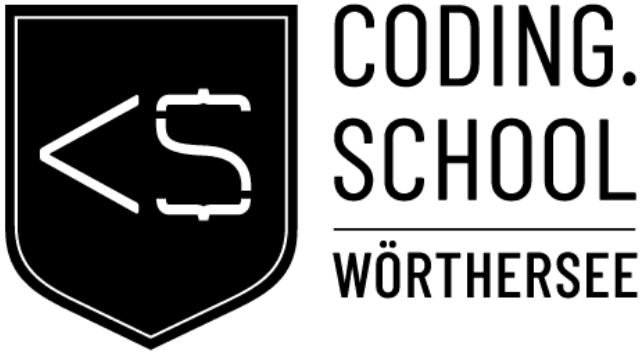


Compliance Training 💪🏻

HoliSec

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, FH Joanneum & Fern FH Porsche
    - Cyber Security Academy
  - HoliSec – Mädchen für alles im Bereich CyberSecurity & IT ;)

HoliSec

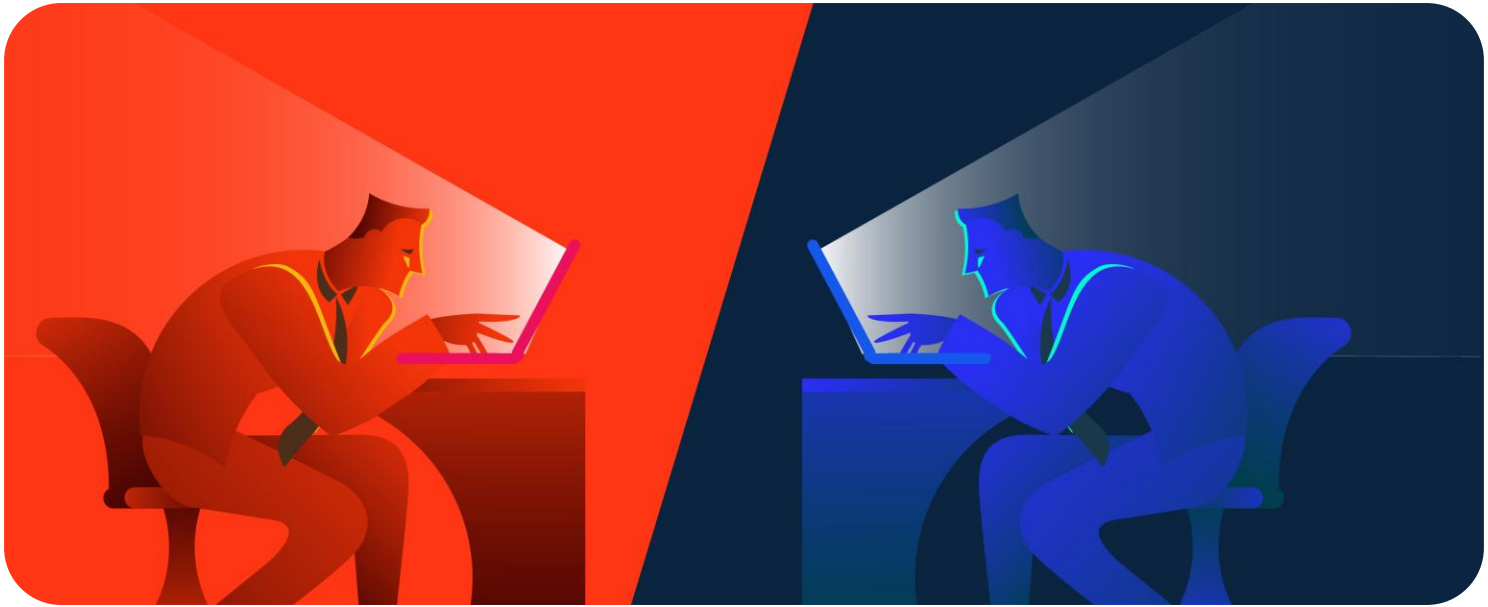
Wer seid ihr ?

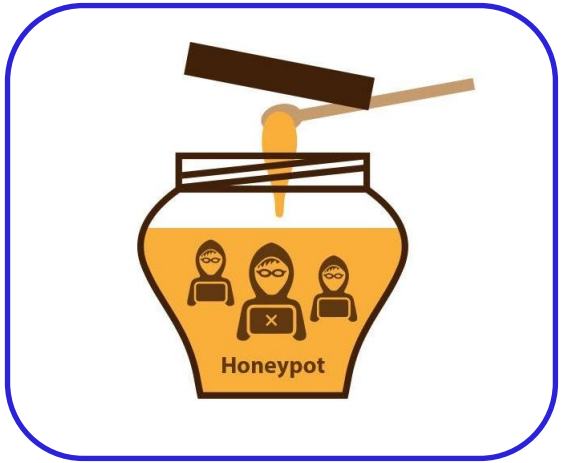
- Hintergrund
  - Job / Aufgabenbereiche
  - Berührungspunkte im Bereich Cyber-Security/Compliance?
- Vorstellungen & Erwartungen
- Nach diesem Workshop will ich in der Lage sein, ...


Mentimeter

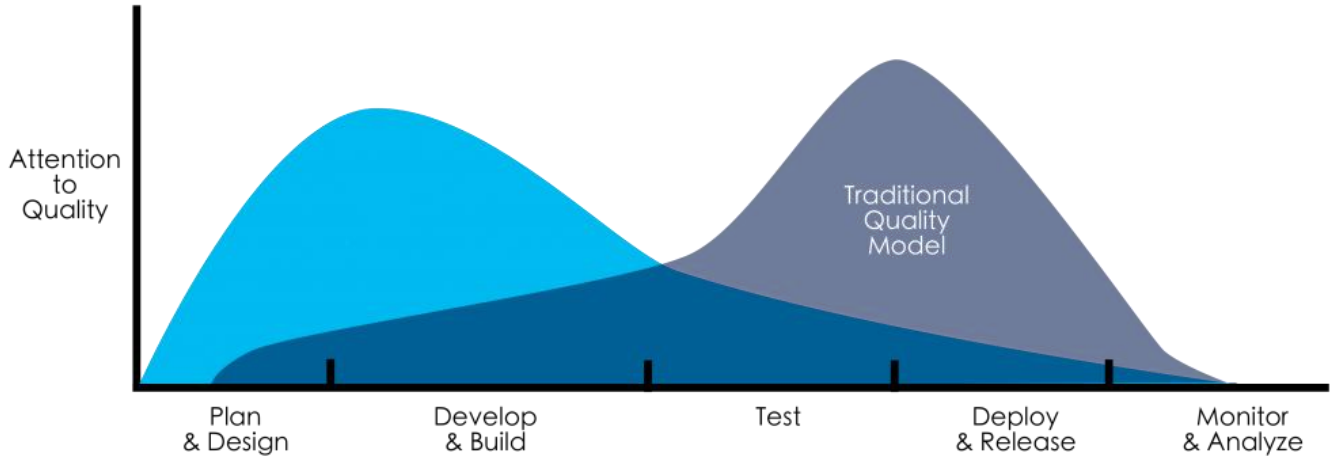
FIPS 140-3™

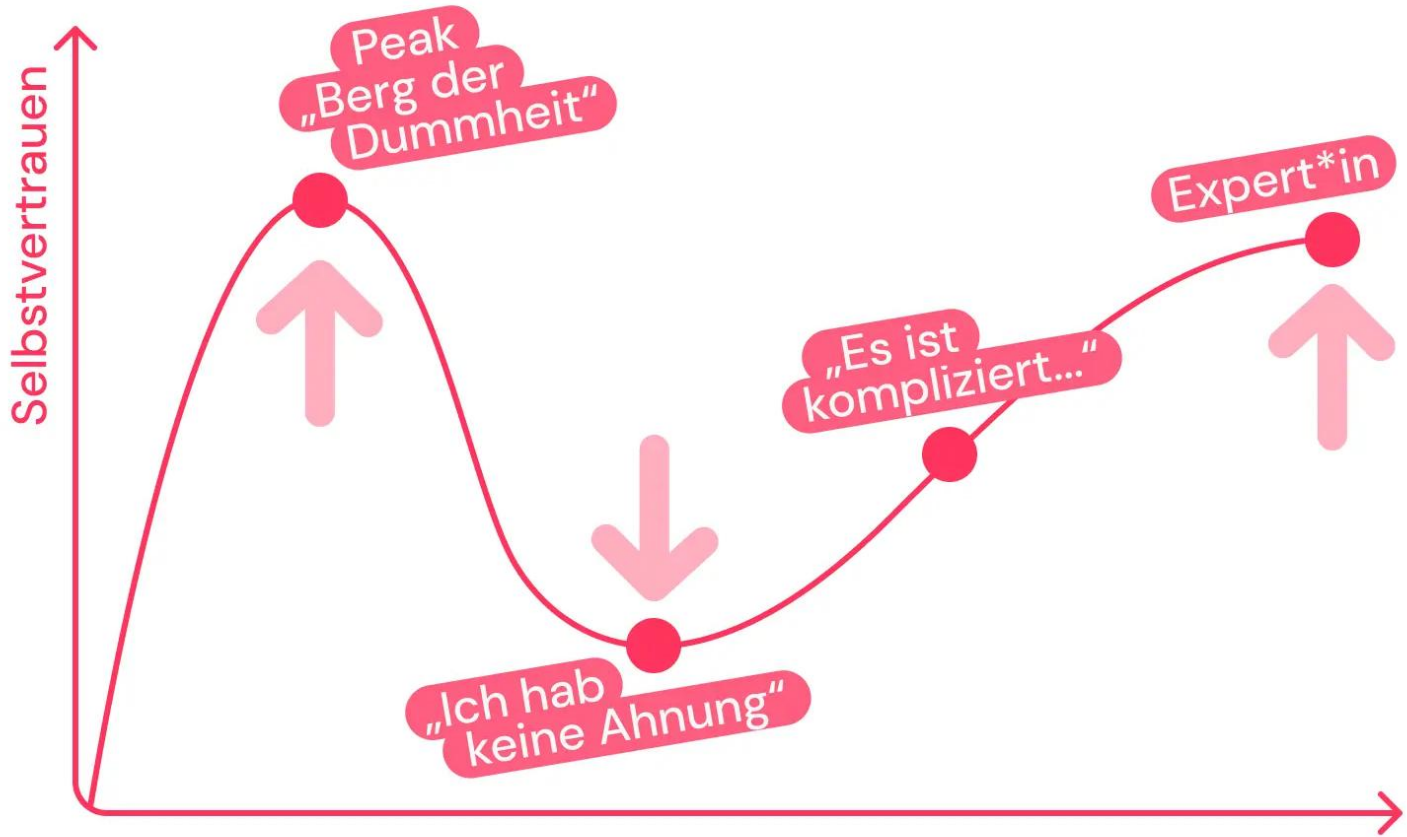
HoliSec




Honeypot


6 2 7

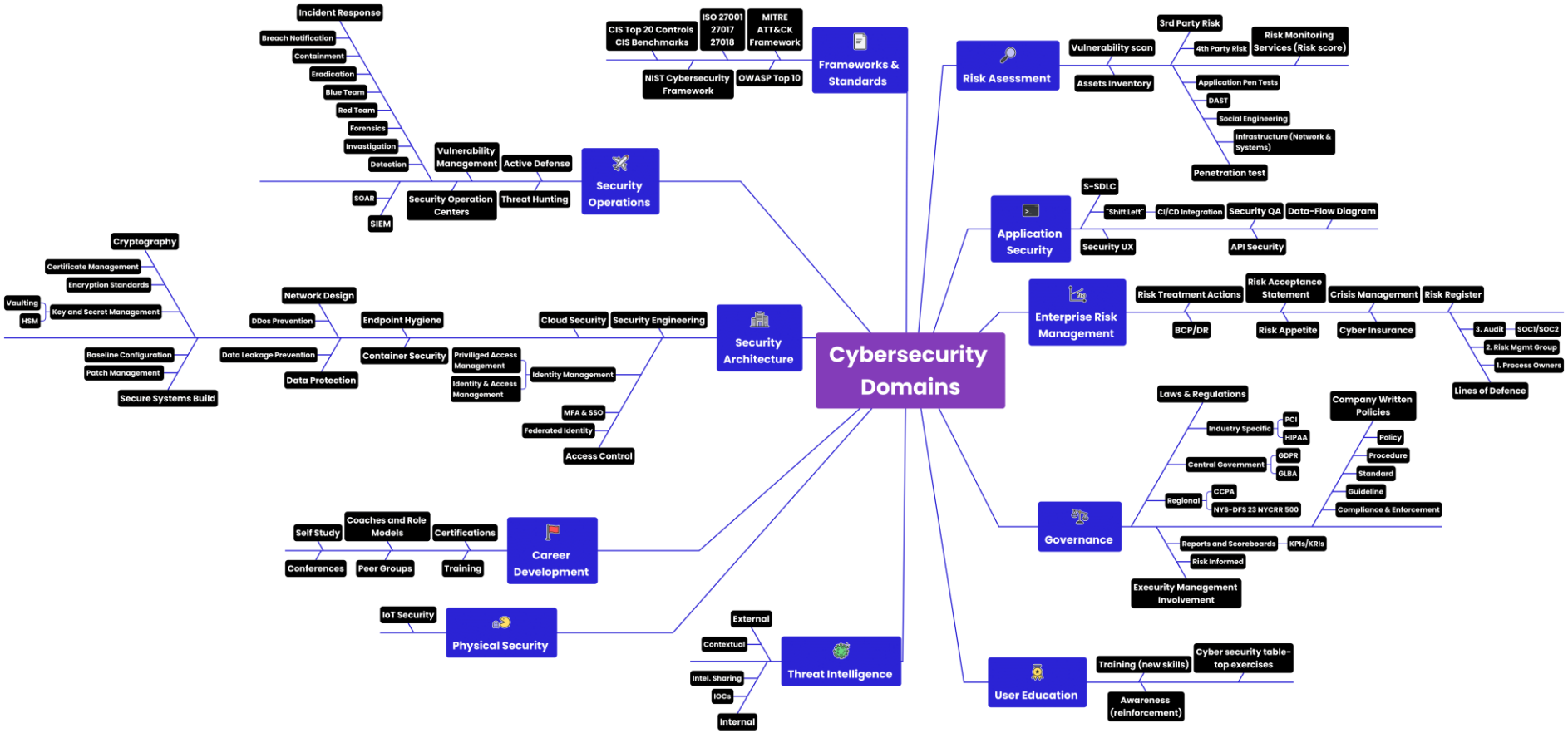

Attention
to
Quality
Traditional
Quality
Model
Plan
& Design
Develop
& Build
Test
Deploy
& Release
Monitor
& Analyze


Selbstvertrauen
Peak „Berg der Dummheit“
„Ich hab keine Ahnung“
„Es ist kompliziert...“
Expert*in

HoliSec

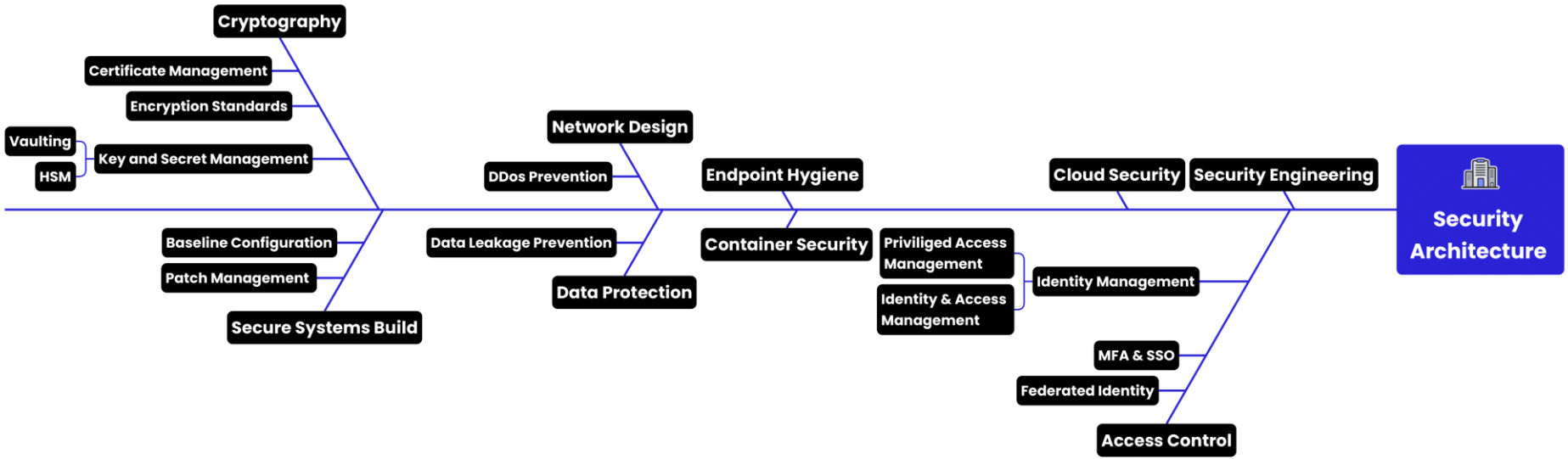
Was ist Compliance für euch?

HoliSec

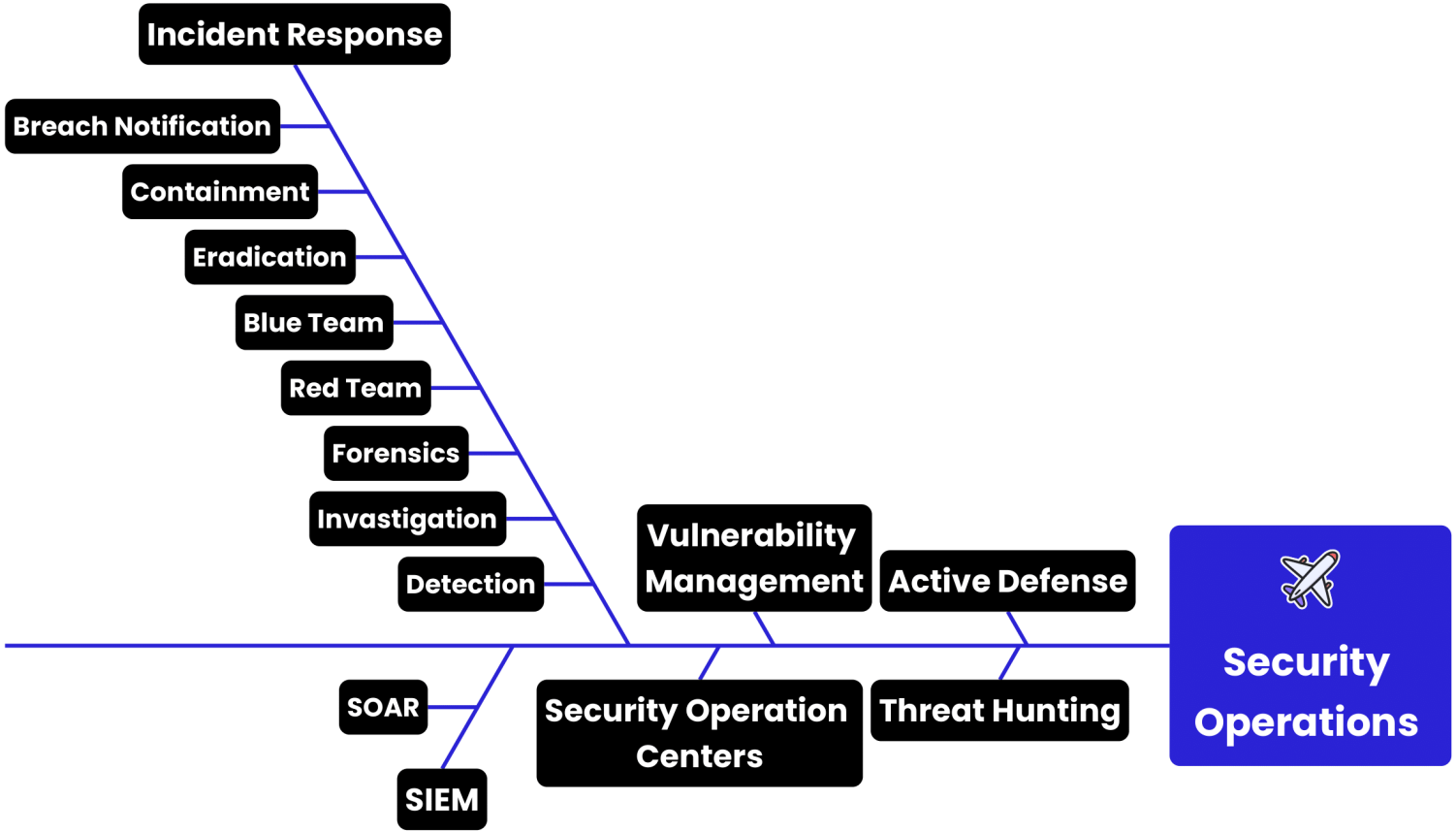


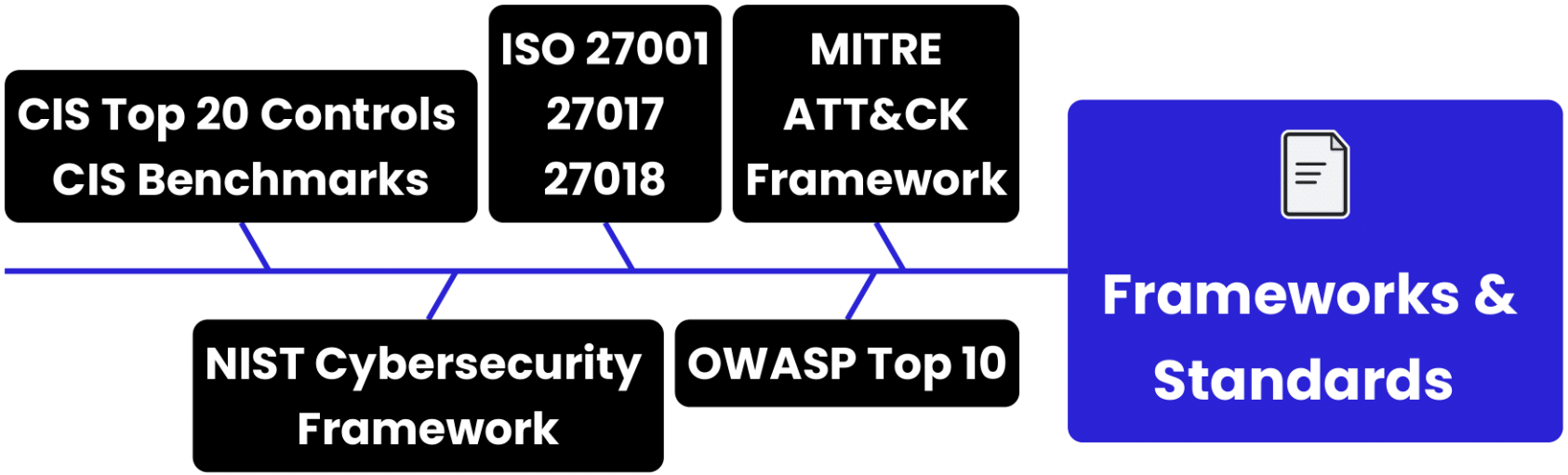
HoliSec

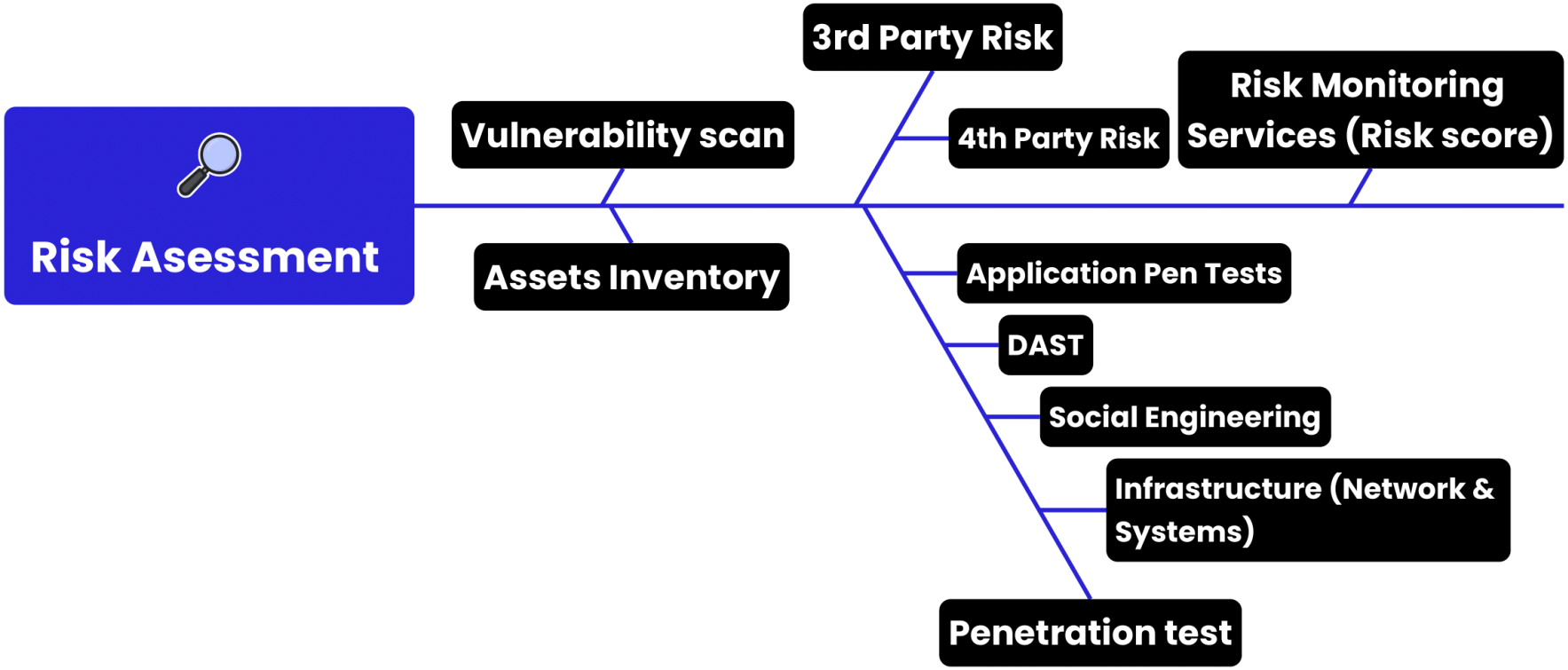
Quelle: https://www.linkedin.com/pulse/cybersecurity-domain-map-ver-30-henry-jiang/


Cryptography
Certificate Management
Encryption Standards
Vaulting
HSM
Key and Secret Management
Baseline Configuration
Patch Management
Secure Systems Build
Network Design
DDos Prevention
Data Leakage Prevention
Data Protection
Endpoint Hygiene
Container Security
Cloud Security
Security Engineering
Priviliged Access Management
Identity & Access Management
Identity Management
MFA & SSO
Federated Identity
Access Control
Security Architecture

