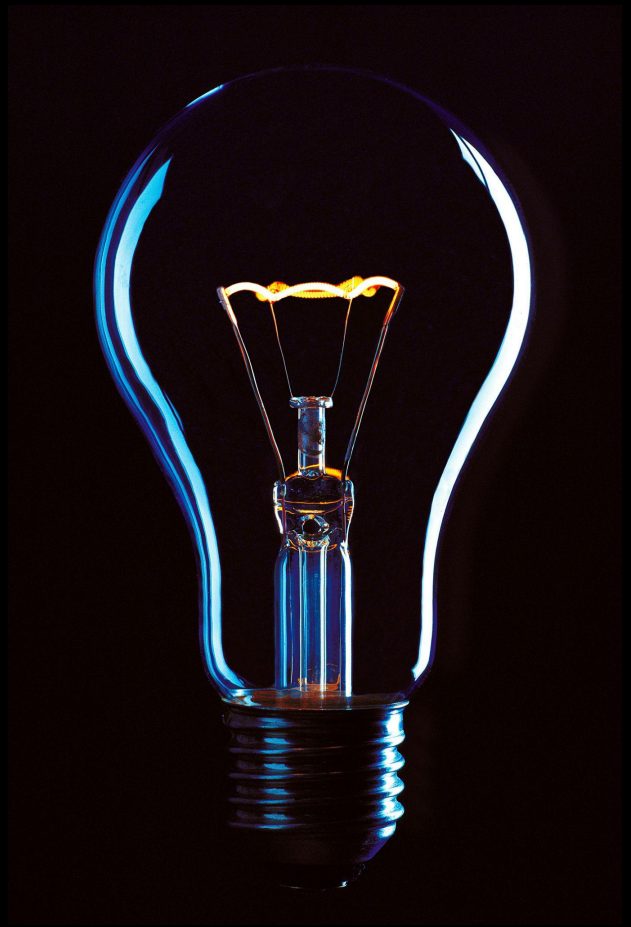
Quelle: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary
Quelle: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Überblick (2)

6. Grenzübergreifende Abhängigkeiten an IKT Services
7. Einfaches und vermehrtes Verbreiten von Fake-News
8. Aufkommen von hybriden Angriffsvektoren (offline & online)
9. Ausnutzen von KI um Cyberangriffe auszuführen
10. Außeneinfluss auf IT Systeme durch verschiedene Disruptionen

Quelle: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary
Quelle: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

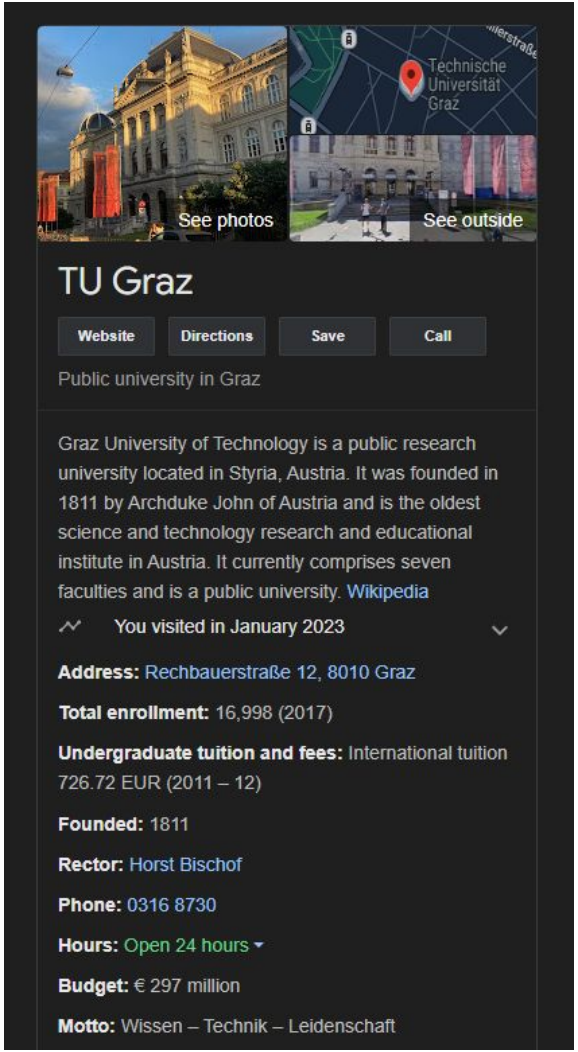
Was ist das Erste, dass ein Angreifer an einem Unternehmen erkennt?



BEISPIEL: Google Suche

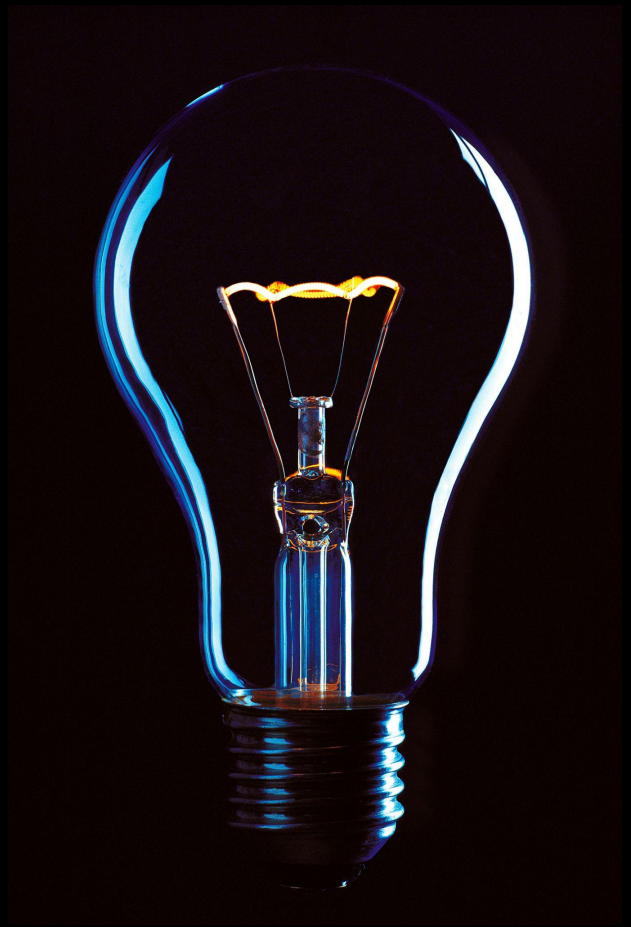
Online erste Information

- Webseite (Domain)
- Kontakt
  - E-Mail und Namen
  - Telefonnummer
- Adresse
- Öffnungszeiten
- Bewertungen



Quelle: https://www.google.com

Was ist das Erste, dass ein Angreifer an einer Einzelperson erkennt?



Wir sollten aufpassen was öffentlich über uns abrufbar ist!

Eine Top Priorität: Das Schützen des Firmennamen und der Domains!

Beispiel: Was kann ich mit einer Domain oder Website herausfinden?

DNS Looking Glass: https://www.who.is/

Information Security Search Engine: https://www.shodan.io/

Websiten Informations Crawler: https://www.wappalyzer.com/

Informationen über euch und eure Firmen

Was können Hacker einfach über euch herausfinden? Wie würdet ihr euch angreifen?

Workout 🔎

- **Ziel:** Findet etwas über euch und eure Unternehmen heraus.
- **Output:** Informationen + potentielle Angriffsvektoren
- **Modus:** Ausarbeitung alleine für 10 min, anschließend Diskussion

Glossar (1)

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

Glossar (2)

- **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. (Examples: https://www.mimecast.com/de/blog/5-common-examples-of-social-engineering/)

- **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.

- **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.

Glossar (3)

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

Glossar (4)

- **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.

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

- **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.

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

Glossar (5)

- **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. Sie können Personen irreführend etwas sagen oder tun lassen, was sie tatsächlich nicht getan haben, und stellen eine Bedrohung für die Integrität von visuellen und auditiven Inhalten dar.

- **Advanced Persistent Threats:** Advanced Persistent Threats (APTs) sind hochentwickelte und langfristig angelegte Cyberangriffe, die von gezielten Gegnern wie Nationen oder organisierten Kriminellen durchgeführt werden, um sensible Daten zu stehlen oder Infrastrukturen zu beeinträchtigen. Sie zeichnen sich durch ihre Heimlichkeit, Raffinesse und Persistenz aus.

- **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, einschließlich regelmäßiger Software-Updates, sicherer Passwörter und sicherer Online-Verhaltensweisen.

Glossar (6)

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.

Sidefacts - Cyberangriffe

- **Öffentliche Informationen:** Cyberangriffe und deren Folgen werden bei vielen Unternehmen nicht veröffentlicht!
- **Ursache:** Meistens zurückzuführen auf ein “falsches” Userverhalten oder fehlendes Know-how im Betrieb von IT-Infrastruktur.
- **Recovery Prozess:** Leider selten durchdacht, bzw. oft überhaupt nicht am Radar (**Keine Backups** und auch **keine Verantwortlichkeiten**).

Cyberangriff auf das Land Kärnten

- **Öffentliche Informationen:** 24.05.2022 Cyberangriff der Hacker-Gruppe “Black Cat - RUS” (Phishing → Ransomware).
- **Ursache:** Phishing E-Mail die von Mitarbeiter:in angeklickt wurde und den Weg ins Unternehmensnetz bereitete. Zuerst unbemerkt!
- **Recovery Prozess:** Da es eine Staatliche Institution ist sind Backups und Recovery Prozeduren sehr ausgereift und eine wiederherstellung ist “relativ” einfach.

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

Maßnahmen und Analyse Land Kärnten

- **Maßnahmen:** Abschottung der Systeme vom Internet um dann den Sachverhalt von Forensic Expert:innen abzuklären.
- **Meldung:** Da kritischer Sektor → Öffentliche Meldung + Meldung von Phishing E-Mail bei Behörden und E-Mail Providern.
- **Fokusgruppe:** Aufbereitung des Vorfalls mit verschiedenen Firmen aus dem Sektor.
- **Zukünftige Maßnahmen:** Schulung von Mitarbeiter:innen die wirklich etwas bringen sollten + Simulationen verschiedener Angriffe. Überarbeitung der Recovery Prozesse.

Cyberangriff auf die Uni-Graz

- **Öffentliche Informationen:** Cyberangriff am 03.02.2023 (Freitag) Täter:in unbekannt. Verschiedene Systeme Betroffen. (Credential loss)

- **Ursache:** User Credentials (von Studenten) kompromittiert und zugriff auf VPN (internes Netzwerk). Nicht zureichende Segmentierung im VPN und ungesicherte Systeme (Exploitable) ausgenutzt.

- **Recovery Prozess:** IDS System hat den Angriff erkannt und der betroffene Account und Systeme wurden Isoliert. Keine Daten wurden verschlüsselt. Angerichteter “schaden” war auf Systeme begrenzt.

Quelle: https://www.uni-graz.at/de/neuigkeiten/cyberangriff-2/

Maßnahmen und Analyse Uni Graz

- **Maßnahmen:** Abschottung der Systeme.
  Sehr strenge Passwortrichtlinien und ein Änderungsintervall von weniger als 6 Monate. MFA mittels TOTP (Time-based One-Time-Password). Strengere Segmentierung der Zugriffe zwischen Systemen und im VPN allgemein.

- **Meldung:** Da Bildungseinrichtung → Öffentliche Meldung. Ordentliche Dokumentation zum Setup des MFA Setups für verschiedene Geräte.

- **Zukünftige Maßnahmen:** Events für Studenten zum Thema Awareness. Onboarding aller Studenten über 35.000 innerhalb von wenigen Tagen/Wochen auf die MFA für alle Systeme der Uni.

- **Lessons Learned:** Wurden weitergegeben an andere Fachhochschulen und Universitäten. MFA ist seitdem bei den meisten Institutionen ein Muss Kriterium.

Weitere Angriffe in Österreich

Wie bereits erwähnt werden die meisten Angriffe verheimlicht und öffentliche Informationen sind nur schwer zu finden (Ausnahme Großunternehmen und kritischer Sektor).

Wird sich in Zukunft ändern → NIS 2 ist am Vormarsch!

Medienbeiträge zu dem Thema:
https://www.meinbezirk.at/tag/cyberangriff

Öffentliche Datenbank von Cyberangriffen:
https://konbriefing.com/de-topics/cyberangriffe.html

Wie können wir uns jetzt Schützen?

...oder wo sollen wir Anfangen?

Ganzheitliches Bild von Cybersicherheit

Beispiel: Vereinfachte Darstellung

Die Idee dahinter?

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

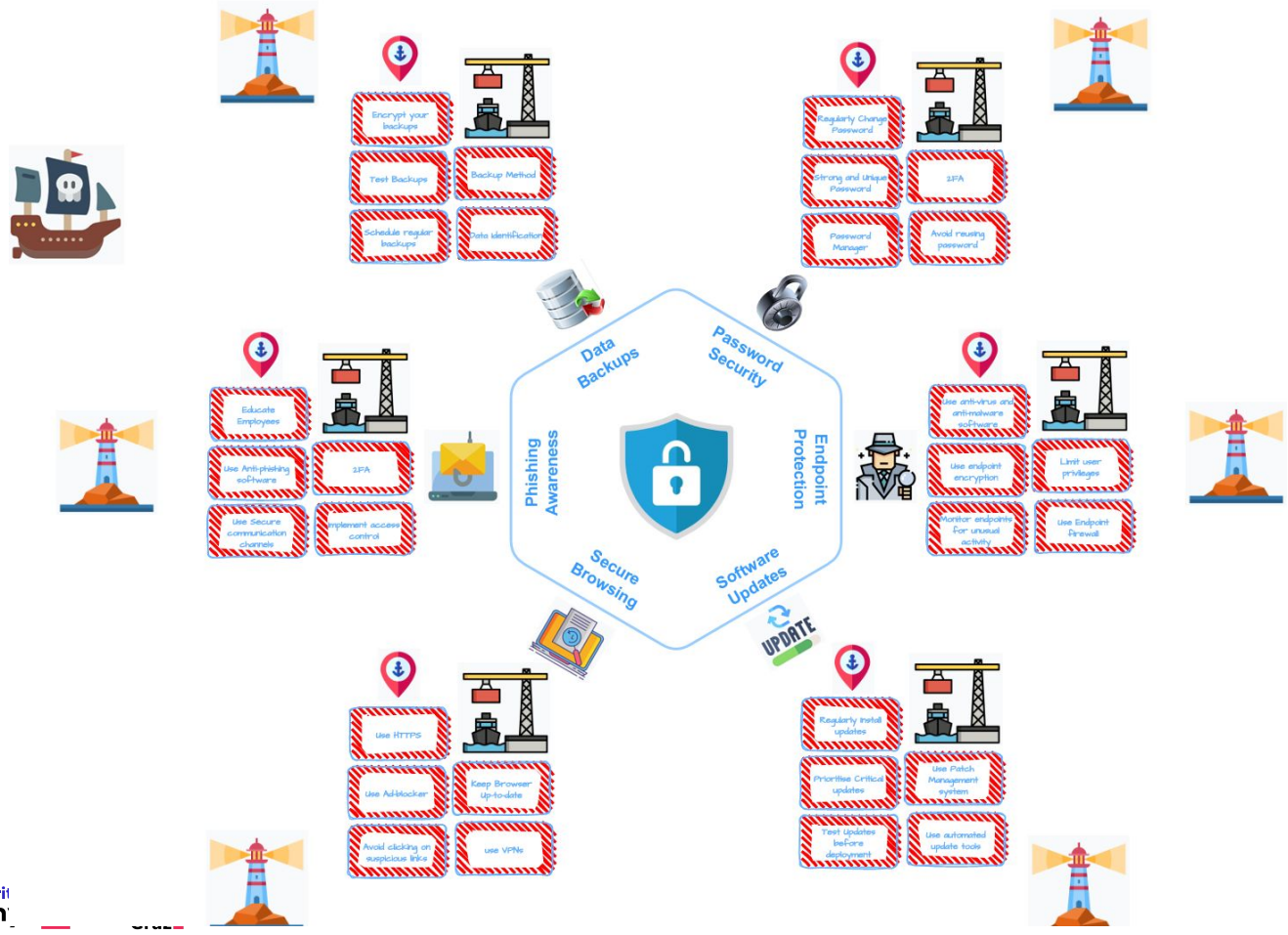
Stellt euch das ganze einfach so vor: Security ist wie die Schale einer Banane 🍌 - Wenn die Schale wegfällt hält die Frucht nicht lange

Ein Sicherheitsbewusstsein sollte bei jeder Person eigentlich ein Teil des “Hausverstandes” sein