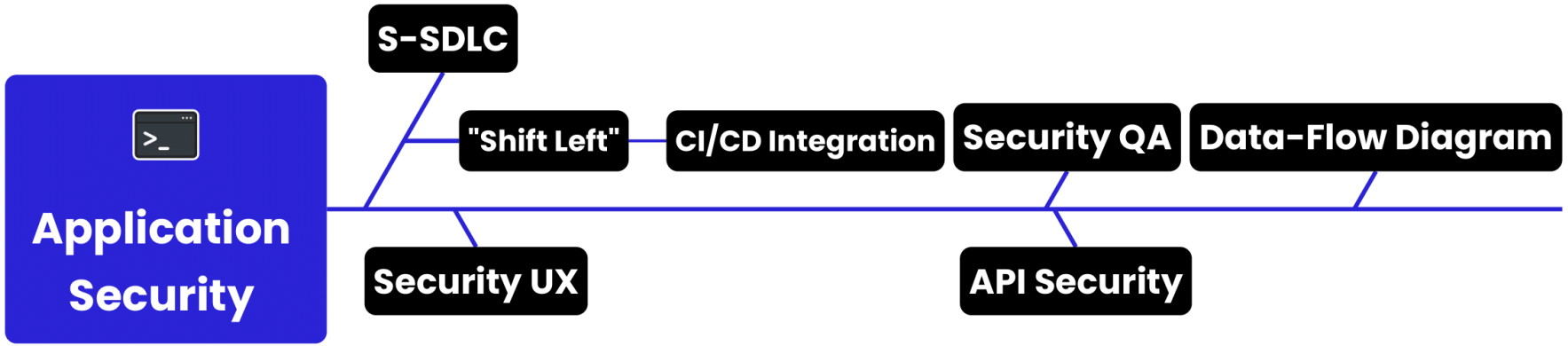
HoliSec

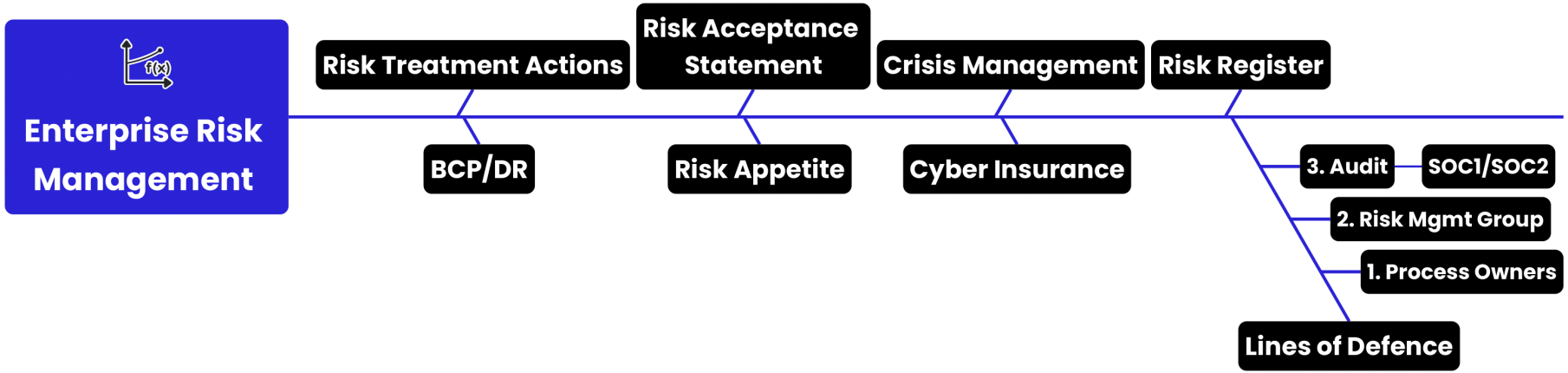

Incident Response
Breach Notification
Containment
Eradication
Blue Team
Red Team
Forensics
Invastigation
Detection
Vulnerability Management
Active Defense
Security Operations
SOAR
SIEM
Security Operation Centers
Threat Hunting

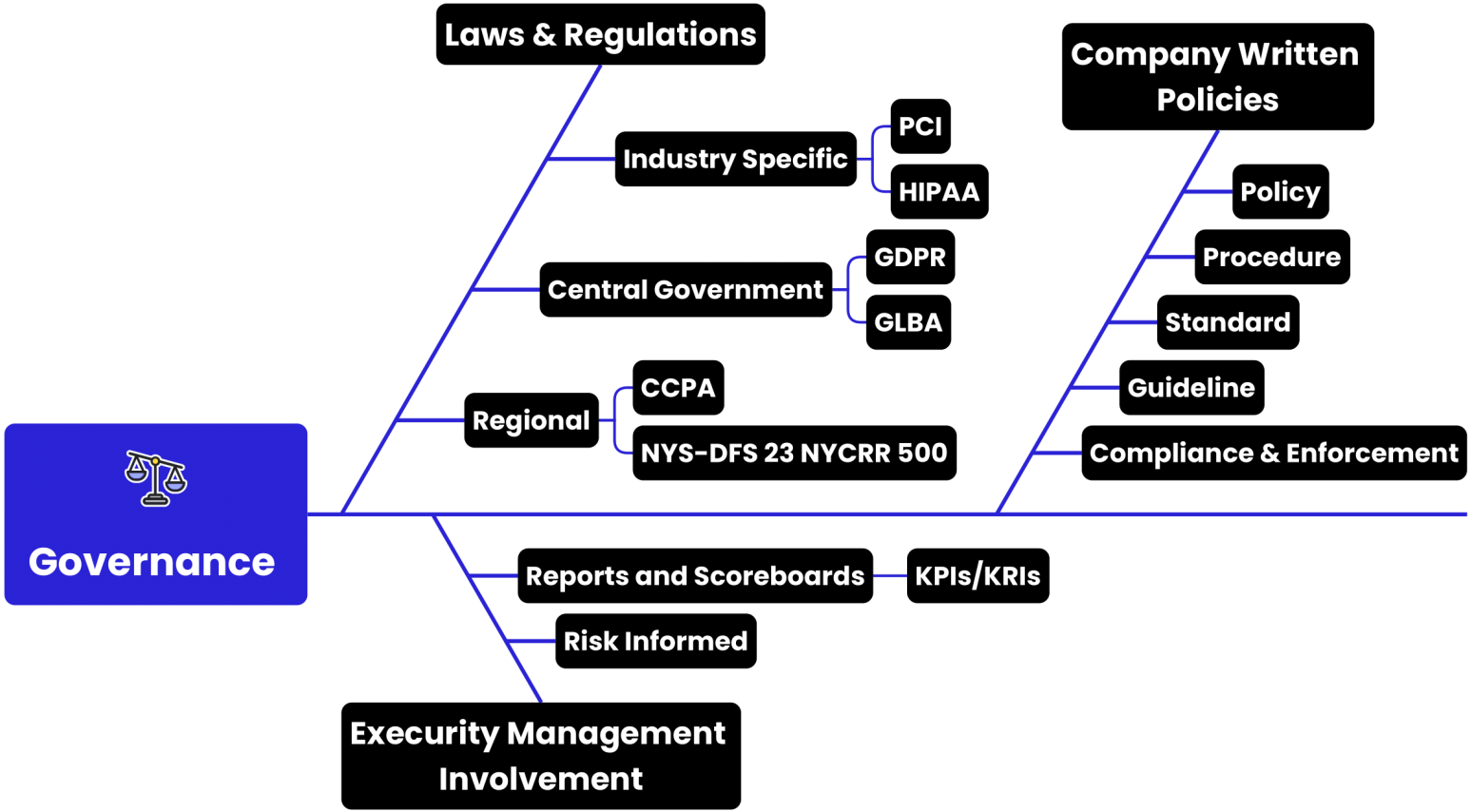

CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
MITRE
ATT&CK
Framework
NIST Cybersecurity
Framework
OWASP Top 10
Frameworks &
Standards

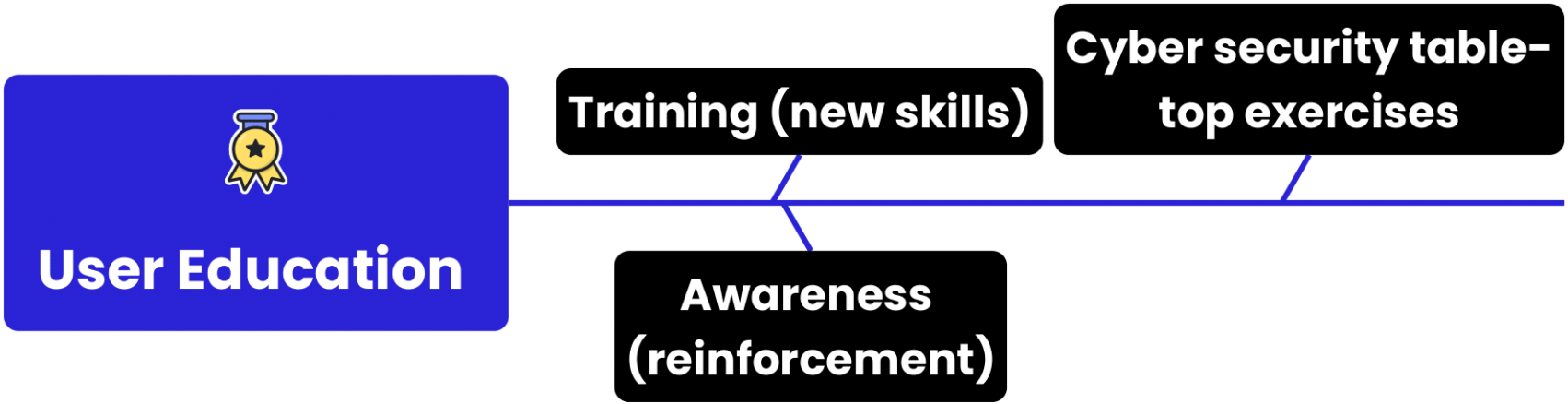

Risk Asessment
Vulnerability scan
Assets Inventory
3rd Party Risk
4th Party Risk
Risk Monitoring Services (Risk score)
Application Pen Tests
DAST
Social Engineering
Infrastructure (Network & Systems)
Penetration test

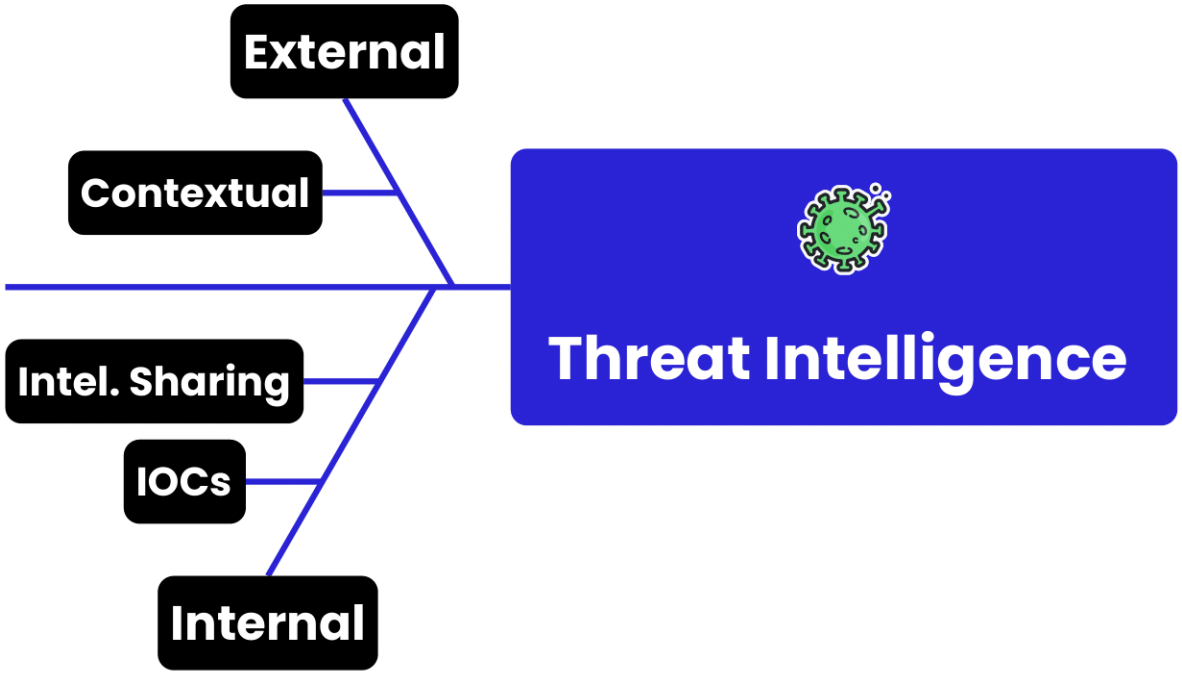
HoliSec


Application Security
S-SDLC
"Shift Left"
CI/CD Integration
Security QA
Data-Flow Diagram
Security UX
API Security


Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Crisis Management
Risk Register
BCP/DR
Risk Appetite
Cyber Insurance
3. Audit
SOC1/SOC2
2. Risk Mgmt Group
1. Process Owners
Lines of Defence

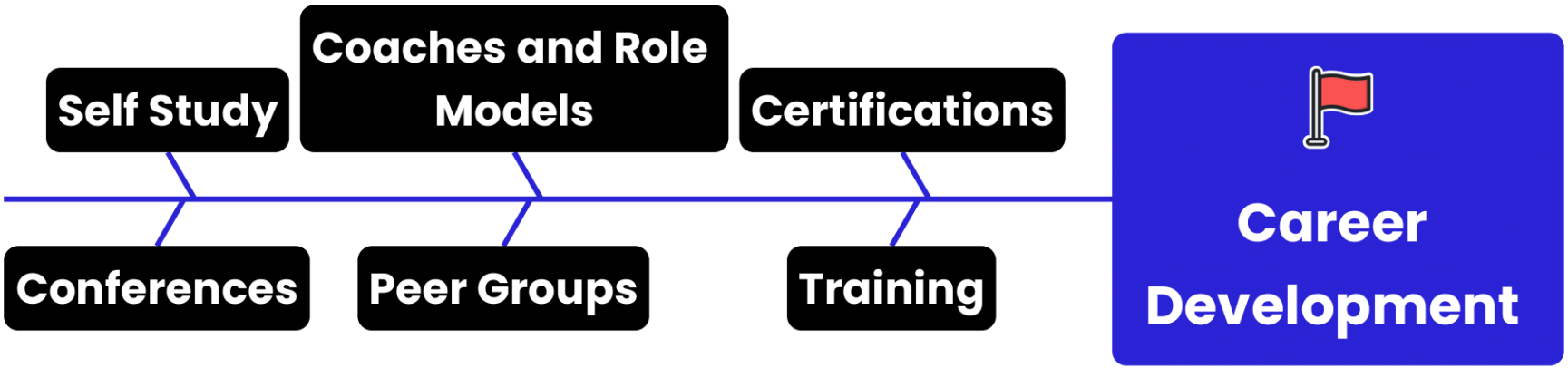

Governance
Laws & Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Company Written Policies
Policy
Procedure
Standard
Guideline
Compliance & Enforcement
Reports and Scoreboards
KPIs/KRIs
Risk Informed
Execurity Management Involvement


User Education
Training (new skills)
Cyber security table-top exercises
Awareness (reinforcement)


External
Contextual
Intel. Sharing
IOCs
Internal
Threat Intelligence

IoT Security

Physical Security


Self Study
Coaches and Role Models
Certifications
Conferences
Peer Groups
Training
Career Development

Welchen Zusammenhang gibt es zu CyberSec?

… oder ist das alles nur mühsamer Overhead?

HoliSec

Inhalte 📦

Inhalte 📦

Cyberangriffe

Inhalte 📦

NIS2 Richtlinie

Inhalte 📦

Datensicherheit

Inhalte 📦

Operationalize Security

Inhalte 📦

Cyberangriff

NIS 2 Richtlinie

Datensicherheit

Operationalize Security

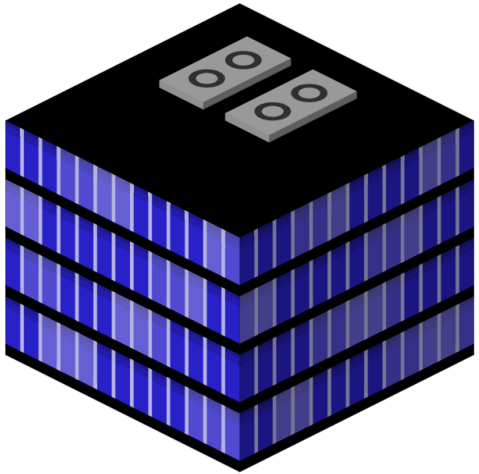
Inhalte 📦

Cyberangriffe | **NIS 2 Richtlinie** | **Datensicherheit** | **Operationalize Security**

Cyberangriffe 

und wie man im Notfall reagiert.

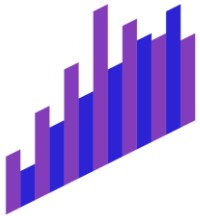
Warum werden Unternehmen gehackt?



Ghost Tech 👻

Mitarbeiter

Programme



Werbung

Wie werden Unternehmen gehackt?

vs.

HoliSec

Lernziele 🚀

- Was sind die wichtigsten Arten von Cyberangriffen?
- Wie erkenne ich Cyberangriffe?
- Was ist zu tun, wenn ich von einem Cyberangriff betroffen bin?

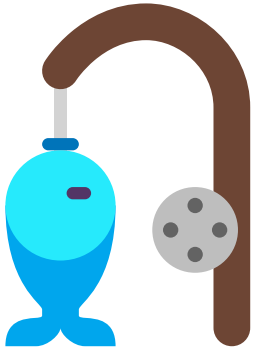
Welche Cyber Angriffsarten kennt Ihr?

Gängigste Cyberangriffe

2024

HoliSec

Phishing



Phishing nutzt Täuschung via E-Mails, Nachrichten oder Websites, um sensible Daten zu stehlen.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Phishing

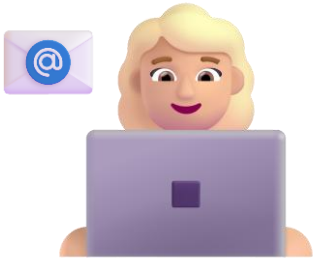
Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Phishing

Hacker



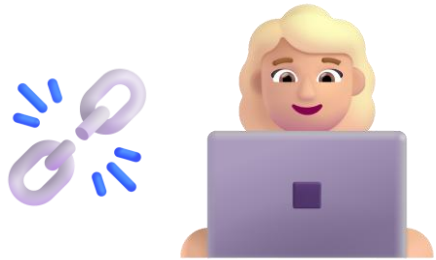
Ziel

1. Hacker sendet Phishing-Mail mit Link.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker



Ziel

2. Benutzer öffnet Link.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

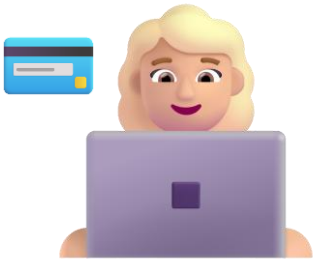
Ziel

2. Benutzer öffnet Link.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker



Ziel

3. Hacker sammelt Benutzerdaten ein.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

3. Hacker sammelt Benutzerdaten ein.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

💳

Ziel

4. Hacker verwendet Benutzerdaten.

Quelle: https://cybersecuritynews.com/

Phishing

Hacker

Ziel

4. Hacker verwendet Benutzerdaten.

Quelle: https://cybersecuritynews.com/

Ransomware

Schadhafter Code, der Daten verschlüsseln kann und für deren Entschlüsselung ein Lösegeld verlangt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

1. Hacker bringt Malware auf Computer von Ziel.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

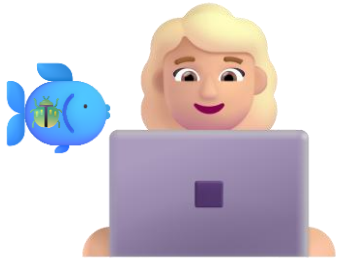
Ziel

1. Zum Beispiel durch Phishing.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



Ziel

1. Zum Beispiel durch Phishing.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

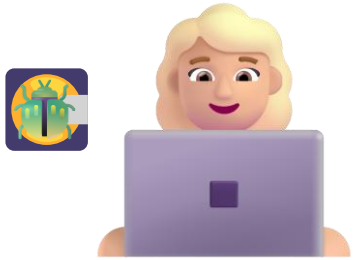
Ziel

1. Oder einem infizierten USB-Stick.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



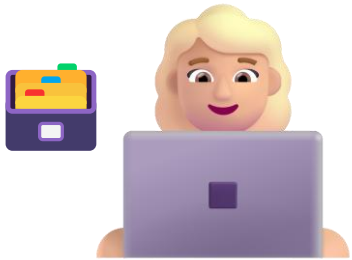
Ziel

1. Oder einem infizierten USB-Stick.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker

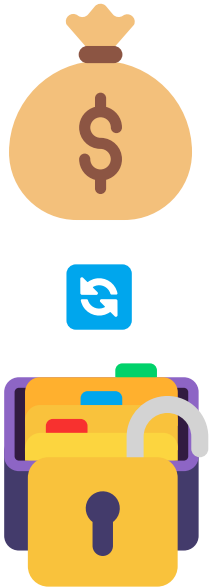
Ziel

2. Daten von Benutzer werden verschlüsselt.

Quelle: https://cybersecuritynews.com/

Ransomware

Hacker



Ziel

3. Hacker fordert Lösegeld für Entschlüsselung.

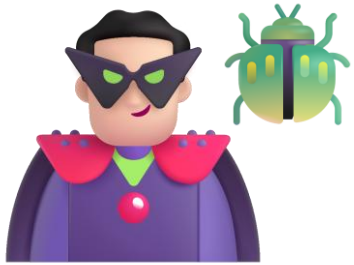
Quelle: https://cybersecuritynews.com/

Denial of Service

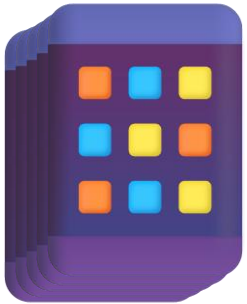
Eine Überlastung von Server oder Netzwerk verursachen, sodass diese nicht mehr ordnungsgemäß funktionieren.

Quelle: https://cybersecuritynews.com/

Denial of Service



Hacker

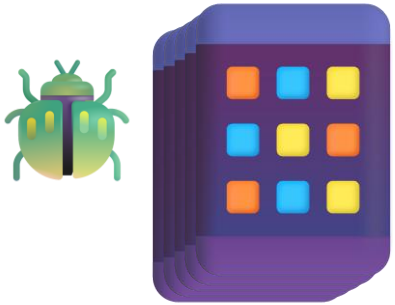


Ziel

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker



Ziel

1. Hacker kompromittiert viele Geräte mit Malware.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

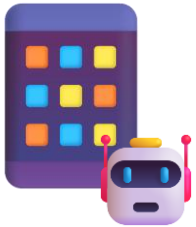
Ziel

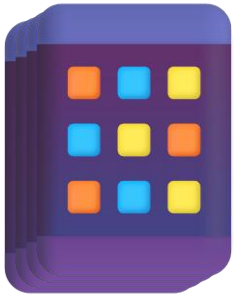
1. Hacker kompromittiert viele Geräte mit Malware.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker





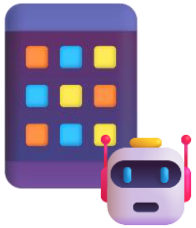
Ziel

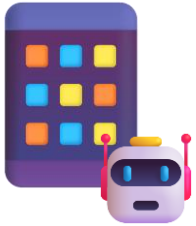
2. Hacker schließt Geräte zu „bot net“ zusammen.

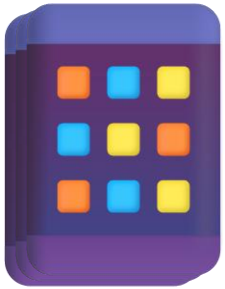
Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker







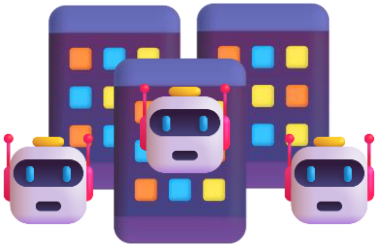
Ziel

2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker



Ziel

2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

2. Hacker schließt Geräte zu „bot net“ zusammen.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

3. Hacker greift mit „bot net“ an.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

3. Hacker greift mit „bot net“ an.

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

4. Ziel Service wird beeinträchtigt.

HoliSec

Quelle: https://cybersecuritynews.com/

Denial of Service

Hacker

Ziel

4. Ziel Service wird beeinträchtigt.

HoliSec

Quelle: https://cybersecuritynews.com/

CEO Fraud

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

CEO Fraud

Geld- oder Datenklau durch gefälschte Anweisungen von Führungskräften.

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

CEO Fraud

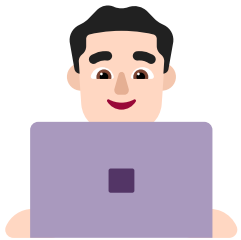
Hacker

Ziel

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker



Ziel

1. Hacker gibt sich als CEO aus.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

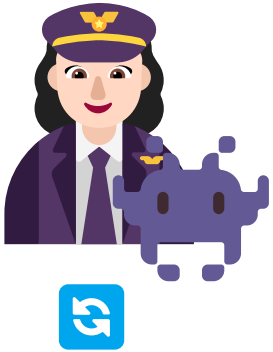
Ziel

1. Hacker gibt sich als CEO aus.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker



Ziel

1. Zum Beispiel mit AI-Voice.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

Ziel

2. Hacker kontaktiert Mitarbeiter.

Quelle: https://cybersecuritynews.com/

CEO Fraud

Hacker

Ziel

2. Hacker kontaktiert Mitarbeiter.

Quelle: https://cybersecuritynews.com/

CEO Fraud

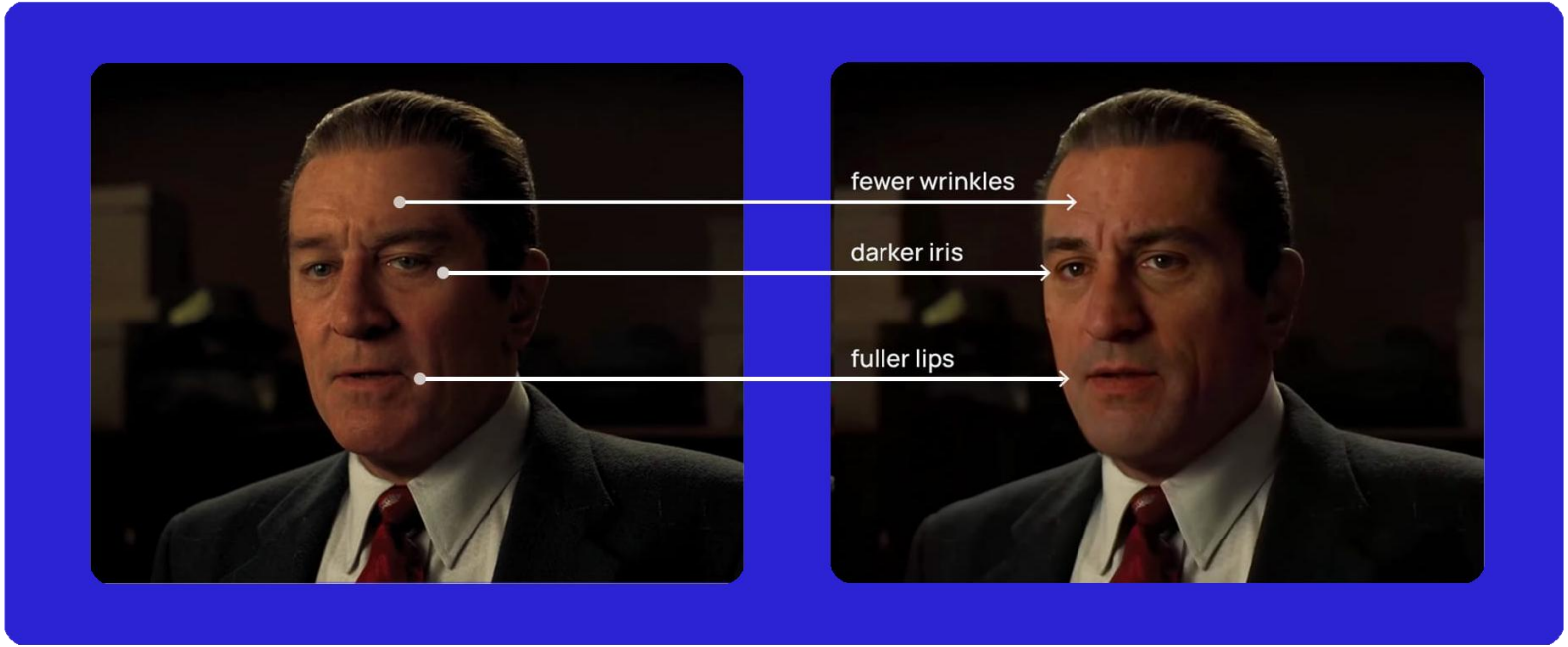
Hacker

Ziel

3. Hacker fordert Geld oder Daten als „CEO“.

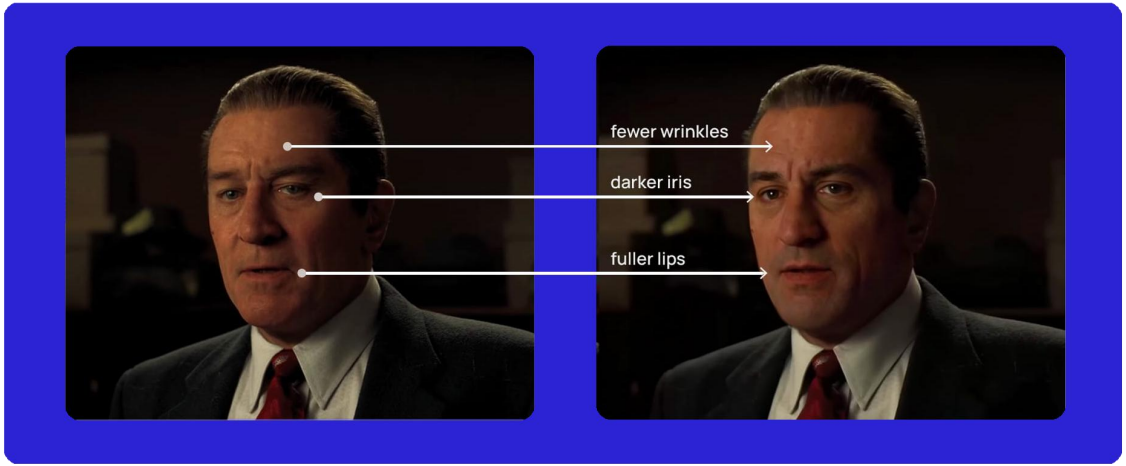
Quelle: https://cybersecuritynews.com/

AI & Deepfakes



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

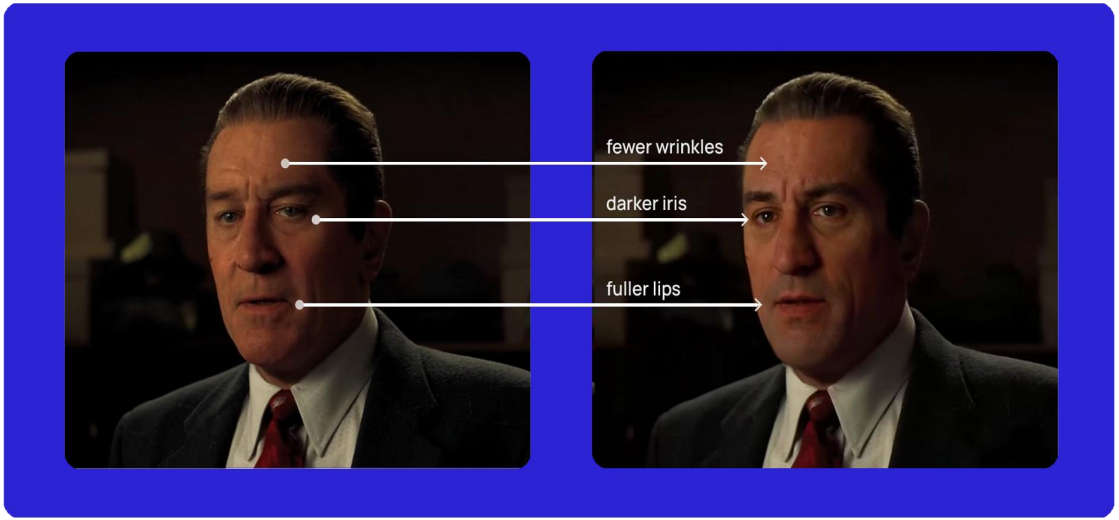
AI & Deepfakes



Fälschung von Videos/Audio zur Täuschung.

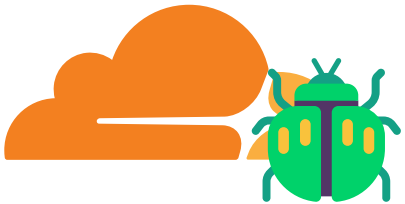
Quelle: https://sosafe-awareness.com/blog/how-to-spot-a-deepfake/

AI & Deepfakes



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

DNS Spoofing



Umleitung auf gefälschte Websites, um Daten abzufangen.

Quelle: https://cybersecuritynews.com/

Was ist DNS ?

Was ist DNS?

Domain **N**ame **S**ystem

Quelle: https://www.cloudflare.com/learning/dns/what-is-dns/

Was ist DNS?

Name

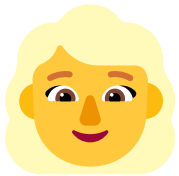
IP-Adresse

www.[kunde].at

10.231.10.114

Quelle: https://www.cloudflare.com/learning/dns/what-is-dns/

Was ist DNS?



Name

IP-Adresse

www.[kunde].at

10.231.10.114

Quelle: https://www.cloudflare.com/learning/dns/what-is-dns/

Live Demo 

DNS Spoofing

Zeit für ein Quiz! 

Jetzt seid Ihr dran! 🚀

Praxisübung - Phishing Research

Ablauf ⏩

- Durchsuche deinen eigenen E-Mail-Account (auch den Spam-Ordner) nach verdächtigen Mails.

Dokumentation 📄

- Merkmale, warum denkst du, es handelt sich um eine Phishing Mail?

Zeit & Format 🕛

- 10 min Recherche
- 5 min Präsentation

Exkurs – Betrugswarnungen

WKO

Kontakt Anmelden

Transforma... Digitalisierung Nachhaltigkeit Startups Creative Industries Innovation Kärnten

Aktuelle Betrugswarnungen für Unternehmen

Übersicht irreführend gestalteter Aussendungen, Betrugsversuchen, Phishing...

Lesedauer: 3 Minuten

© christianchan | stock.adobe.com

17.01.2023

HoliSec

Cyberbedrohungen 2030

HoliSec


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.

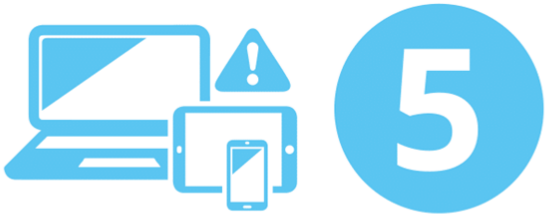
?

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



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

Live Demo 

Reconnaissance

Jetzt seid Ihr dran! 🚀

Praxisübung - Reconnaissance

Ablauf ⏩

- Finde öffentliche Informationen zu deinem Unternehmen heraus.

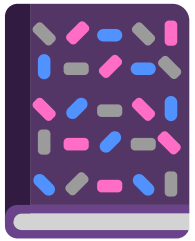
Dokumentation 📄

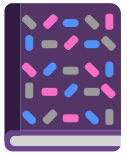
- verwertbare Informationen & potentielle Angriffsvektoren

Zeit & Format 🕛

- 10 min Recherche
- 5 min Diskussion

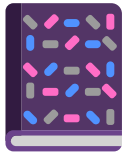
Wichtige Begriffe in der Cyber Security





Cybersecurity

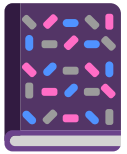
Wichtige Begriffe in der Cyber Security



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

Awareness

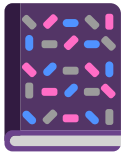
Wichtige Begriffe in der Cyber Security



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

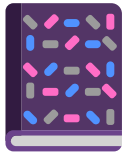
Awareness: Das Bewusstsein für Cybersecurity-Risiken und die Bedeutung sicherer Verhaltensweisen im digitalen Umfeld.

Wichtige Begriffe in der Cyber Security



Angriffsvektoren

Wichtige Begriffe in der Cyber Security



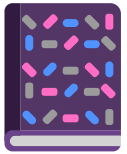
Cybersecurity: Der Schutz von Computersystemen, Netzwerken und Daten vor Diebstahl, Beschädigung oder unbefugtem Zugriff.

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

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.

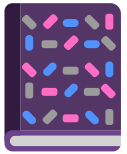
Angriffsvektoren: Die verschiedenen Methoden und Techniken, die von Angreifern verwendet werden, um in Computersysteme einzudringen oder sie zu kompromittieren.

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

Wichtige Begriffe in der Cyber Security

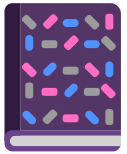


Malware: Schädliche Software, die dazu entwickelt wurde, in Computersysteme einzudringen und Schaden zu verursachen, wie z. B. Viren, Trojaner, Würmer und Ransomware.

Wichtige Begriffe in der Cyber Security

Social Engineering

Wichtige Begriffe in der Cyber Security



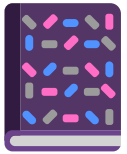
Malware: Schädliche Software, die dazu entwickelt wurde, in Computersysteme einzudringen und Schaden zu verursachen, wie z. B. Viren, Trojaner, Würmer und Ransomware.

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.

Wichtige Begriffe in der Cyber Security

Zero-Day-Exploits

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.

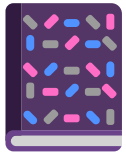
Social Engineering: Eine Methode, bei der Angreifer menschliche Manipulationstechniken einsetzen, um Informationen zu erhalten oder Zugang zu Systemen zu erlangen, indem sie sich als vertrauenswürdige Personen ausgeben oder das Vertrauen der Opfer gewinnen.

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

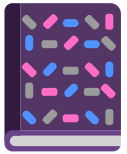
Firewall

Wichtige Begriffe in der Cyber Security



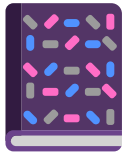
Firewall: Ein Sicherheitsmechanismus, der den Datenverkehr zwischen einem internen Netzwerk und externen Netzwerken überwacht und filtert, um unerwünschte Zugriffe zu verhindern.

Wichtige Begriffe in der Cyber Security



Multi-Faktor-Authentifizierung

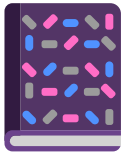
Wichtige Begriffe in der Cyber Security



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

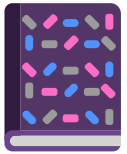
Multi-Faktor-Authentifizierung (MFA): Ein Sicherheitsverfahren, das mehrere Identitätsnachweise erfordert, um auf ein Konto oder eine Anwendung zuzugreifen, wie z. B. die Kombination aus Passwort und einem einmaligen Code, der per SMS oder App gesendet wird.

Wichtige Begriffe in der Cyber Security



Datenschutz

Wichtige Begriffe in der Cyber Security

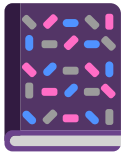


Firewall: Ein Sicherheitsmechanismus, der den Datenverkehr zwischen einem internen Netzwerk und externen Netzwerken überwacht und filtert, um unerwünschte Zugriffe zu verhindern.

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.

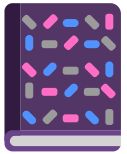
Datenschutz: Die Praxis, personenbezogene Daten zu schützen und sicherzustellen, dass sie angemessen verwendet, gespeichert und übertragen werden, um die Privatsphäre und die Rechte der Personen zu wahren.

Wichtige Begriffe in der Cyber Security



Verschlüsselung

Wichtige Begriffe in der Cyber Security

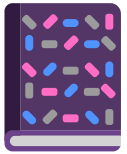


Verschlüsselung: Der Prozess der Umwandlung von lesbaren Informationen in eine nicht lesbare Form (Chiffre), um sie vor unbefugtem Zugriff zu schützen.

Wichtige Begriffe in der Cyber Security

Penetrationstest

Wichtige Begriffe in der Cyber Security



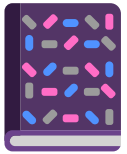
Verschlüsselung: Der Prozess der Umwandlung von lesbaren Informationen in eine nicht lesbare Form (Chiffre), um sie vor unbefugtem Zugriff zu schützen.

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

Wichtige Begriffe in der Cyber Security

Intrusion Detection System

Wichtige Begriffe in der Cyber Security

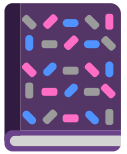


Verschlüsselung: Der Prozess der Umwandlung von lesbaren Informationen in eine nicht lesbare Form (Chiffre), um sie vor unbefugtem Zugriff zu schützen.

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

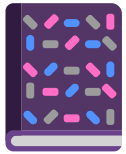
Intrusion Detection System (IDS): Eine Sicherheitssoftware oder -gerät, das den Datenverkehr in einem Netzwerk überwacht und nach Anzeichen von ungewöhnlichem oder verdächtigem Verhalten sucht, um potenzielle Angriffe zu erkennen.

Wichtige Begriffe in der Cyber Security



Intrusion Prevention System

Wichtige Begriffe in der Cyber Security

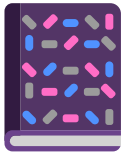


Intrusion Prevention System (IPS): Ein Sicherheitsmechanismus, der auf einem IDS aufbaut und aktiv Maßnahmen ergreift, um verdächtige Aktivitäten zu blockieren oder zu stoppen, bevor sie das Netzwerk erreichen.

Wichtige Begriffe in der Cyber Security

Patch

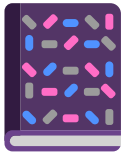
Wichtige Begriffe in der Cyber Security



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.

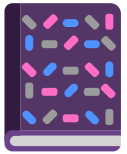
Patch: Ein Software-Update, das entwickelt wurde, um eine Schwachstelle in einem Programm oder Betriebssystem zu beheben und Sicherheitslücken zu schließen.

Wichtige Begriffe in der Cyber Security



Vulnerability Managament

Wichtige Begriffe in der Cyber Security

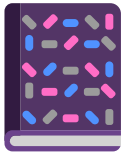


Intrusion Prevention System (IPS): Ein Sicherheitsmechanismus, der auf einem IDS aufbaut und aktiv Maßnahmen ergreift, um verdächtige Aktivitäten zu blockieren oder zu stoppen, bevor sie das Netzwerk erreichen.

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

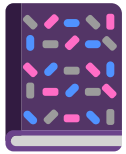
Vulnerability Management: Der Prozess der Identifizierung, Bewertung und Behandlung von Sicherheitslücken in Computersystemen, Anwendungen oder Netzwerken, um das Risiko von Cyberangriffen zu minimieren.

Wichtige Begriffe in der Cyber Security



Advanced Persistent Threats

Wichtige Begriffe in der Cyber Security

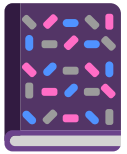


Advanced Persistent Threats: Advanced Persistent Threats (APTs) sind hochentwickelte und langfristig angelegte Cyberangriffe, die von gezielten Gegnern wie Nationen oder organisierten Kriminellen durchgeführt werden.

Wichtige Begriffe in der Cyber Security

Data Breach

Wichtige Begriffe in der Cyber Security

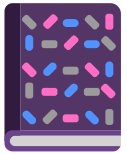


Advanced Persistent Threats: Advanced Persistent Threats (APTs) sind hochentwickelte und langfristig angelegte Cyberangriffe, die von gezielten Gegnern wie Nationen oder organisierten Kriminellen durchgeführt werden.

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

Deep Fake

Wichtige Begriffe in der Cyber Security

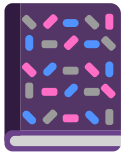


Advanced Persistent Threats: Advanced Persistent Threats (APTs) sind hochentwickelte und langfristig angelegte Cyberangriffe, die von gezielten Gegnern wie Nationen oder organisierten Kriminellen durchgeführt werden.

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

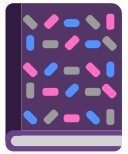
Deepfake: Eine Art von synthetischen Medien, die mithilfe von künstlicher Intelligenz erstellt werden, um das Aussehen und Verhalten einer Person in Videos, Bildern oder Audioaufnahmen zu manipulieren.

Wichtige Begriffe in der Cyber Security



Endpoint Security

Wichtige Begriffe in der Cyber Security

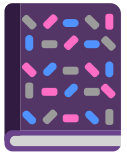


Endpoint Security: Die Sicherheitsmaßnahmen, die auf einzelnen Endgeräten wie Computern, Laptops, Tablets und Smartphones implementiert werden, um sie vor Bedrohungen und Angriffen zu schützen.

Wichtige Begriffe in der Cyber Security

Cyberhygiene

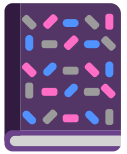
Wichtige Begriffe in der Cyber Security



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

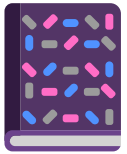
Cyberhygiene: Die Praxis der Einhaltung grundlegender Sicherheitsverfahren und -richtlinien, um das Risiko von Cyberangriffen zu reduzieren.

Wichtige Begriffe in der Cyber Security



Incident Response Plan

Wichtige Begriffe in der Cyber Security



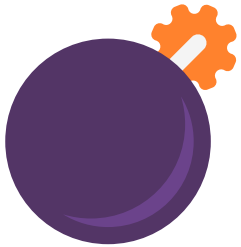
Endpoint Security: Die Sicherheitsmaßnahmen, die auf einzelnen Endgeräten wie Computern, Laptops, Tablets und Smartphones implementiert werden, um sie vor Bedrohungen und Angriffen zu schützen.

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.

Zeit für ein Quiz! 

Incident Response  



Was würdet ihr jetzt tun?

Was tun bei einem Angriff/Verdacht?

Öffnen von Links/Anhängen vermeiden

Was tun bei einem Angriff/Verdacht?

Öffnen von Links/Anhängen vermeiden

Ändern von Passwörtern inkl. Account Logout

Was tun bei einem Angriff/Verdacht?

Öffnen von Links/Anhängen vermeiden

Ändern von Passwörtern inkl. Account Logout

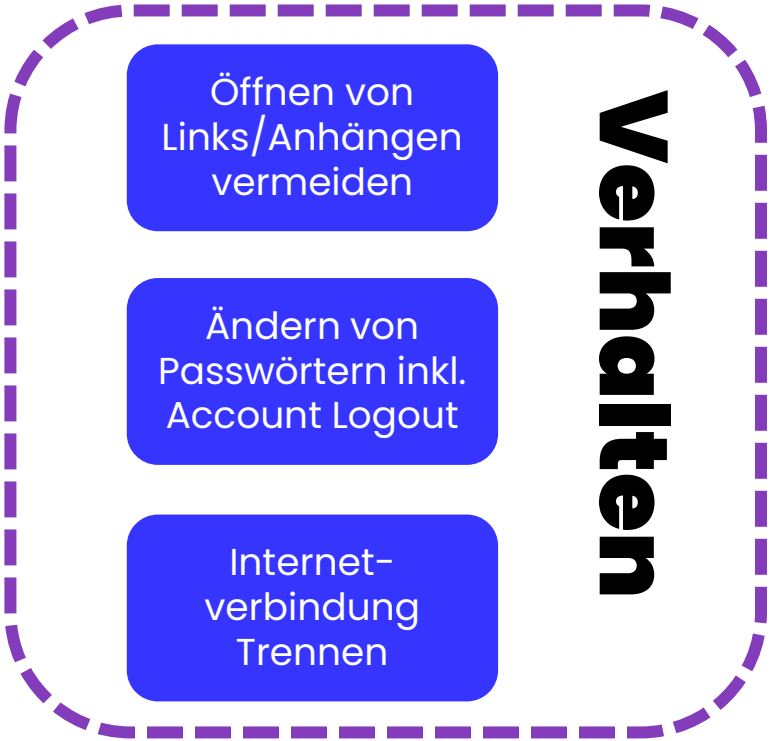
Internet-verbindung Trennen

Was tun bei einem Angriff/Verdacht?

- Öffnen von Links/Anhängen vermeiden
- Ändern von Passwörtern inkl. Account Logout
- Internet-verbindung Trennen

Verhalten

Was tun bei einem Angriff/Verdacht?



Was tun bei einem Angriff/Verdacht?

Mitarbeiter:innen verständigen

HoliSec

Was tun bei einem Angriff/Verdacht?

Mitarbeiter:innen verständigen

Nichts weiterleiten an andere

HoliSec

Was tun bei einem Angriff/Verdacht?

Mitarbeiter:innen verständigen

Nichts weiterleiten an andere

Stakeholder und ggf. Behörden verständigen

Was tun bei einem Angriff/Verdacht?

Meldung

- Mitarbeiter:innen verständigen
- Nichts weiterleiten an andere
- Stakeholder und ggf. Behörden verständigen

Was tun bei einem Angriff/Verdacht?

Verhalten

- Öffnen von Links/Anhängen vermeiden
- Ändern von Passwörtern inkl. Account Logout
- Internet-verbindung Trennen

Meldung

- Mitarbeiter:innen verständigen
- Nichts weiterleiten an andere
- Stakeholder und ggf. Behörden verständigen

Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Falls notwendig Backups einspielen

Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Security Einstellungen an Systemen prüfen

Falls notwendig Backups einspielen

Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Security Einstellungen an Systemen prüfen

Falls notwendig Backups einspielen

Datenschutz Meldung falls notwendig

Was tun nach einem Angriff/Verdacht?

Scan von Betriebssystem auf Malware

Security Einstellungen an Systemen prüfen

Falls notwendig Backups einspielen

Datenschutz Meldung falls notwendig

Nacharbeit

Regulärer Prozess eines Incidents 🔁

Incident Response Prozess

Incident

Incident Response Prozess

Incident

Ruhe bewahren

Incident Response Prozess

Incident

Ruhe bewahren

Incident Response Prozess

Meldung an relevante Beteiligte

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

Incident Response Prozess

Incident

Ruhe bewahren

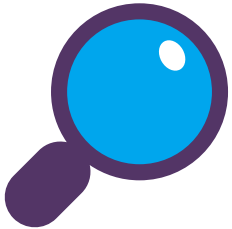
Meldung an relevante Beteiligte

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

HoliSec

Incident Response Prozess

Sammeln und filtern von Infos



Logs von Servern, Applikationen und Devices

Incident Response Prozess

Incident

Ruhe bewahren

Logs von Servern, Apps und Devices

Sammeln und filtern von Infos

Meldung an relevante Beteiligte

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

HoliSec

Incident Response Prozess

Entscheidung treffen

IT-Manager, GF

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

HoliSec

Incident Response Prozess

Hilfe anfordern

SOS

Expert:innen, Stakeholder?

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?

HoliSec

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

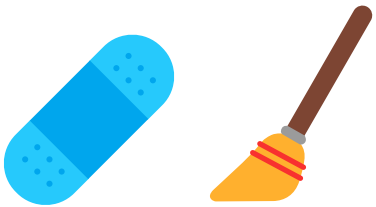
SOS

Expert:innen, Stakeholder?

HoliSec

Incident Response Prozess

Incident lösen & Aufräumen



MA, GF, IT, Stakeholder

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

HoliSec

Incident Response Prozess

Sicheren Kommunikationskanal verwenden

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

HoliSec

Incident Response Prozess

Durchstarten.

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

HoliSec

Jetzt seid Ihr dran! 🚀

Praxisübung - Business Continuity

Ablauf ⏩

- Überlegt euch, was ihr täglich zum Arbeiten benötigt. Hardware, Software und sonstige digitalen Assets.

Tipps 💡

- Geht einen normalen Arbeitstag durch und überlegt euch was ihr braucht.

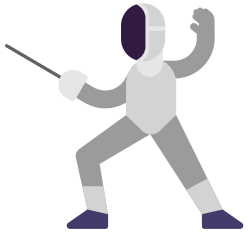
Dokumentation 📄

- Auflistung der Assets
- Klassifizierung nach Kritikalität

Zeit & Format 🕐

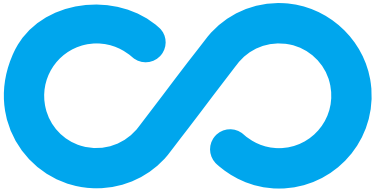
- 10 min
- 5 min Diskussion

HoliSec



Wie können wir uns schützen?

Ganzheitliches Bild von Cybersecurity



Security is Everywhere

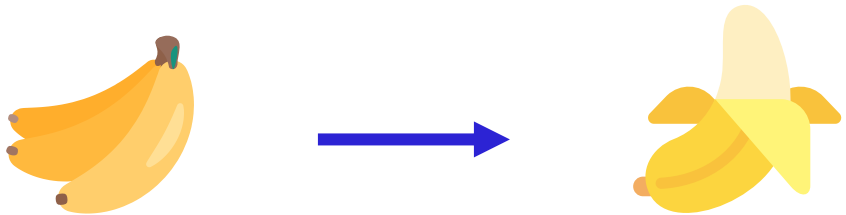
Ganzheitliches Bild von Cybersecurity

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

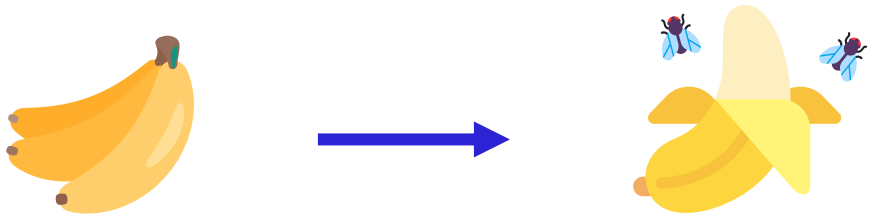
Die Bananenschale

Die Bananenschale

Die Bananenschale

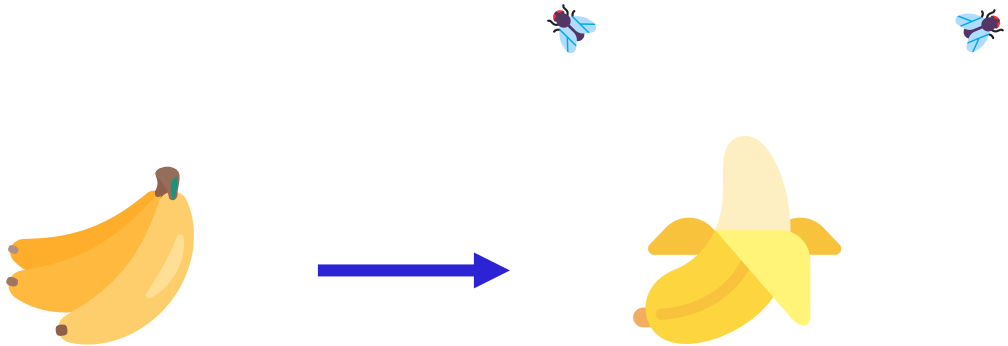


Die Bananenschale



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

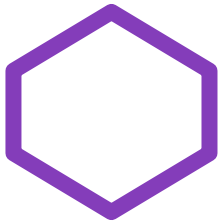
Ganzheitliches Bild von Cybersecurity

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.

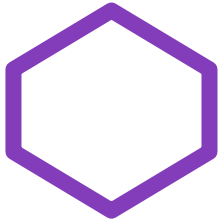
Hausverstand : Sicherheitsbewusstsein sollte bei jeder Person Teil davon sein.