Ganzheitliches Bild von Cybersicherheit

Beispiel: Vereinfachte Darstellung

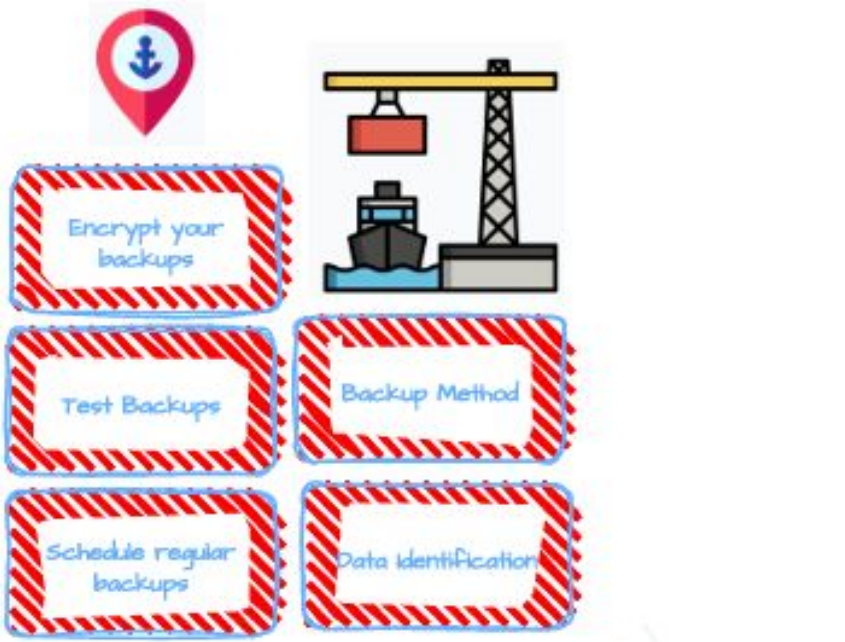
Cyber Security 101



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

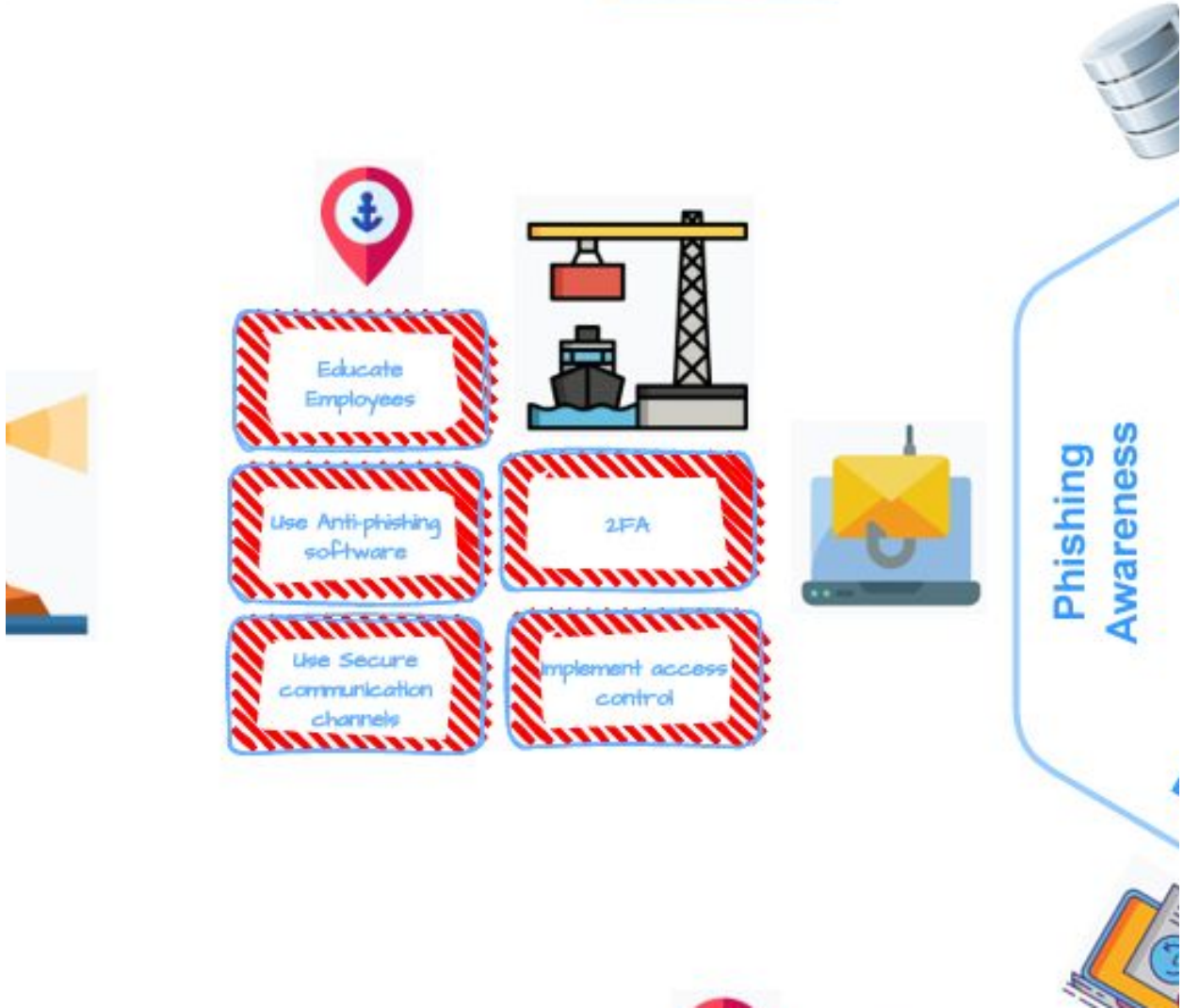
Zoom In:

Daten und Backups



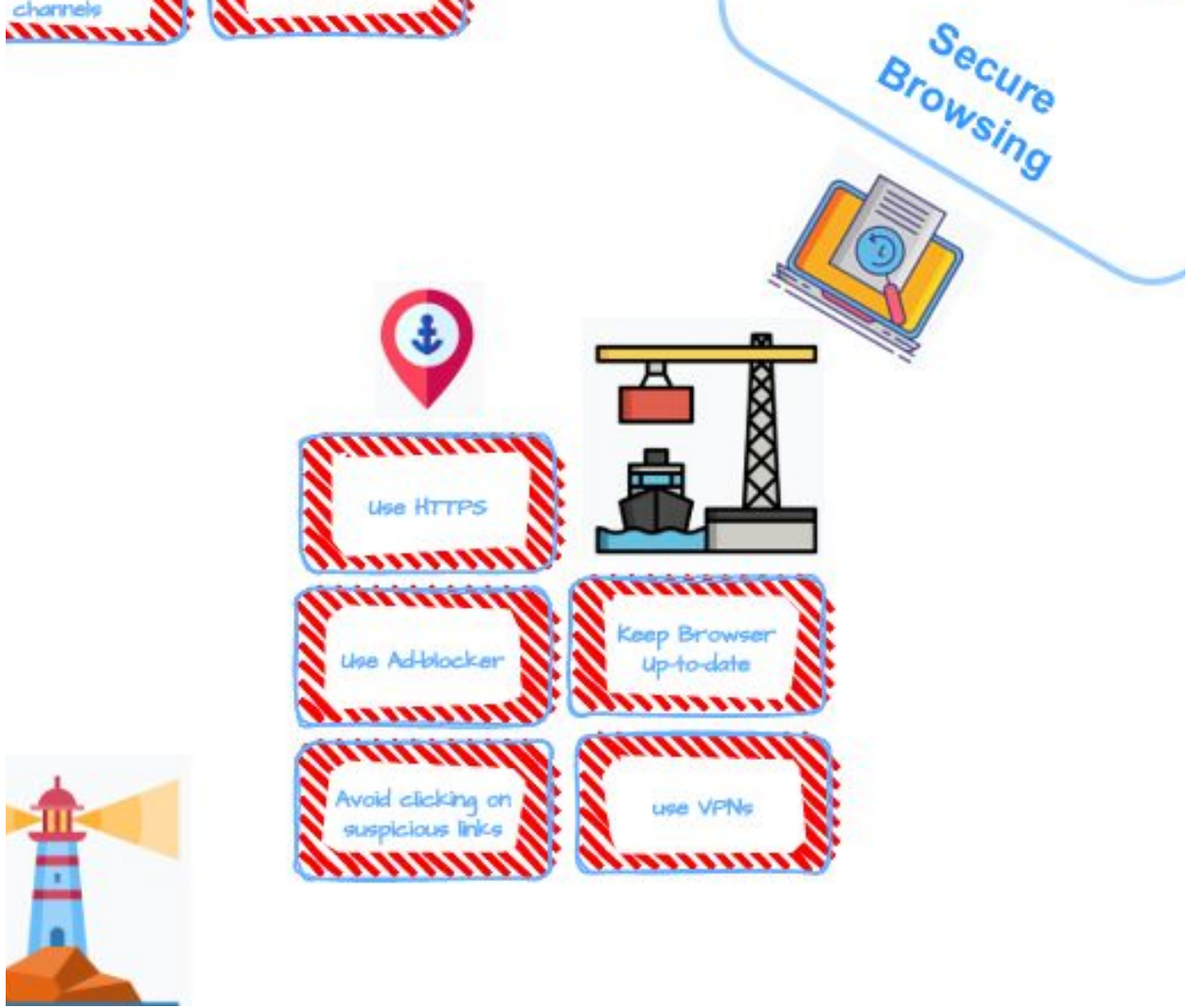
Zoom In:

Phishing Awareness



Zoom In:

Sicheres Browsen im Internet



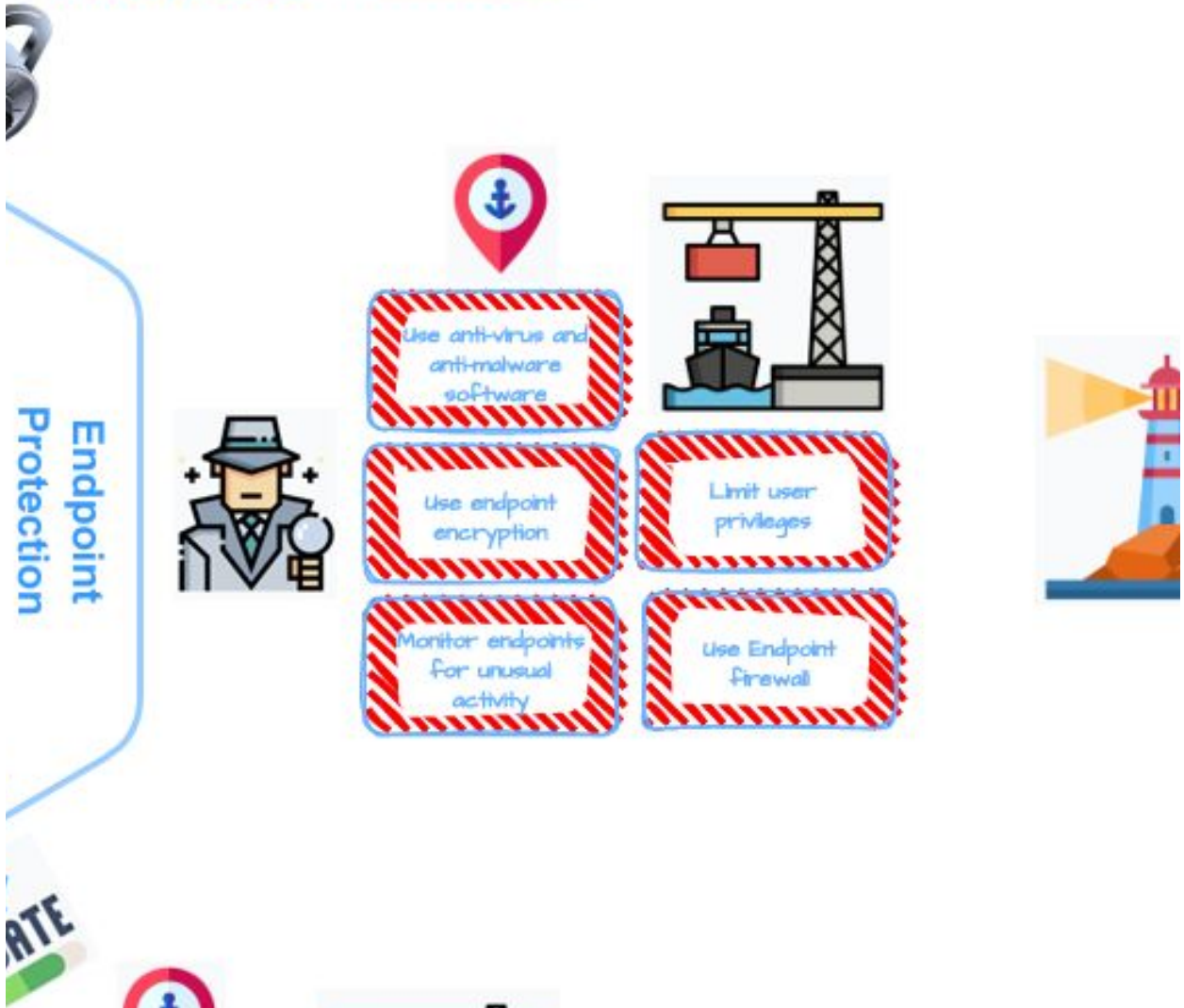
Zoom In:

Software und OS updates

OS – Operating System (Betriebssystem)

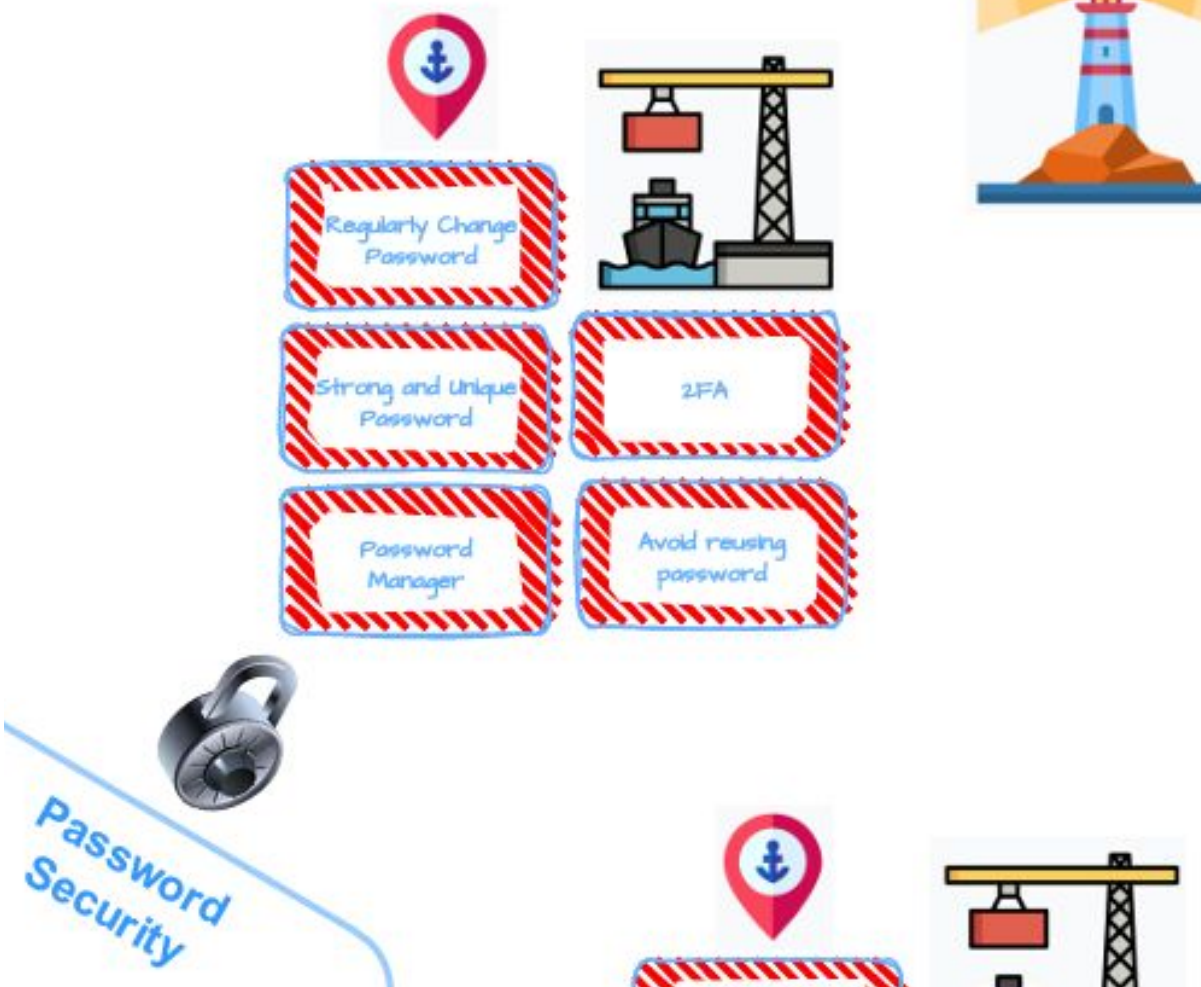
Zoom In:

Endgeräte Absichern



Zoom In:

Passwort Sicherheit



Zeit für ein Quiz! 