Wie funktioniert das in der Praxis?



Cybersecurity 101

HoliSec

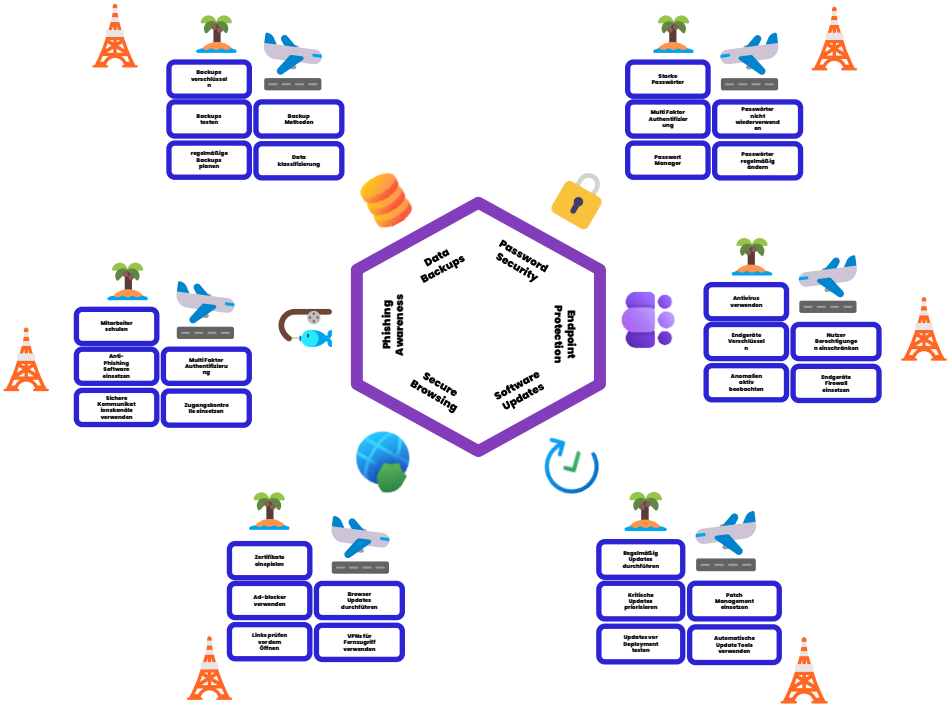


Cybersecurity 101

Überblick der wichtigsten Cybersecurity Maßnahmen

HoliSec

Cybersecurity 101



HoliSec

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

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

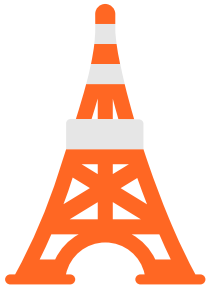
Kritische Updates priorisieren

Patch Management einsetzen

Updates vor Deployment testen

Automatische Update Tools verwenden

HoliSec



Backups verschlüsseln

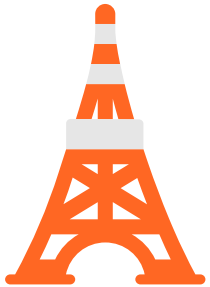
Backups testen

Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups



Backups verschlüsseln

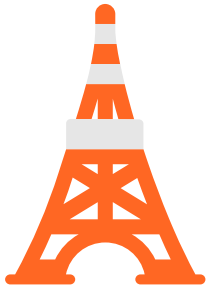
Backups testen

Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups



Backups verschlüsseln

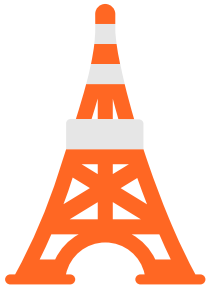
Backups testen

Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups



Backups verschlüsseln

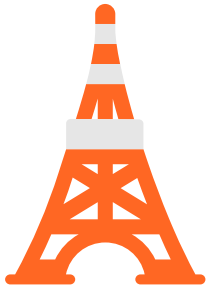
Backups testen

Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups



Backups verschlüsseln

Backups testen

Backup Methoden

regelmäßige Backups planen

Daten Klassifizierung

Data Backups

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

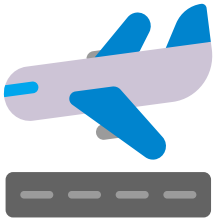
Patch Management einsetzen

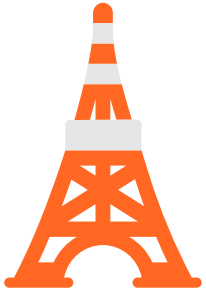
Updates vor Deployment testen

Automatische Update Tools verwenden

HoliSec

Passwort Security





Starke Passwörter

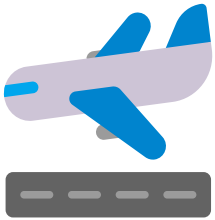
Multi Faktor Authentifizierung

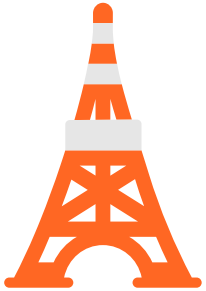
Passwörter nicht wiederverwenden

Passwort Manager

Passwörter regelmäßig ändern

Passwort Security





Starke Passwörter

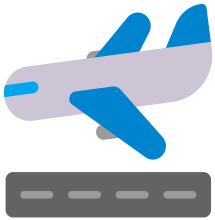
Multi Faktor Authentifizierung

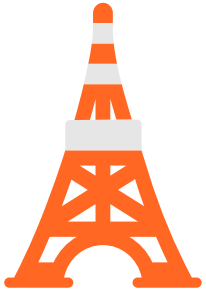
Passwörter nicht wiederverwenden

Passwort Manager

Passwörter regelmäßig ändern

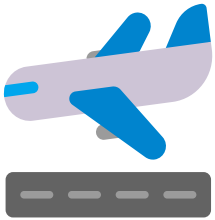
Passwort Security

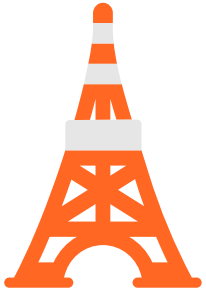




- Starke Passwörter
- Multi Faktor Authentifizierung
- Passwörter nicht wiederverwenden
- **Passwort Manager**
- Passwörter regelmäßig ändern

Passwort Security





Starke Passwörter

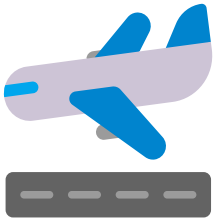
Multi Faktor Authentifizierung

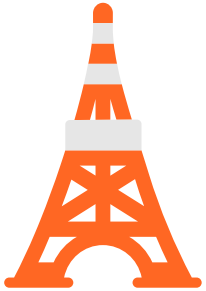
Passwort Manager

Passwörter nicht wiederverwenden

Passwörter regelmäßig ändern

Passwort Security





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

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

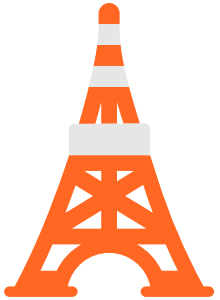
Patch Management einsetzen

Updates vor Deployment testen

Automatische Update Tools verwenden

HoliSec

Endpoint Protection



Antivirus verwenden

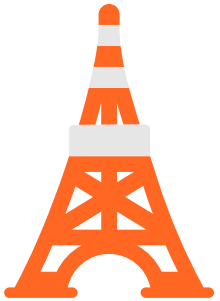
Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Endpoint Protection



Antivirus verwenden

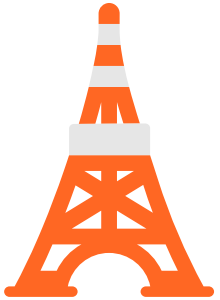
Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

Endgeräte Firewall einsetzen

Endpoint Protection



Antivirus verwenden

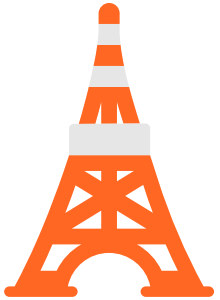
Endgeräte Verschlüsseln

Nutzer Berechtigungen einschränken

Anomalien aktiv beobachten

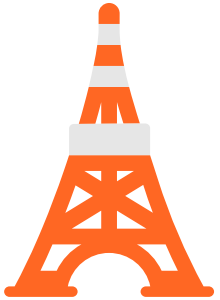
Endgeräte Firewall einsetzen

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

HoliSec

Software Updates

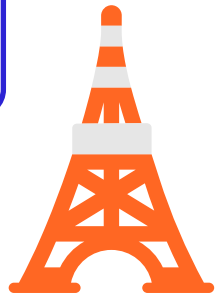
Regelmäßig Updates durchführen

kritische Updates priorisieren

Patch Management einsetzen

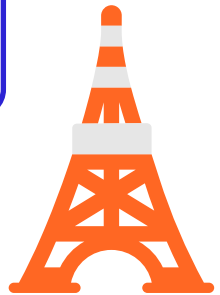
Updates vor Deployment testen

Automatische Update Tools verwenden



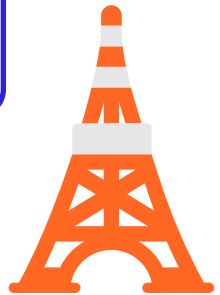
Software Updates

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



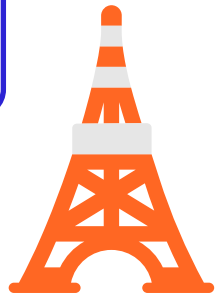
Software Updates

- 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

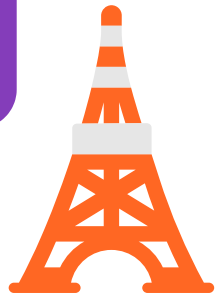
Regelmäßig Updates durchführen

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

HoliSec

Secure Browsing

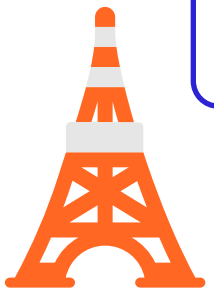
Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

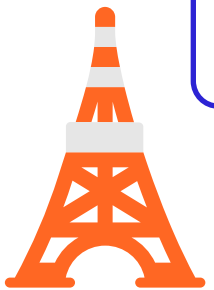
Links prüfen vor dem Öffnen

VPNs für Fernzugriff verwenden



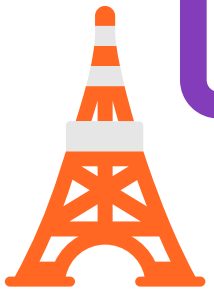
Secure Browsing

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



Secure Browsing

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



Secure Browsing

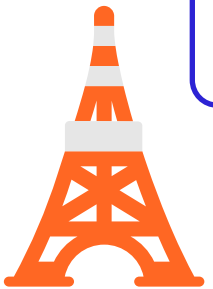
Zertifikate einspielen

Ad-blocker verwenden

Browser Updates durchführen

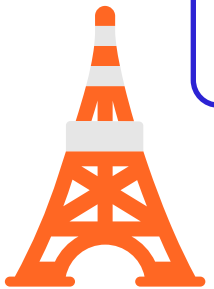
Links prüfen vor dem Öffnen

VPNs für Fernzugriff verwenden



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

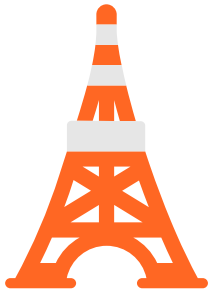
Patch Management einsetzen

Updates vor Deployment testen

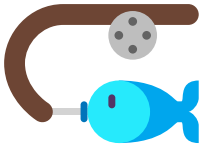
Automatische Update Tools verwenden

HoliSec

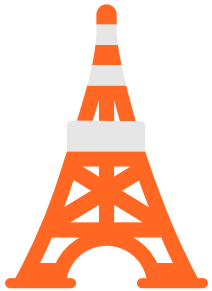
Phishing Awareness

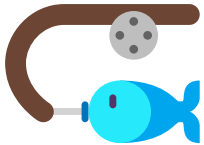


- **Mitarbeiter schulen**
- **Anti-Phishing Software einsetzen**
- **Multi Faktor Authentifizierung**
- **Sichere Kommunikationskanäle verwenden**
- **Zugangskontrolle einsetzen**



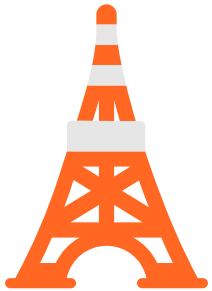
Phishing Awareness



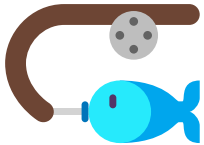


- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- Multi Faktor Authentifizierung
- Sichere Kommunikationskanäle verwenden
- Zugangskontrolle einsetzen

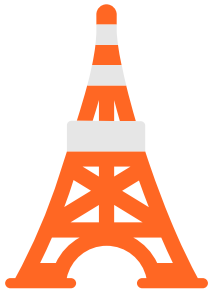
Phishing Awareness



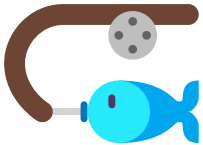
- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- Multi Faktor Authentifizierung
- Sichere Kommunikationskanäle verwenden
- Zugangskontrolle einsetzen



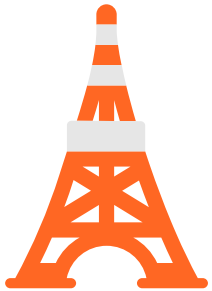
Phishing Awareness

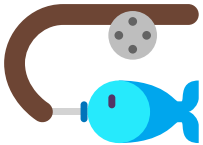


- Mitarbeiter schulen
- Anti-Phishing Software einsetzen
- Sichere Kommunikationskanäle verwenden
- **Multi Faktor Authentifizierung**
- Zugangskontrolle einsetzen



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

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

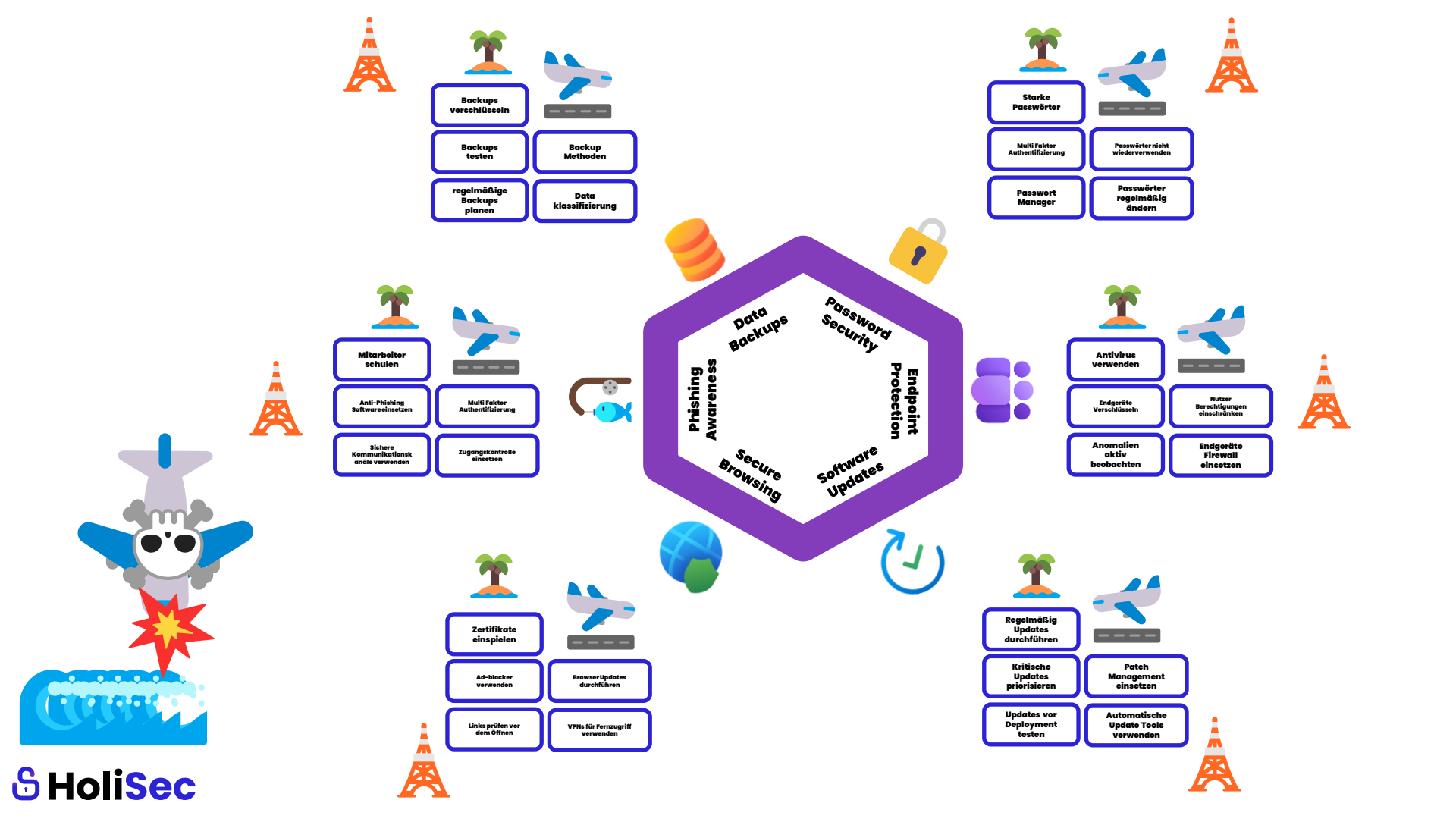
Kritische Updates priorisieren

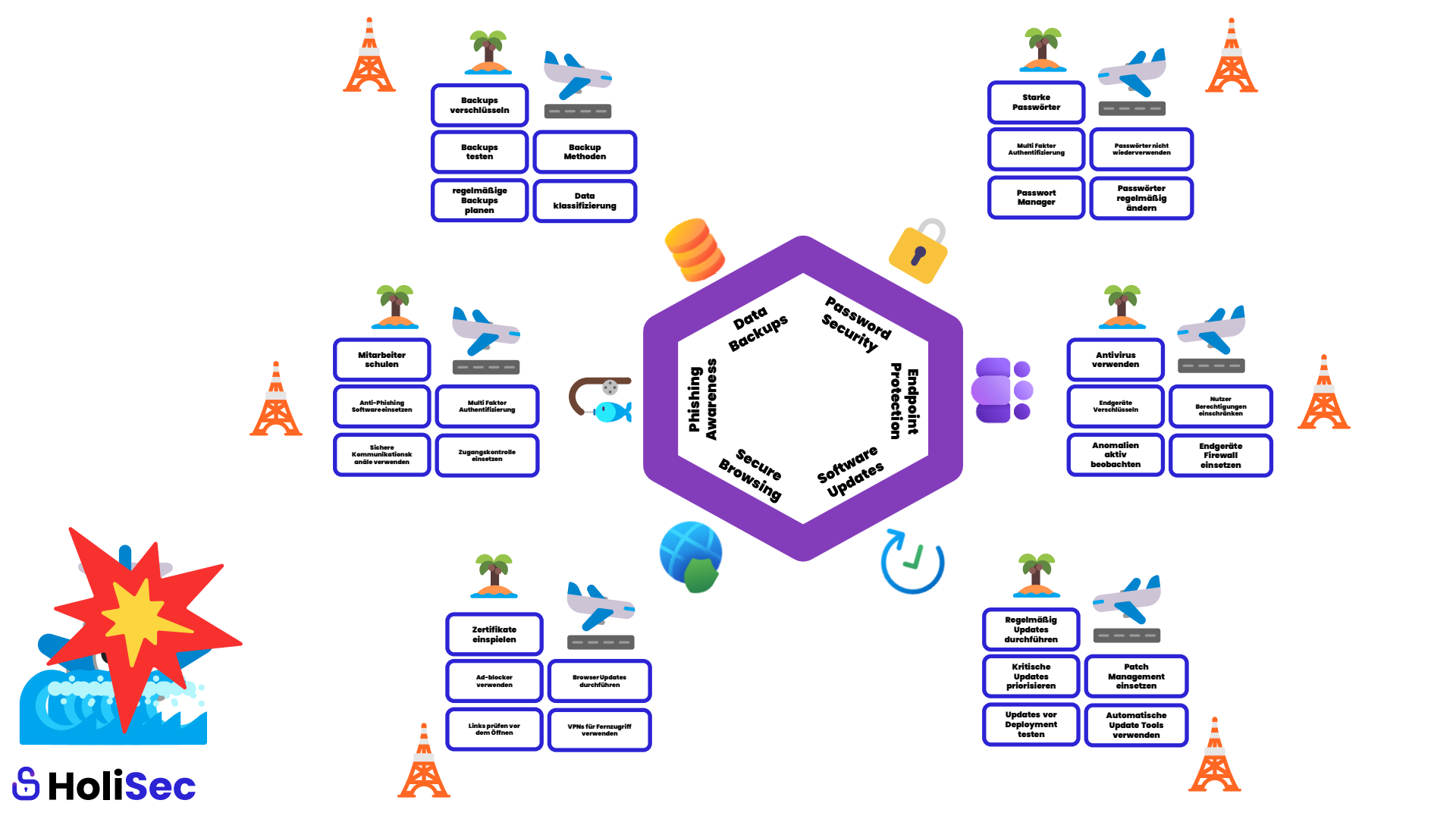
Patch Management einsetzen

Updates vor Deployment testen

Automatische Update Tools verwenden

HoliSec


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
HoliSec


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
HoliSec

Zeit für ein Quiz! 

Inhalte 📦

Cyberangriffe

NIS 2 Richtlinie

Datensicherheit

Operationalize Security

HoliSec

Inhalte 📦

Cyberangriffe

NIS 2 Richtlinie

Datensicherheit

Operationalize Security

Frameworks

und sonstige Maßnahmen der EU.

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

HoliSec

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

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

HoliSec

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

HoliSec

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

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 Regulierung ?

HoliSec

Richtlinie

EU Recht

Interpretation

Nationales Recht

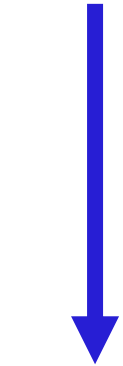
Gesetz

Unternehmen & Bürger

Verordnung

EU Recht

Gesetz



Unternehmen & Bürger

VS.

Richtlinie

EU Recht

Interpretation

Nationales Recht

Gesetz

Unternehmen & Bürger

HoliSec

Rechtsgrundlagen der EU

Verordnung

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

Richtlinie

- NIS 2

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

HoliSec

Ist die NIS2 eigentlich schon scharf geschalten?

NIS 2 – Timeline

NIS 1 Regulierung: 06.07.2016

NIS 2 – Timeline

⬇️

NIS 1
Regulierung:
06.07.2016

NIS 2 – Timeline

NIS 1 Umsetzung:
09.05.2018

NIS 2 – Timeline

NIS 1
Regulierung:
06.07.2016

NIS 1
Umsetzung:
09.05.2018

NIS 2 – Timeline

NIS 2 Regulierung:
14.12.2022

NIS 2 – Timeline

NIS 1
Regulierung:
06.07.2016

NIS 1
Umsetzung:
09.05.2018

NIS 2
Regulierung:
14.12.2022

NIS 2 – Timeline

NIS 2 nationale Deadline: 17.10.2024

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

Sitzung im NR am 12.12.2025 zu NISG 2026

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

Sitzung im NR am 12.12.2025 zu NISG 2026

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

NIS 1 vs. NIS 2

Unterscheidungsmerkmale

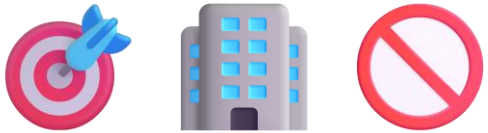
NIS 1 vs. NIS 2 – Unterscheidungsmerkmale

Betroffene Unternehmen

Lieferkette

Kleine & mittlere Unternehmen

Sanktionen



Betroffene Unternehmen

NIS 1	NIS 2
99 – Kritis	5000

NIS 1

Lieferkette

NIS 2

99 (Kritis)		5000
Nicht Betroffen	⬅ ➡	Betroffen

HoliSec


Kleine & mittlere Unternehmen

NIS 1

99 (Kritis)
Nicht Betroffen
Nicht geregelt

NIS 2

5000
Betroffen
Zertifizierbar

HoliSec

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

HoliSec

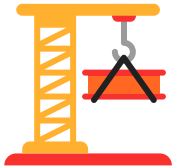
NIS 1 vs. NIS 2 – Unterschiede

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

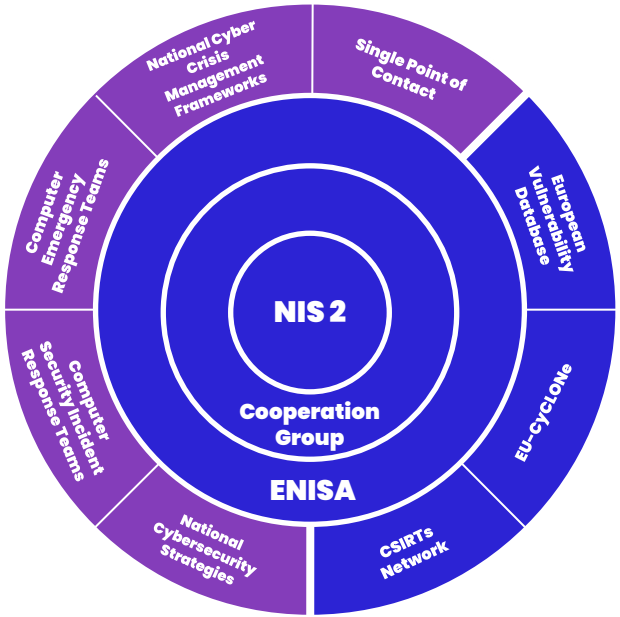
HoliSec



Was denkt ihr, wie ist die NIS2 Richtlinie aufgebaut ?