Lernziele 🎯

- Was sind die wichtigsten Arten von Cyberangriffen?
- Wie schauen die Cyber Security Trends in Europa aus?
- Wie ist ein ganzheitlicher Cyber Security Ansatz?

EU x Cybersicherheit und das NIS 2 Gesetz

Was sind aktuelle EU bewegungen und wie ist das NIS 2 Gesetz aufgebaut?

Lernziele 🎯

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

Lernpfad

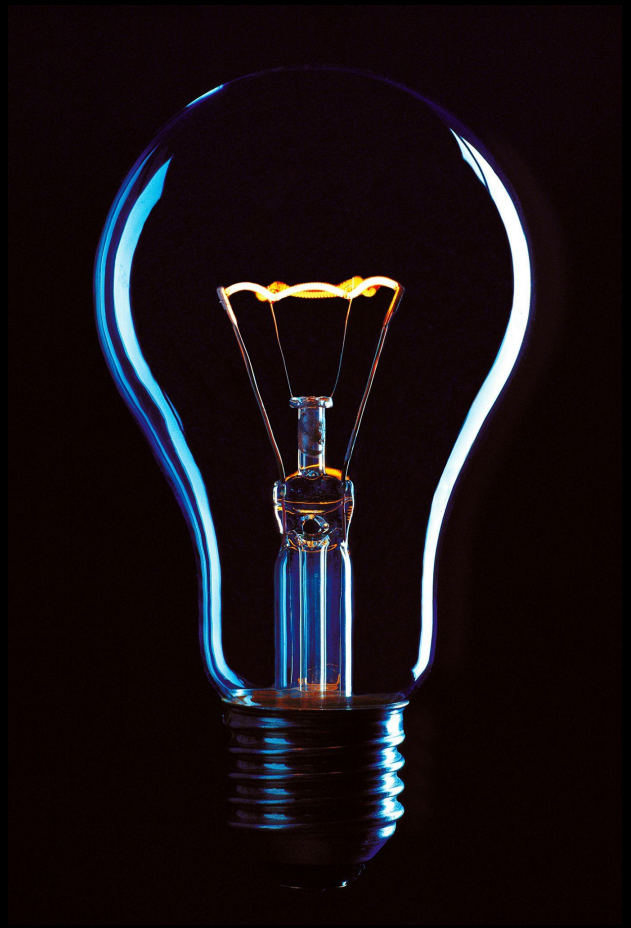
FA01: Cybersicherheits-bedrohungen und ganzheitlicher Ansatz

FA02: EU x Cybersicherheit und das NIS 2 Gesetz

FA03: Praktische Sicherheits-maßnahmen anhand von NIS 2

FA04: Compliance und kontinuierliche Verbesserung

Welche Cybersecurity Maßnahmen der EU kennst du?

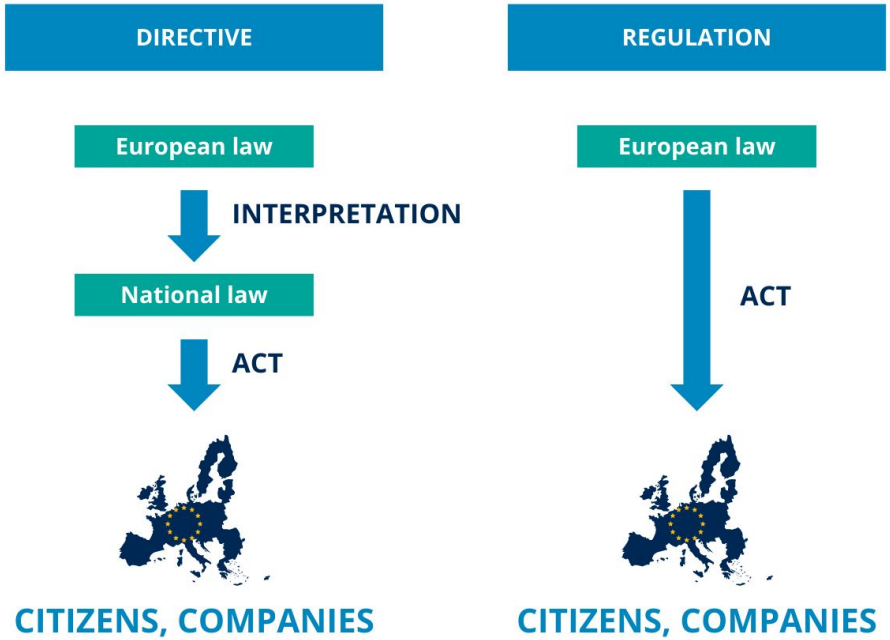


Europäischen Rechtsgrundlagen

- Datenschutzgrundverordnung
- Cyber Resilience Act
- Digital Operational Resilience Act
- Cybersecurity Act
- Cyber Solidarity Act
- AI Act
- NIS Regulierungen

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

Was ist der Unterschied zwischen einer Verordnung und einer Regulierung



Quelle: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_de
Grafik:
https://qbdgroup.com/en/blog/revision-of-the-eu-general-pharmaceutical-legislation/

Datenschutzgrundverordnung

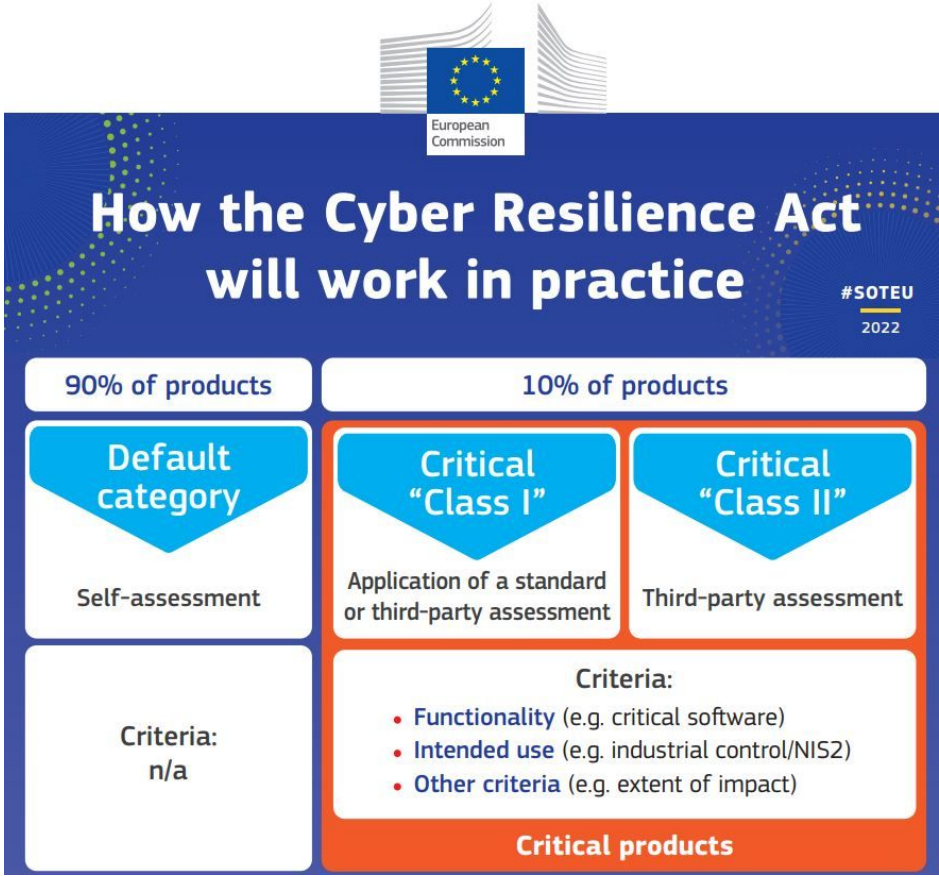
- In Kraft seit: 25.05.2018
- Stärkere Verantwortung für Verantwortliche und Auftragsverarbeiter bei Datenverarbeitung
- Pflicht zur Führung eines "Verzeichnisses von Verarbeitungstätigkeiten" für Unternehmen
- Meldepflicht bei Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und betroffene Personen
- Neue Informationspflichten, Betroffenenrechte und Regelungen zur Datenverarbeitung

Quelle: https://www.wko.at/datenschutz/uebersicht

Cyber Resilience Act (CRA)

- Noch nicht in Kraft → **Kommt bald!**
- Verpflichtende Cybersicherheitsanforderungen für digitale Produkte und Software
- Harmonisierte Regeln für den gesamten Produktlebenszyklus
- CE-Kennzeichnung zur Angabe der Einhaltung neuer Cybersicherheitsstandards

CE - Conformité Européenne
(Europäische Konformität)



Quelle: https://www.european-cyber-resilience-act.com/

Das ist alles sehr viel und den Überblick zu behalten ist schwer. Es ist auch immer "schwammig" definiert wer genau betroffen ist.

Wo können wir hier aktuelle Informationen abgreifen?

Ich finde die Informationen der Firma Cyber Risk GmbH immer sehr nützlich: https://www.cyber-risk-gmbh.com/Cyber_Risk_Links.html

Und natürlich die Informationen von ENISA:
https://www.enisa.europa.eu/

Jetzt aber zur NIS (Network and Information Systems)

Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

Wurde in Österreich nicht geschafft → Es wird eine ⅔ Mehrheit benötigt

Timeline

NIS 1 Regulierung: 06.07.2016

NIS 1 Umsetzung: 09.05.2018

NIS 2 Regulierung: 14.12.2022

NIS 2 Gesetz muss stehen: 17.10.2024

AUT - Ungewiss wird vermutlich 2025 kommen

Grobe Unterschiede zwischen NIS 1 und NIS 2

Die Hauptunterschiede befassen sich vor allem mit den betroffenen Unternehmen, der Lieferkette, dem Meldeverhalten, wie Sanktioniert wird und was genau Umgesetzt werden sollte.

NIS 1 - Key Facts

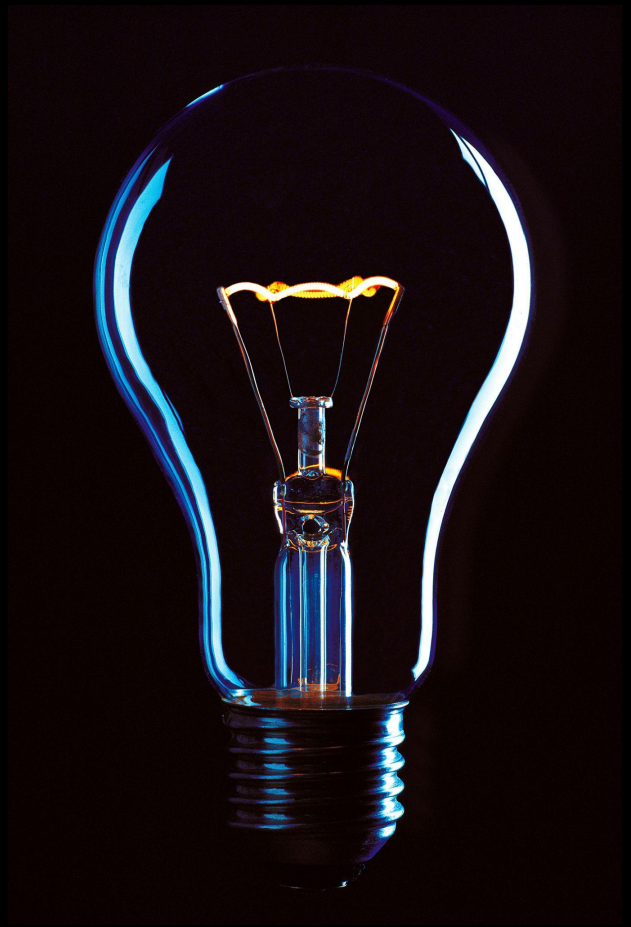
- **Betroffene Unternehmen:** 99 - “KRITIS”
- **Lieferkette:** Nicht mitbedacht
- **Regelung für KMU:** Außen vor Gelassen
- **Nationale Ausrichtung:** Grundstein für Cybersicherheit in Österreich

NIS 2 - Key Facts

- **Betroffene Unternehmen:** 3400-5000 fix (bis zu 15000)
- **Lieferkette:** Ist betroffen
- **Regelung für KMU:** Empfehlungen und “Zertifizierbar”
- **Nationale Ausrichtung:** Ganzheitliche Cybersicherheitsstrategie

Hast du eine Vorstellung wie so eine EU-weite NIS Richtlinie aufgebaut ist?

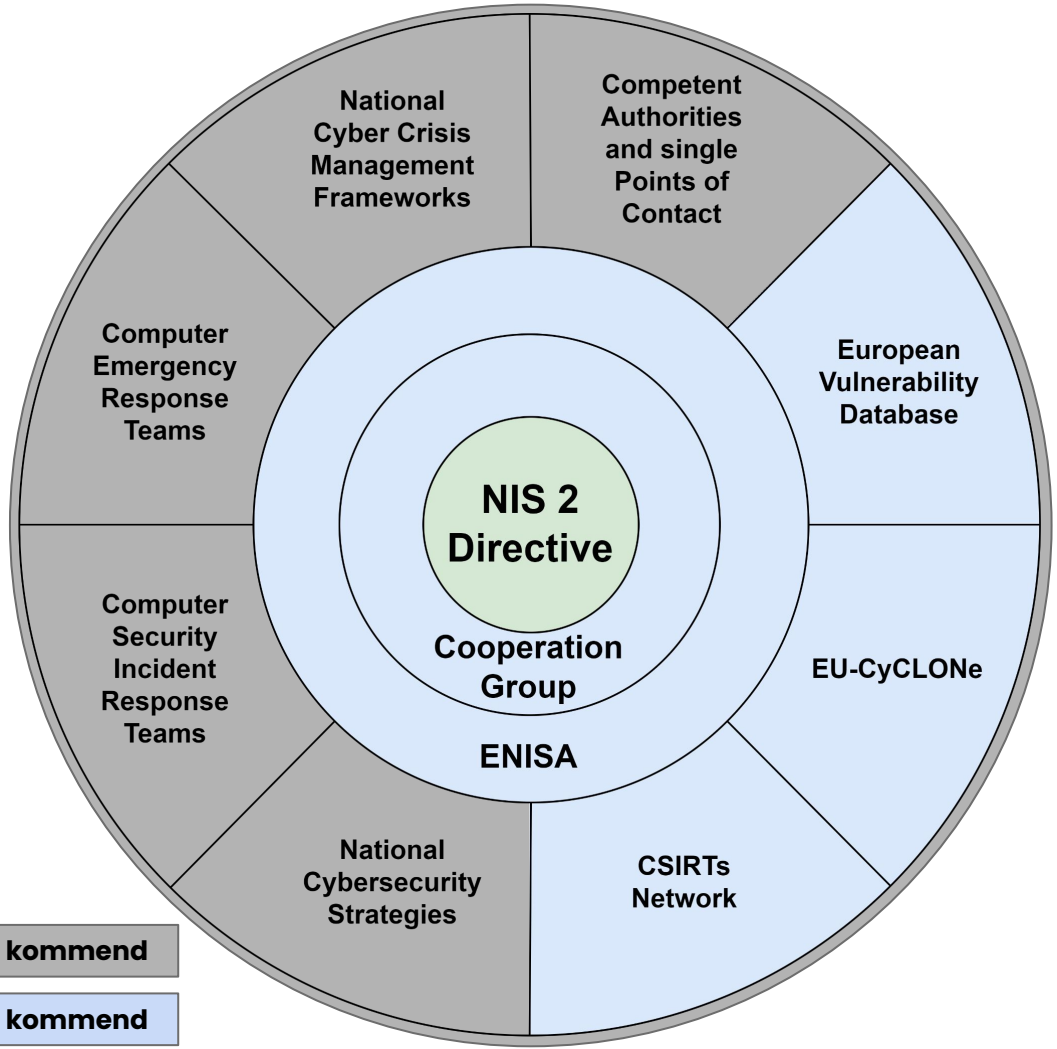
Wer sind die Akteure?



NIS 2 – Die Akteure

Was wollen wir uns Mitnehmen?