HoliSec

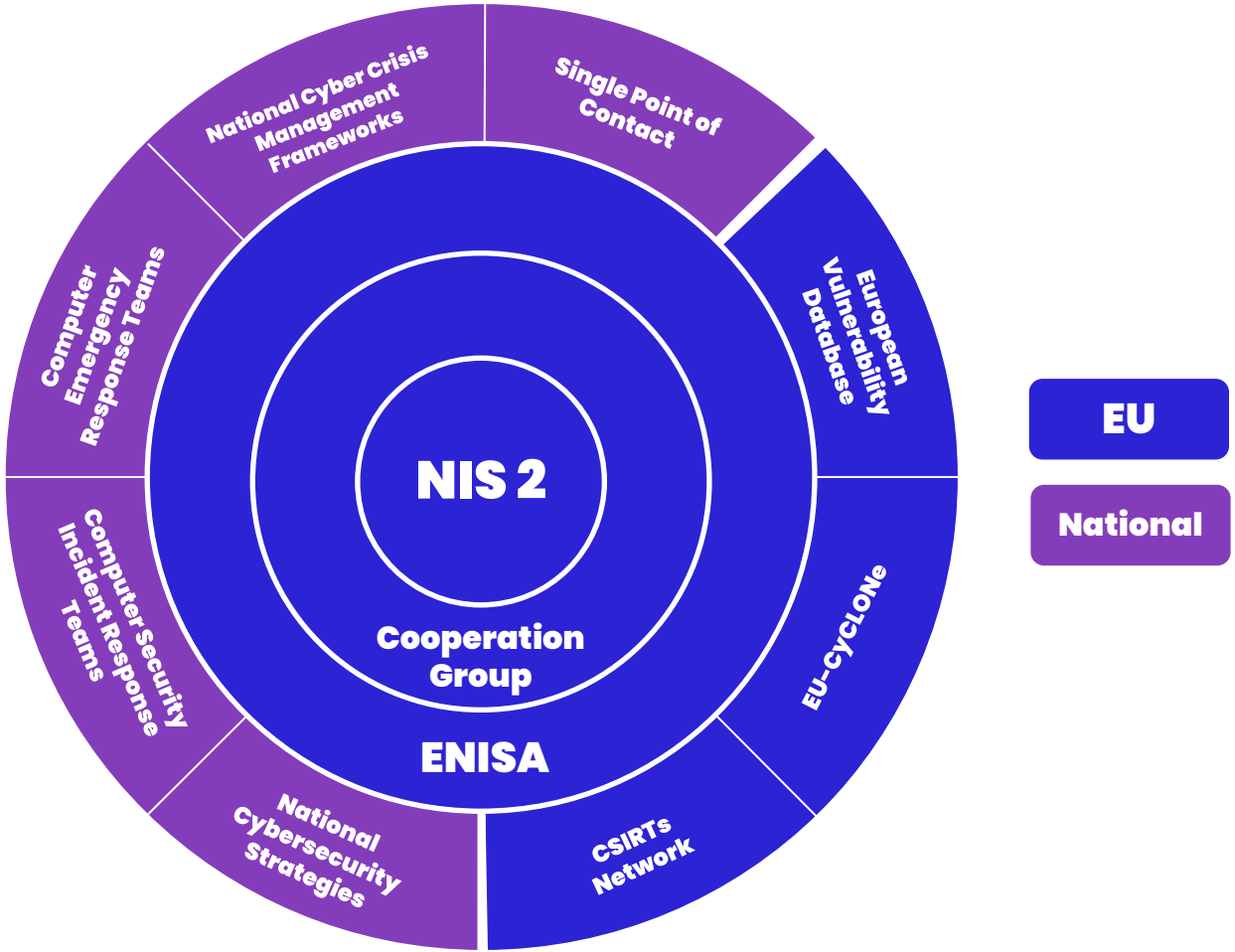
NIS2 – Aufbau/Akteure



EU

National

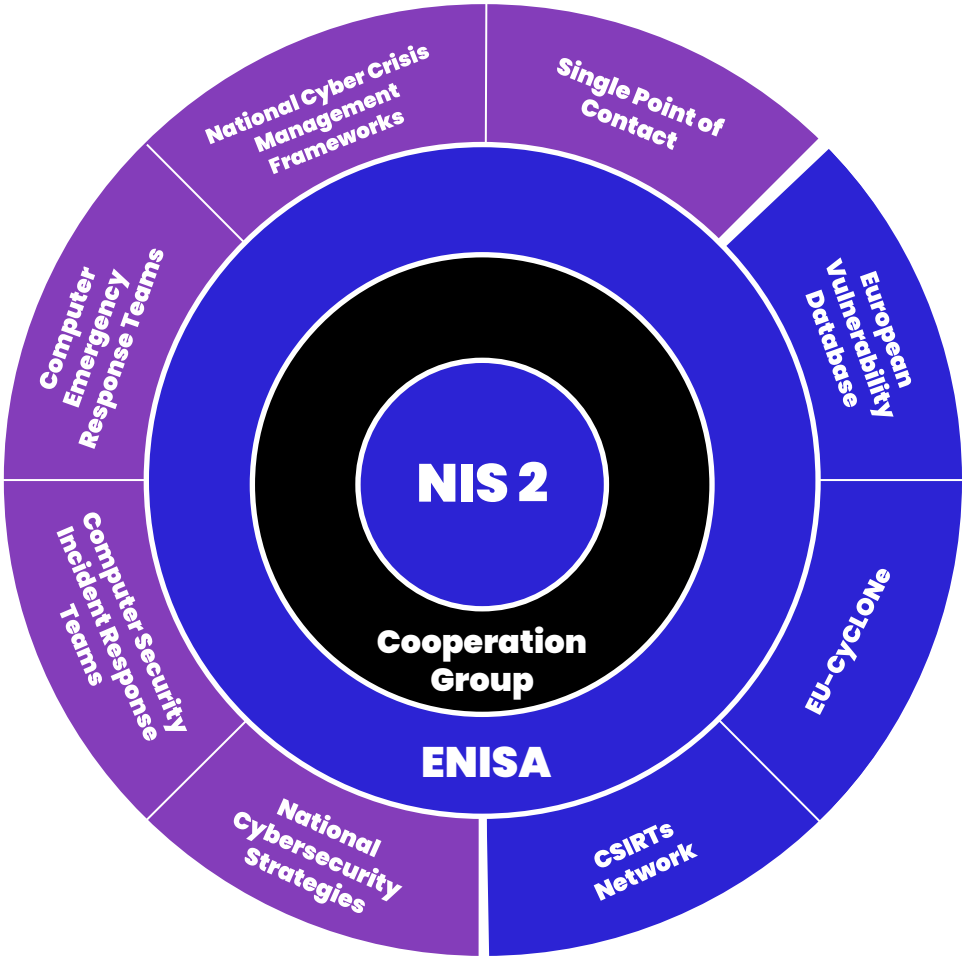
HoliSec


National Cyber Crisis Management Frameworks
Single Point of Contact
European Vulnerability Database
EU-CyCLONe
CSIRTs Network
National Cybersecurity Strategies
Computer Security Incident Response Teams
Computer Emergency Response Teams
NIS 2
Cooperation Group
ENISA
EU
National

HoliSec

Die EU stellt bereit:

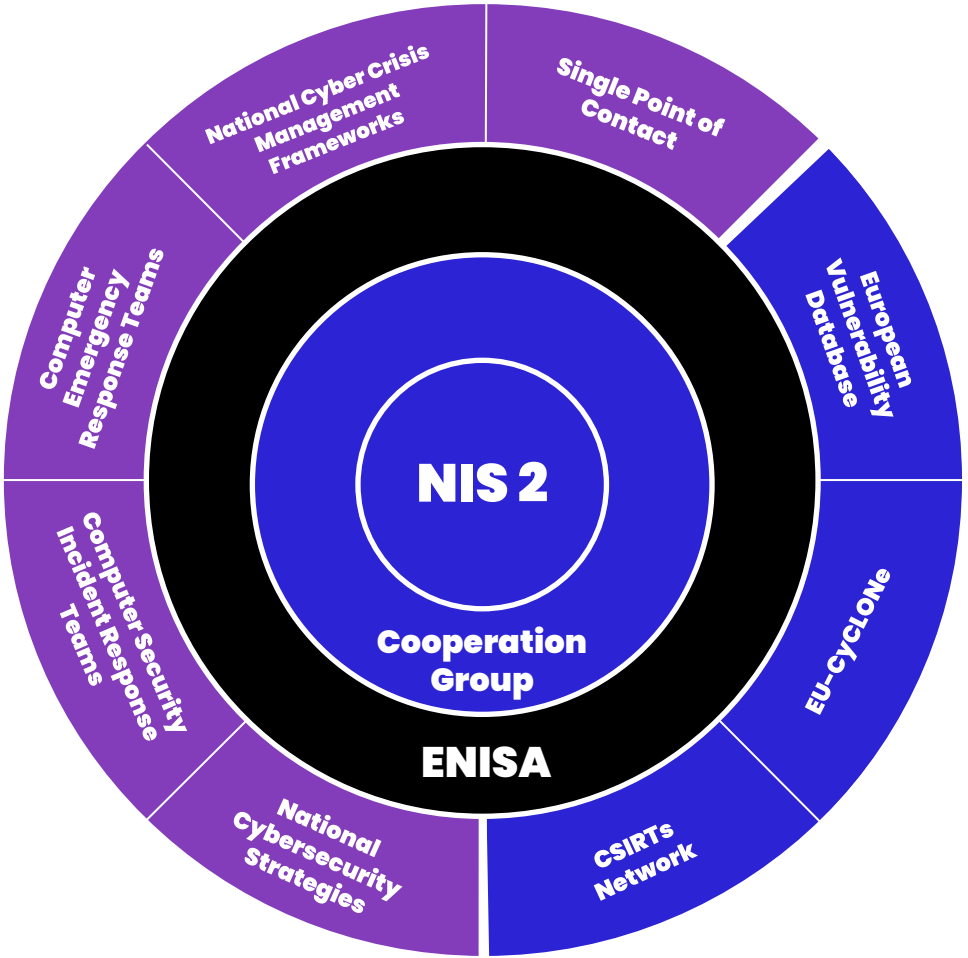
Cooperation Group



HoliSec

Die EU stellt bereit:

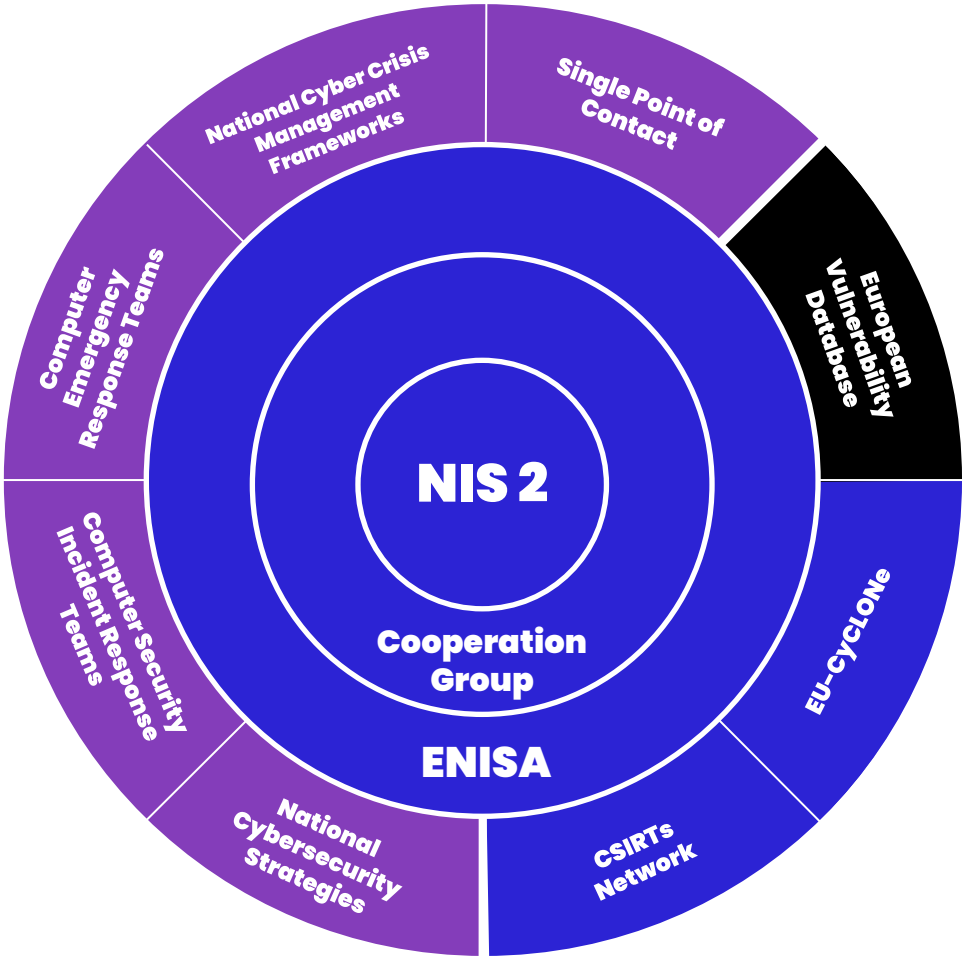
ENISA



HoliSec

Die EU stellt bereit:

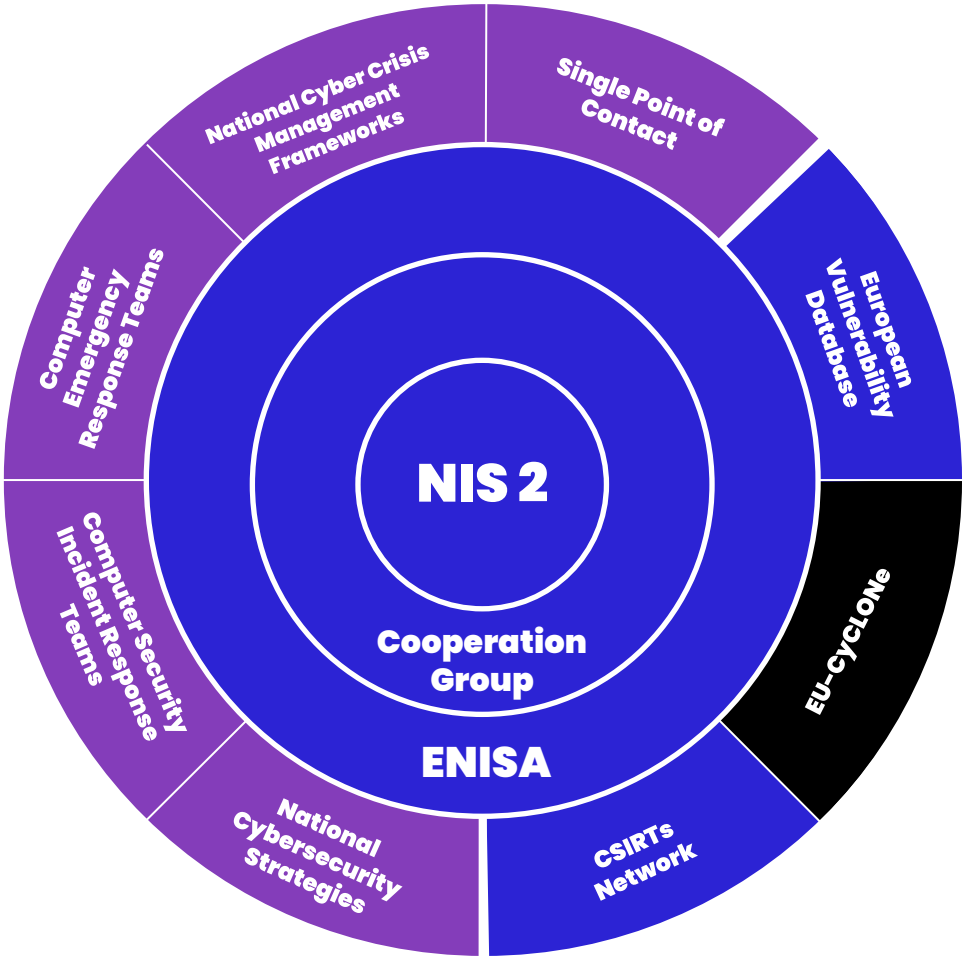
EVD



HoliSec

Netzwerke der EU:

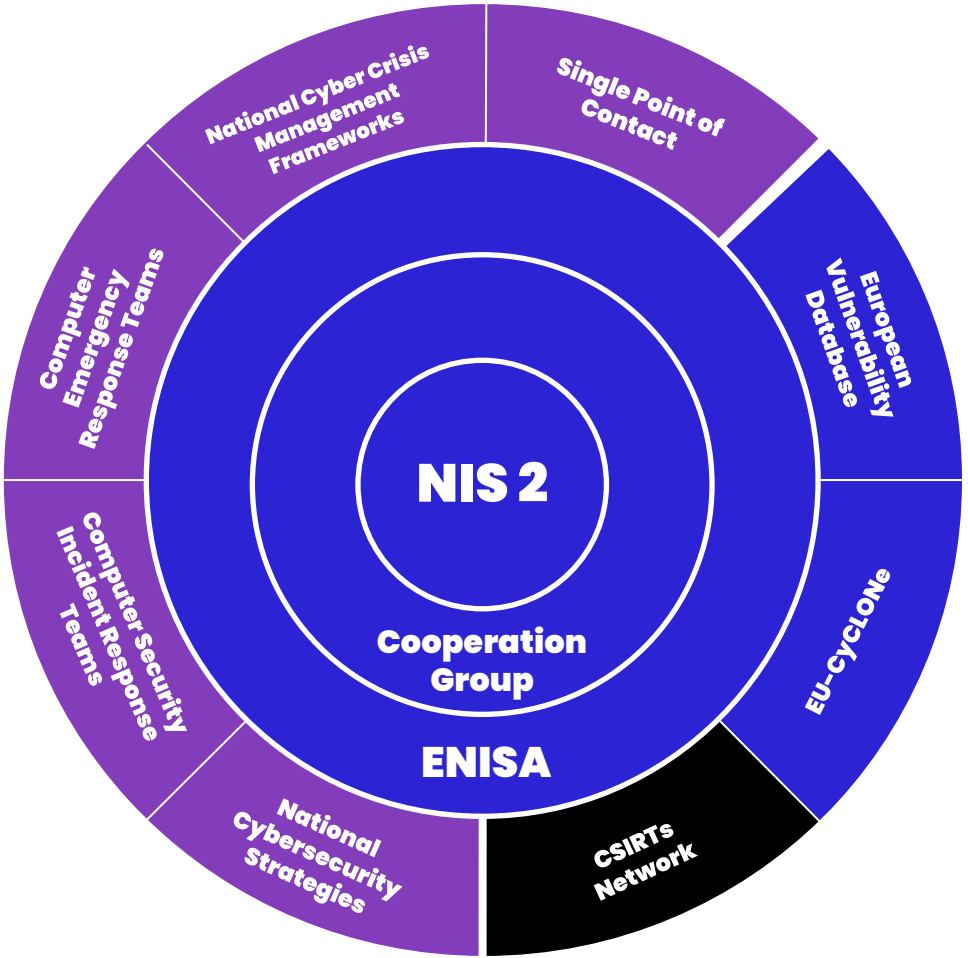
EU-CyCLONE



HoliSec

Netzwerke der EU:

CSIRTs Network

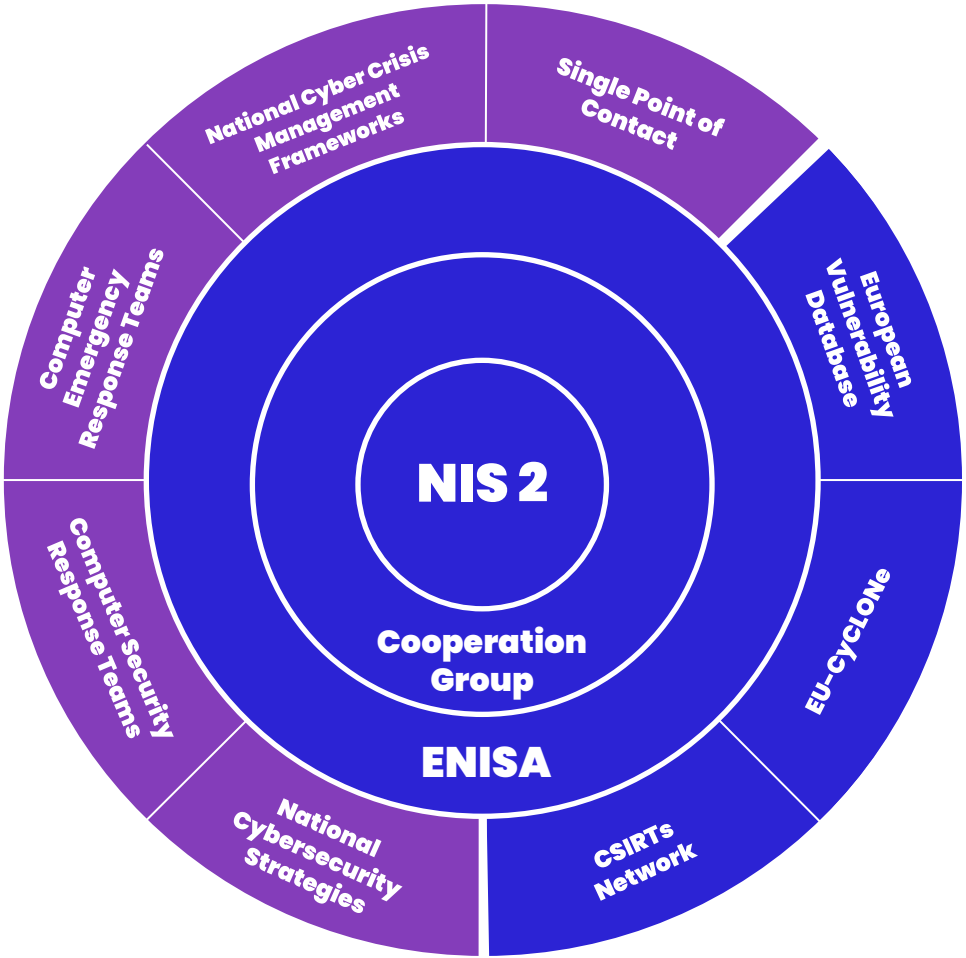


HoliSec

EU

Cooperation Group
ENISA
EVD

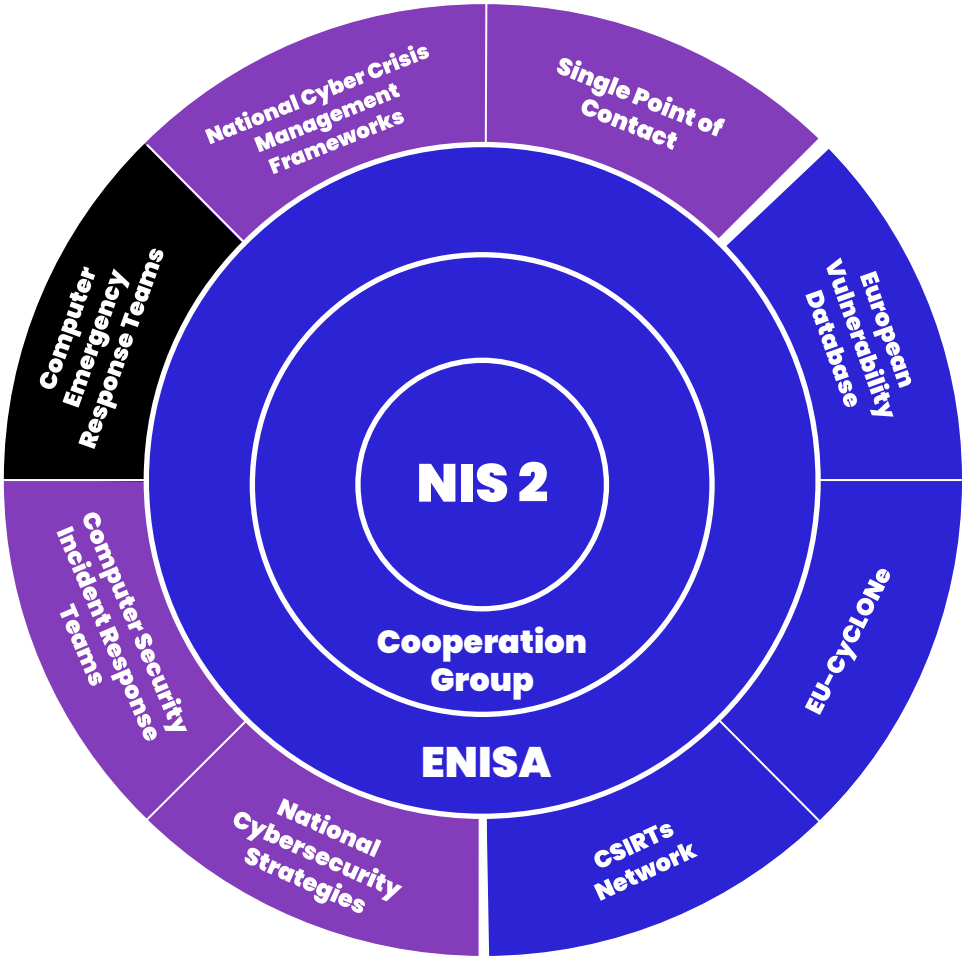
CSIRTs Network
CyCLONe



HoliSec

Österreich muss bereitstellen:

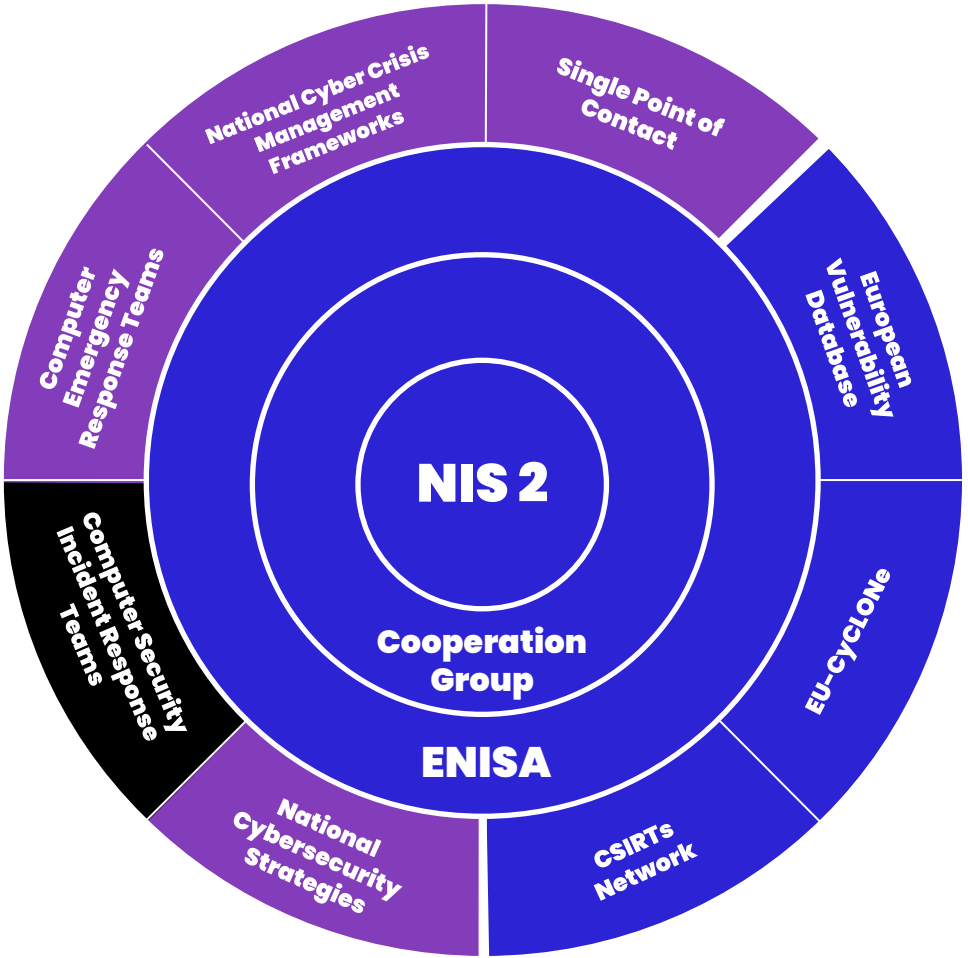
CERT



HoliSec

Österreich muss bereitstellen:

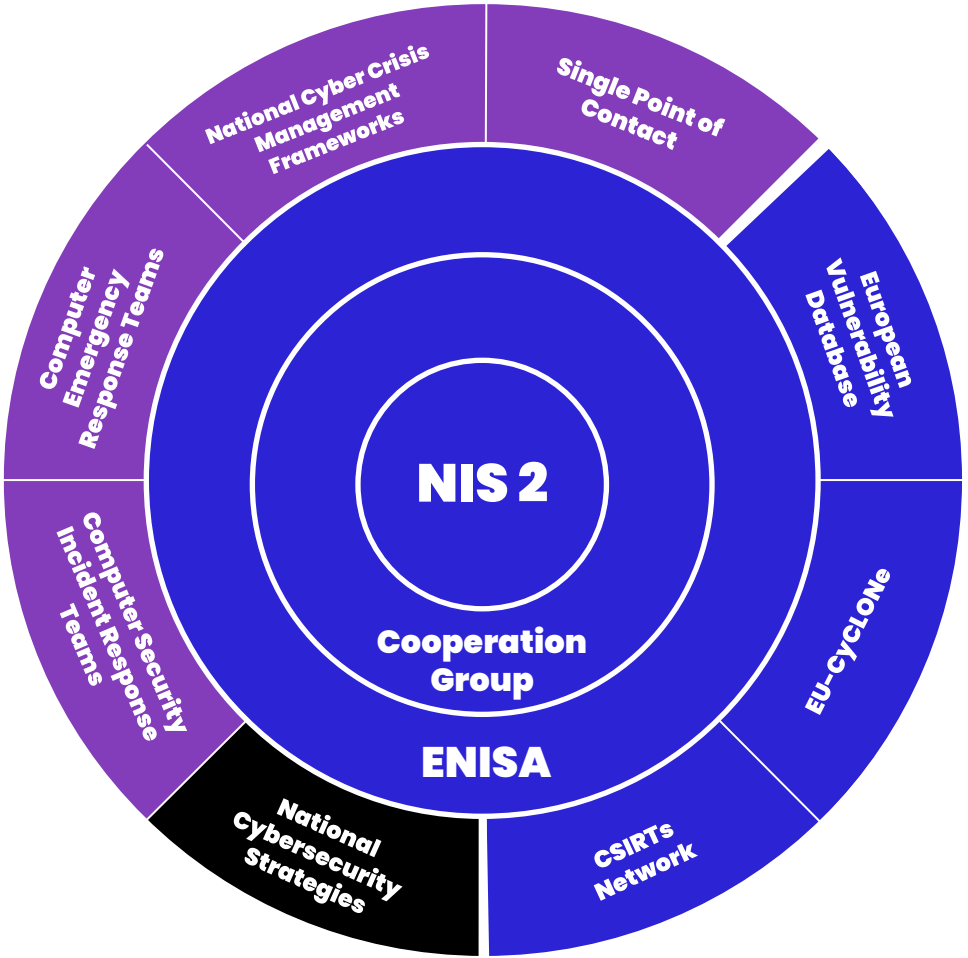
CSIRTs



HoliSec

Österreich muss bereitstellen:

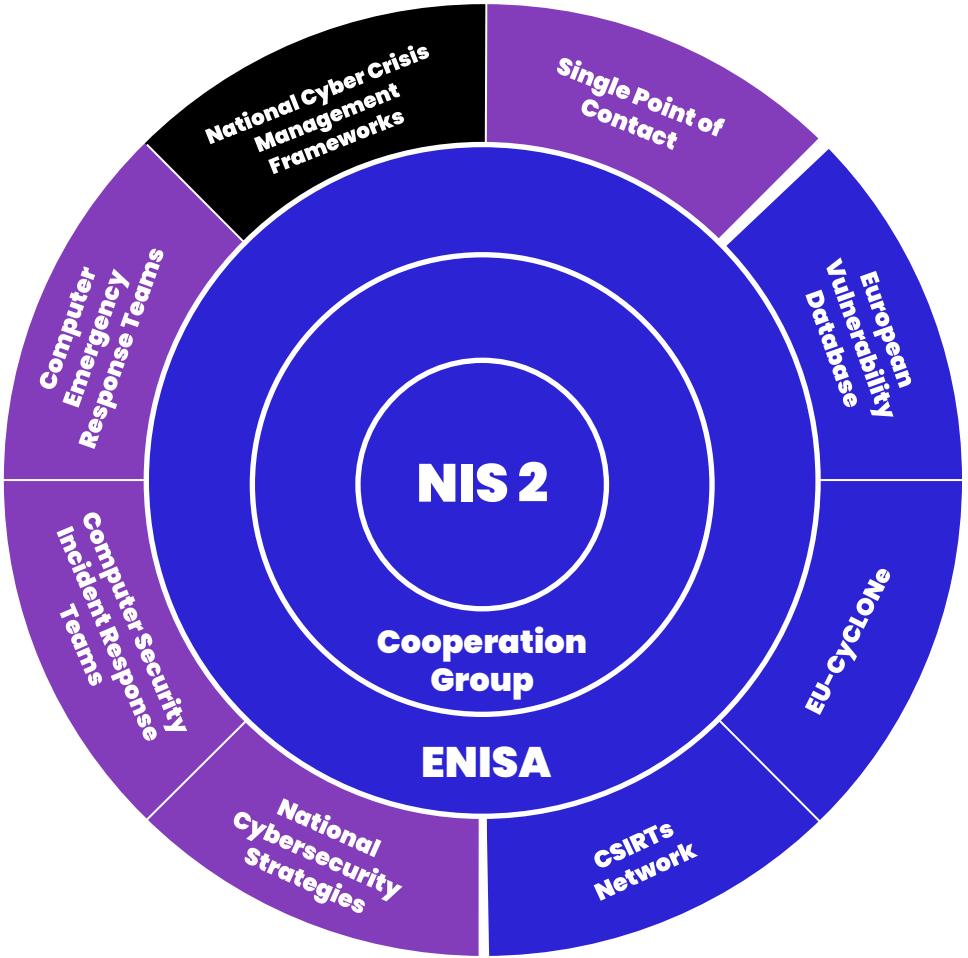
NCS



HoliSec

Österreich muss bereitstellen:

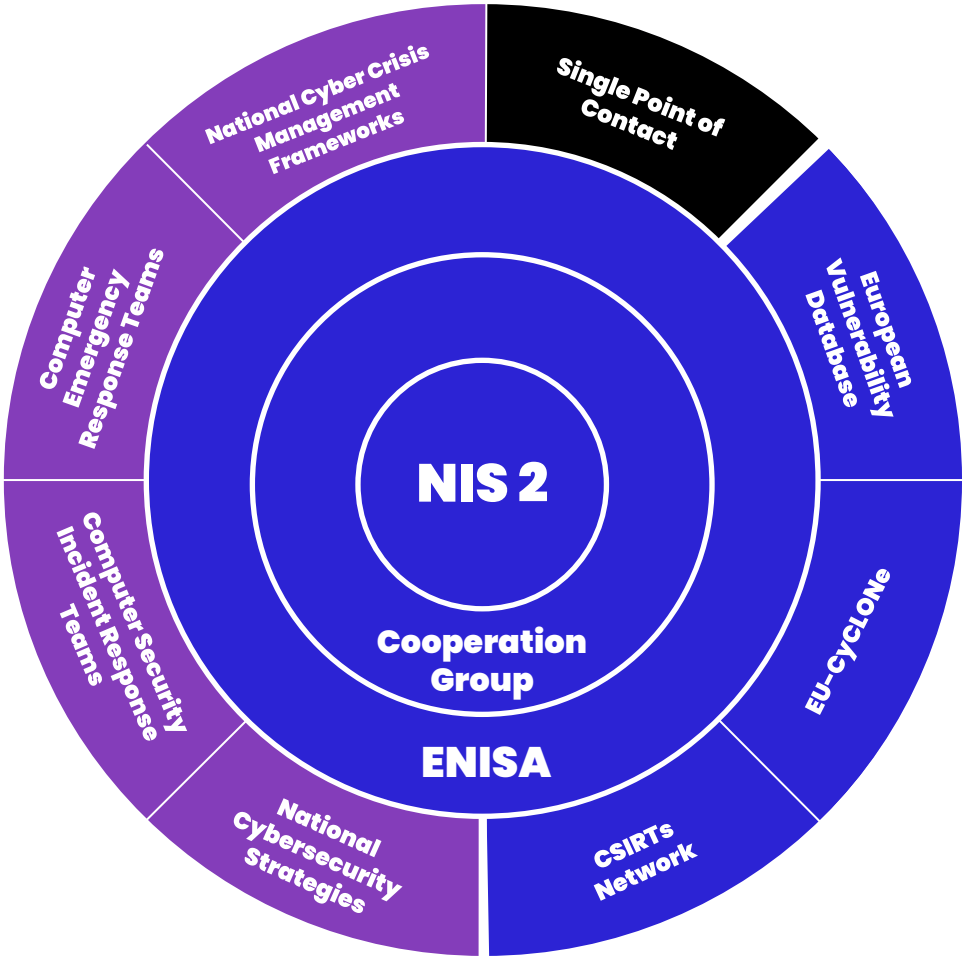
NCCMF



HoliSec

Österreich muss bereitstellen:

SPoC



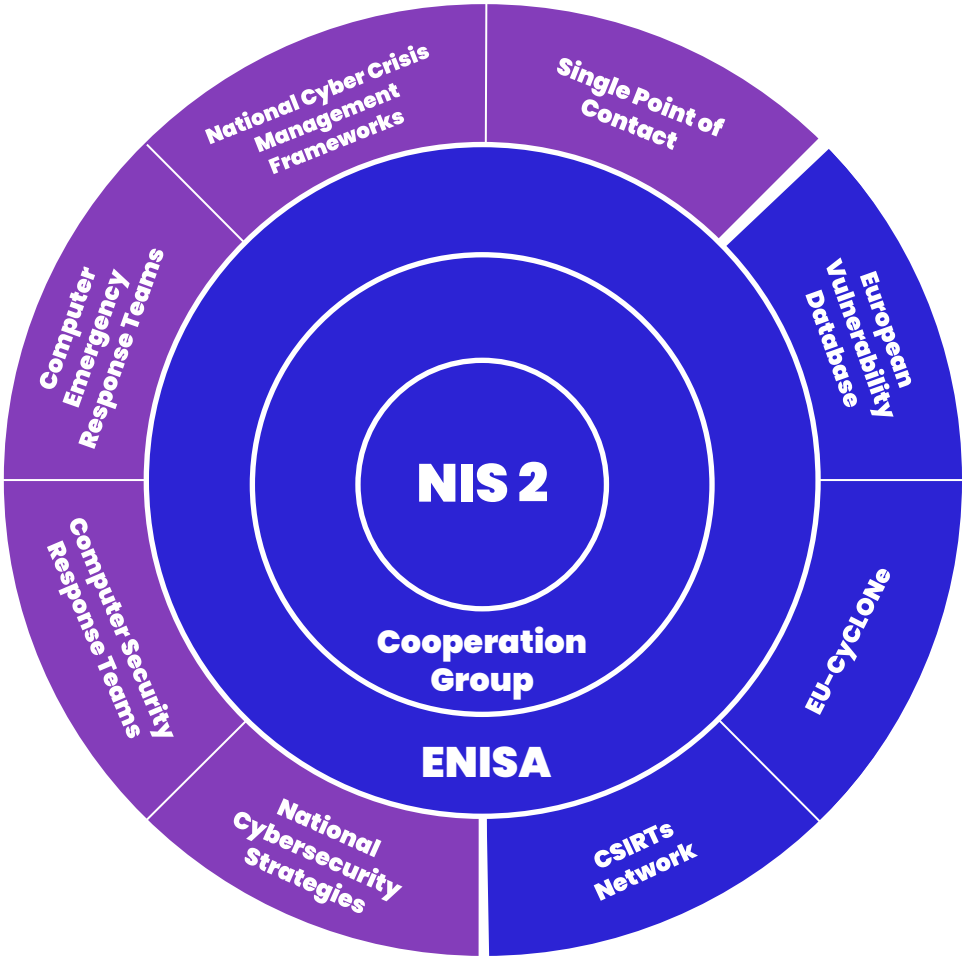
HoliSec

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

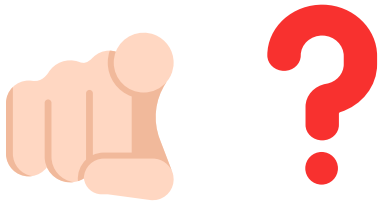


HoliSec

Live Browsing 

NIS 2 Informationen von ENISA

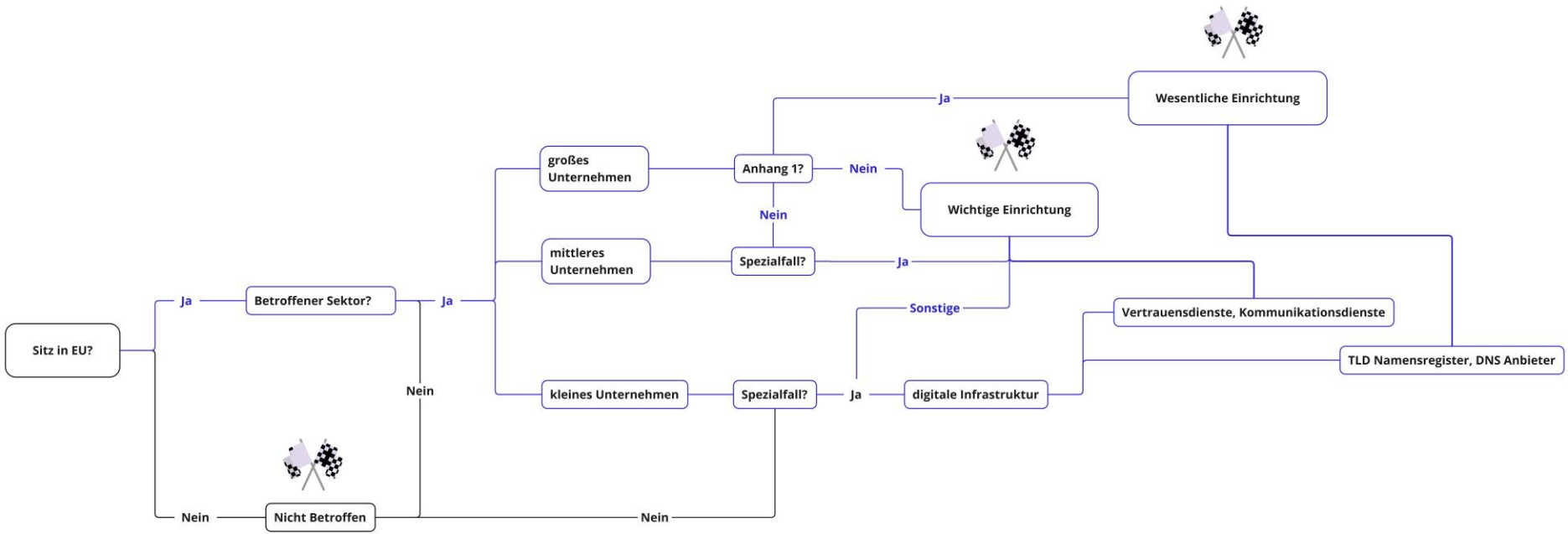
HoliSec



Wer denk ihr ist von der NIS 2 betroffen ?

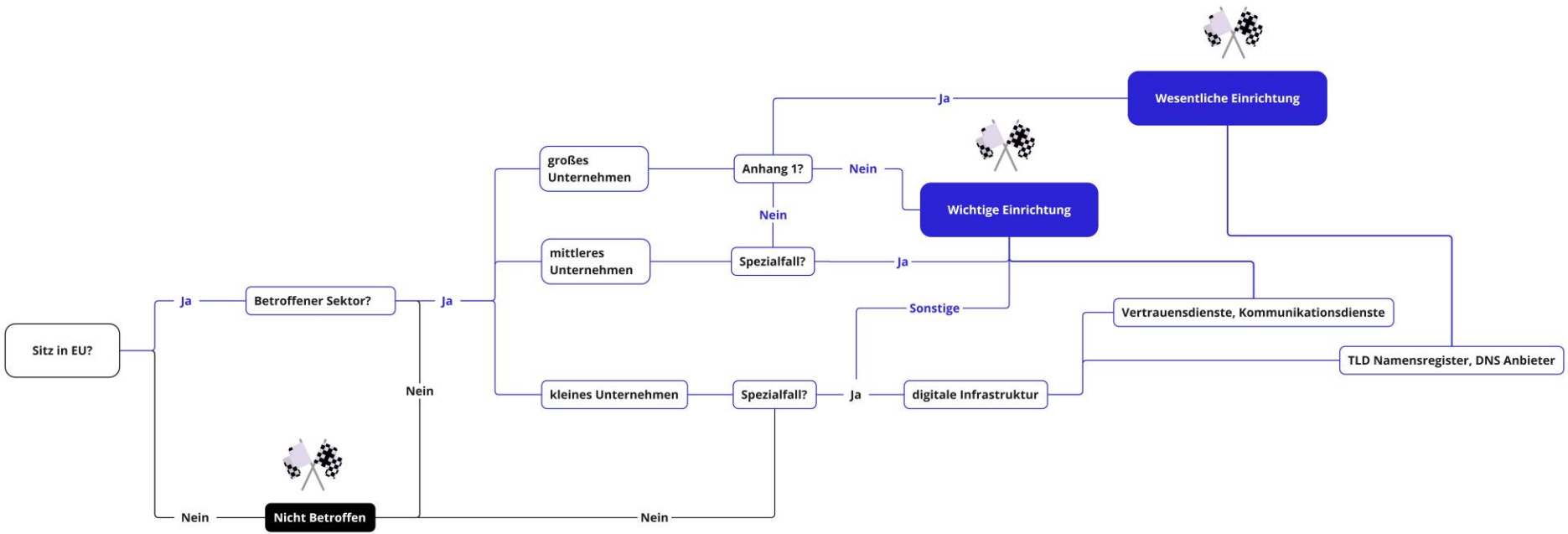
Disclaimer – folgende Darstellungen basieren auf einem Gesetzesentwurf der sich noch ändern kann!

NIS 2 Betroffen?



HoliSec

NIS 2 Betroffen?



HoliSec

NIS 2 Betroffen?

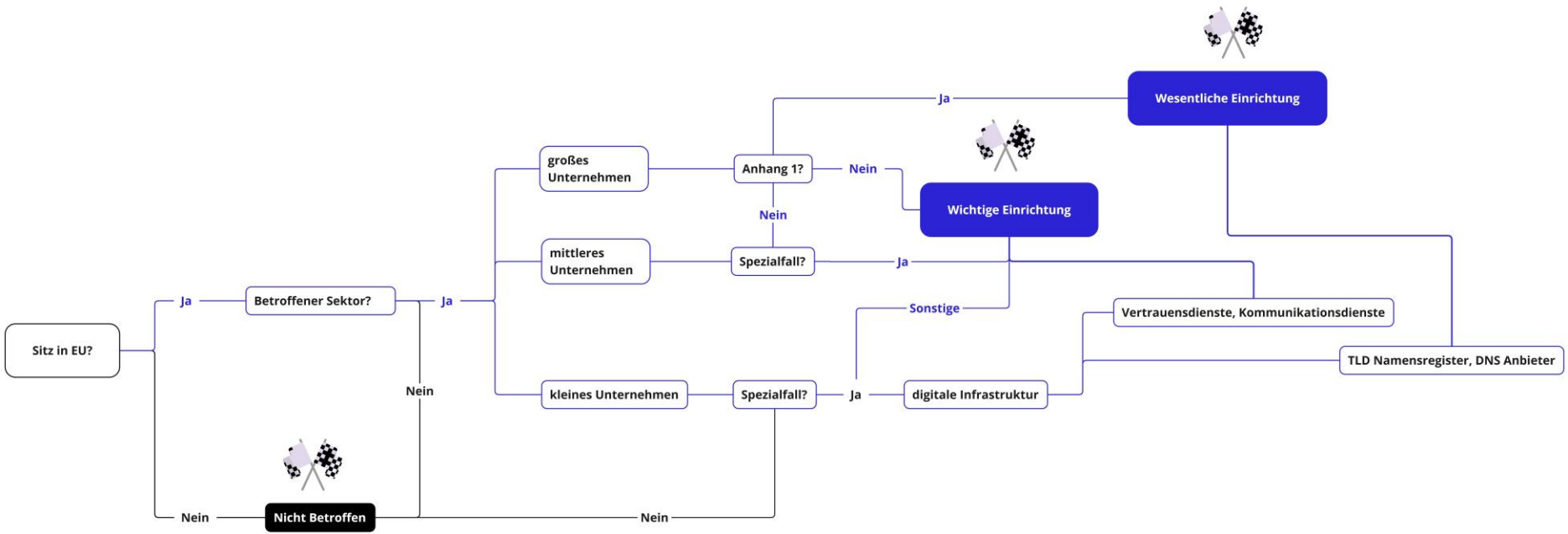
Nicht Betroffen

Wichtige Einrichtung

Wesentliche Einrichtung

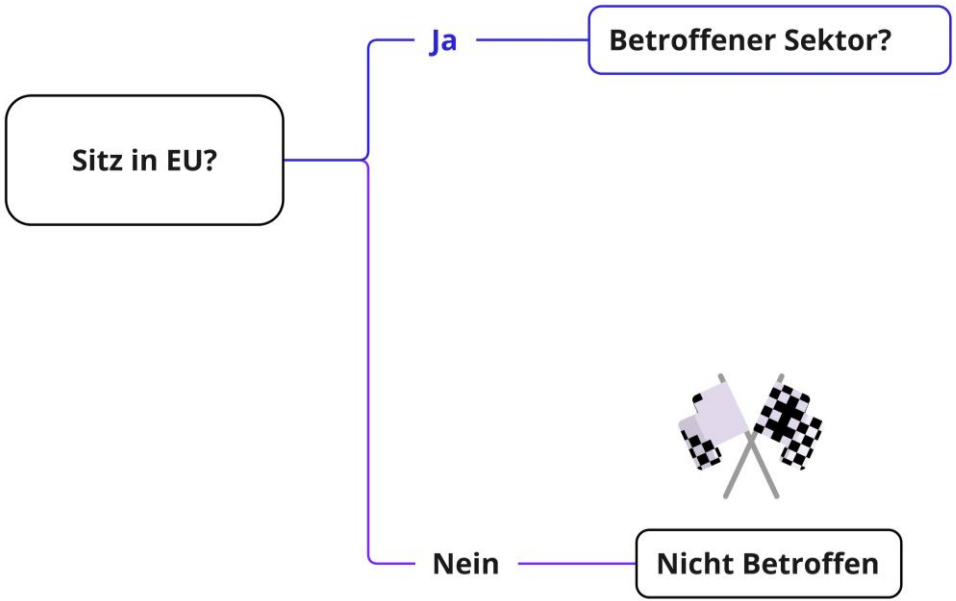
HoliSec

NIS 2 Betroffen?



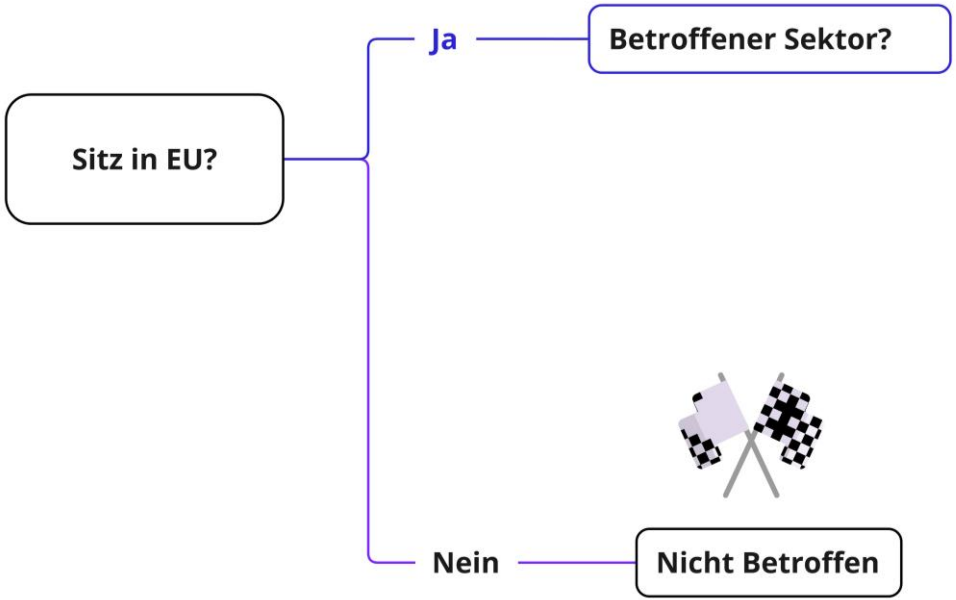
HoliSec

NIS 2 Betroffen?



HoliSec

NIS 2 Betroffen?



HoliSec

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

HoliSec

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.

Dokumentation 📃

- Sektor v. euren Unternehmen
- Lieferkette u. Teilsektoren

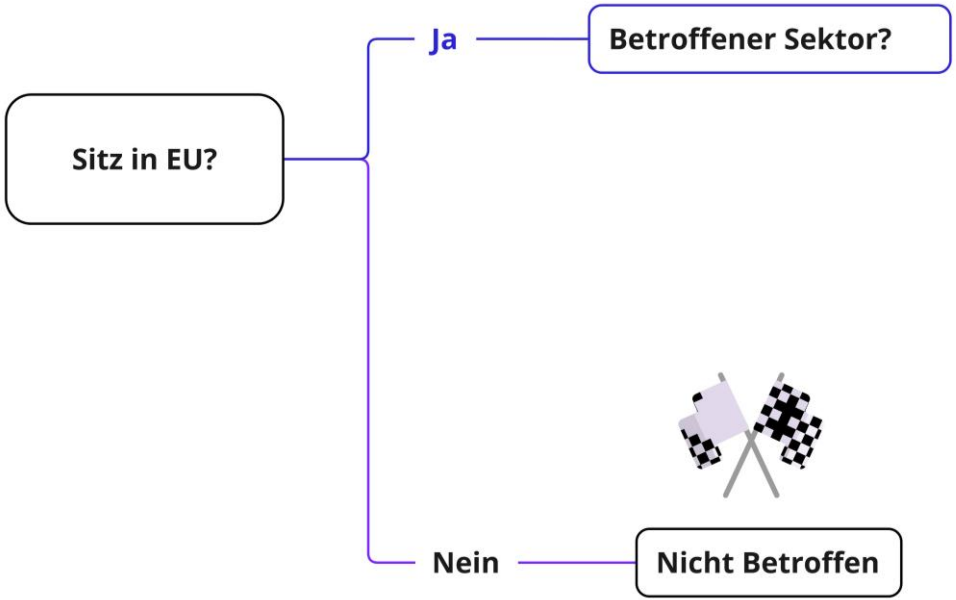
Tipps 💡

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

Zeit & Format 🕐

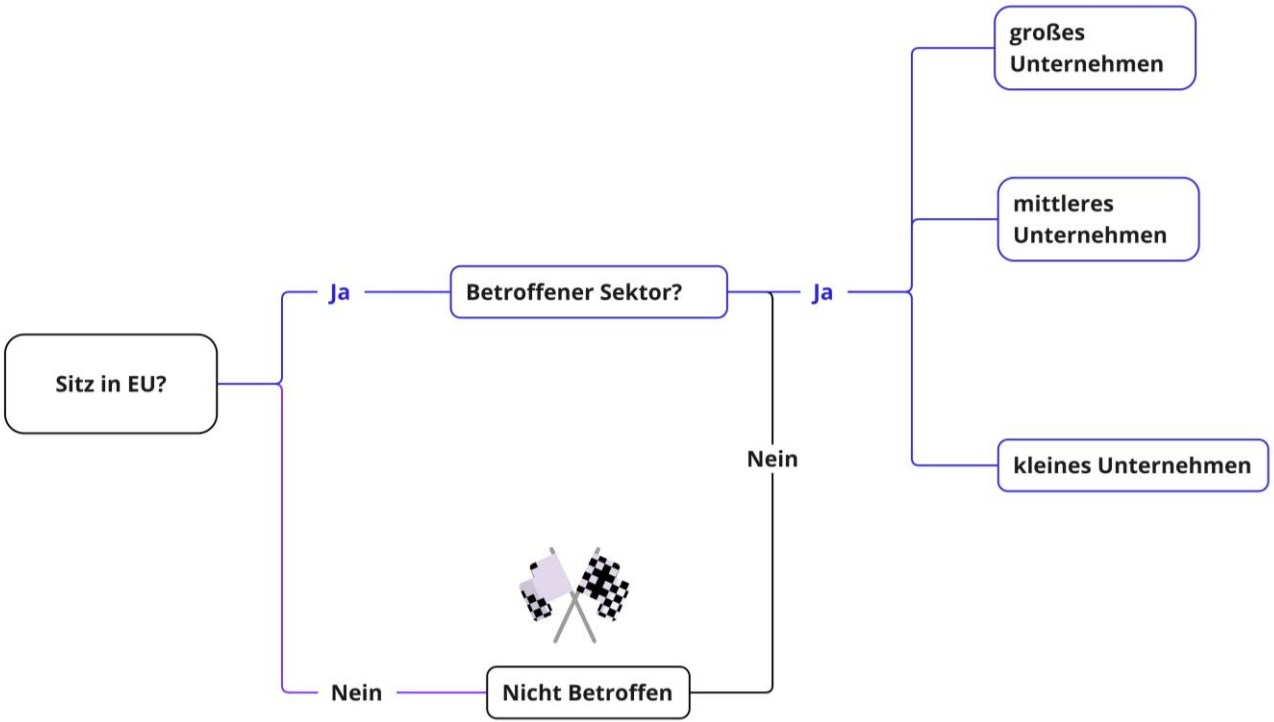
- 10 min
- 5 min Diskussion

NIS 2 Betroffen?