- **Aufbau der Regulierung**
- **EU stellt bereit:**
  - Cooperation Group
  - ENISA
  - EVD
- **Österreich muss bereitstellen:**
  - CERT
  - CSIRTs
  - NCS
  - NCCMF
  - Single Point of Contact
- **Zusätzlich von EU:**
  - CSIRTs Netzwerk
  - CyCLONe



Vom Staat kommend

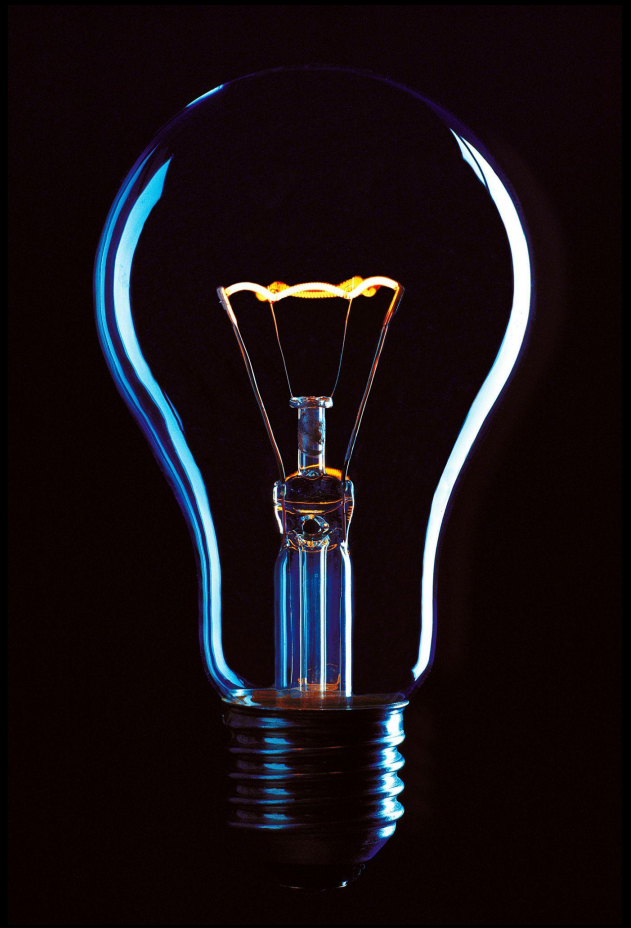
Von der EU kommend

Live Browsing 

NIS 2 Informationen von ENISA

NIS 2 Betroffene Unternehmen

Wer ist jetzt genau in Österreich betroffen?



NIS 2 – Generisches Prüfschema

1. **EU?**

2. **Sektor:** Anhang I und Anhang II Spalte 3 aus der EU Regulierung

3. **mittleres oder großes Unternehmen?***

4. **wesentliche oder wichtige Einrichtung?**

*Sonderregel für Digitale Infrastruktur oder wenn als kritisch Eingestuft

Anhang I

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

*) Im Finanzsektor hat **DORA** Vorrang → 17.01.2025

Anhang II

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

**) In gewissen ÖNACE Klassen

Unterscheidungsmerkmal wesentliche vs. wichtige Einrichtungen

Wesentliche Einrichtungen

große Einrichtungen
laut Anhang I

Wichtige Einrichtungen

mittlere Einrichtungen Anhang I
große und mittlere Einrichtungen Anhang II

Wesentliche vs. Wichtige Einrichtungen

Thema: Aufsicht

Wesentliche Einrichtungen

ex-ante Aufsicht und ex-post Aufsicht

- **regelmäßige und gezielte Sicherheitsprüfungen**
- **Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, Stichprobenkontrollen**
- **Bußgeldrahmen 10 Mio € oder 2 % des Weltweiten Jahresumsatzes (higher wins)**

Wichtige Einrichtungen

ex-post Aufsicht

- **nur bei begründetem Verdacht**
- **Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen**
- **7 Mio € oder 1.4 % des Weltweiten Jahresumsatzes (higher wins)**

Mini-Workout – 10 min

Ein Blick in die Regulierung: Findet den aktuellen Gesetzesentwurf für Österreich und findet mehr über diese Betroffenen Unternehmen in Spalte 3 (bzw. Anlage 1-2) heraus.

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

Wer kennt sich jetzt aus?

Ab wann gilt ein Unternehmen als groß oder mittel oder klein?

Größenklasse	Beschäftigte (VZÄ)	Jahresumsatz	Jahresbilanzsumme
Kleines Unternehmen (KU)	< 50 **und**	⩽ 10 Mio. Euro **oder**	⩽ 10 Mio. Euro
Mittleres Unternehmen (MU)	< 250 **und**	⩽ 50 Mio. Euro **oder**	⩽ 43 Mio. Euro
Großes Unternehmen (GU)	⩾ 250 **oder**	> 50 Mio. Euro **und**	> 43 Mio. Euro

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

Demnach ist das “klassische” österreichische KMU nicht wirklich betroffen.

Spezialfall Digitale Infrastruktur

Sektor	Art der Einrichtung	groß	mittel	klein
Digitale Infrastruktur	**TLD-Namenregister** **qualifizierte Vertrauensdiensteanbieter**	wesentlich		
	DNS Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)			
	Anbieter öffentlicher elektronischer **Kommunikationsnetze** oder elektronischer **Kommunikationsdienste**	wesentlich		wichtig
	Vertrauensdiensteanbieter	wesentlich	wichtig	
	Betreiber von **Internet-Knoten**	wesentlich	wichtig	
	Anbieter von **Cloud-Computing-Diensten**			
	Anbieter von **Rechenzentrumsdiensten**			
	Betreiber von **Content Delivery Networks** (CDN)			

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

Ausnahmen für KMUs

Digitale Infrastruktur

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

- 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.
- als wichtig eingestuft

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

Mini-Workout - 5min

Selfcheck Übung: Überprüft ob ihr betroffen seid! Testet mehrere Unternehmen wenn möglich.

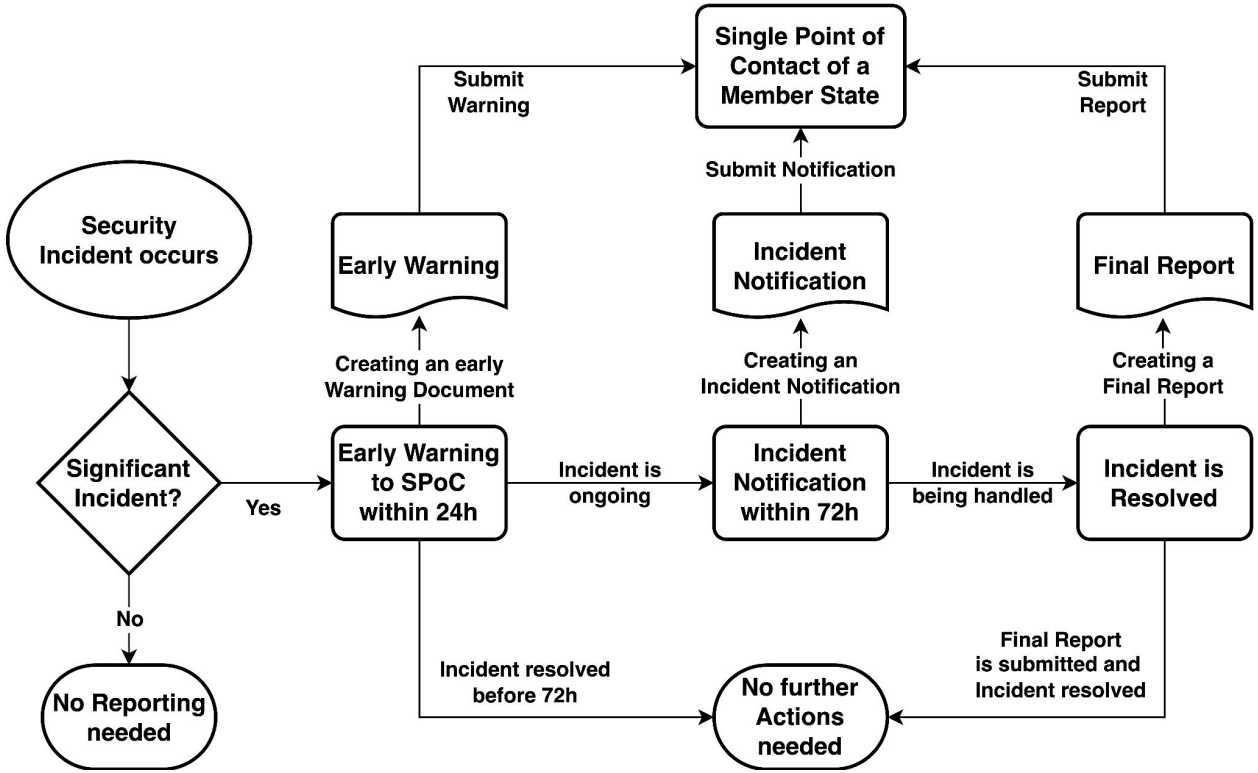
Selfcheck: https://ratgeber.wko.at/NIS2/

Anlaufstellen und Ressourcen für NIS 2

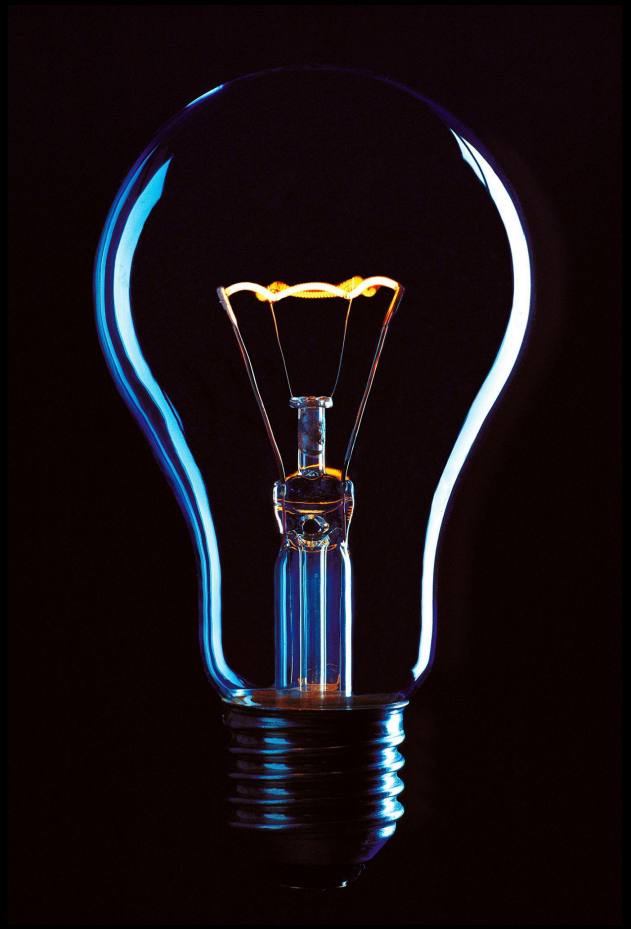
Meldewesen bei NIS 2

Prozess des Meldens:

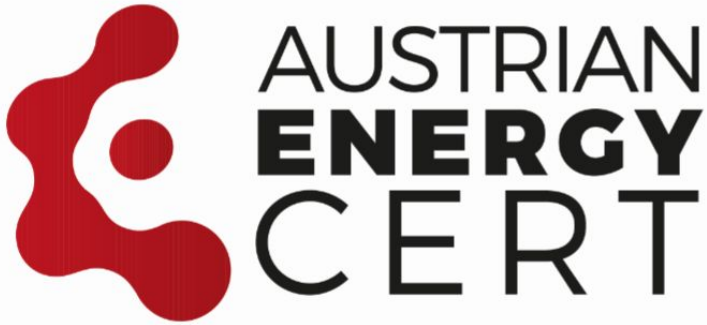
- **Frühwarnung** binnen 24h
- **Ordentliche Meldung** nach 72h
- **Endbericht** bis 1 Monat nach Meldung



Welche Institutionen mit NIS 2 Bezug kennt ihr?



CSIRT – In Österreich gibt es 3 Teams



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

CERT - Es gibt mehrere in Österreich da seit langem relevant und gesetzlich Verpflichtend

Mini-Workout - 10min

Aufgabe: Recherchiert welche CERTs es in Österreich gibt und was deren Fokus Gebiete sind

Was habt ihr herausgefunden?

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

CERT - Computer Emergency Response Teams

- Bieten Reaktion und Koordination bei Computer- und Netzwerknotfällen.
- Konzentrieren sich auf Vorfallserkennung, -reaktion, -behebung und -prävention.
- Arbeit auf nationaler oder regionaler Ebene.
- Verbunden mit Regierungsbehörden, Bildungseinrichtungen oder Unternehmen.

CSIRT - Computer Security Incident Response Teams

- Reagieren auf Sicherheitsvorfälle innerhalb der Organisation.
- Identifizieren, analysieren und melden Sicherheitsvorfälle.
- Implementieren Maßnahmen zur Sicherheitsverbesserung.
- Haben spezialisierte Kenntnisse in forensischer Analyse und Incident-Response-Techniken.

Nationale Cybersicherheitstrategie

- Letzte Version von 2021
- Wird wahrscheinlich auch noch für NIS 2 angepasst
- EU Mitgliedstaaten müssen eine solche Strategie haben
- Geht vom Bundeskanzleramt aus

Quelle: https://www.onlinesicherheit.gv.at/Services/Initiativen-und-Angebote/Koordination-und-Strategie.html

Mini-Workout - 10min

Aufgabe: Nationale Cybersicherheit Strategien und Anlaufstellen - ENISA

Begebt euch auf die ENISA Webseite und findet etwas über die Nationalen Cybersicherheitsstrategien heraus.

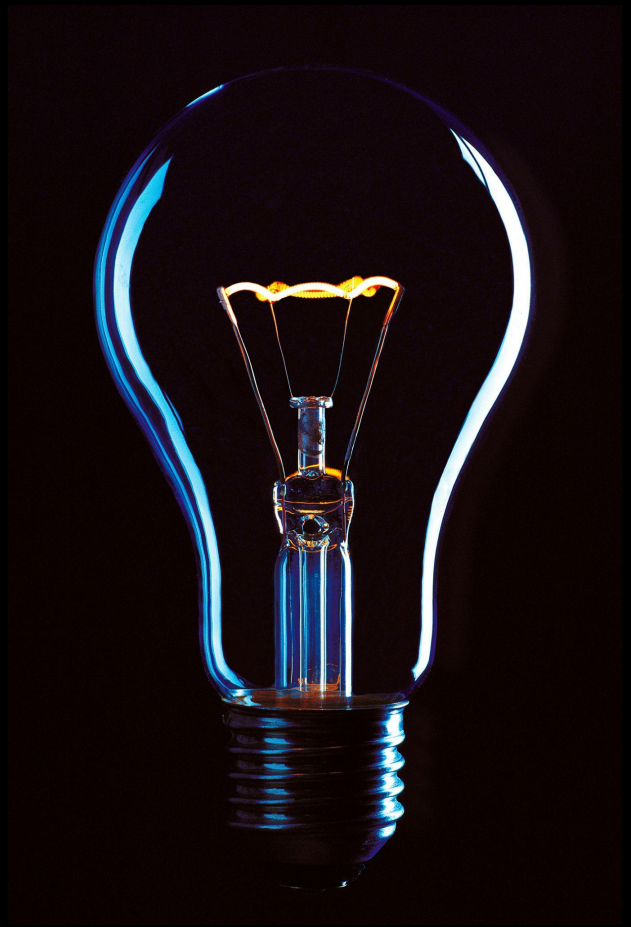
Was sind die Details der Österreichischen?

Nützliche Links

CSIRT Network	https://csirtsnetwork.eu/
EU-CyCLONe	https://www.enisa.europa.eu/topics/incident-response/cyclone
NIS Cooperation Group	https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
Data Breach Meldung	https://www.wko.at/datenschutz/eu-dsgvo-meldung-von-datenschutzverletzungen
NIS Meldung	https://www.nis.gv.at/nis-meldungen.html
Watchlist Internet AT	https://www.watchlist-internet.at/melde-formular/
WKÖ NIS Übersicht	https://www.wko.at/it-sicherheit/nis2-uebersicht
Basissicherheit KMUs	https://wko.at/basissicherheit
IT Sicherheit für Firmen	www.it-safe.at

Umsetzung von NIS 2 Anforderungen

Was glaubt ihr: Welche Anforderungen müssen Unternehmen umsetzen?



Es ist eigentlich relativ straight forward und es handelt sich um Basics!

Wichtig: Je nach Unternehmen müssen passende Maßnahmen getroffen werden.

Es sollten 10 Risikomanagementmaßnahmen getroffen werden – “Mindestmaßnahmen” (1)

- Konzept Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT

Es sollten 10 Risikomanagementmaßnahmen getroffen werden – “Mindestmaßnahmen” (2)

- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle
- Multi-Faktor-Authentifizierung

Zeit für ein Quiz! 

Lernziele 🎯

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



Recap Tag 1

Ganzheitlicher Cybersicherheitsansatz

Europa und Cybersicherheit

Haben sich Fragen ergeben?

Wollt ihr noch etwas spezielles wissen?

Überlegung: Arbeitswoche

Wie arbeitet ihr?
Welche Systeme verwendet ihr (intern & extern)?
Wo liegen Dokumente bzw. Daten?
Was ist eure Haupttätigkeit und was benötigt ihr dafür?

Workout 🔎

- **Ziel:** Erstelle eine Liste oder Mindmap aller Systeme die du im “Daily Business” brauchst.
- **Output:** Welche Sicherheitsmaßnahmen habt ihr für diese Systeme (z.B. MFA)? Gibt es überall ein Backup?
- **Modus:** Ausarbeitung alleine für 20 min, anschließend Diskussion

Praktische Sicherheits-maßnahmen anhand von NIS 2

Wie können diese Risikomanagement Maßnahmen systematisch adressiert werden?

Lernziele 🎯

- Was bedeuten die Risikomanagementmaßnahmen für mein Unternehmen?
- Welche Vorgehensweise macht hier Sinn?
- Habe ich genügend Know-how im Unternehmen?

Lernpfad

FA01: Cybersicherheits-bedrohungen und ganzheitlicher Ansatz

FA02: EU x Cybersicherheit und das NIS 2 Gesetz

FA03: Praktische Sicherheits-maßnahmen anhand von NIS 2

FA04: Compliance und kontinuierliche Verbesserung

Risikomanagementmaßnahmen

Konzept Risikoanalyse und Sicherheit für Informationssysteme

Anfang für NIS Umsetzung

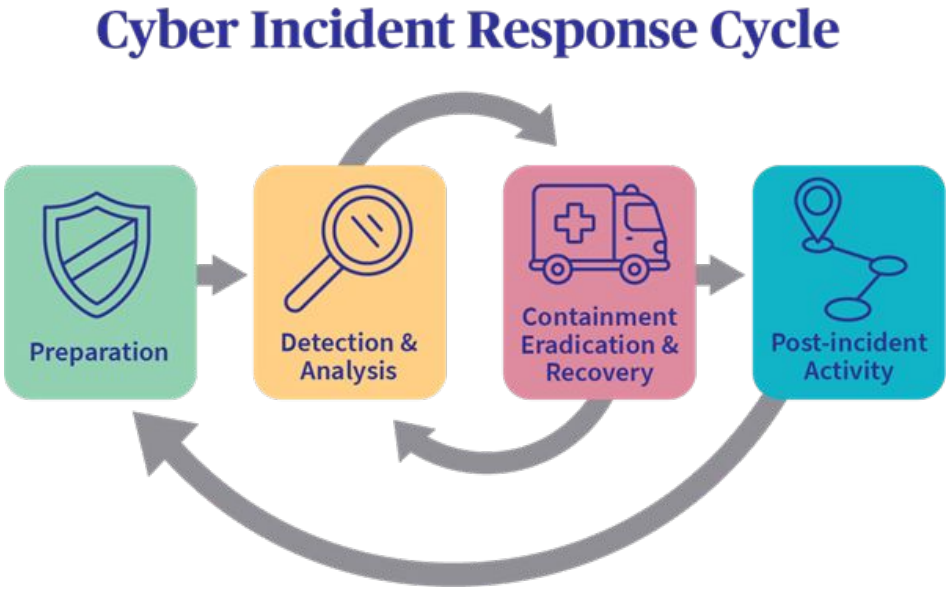
- IT Asset Management
  - Welche Assets habe ich?
  - Wo befinden sich diese?
  - Wer ist verantwortlich?
  - Cloud? Operational Technology?
  - Wer hat Zugriff auf diese?
- Gefahrenidentifikation
- Ist es für mich für mein Unternehmen relevant?
- Welche Maßnahmen gehe ich in welcher Reihenfolge an?

Quelle: https://searchinform.com/

Bewältigung von Sicherheitsvorfällen

Basisthemen:

- Incident Response Plan
- Klare Prozesse
- Genügend Ressourcen
- Beratung/Partner?



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

Zusatzfaktoren:

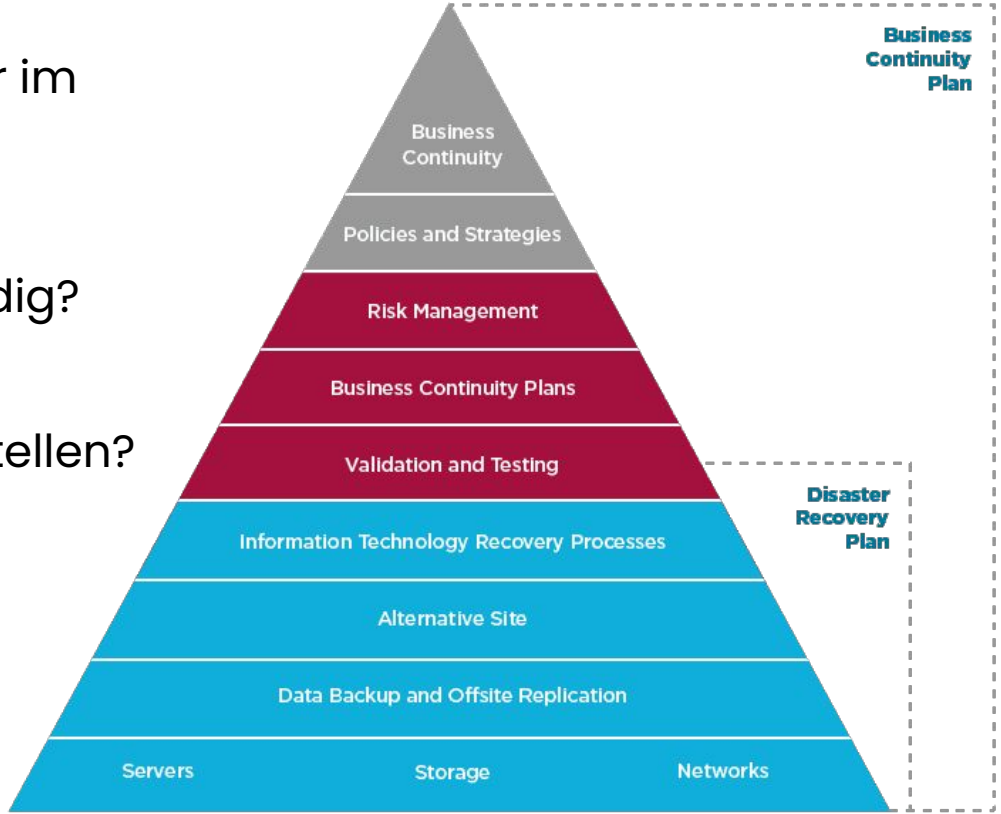
- NIS 2 Meldeverhalten
- Hilfestellungen durch Institutionen

Business Continuity und Krisenmanagement

Tipp: klein anfangen und immer im Hinterkopf haben.

- Was ist überlebensnotwendig?
- Wird das abgesichert?
- Wo wird es abgesichert?
- Wie können wir wiederherstellen?
- Wer kann das?
- Haben wir es getestet?

Und das für jede Abteilung!

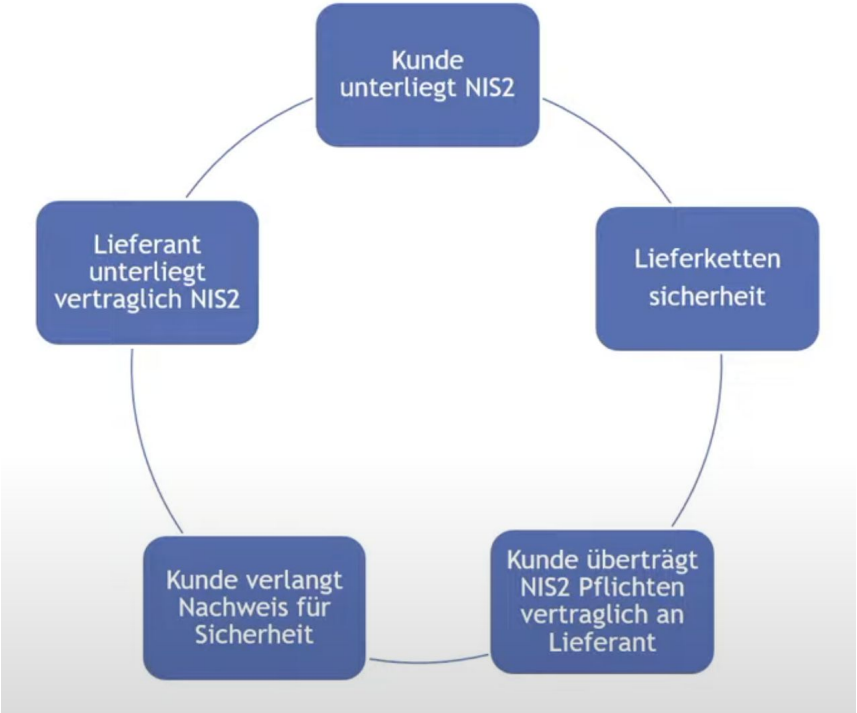


Quelle: https://www.boxuk.com/insight/business-continuity-disaster-recovery-why-should-you-care/

Sicherheit der Lieferkette

Themen:

- Wer sind meine Kunden?
- Wer sind meine Lieferanten?
- Was muss ich nachweisen können?
- Habe ich etwas nachzuweisen?



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

Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT

Cyber Security Academy TU Graz

Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT

Wichtige Themen:

- Wer ist dein Lieferant?
- Wie sind Produkte Zertifiziert?
- Befolgen Lieferanten gewisse Sicherheitsstandards?
- Passen Produkte/Systeme zu einem “Ganzheitlichen Cybersicherheitsansatz”?

Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen

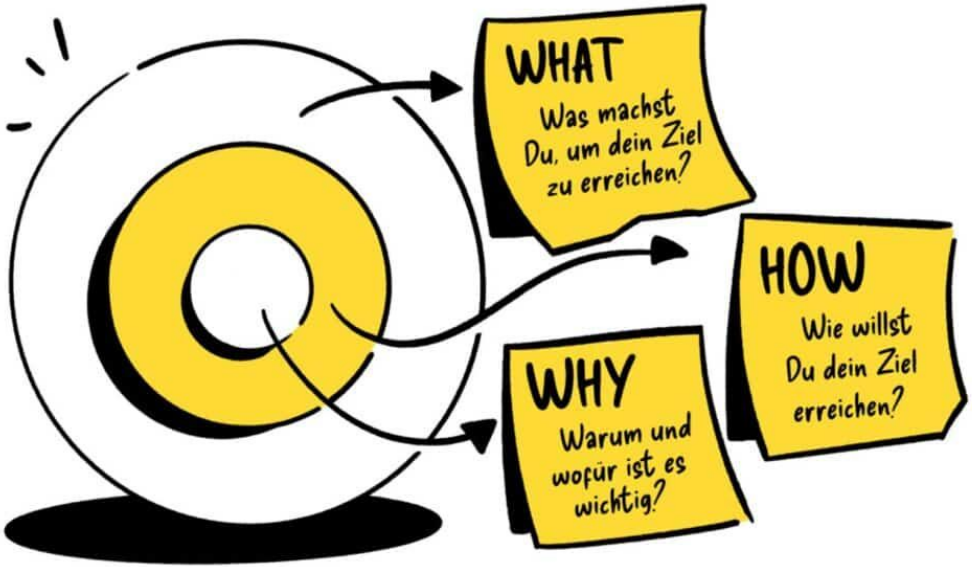
Grundfragestellung:

- 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?

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

Cyberhygiene und Schulungen zur Cybersicherheit

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



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

Es fehlen:

- Der Bezug zur Thematik
- Das ganzheitliche Bild
- Bezug zur Rolle im Unternehmen
- Mangement Support

Kryptographie

Kryptographie ist ein extrem breites Thema... Einige Kernaspekte sind:

- Confidentiality
- Integrity
- Authentication
- Secure Communication
- Access Control
- Non Repudiation

Quelle: https://us.norton.com/blog/emerging-threats/cryptography

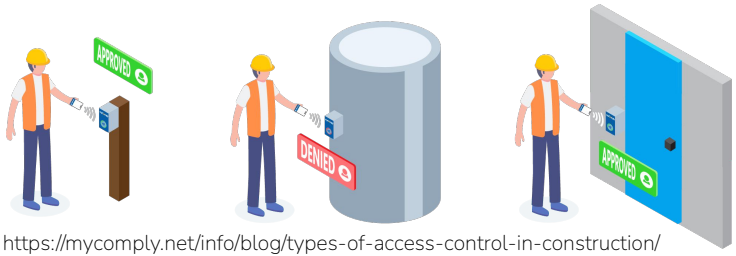
Sicherheit des Personals, Konzepte für die Zugriffskontrolle

Technologie:

- Schlüssel
- Chips
- Apps
- Triple A
  - Authenticate
  - Authorise
  - Account

Sicherheit:

- Kryptographie
- Mehrere Faktoren
  - Gesicht
  - Biometrie
  - Sprache



Quelle: https://mycomply.net/info/blog/types-of-access-control-in-construction/

Alles immer je nach Kritikalität zu sehen!

Außerdem müssen Mitarbeiter:innen richtig geschult sein!

Multi Faktor Authentication - Everywhere

Grundlage:

- Technologisch Bereit
- Einsatz von PW-Managern

Umsetzung:

- Enforcement (Richtlinien etc.)
- Applikationssupport

Generell → Sollte Standard sein bei allen kritischen Accounts und Applikationen!

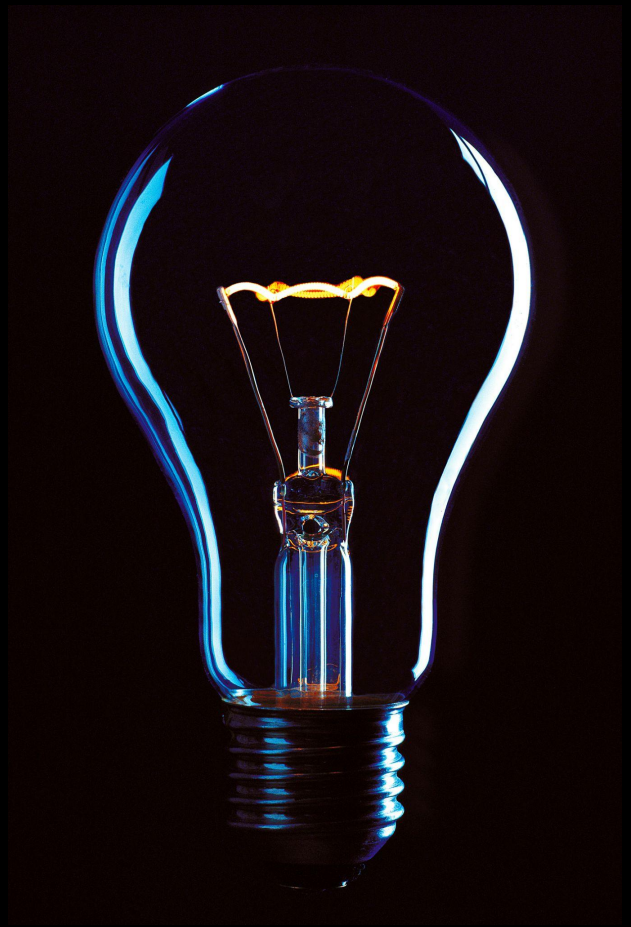
Was ist Multi-Faktor-Authentifizierung (MFA)?

Akamai

Quelle: https://www.akamai.com/de/glossary/what-is-multifactor-authentication

Zeit für ein Quiz! 

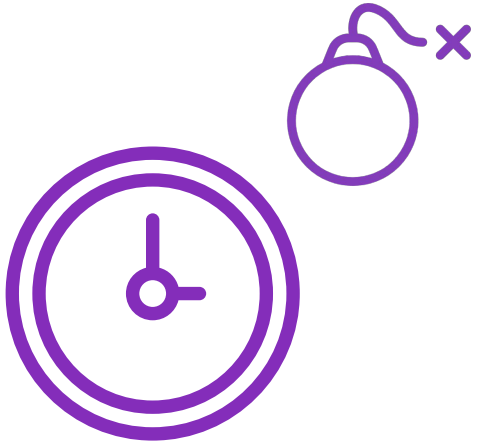
Wo sollten wir jetzt starten bzw. wie können wir das angehen?



Zuvor noch ein Appell

Auch wenn ihr nicht betroffen seid!

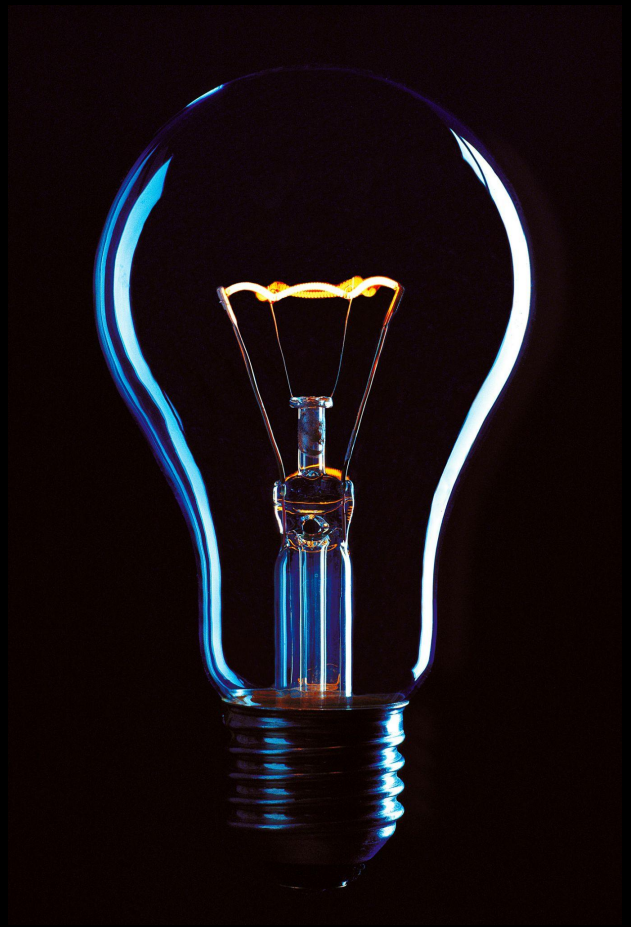
- Verliert auf keinen Fall Zeit!
- Wartet nicht auf das Gesetz!
- Die wesentlichen Grundlagen zur Informationssicherheit sind längst etabliert, hinlänglich bekannt und allgemein zugänglich - packt es direkt an! Am besten noch in dieser Woche!



Security Timer

Es dreht sich alles um das Thema Risikomanagement

Wie können wir unsere Risiken identifizieren und dann managen?

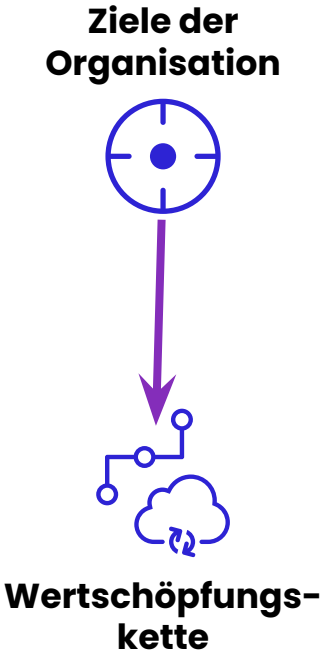


Prozess – Step 1

Ziele der Organisation

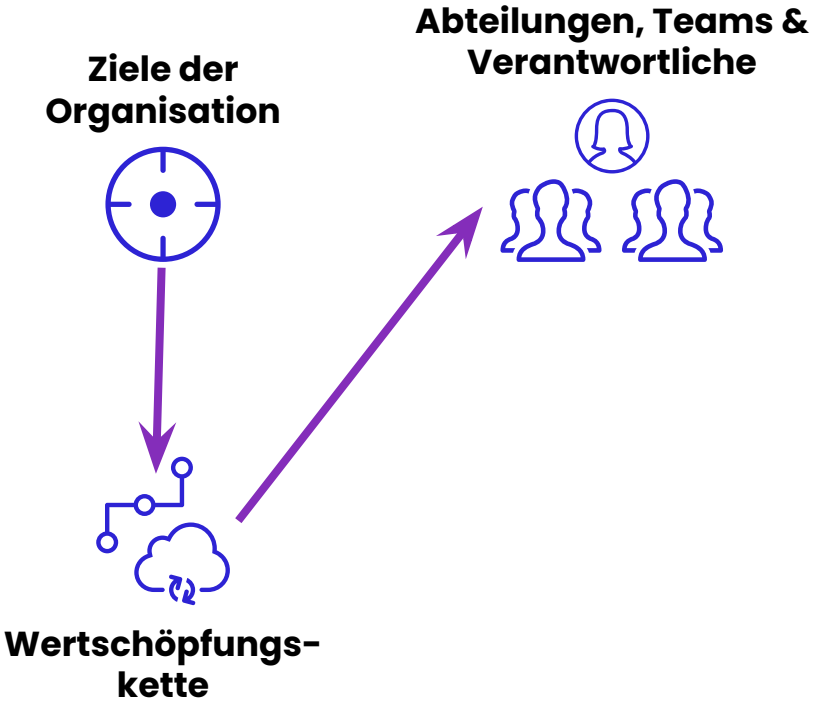
1. Was ist das aktuelle Unternehmensziel?
   a. Vision?
   b. Mission?
2. Wie ist die Arbeitsweise/Kultur
3. Wie werden diese Ziele kommuniziert?

Prozess - Step 2



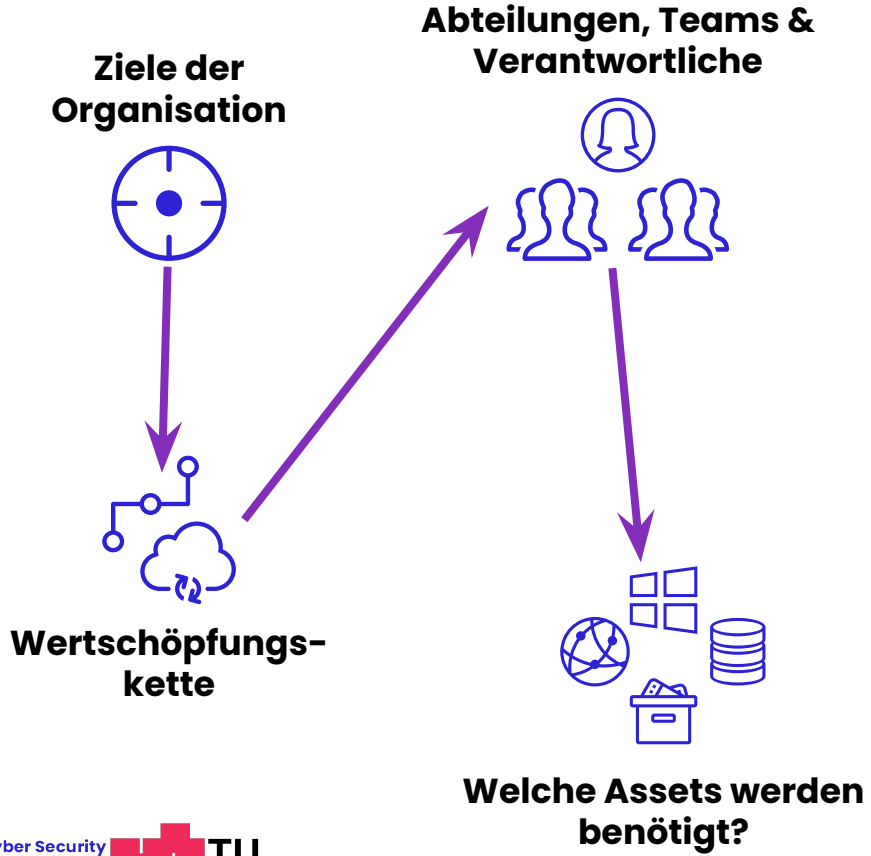
1. Wie passiert die Wertschöpfung?
2. Wie viele Produkte/Dienstleistungen gibt es?
3. Wie kommen diese an die Kunden?

Prozess - Step 3



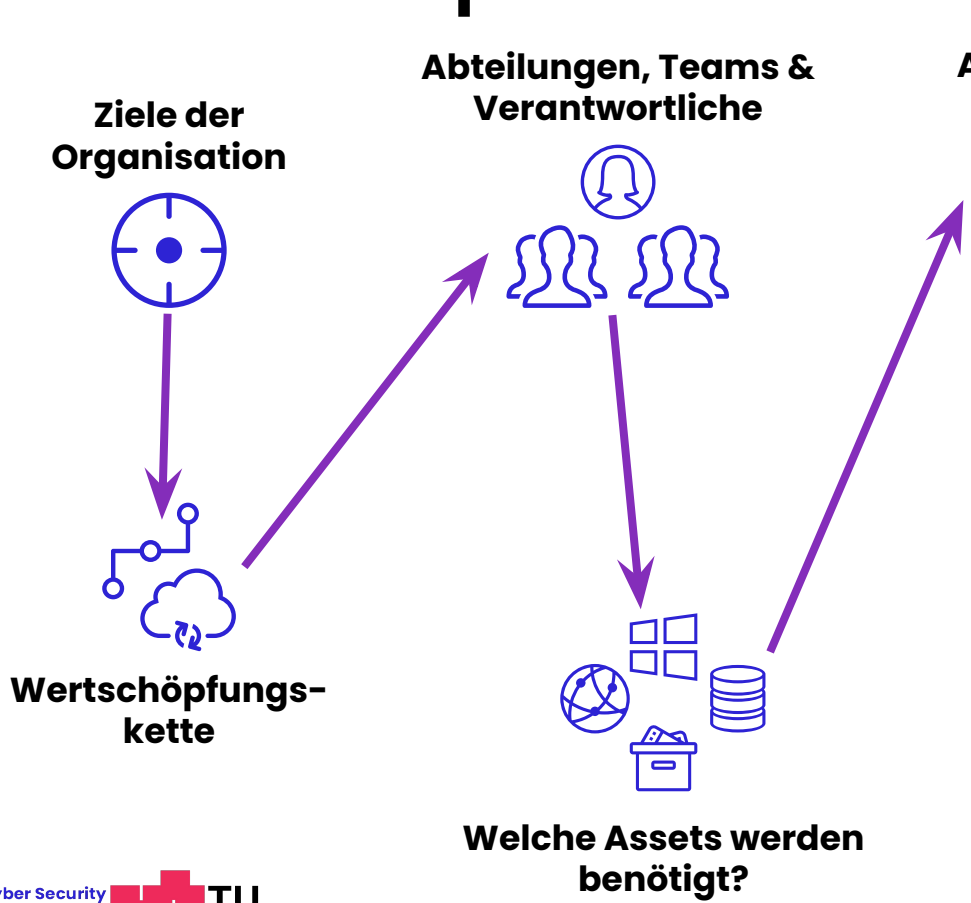
1. Welche Teams und Abteilungen gibt es?
2. Wie arbeiten diese Teams?
3. Was brauchen diese Teams täglich zum Arbeiten?
4. Wer ist für die IT-Security verantwortlich?

Prozess - Step 4



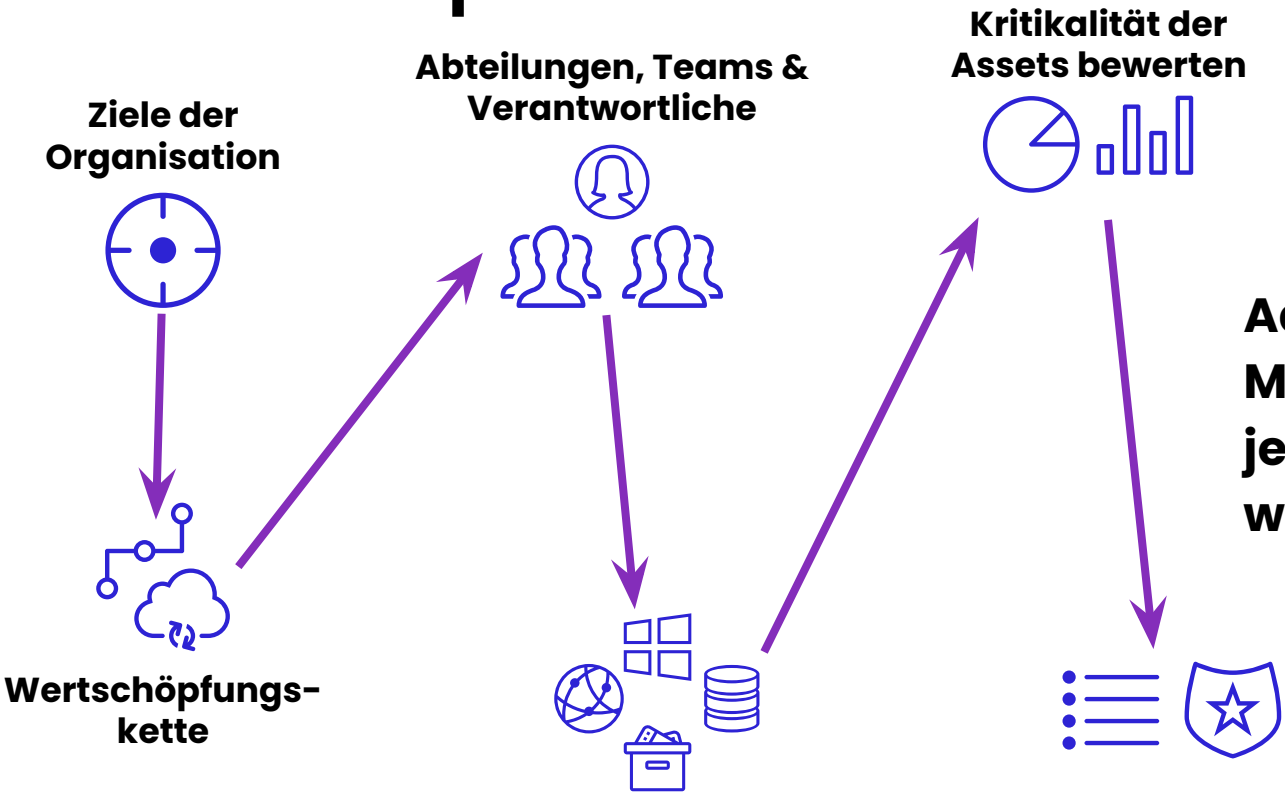
1. Ziele → Wertschöpfung → Teams
2. Welche “Assets” benötigt man für alles?
3. Auflistung/Inventar
   a. Software
   b. Hardware
   c. Services
   d. Lieferanten
   e. etc.

Prozess - Step 5



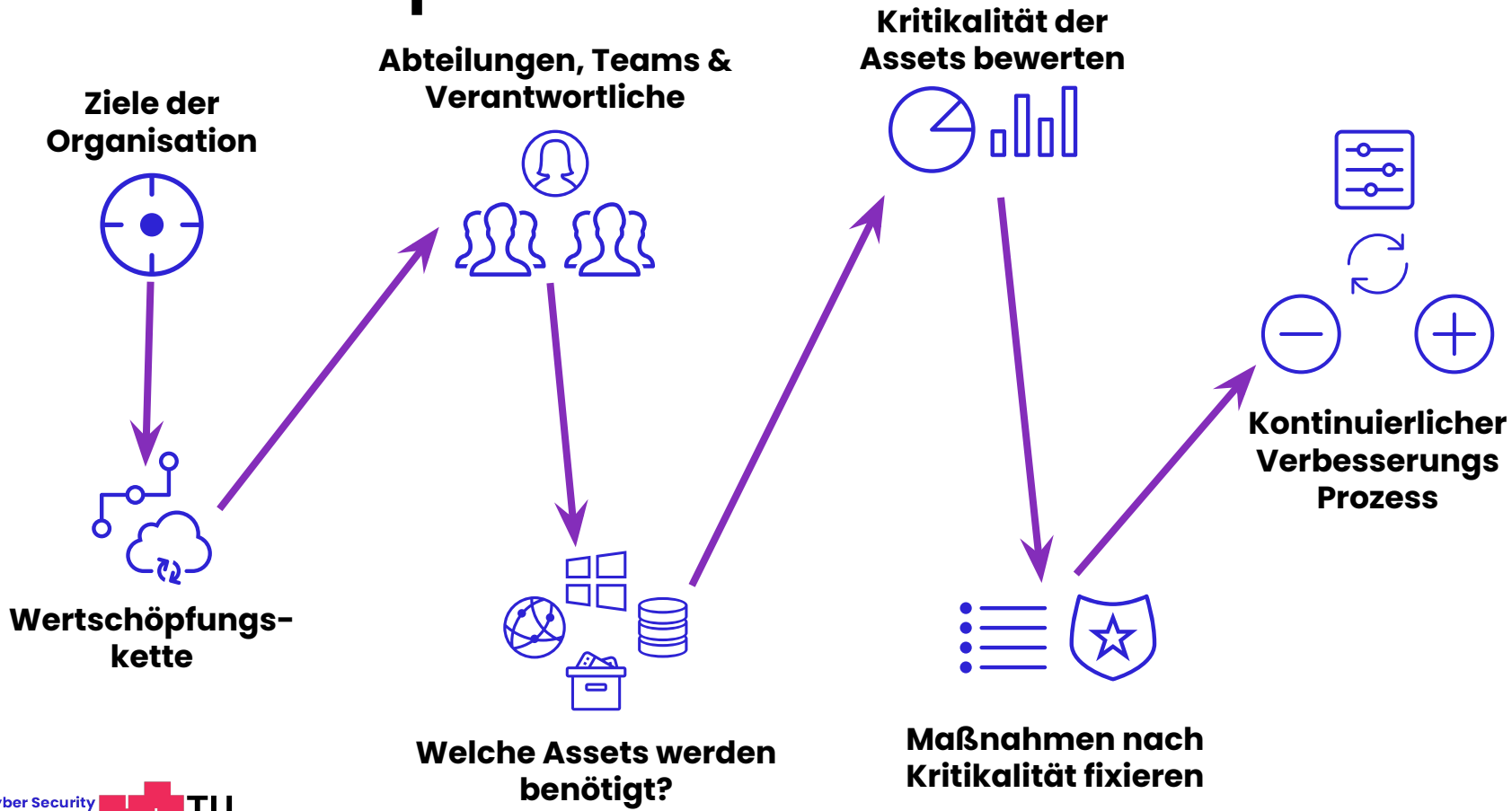
1. Wie kritisch ist ein Asset für mein Ziel?
2. Einfache Skala wählen:
   a. Stark
   b. Mittel
   c. Leicht

Prozess - Step 6



Adäquate Maßnahmen für jeweilige Kritikalität wählen und Umsetzen!

Prozess - Step 7



Blick hinter die Kulissen

Anhang 3 und NIS Fact Sheets

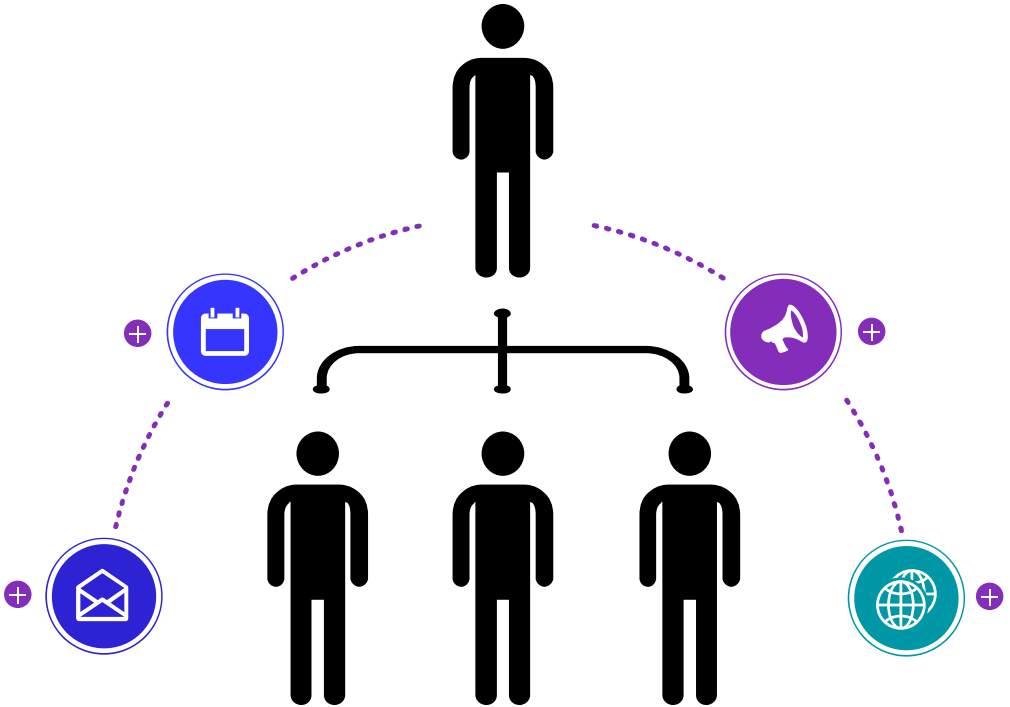
Status Quo in deinem Unternehmen!

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

Workout 🔎

- **Ziel:** Führe diesen Prozess einmal bei deinem Unternehmen durch!
- **Output:** Assets die in deiner Rolle von Bedeutung sind + Kritikalität!
- **Modus:** Ausarbeitung alleine für 30 min, anschließend Diskussion

Ziel sollte es sein, dass auf Unternehmensebene durchzuführen



Lernziele 🎯

- Was bedeuten die Risikomanagementmaßnahmen für mein Unternehmen?
- Welche Vorgehensweise macht hier Sinn?
- Habe ich genügend Know-how im Unternehmen?



Compliance und kontinuierliche Verbesserung

Wie können diese Risikomanagement Maßnahmen systematisch adressiert werden?

Lernziele 🎯

- Was ist ein gutes Cybersicherheit Basislevel für mein Unternehmen?
- Wie kann ich eine Security Kultur im Unternehmen fördern?
- Ich weiß, was zu tun ist bei einem Security Incident?

Lernpfad

FA01: Cybersicherheits-bedrohungen und ganzheitlicher Ansatz

FA02: EU x Cybersicherheit und das NIS 2 Gesetz

FA03: Praktische Sicherheits-maßnahmen anhand von NIS 2

FA04: Compliance und kontinuierliche Verbesserung

NIS 2 betroffen bzw. indirekt betroffen!

Mit welchem System können wir jetzt unsere Maßnahmen belegen und dokumentieren?

Ausgangslage ist ein Asset Management!

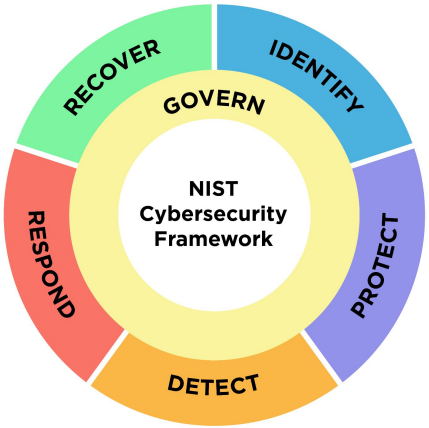
Es gibt jedoch noch mehr Basics die Sinn machen

Security Zertifizierungen nach Standards/Normen

Es gibt sehr viele Standards und Normen für Cybersicherheit. Das Problem ist, sie sind für Enterprises ausgelegt!

Beispiele:

- ISO 27001
- IEC 62443
- NIST SP 800 - CSF
- CIS Controls
- etc.



Das kann kein KMU vernünftig Umsetzen

Probleme:

- Know-How Mangel
- Budget für die Umsetzung
- Kauf von Hardware
- Cybersecurity meistens ein neues Thema
- Standards sind viel zu Breit
  - Passt nicht zum KMU scope!
  - Passt auch nicht zu Budget!

Was jetzt wenn wir Kunden oder einer Versicherung etwas zeigen müssen?

Bsp. Indirekte Betroffenheit von NIS-2 durch → Lieferkette

Lösungsansätze und Empfehlungen

Wenn man wirklich betroffen ist durch die Lieferkette bzw. man eine Versicherung etwas vorlegen muss, sollte man sich überlegen wie man belegen kann, dass im Unternehmen gewisse Maßnahmen umgesetzt werden.

Hilfestellungen:

- Förderung https://www.ncc.gv.at/foerderungen.html
- www.it-safe.at → Informationen rund um das Thema Cybersicherheit im Unternehmen
- IT-Sicherheitsexperten (WKÖ)

Zertifizierung → CyberRisk Rating Österreich

Folgende Ratings stehen hierbei zur Auswahl:

- B-Rating:
  Basis-Cyber-Schutzniveau,
  umfasst 14 Anforderungen

- A-Rating: umfasst alle 25 Anforderungen des KSÖ

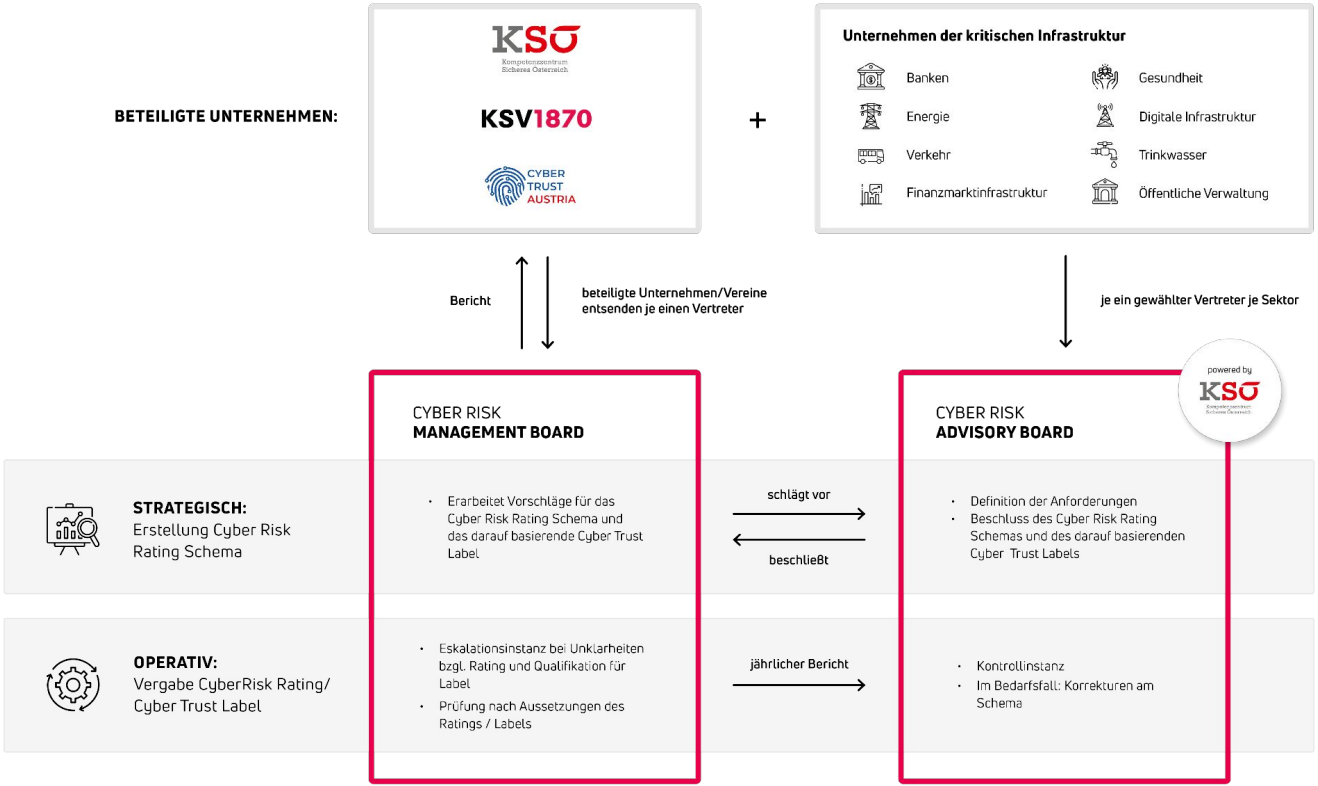
- "A+"-Rating: bietet zusätzlich einen Bericht eines Audit-Partners

KSÖ
Kompetenzzentrum Sicheres Österreich

CYBER TRUST AUSTRIA

KSV1870

CyberRisk Rating Österreich → Qualität?



Blick in das Schema

Cyber Risk Rating & Cyber Trust Label

Schema Policy 2025

Cyber Risk Rating & Cyber Trust Label

Schema Policy 2024

Takeaways Meeting CTA

Die Anzahl der ausgestellten Zertifizierungen/Akkreditierungen steigt ständig an.

Die Beantragung erfolgt über ein Online-Formular und gewisse Dokumente die einzureichen sind.

Cyber Trust Austria & KSV1870 checken dann den Antrag und bewerten das Szenario → Es müssen gewisse Punkte erreicht werden.

Überblick und Ablauf der Zertifizierung

- Online-**Beantragung**
- **Beantwortung** des Online Fragebogens
- **Durchführung** des automatisierten Web Scorings (der angegebenen qualifizierten Domäne)
- **Validierung** der Antworten & Errechnung des vorläufigen Cyber Risk Ratings
- **Möglichkeit zur Klärung** offener Punkte & Richtigstellung
- **Erstellung** des finalen Cyber Risk Ratings
- **Ausstellung** des Labels & Eintrag in die Cyber Trust Label Datenbank

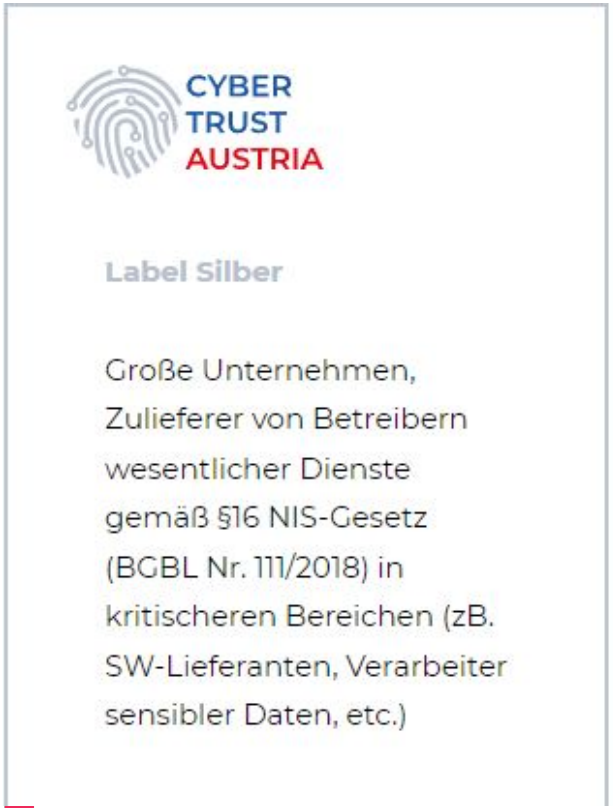
Quelle: https://www.youtube.com/watch?v=h5LhmYimM0Q

B – Rating

- 14 Anforderungen
- Validierte Selbstdeklaration
- 890€
- Vorliegen eines gültigen KSV1870 CyberRisk B-Ratings von 190 oder besser

Quelle: https://www.cyber-trust.at/labeluebersicht/

A - Rating



- 25 Anforderungen
- Validierte Selbstdeklaration
- 1390€
- Vorliegen eines gültigen KSV1870 CyberRisk A-Ratings von 190 oder besser

A+ Rating

- 25 Anforderungen
- Validierte Selbstdeklaration plus externer Audit
- 1490€ + Auditkosten
- Vorliegen eines gültigen KSV1870 CyberRisk A-Ratings von 190 oder besser

Auditpartner

Anforderungen → Step by Step

Wir gehen jetzt Step by Step das Schema durch

Bitte macht begleitend für euer Unternehmen ein Demo Assessment:
https://demo.cyberrisk-rating.at/

Bzw. schreibt in einem Word mit um das in Zukunft angehen zu können

B1. Informationssicherheitsrichtlinie

Anforderung:
Haben sie eine aktuelle Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie), die für ihr Unternehmen gültig ist?

Anforderungskriterien:
Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen (zB. ISO 27001/27002, NIST 800, IT-Grundschutz, IT-Sicherheitshandbuch der WKO u.ä.). Die Richtlinie muss von der Geschäftsführung freigegeben und für alle Mitarbeiter verfügbar sein.

Was ist eine Informations-sicherheits Richtlinie?

Was stellt ihr euch darunter vor und habt ihr sowas in eurem Unternehmen?

B1. Informationssicherheitsrichtlinie - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- ISO 27001 - Control 5.1
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com

B2. Security Schulungen

Anforderung:

Schulen Sie ihre Mitarbeiter regelmäßig in Informationssicherheit?

Anforderungskriterien:

Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen:

- Sicherer Umgang mit Computern und Informationen
- Passwörter richtig auswählen und verwalten
- Sicher im Internet (zB. Nutzung von Firmendaten in KI Diensten und sozialen Netzen)
- E-Mails, Spam und Phishing
- Gefährliche Schadprogramme
- Verhalten und Vorgehen bei Verdacht auf IT-Sicherheitsvorfall

Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.

Macht ihr Schulungen bei euch im Unternehmen?

Wenn ja wann, wie oft und mit welchen Unterlagen?

B2. Schulungen - Quellen

- DIN SPEC 27076
- IT-Grundschutz BSI
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com/ratgeber/cybersecurity-schulung-kostenlos/

B3. Security Verantwortung

Anforderung:
Gibt es in ihrem Unternehmen eine oder mehrere benannte Personen, die für das Thema Informationssicherheit zuständig sind?

Anforderungskriterien:
Es muss zumindest eine benannte Person geben, die für das Thema Informationssicherheit zuständig ist, d.h. die Richtlinie erstellt und sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben und sich laufend über Cyberrisken informieren. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.

Gibt es bei euch einen oder mehrere Security Verantwortlichen?

Wenn ja haben diese die Notwendigen Ressourcen und das passende Know-How? Das muss nachweisbar sein.

B3. Security Verantwortung

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com/ratgeber/cybersecurity-schulung-kostenlos/ → Ausbildungen in diesem Bereich

B4. Asset Management + Stakeholder

Anforderung:
Pflegen Sie regelmäßig ein Verzeichnis all Ihrer IT-Assets und -Services (inkl. Cloud-Dienste) sowie der damit verbundenen Verantwortlichkeiten?

Anforderungskriterien:

- Es muss ein Verzeichnis aller verwendeten IT-Assets (Systeme, Dienste - Cloud und on premise) geben. Dieses Verzeichnis muss zumindest Name und Version des Systems und den Namen der dafür verantwortlichen Person enthalten.
- Das Verzeichnis muss vollständig und aktuell gehalten werden.

Habt ihr im Unternehmen ein Asset Management?

Ist dieses up-to-date? Wird es regelmäßig gepflegt?

B4. Asset Management + Stakeholder - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Theoretisch würde hier eine sauber gepflegte Excel Tabelle auch reichen ist jedoch nicht optimal

Short Research: Findet heraus was hier so an tooling verfügbar wäre auch als Open Source Variante.

B5. Permission Konzept + Enforcement

Anforderung:
Verwalten Sie den Zugang zu Ihren Systemen nach einem Berechtigungskonzept, das jedem nur die für seine Arbeit notwendigen Rechte einräumt?

Anforderungskriterien:

- Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, dass nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben (Need-to-know).
- Es gibt eine dokumentierte Vorgehensweise zur Vergabe und Entzug von Berechtigungen.

Wie kann man so ein Konzept einfach Umsetzen?

Idee: Anhand einer Matrix der Systeme und “Usergruppen”

B5. Permission Konzept - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Excel → Matrix mit Gruppen und Assets (+ Physischen Access)
- Frage: Welche Technologien haben wir im Einsatz und was supporten diese Technologien im Bezug auf Permission Controls

B6. Passwort Richtlinien & Management

Anforderung:
Verlangen Sie von Ihren Mitarbeitern für alle Anwendungen Passwörter mit einer sicheren Mindeststärke zu verwenden?

Anforderungskriterien:

Es muss klar beschriebene Mindestkriterien für Passwörter geben, die die Empfehlungen aktueller Standards umsetzen (Passwortstärke, keine Mehrfachverwendung von Passworten, etc.). Referenz: BSI, NIST 800, etc.

Habt ihr hier Regeln definiert?

Wenn ja welche? Rotations? Wiederverwendung? Allgemein?

Was macht hier eigentlich Sinn?

B6. Passwort Richtlinien - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- NIS GV Kennwortsicherheit
- Allgemein wissen wir alle MFA enablen und enforcen wo es geht und bitte Passwort Management Umgebung für Mitarbeiter:innen bereitstellen von Tag 1 an!

B7. Best Practice Security Config

Anforderung:
Verwenden Sie die vom Hersteller empfohlenen Sicherheitseinstellungen und achten Sie auf eine sichere Konfiguration all Ihrer IT-Systeme?

Anforderungskriterien:

Es muss ein Dokument geben, das die Anforderungen an die sichere Konfiguration der eingesetzten Systeme beschreibt. Verweise auf Herstellerempfehlungen sind ausreichend. Diese Einstellungen müssen auch auf allen verwendeten Geräten - soweit technisch möglich - tatsächlich umgesetzt sein. Alternativ wird ein Schwachstellenscan vor Inbetriebnahme nachweislich durchgeführt.

Habt ihr alles “vernünftig” konfiguriert?

Habt ihr verwendete Versionen/Betriebssysteme im Überblick?

B7. Best Practice Security Config - Quellen

- Technische Quellen von NIST, CISA, etc.
- Herstellerdokumentation
  - Netzwerk
  - Endgeräte
  - Software
  - etc.
- https://kmusec.com
- Hier sollte zumindest im Asset Management grob hinterlegt sein, welche Security Maßnahmen implementiert sind

B8. Öffentliche Schnittstellen

Anforderung:
Überprüfen Sie - sofern vorhanden - individuell entwickelte, aus dem Internet zugängliche Anwendungen auf Sicherheitslücken vor Inbetriebnahme?

Anforderungskriterien:

Individualsoftware (zB. angepasste Open Source Software, aber nicht Standardsoftware), die aus dem Internet erreichbar ist, muss vor Inbetriebnahme durch einen - auf die Individualsoftware angepassten - Penetration Test auf Schwachstellen geprüft werden.

Habt ihr solche Software im Einsatz?

Wenn ja überlegt ihr über einen Pentest?

B8. Öffentliche Schnittstellen - Quellen

- Technische Quellen von NIST, CISA, etc.
- Pentest Information Online
- Google: Pentest Österreich
- https://kmusec.com
- Wichtig hierbei handelt es sich um Schnittstellen, auf die im Prinzip “verkauft” werden an Kunden und gleichzeitig

B9. Patch Management

Anforderung:

Aktualisieren Sie alle IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates?

Anforderungskriterien:

Regelmäßige Aktualisierung der Systeme mit Updates, die vom Hersteller zur Verfügung gestellt werden. Kein Systemupdate darf länger als ein Quartal überfällig sein (außer es gibt einen dokumentierten Grund, warum ein Update nicht eingesetzt werden kann).

Systeme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden, werden rechtzeitig außer Betrieb genommen bzw. es gibt definierte Ausnahmeprozesse inklusive einer Abweichungsliste.

Wie patcht ihr aktuell Server, Applikationen und Endgeräte?

Was ist euer Intervall bzw. Ansatz?

B9. Patch Management - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Auch wieder Ergänzend zum Thema Asset Management zu sehen.

B10. Network Security

Anforderung:
Sichern Sie Ihr Netzwerk vor unberechtigtem Zugriff von außen ab?

Anforderungskriterien:

Es ist eine Netzwerk-Segmentierungseinrichtung (zB. Firewall, Router, etc.) im Einsatz, die auf Basis möglichst restriktiv gesetzter Regeln den Netzwerkverkehr aus dem Internet in das interne Netzwerk beschränkt.

Wie setzt ihr eure Netzwerk Sicherheit um?

Was wollt ihr ändern in Zukunft?

B10. Network Security - Quellen

- IT-Grundschutz BSI
- NIST/CIS Standards
- Network Security - Quick Wins
  - Least Privilege Access
  - Macro and Micros Segmentation
  - Firewall mit VLANs
  - Perimter Absichern
  - Unterschied zwischen Public und Private Zonen

B11. Antivirus auf Assets

Anforderung:
Überwachen Sie Ihre IT-Systeme auf Malware?

Anforderungskriterien:

Es muss zumindest eine Antivirussoftware im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware überprüft. Die Software muss laufend aktualisiert werden und diese Aktualisierung zumindest einmal monatlich zentral geprüft werden. Im Verdachtsfall erfolgt eine Alarmierung im Unternehmen.

Welchen AV habt ihr im Einsatz? Ist dieser mit einem Device Mgmt verknüpft?

Habt ihr das auch auf Servern?

B11. Antivirus auf Assets - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Auch wieder Ergänzend zum Thema Asset Management zu sehen.

B12. Verschlüsselte Kommunikation

Anforderung:
Verschlüsseln Sie sensible Daten bei der Übertragung im Internet?

Anforderungskriterien:

Es muss die Möglichkeit bestehen, Dateien verschlüsselt zu übertragen, entweder per E-Mail (zB. S/MIME, PDF verschlüsselt, mandatory enforced TLS, etc.) oder per verschlüsseltem Upload.

Formulardaten auf der Webseite werden ausschließlich über https hochgeladen.

Wie kommuniziert ihr mit Kunden?

Wie tauscht ihr Nachrichten, Daten und andere Inhalte aus? Betreibt ihr Datenklassifikation?

B12. Verschlüsselte Kommunikation - Quellen

- Sollte eigentlich mittlerweile überall Standard sein!
- Wichtig gilt hier nur bei Austausch von Daten übers Internet!
- Bei E-Mail Provider muss das enabled/supported sein.
- Filesharing über https webplattform ist legitim → Sonst über ssl/tls verschlüsselten Service

B13. Aufbewahrung von Logs jeglicher Art

Anforderung:
Protokollieren Sie die Nutzung Ihrer IT-Systeme, um Sicherheitsvorfälle nachvollziehbar zu machen?

Anforderungskriterien:

Es müssen zumindest die Standardprotokolle der Betriebssysteme aktiviert sein. Die Protokolle müssen dem Unternehmen zur Verfügung stehen.

Es existiert eine Übersicht aller aktiven Systemprotokolle und deren Speicherort.

Die Protokolle werden zumindest drei Monate aufbewahrt.

Habt ihr die möglichkeit zentral Log Events zu speichern?

Was könnt bzw. wollt ihr alles loggen?

B13. Aufbewahrung von Logs - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- NIS GV - Log Aufbewahrung

B14. Verhalten im Notfall

Anforderung:
Haben Sie einen Notfallplan, anhand dessen Sie auf einen IT-Sicherheitsvorfall reagieren?

Anforderungskriterien:

Der Notfallplan muss beschreiben, wie auf einen schwerwiegenden IT-Sicherheitsvorfall reagiert wird. Schwerwiegende Sicherheitsvorfälle sind zum Beispiel:

- Ausfall der Systeme,
- Schadsoftware-Befall (inkl. Kryptolocker) sowie
- Data Leakage

Die Pläne müssen mindestens alle zwei Jahre getestet werden. Der Test muss zumindest die Daten- und Service Wiederherstellung umfassen.

Was ist das wichtigste an dieser Planung?

Testen und Validieren!!!

B14. Verhalten im Notfall - Quellen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch WKO + Basismaßnahmen
- KSV 1870 - Snacks
- https://kmusec.com
- Das alles bringt nur was mit Testszenarios und Pflege der Notfallpläne

Überblick: Verschiedene Pläne und Szenarien

Plan	Objective	Approach and Scope	Implementation and Maintenance
Business Continuity	Ensure critical business functions continue during a disruption	Identify critical busines processes and develops continuity strategies	Regular review and testing, including updating as needed
Disaster Recovery	Restore IT systems and infrastructure quickly after a disaster	Restore IT infrastructure and systems, including data backup and recovery	Regular backup and testing of recovery process
Incident Response	Identify, contain, eradicate, and recover from cybersecurity incidents	Structured approach to incident detection, containment, eradication, and recovery	Regular assessment and testing of the incident response plan

Quelle: https://preyproject.com/blog/business-continuity-disaster-recovery-and-incident-response

Ausarbeitung eines Disaster Recovery Plans

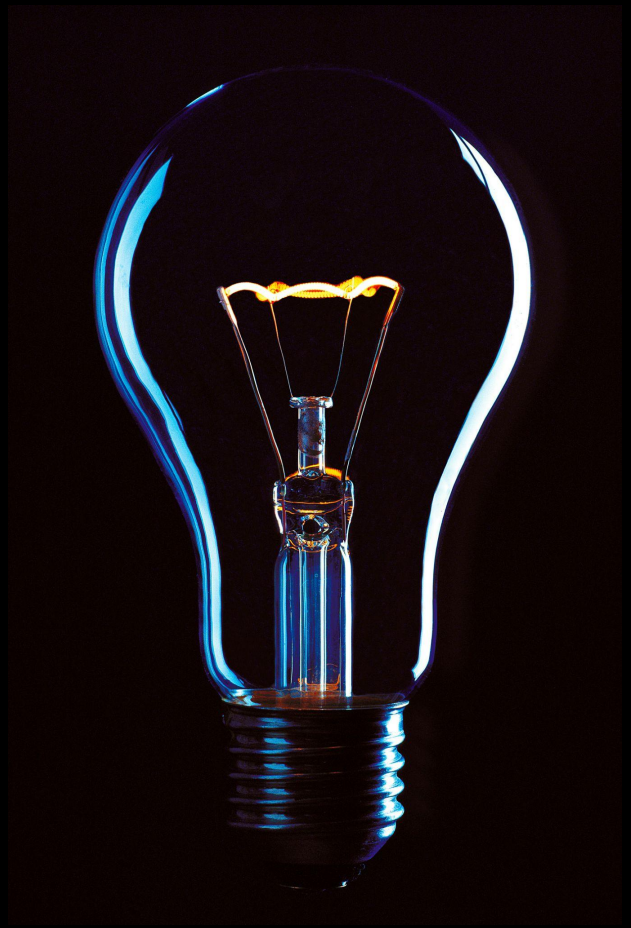
Wichtig hierbei schaut euch eure Assets an! Welche sind die kritischsten und wie könnt ihr diese wiederherstellen?

Workout

- **Ziel:** Finde heraus was in einem Disaster Recovery Plan sein sollte.
- **Output:** Wie sollte er aussehen für dein gewähltes Unternehmen.
- **Modus:** Ausarbeitung in Gruppen (20min)

Q & A

Wie ist es euch dabei gegangen?



Abschließende Empfehlungen

- Werdet euch bewusst, welche Assets ihr benötigt und wie eure Teams/Abteilungen arbeiten.
- Probiert für alle Assets/Teams/Abteilungen passende Grundmaßnahmen zu treffen.
- Macht euch gedanken wie ein BC & DR für die Teams/Abteilungen ausschauen kann.
- Animiert eure IT-Dienstleister dazu, best practices bei bezogenen IKT-Dienstleistungen/Produkten umzusetzen.
- Kommuniziert Security Top-down im Unternehmen und versucht es als etwas positives zu sehen! 🍌

Lernziele 🎯

- Was ist ein gutes Cybersicherheit Basislevel für mein Unternehmen?
- Wie kann ich eine Security Kultur im Unternehmen fördern?
- Ich weiß, was zu tun ist bei einem Security Incident?



Stay in Touch

- **Christian Gubesch**
  - LinkedIn
  - christian@cybersecurityacademy.at
- **TU-Graz Life Long Learning**
  - s.meinhardt@tugraz.at

Zusatzinhalte

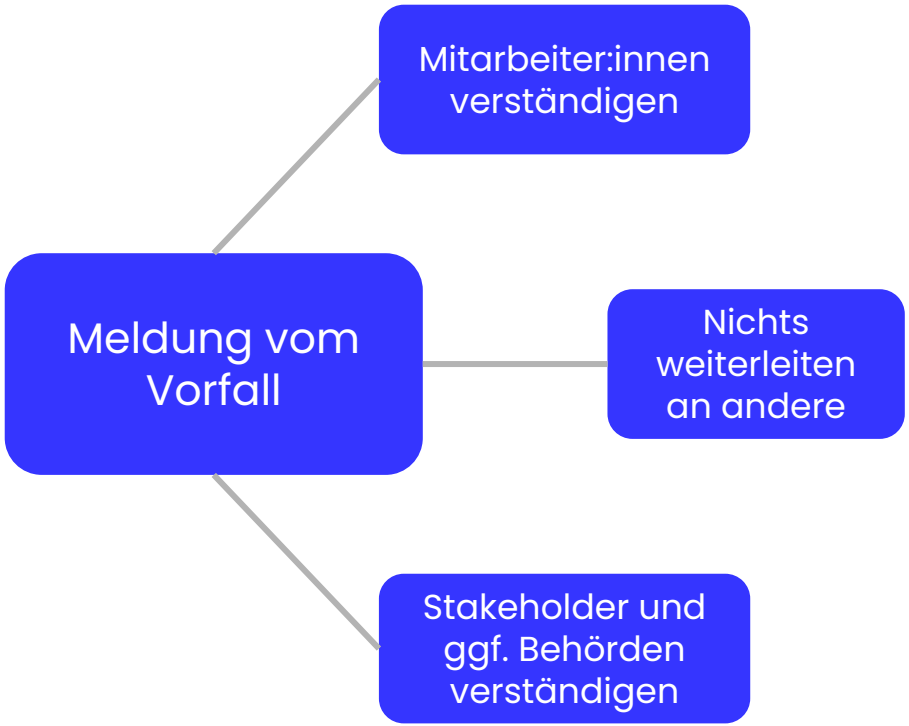
Ein Angriff ist passiert! Was solltet ihr jetzt machen? Bzw. was würdet ihr jetzt tun?

Was tun bei einem Angriff/Verdacht?

Öffnen von Links/Anhängen vermeiden

Ändern von Passwörtern inkl. Account Logout

Internet-verbindung Trennen



Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Security Einstellungen an Systemen prüfen

Falls notwendig Backups einspielen

Datenschutz Meldung falls notwendig

Regulärer Prozess eines Incidents 🔁

Incident Response Prozess - Organisatorisch