HoliSec

NIS 2 Betroffen?



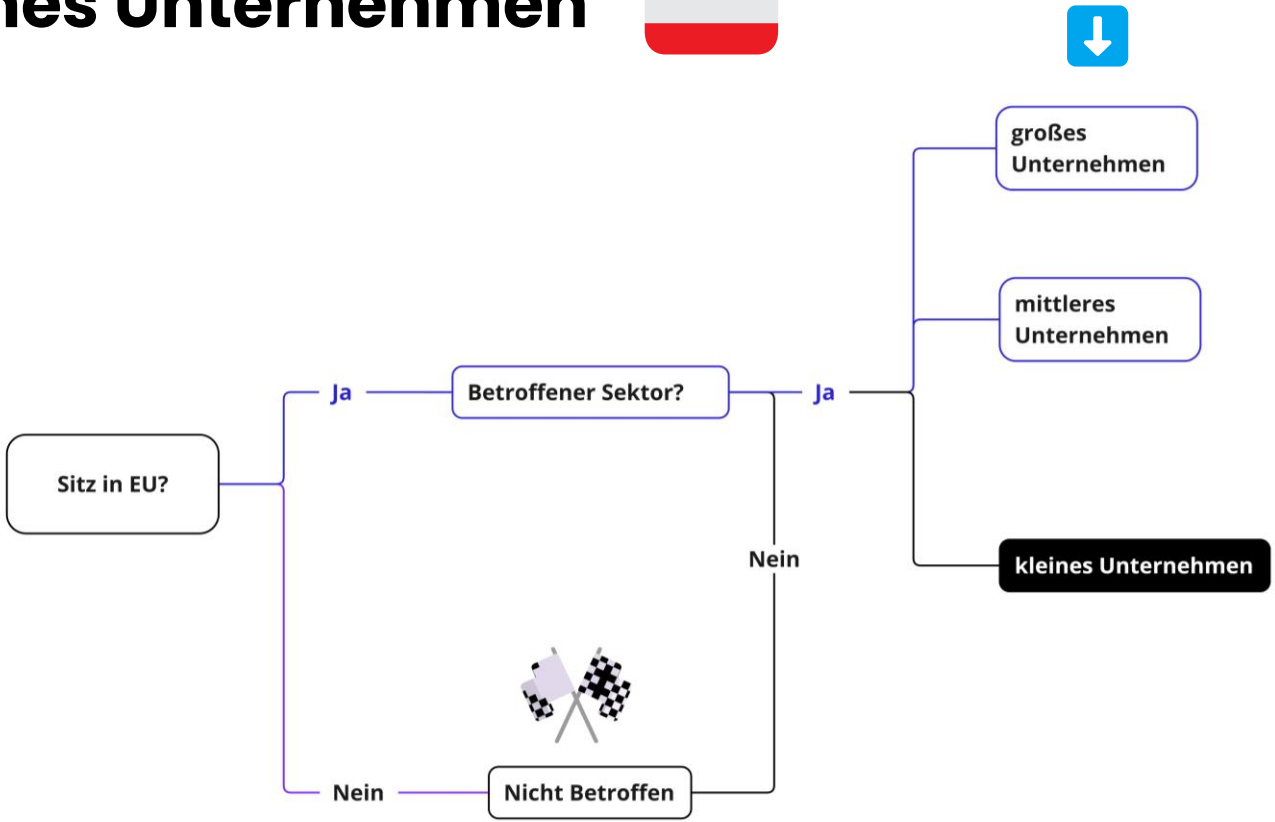
HoliSec

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. €

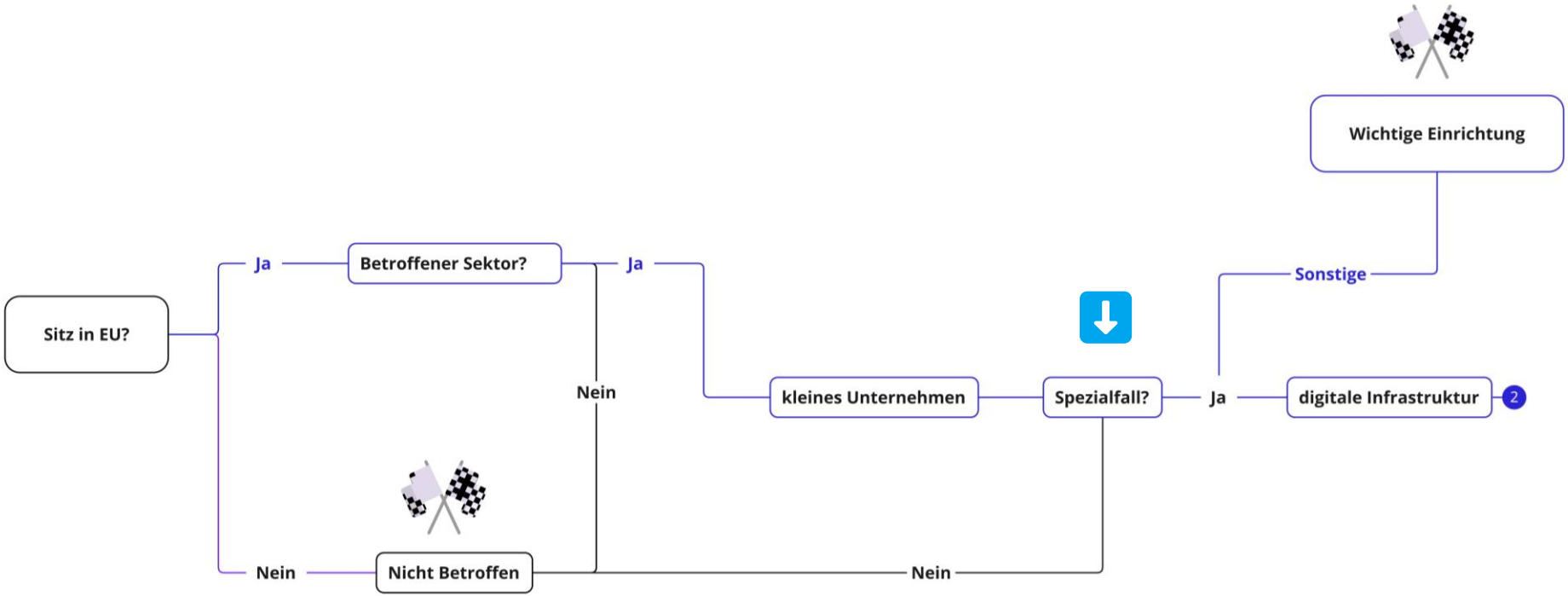
HoliSec

kleines Unternehmen



HoliSec

kleines Unternehmen



HoliSec

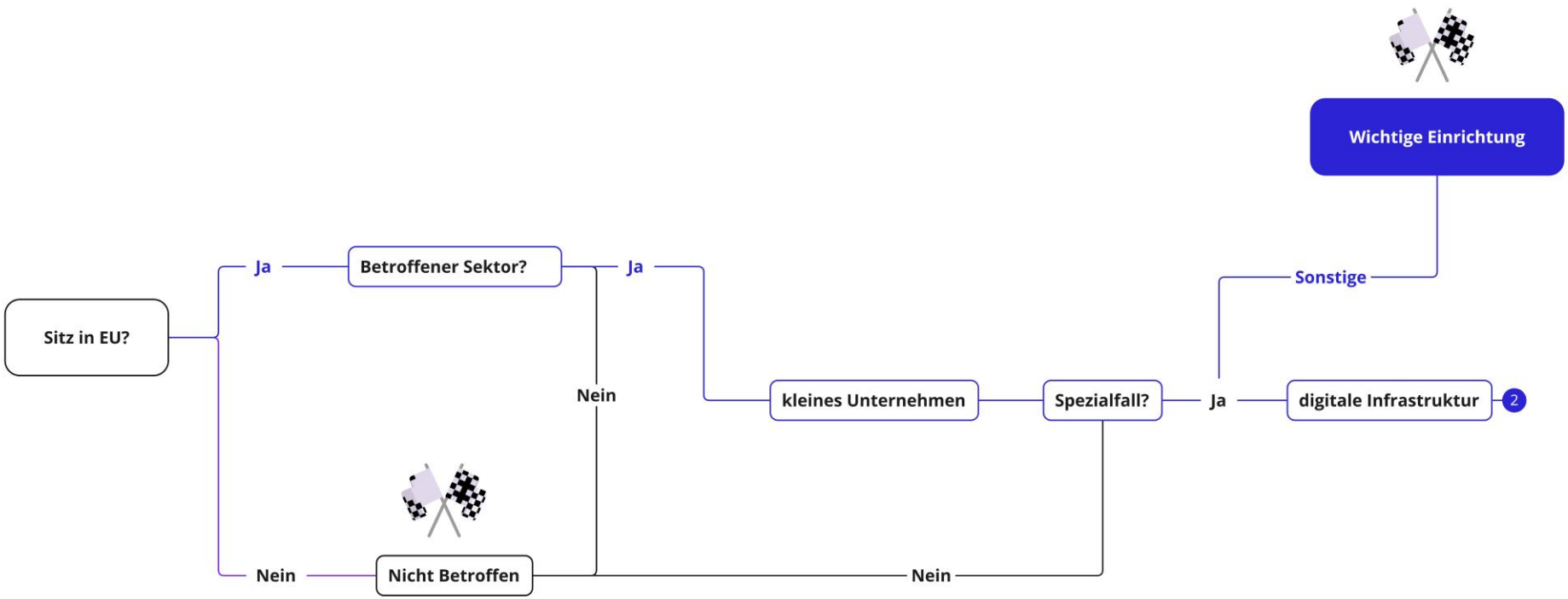
NIS 2- Spezialfälle

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.**

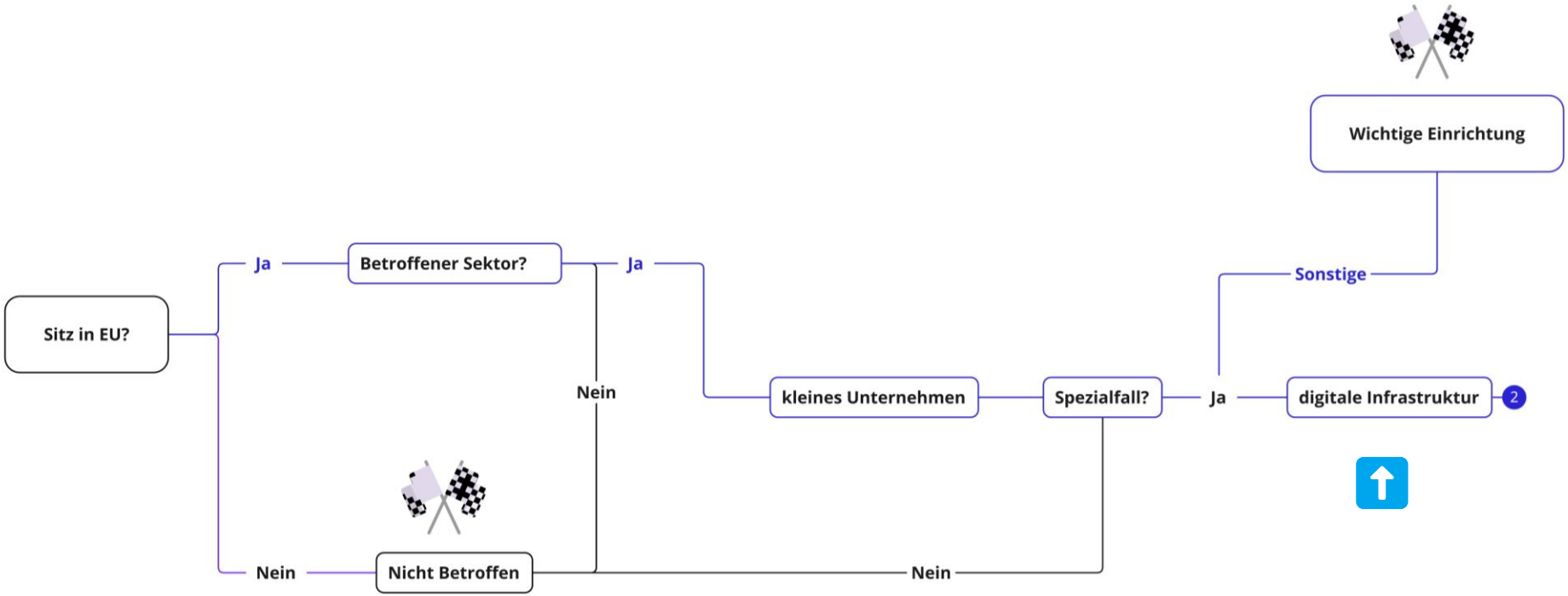
Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht

kleines Unternehmen



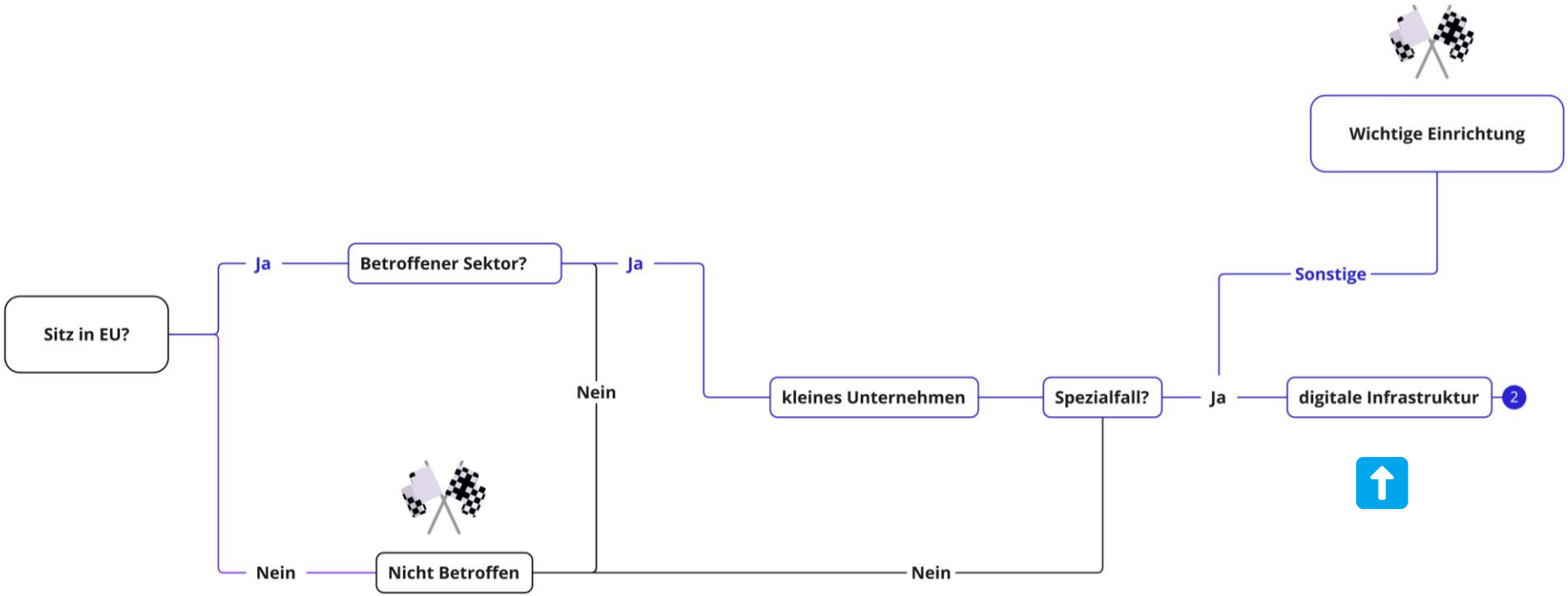
HoliSec

kleines Unternehmen



HoliSec

kleines Unternehmen



HoliSec

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)**

HoliSec

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

HoliSec

kleines Unternehmen

Wesentliche Einrichtung

Wichtige Einrichtung

Sonstige

Vertrauensdienste, Kommunikationsdienste

TLD Namensregister, DNS Anbieter

kleines Unternehmen — Spezialfall? — Ja — digitale Infrastruktur

Nein

HoliSec

kleines Unternehmen

Wesentliche Einrichtung

Wichtige Einrichtung

Sonstige

Vertrauensdienste, Kommunikationsdienste

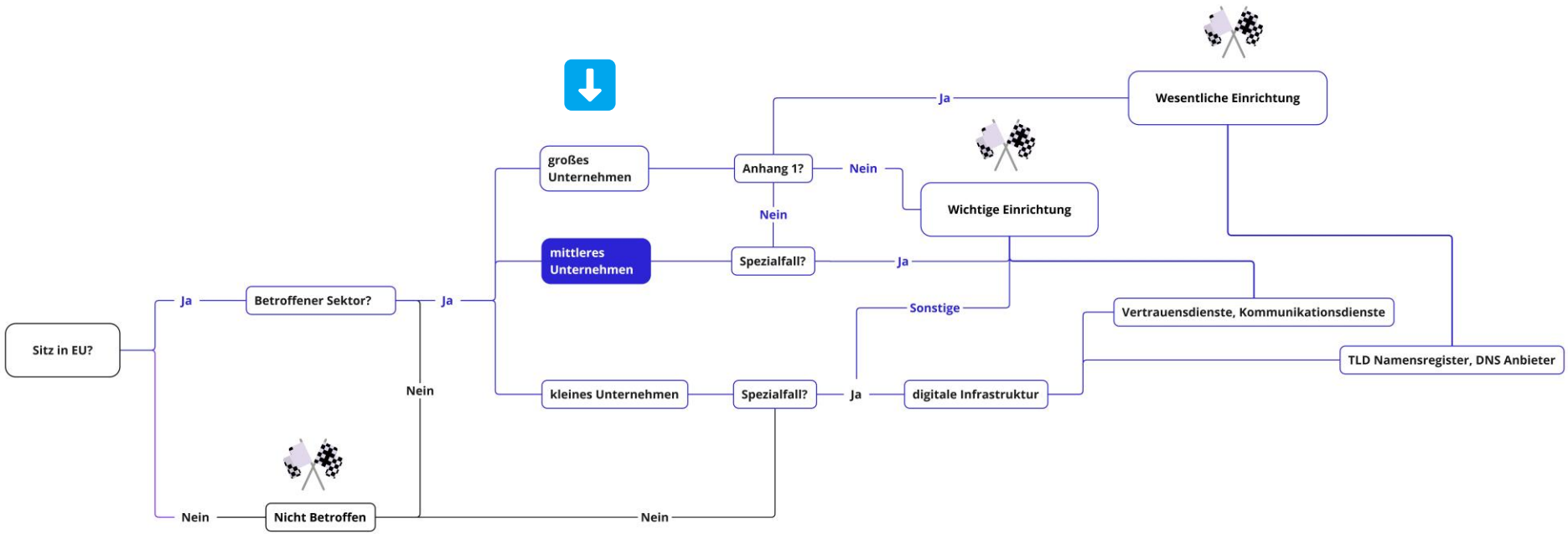
TLD Namensregister, DNS Anbieter

kleines Unternehmen — Spezialfall? — Ja — digitale Infrastruktur

Nein

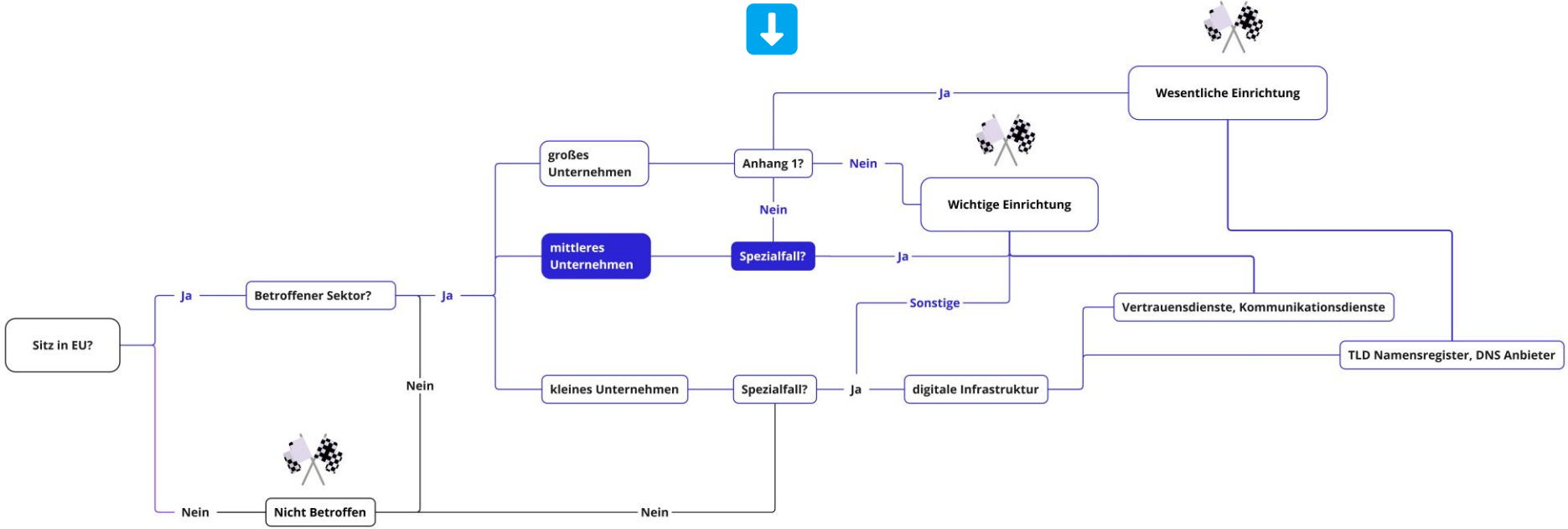
HoliSec

mittleres Unternehmen



HoliSec

mittleres Unternehmen



HoliSec

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.**

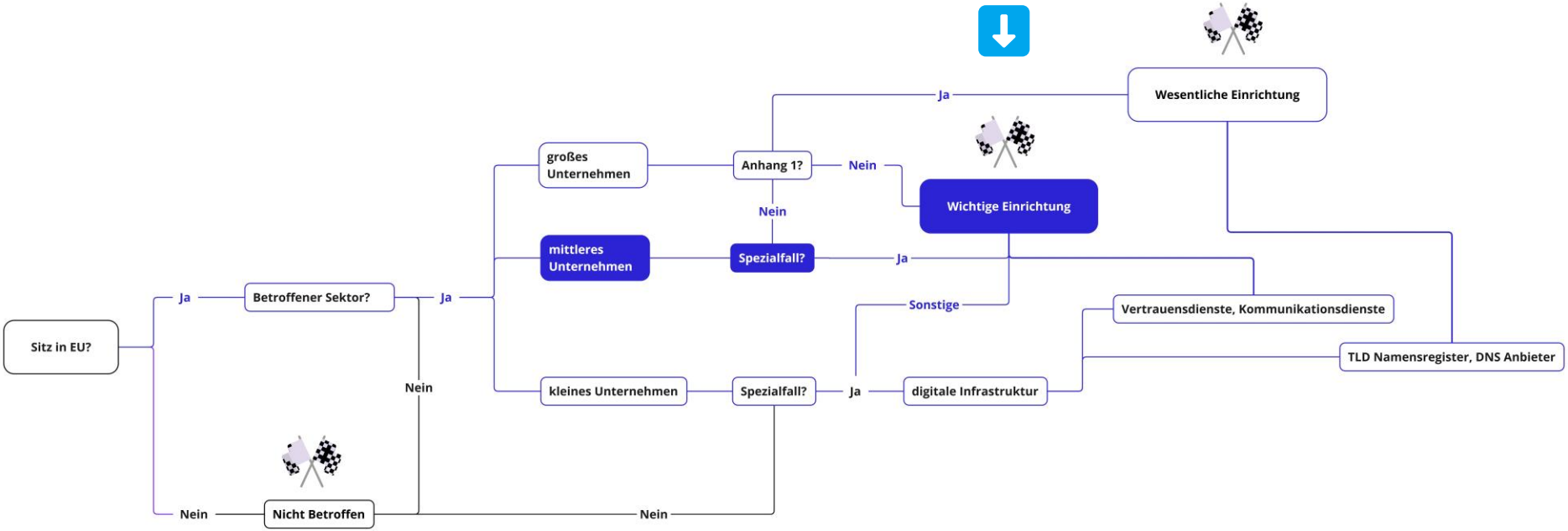
Digitale Infrastruktur

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

HoliSec

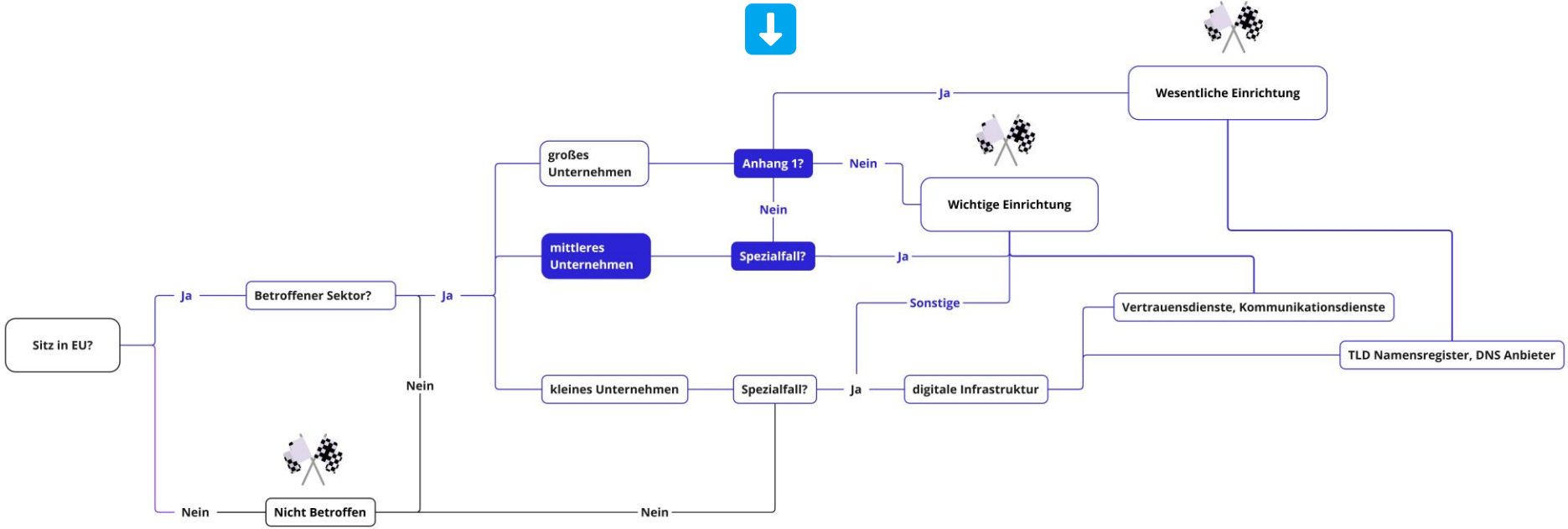
Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht

mittleres Unternehmen



HoliSec

mittleres Unternehmen



HoliSec

Betroffene Sektoren

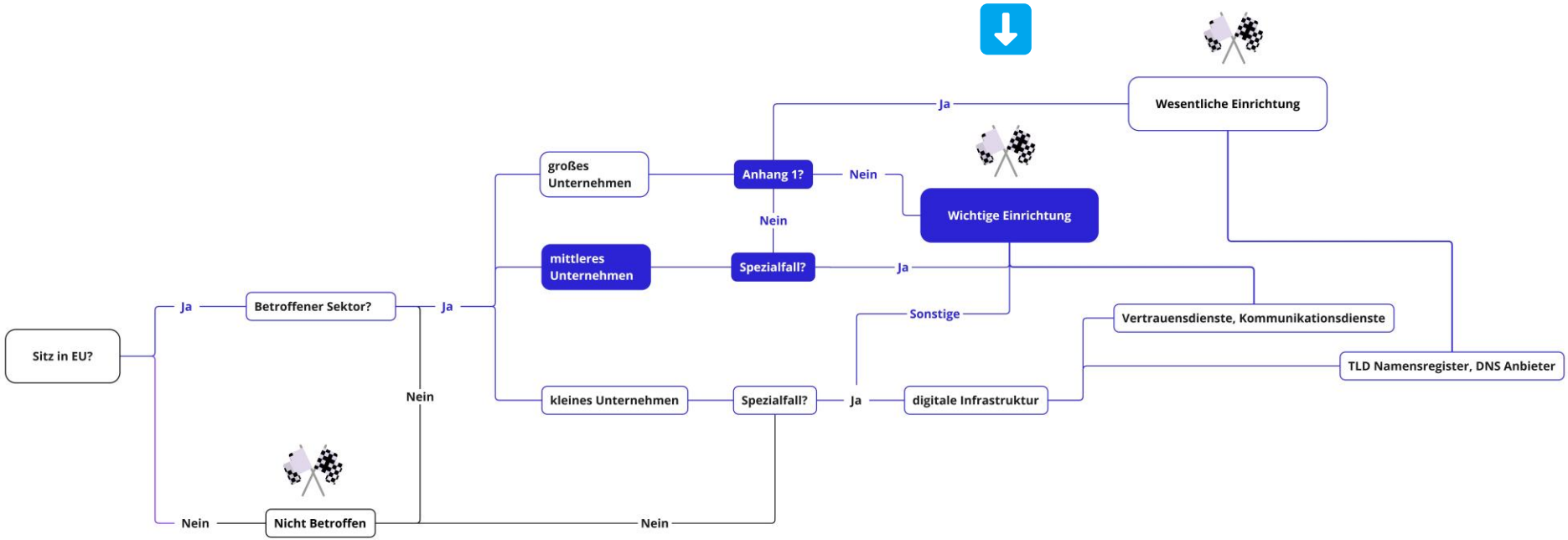
Anhang 1

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

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

Wenn nein ->

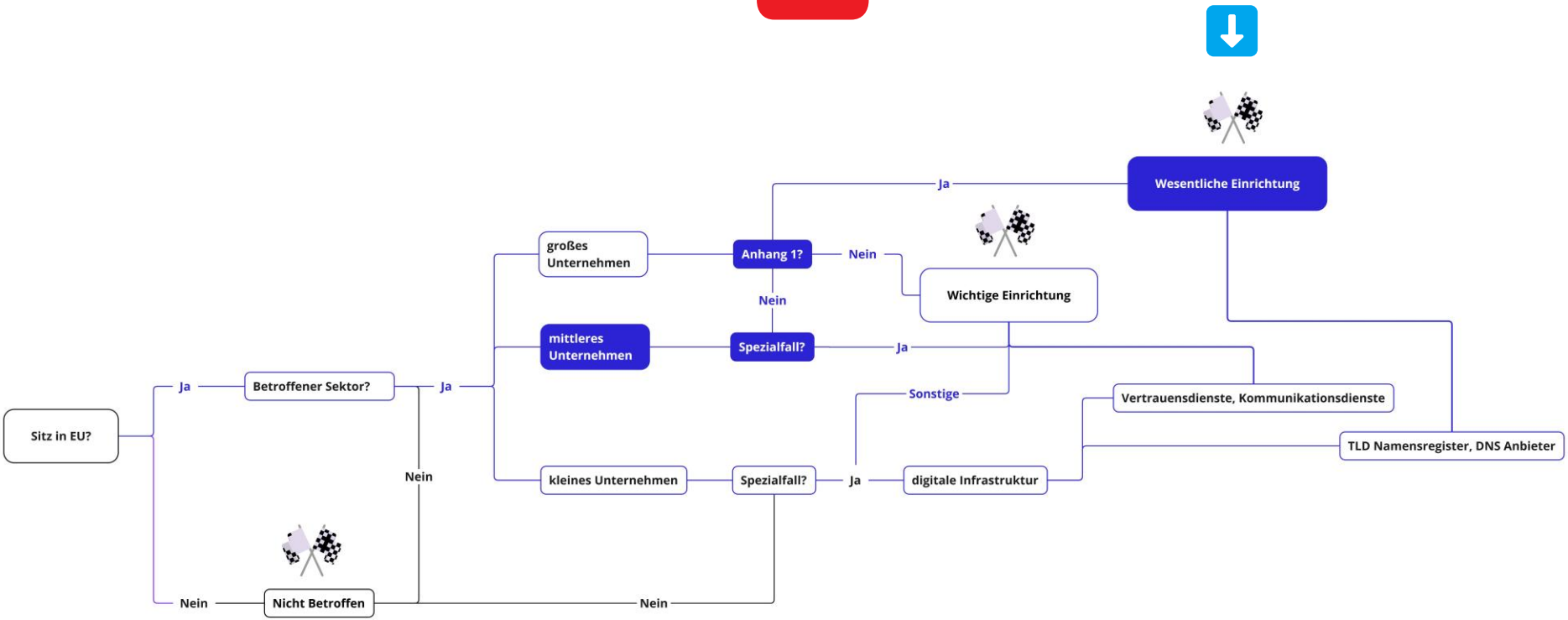
mittleres Unternehmen



HoliSec

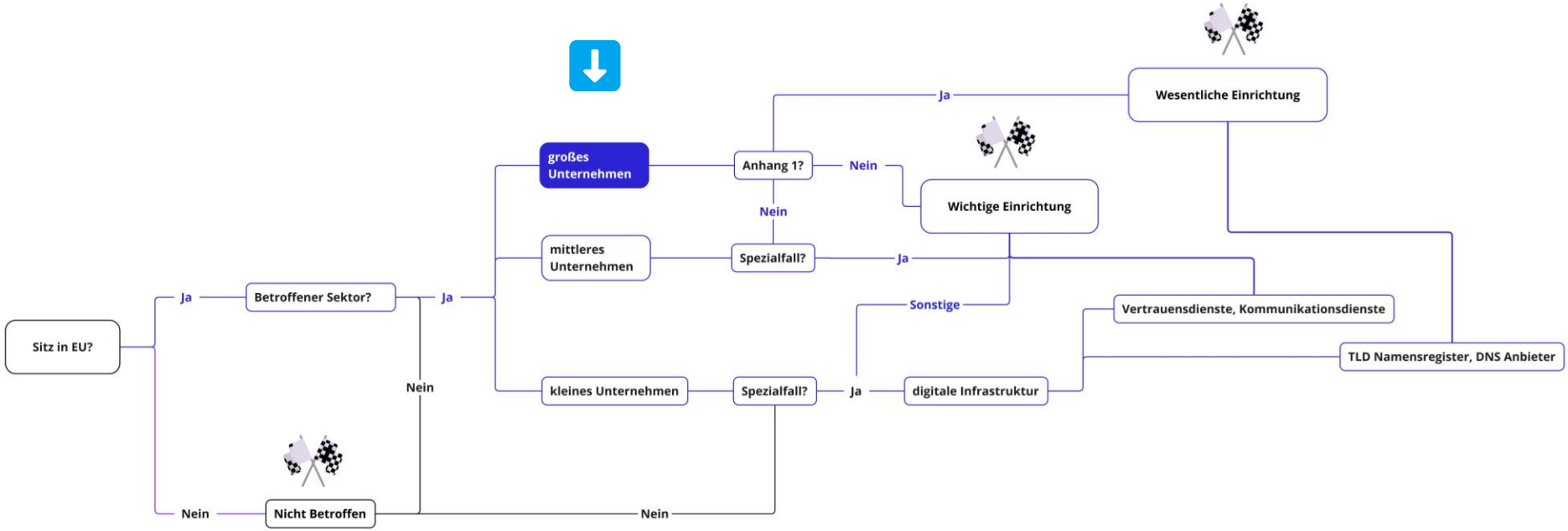
Wenn ja ->

mittleres Unternehmen



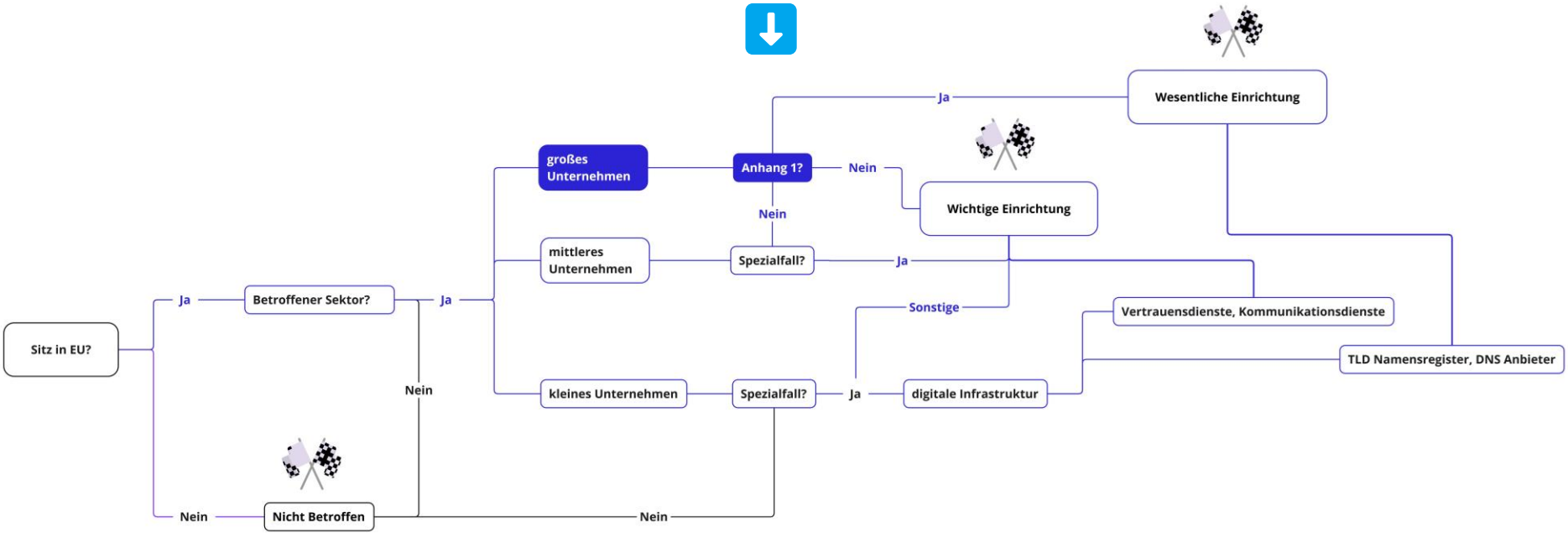
HoliSec

großes Unternehmen



HoliSec

großes Unternehmen



HoliSec

Betroffene Sektoren

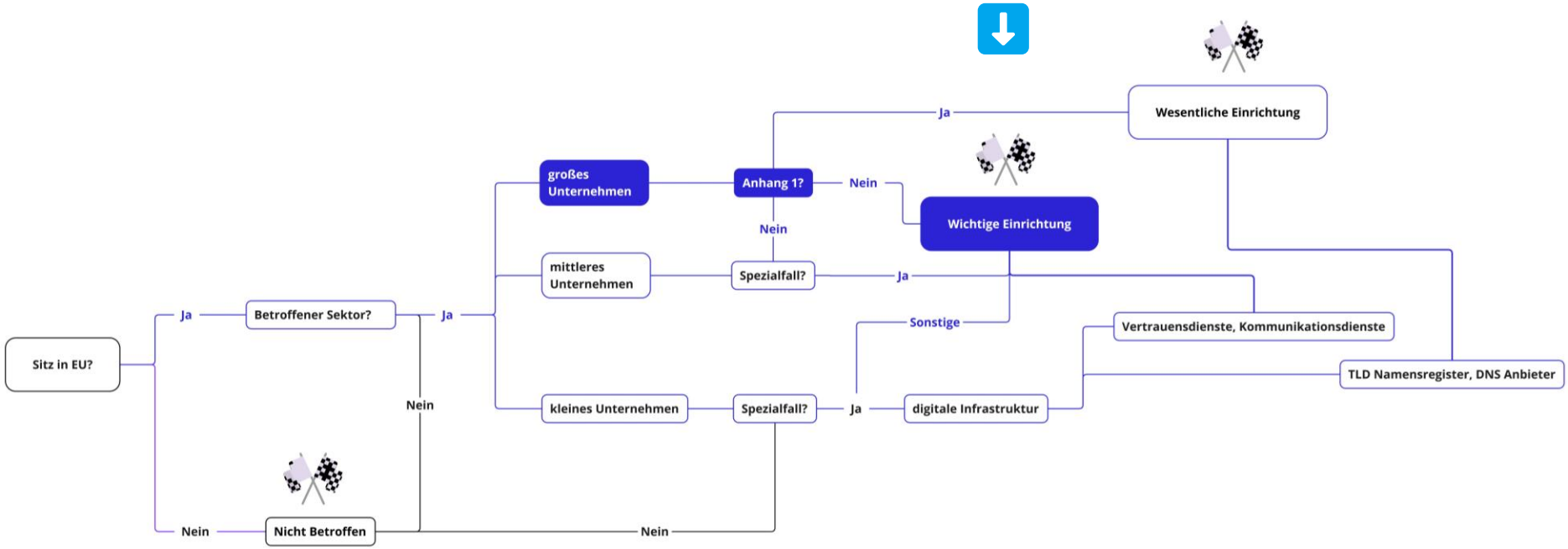
Anhang 1

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

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

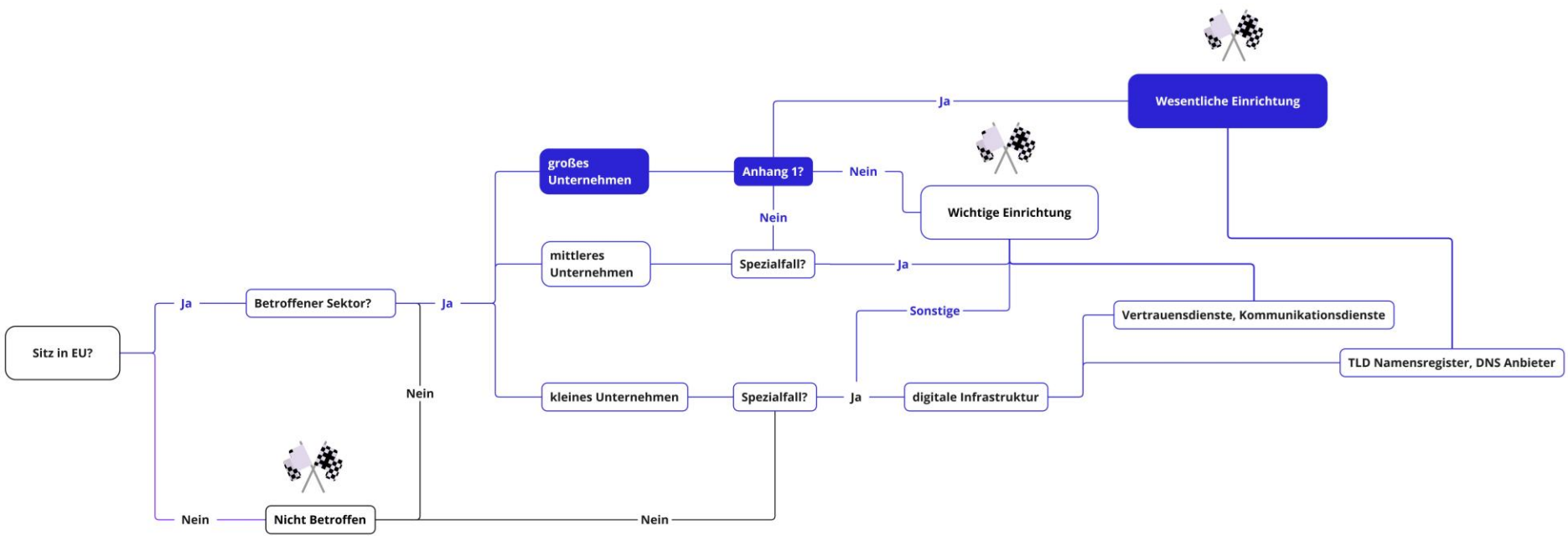
Wenn nein ->

großes Unternehmen



Wenn ja ->

großes Unternehmen



HoliSec

Ist das Vorgehen für euch verständlich?

Zeit für ein Quiz! 

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

HoliSec

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

HoliSec

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)

HoliSec

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.

Tipps 💡

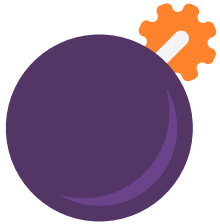
- Ruft den Ratgeber der WKO auf.
  [WKO Online Ratgeber NIS 2]

Dokumentation 📄

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

Zeit & Format 🕐

- 10 min
- 5 min Diskussion



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

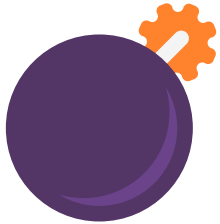
MA, GF, IT, Stakeholder

HoliSec

Mit der NIS 2 kommen weitere Aufgaben dazu.

Meldefristen – NIS 2

24h	72h	1 Monat
		
Frühwarnung	**Ordentliche Meldung**	**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:

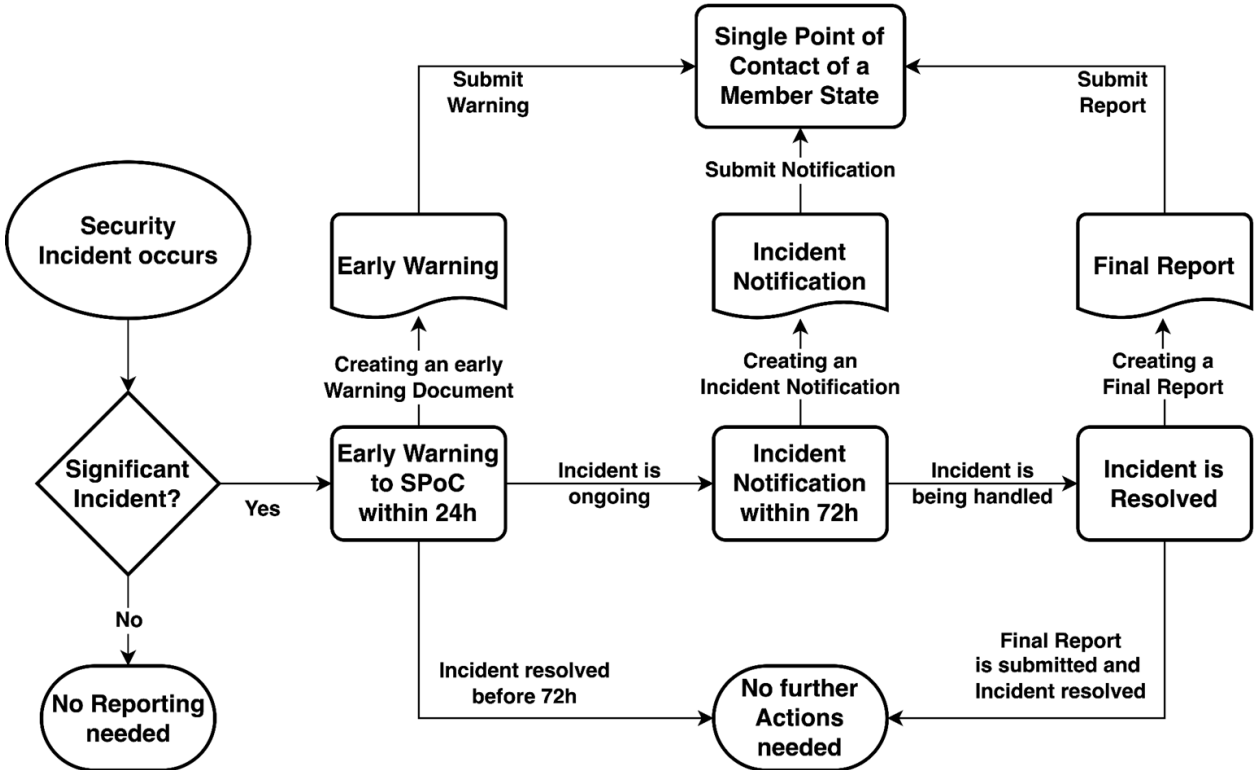
Ein Cybersicherheitsvorfall liegt vor bei..

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.

CERT.at

Welche Institutionen, mit NIS 2 Bezug sind euch bekannt ?

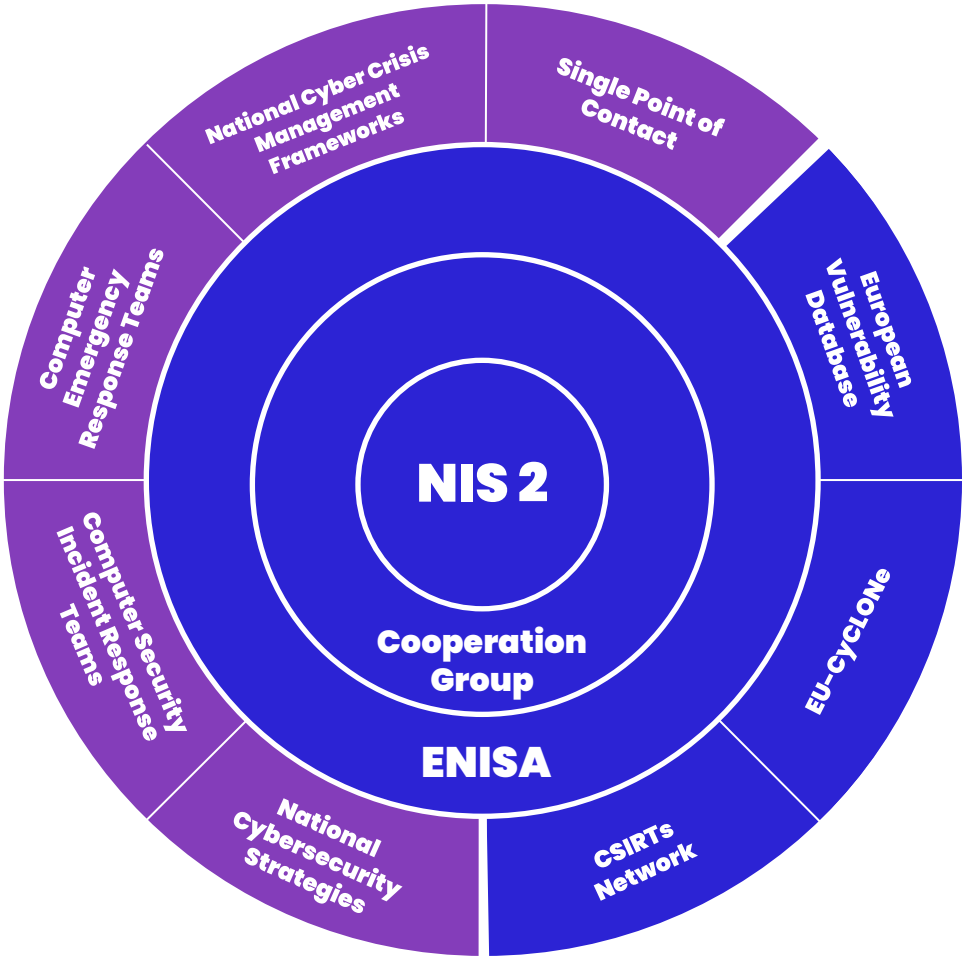
Als kurze Erinnerung, hier nochmal der vorgegebene Aufbau.

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



HoliSec

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.

HoliSec

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.

HoliSec

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.

HoliSec

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

Zeit für ein Quiz! 

Habt ihr noch Fragen zu dem Thema NIS 2?

Rechtsgrundlagen der EU

Cyber Resilience Act

Vorschlag für eine

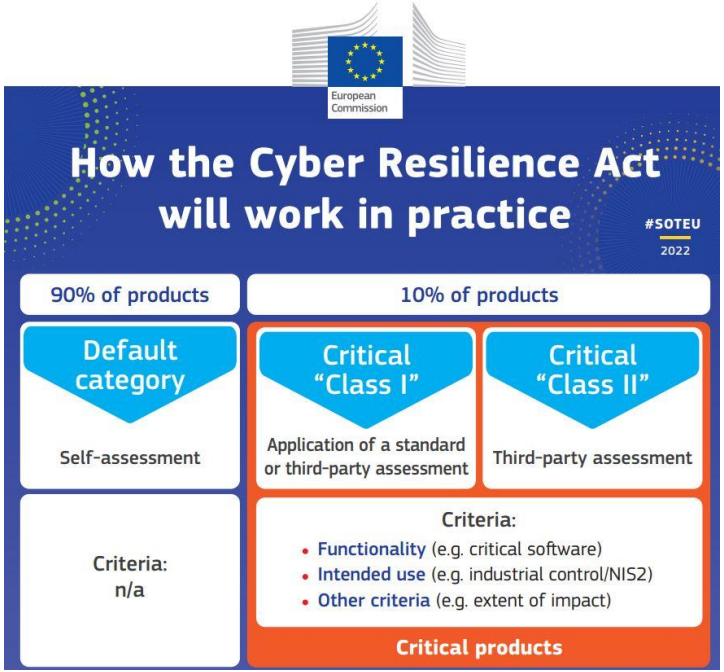
VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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

Cyber Resilience Act

- Verpflichtende Cybersicherheitsanforderungen für digitale Produkte und Software
- Harmonisierte Regeln für den gesamten Produktlebenszyklus
- CE-Kennzeichnung zur Angabe der Einhaltung neuer Cybersicherheitsstandards



HoliSec

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

Cyber Resilience Act

- **Klasse I**: z. B. Passwortmanager, Firewalls, VPNs.
- **Klasse II**: z. B. Betriebssysteme, Netzwerkmanagement-Systeme, industrielle Sicherheitslösungen.

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

Wer ist betroffen?

- Betrifft digitale Produkte (Hard- & Software) mit Netzwerkverbindung
- Umfasst auch einzelne Komponenten dieses Produkts

Ausnahmen

- nicht kommerzielle Produkte
- reine Dienstleistungen
- medizinische Geräte und In-vitro-Diagnostika mit bereits bestehenden Regelungen
- Fahrzeuge, Flugsysteme, Schiffsausrüstung und Bereiche für die bereits Regelungen mit gleichwertigen Anforderungen bestehen

Was ist zu tun ?

- Sicherheitsanforderungen während Produktlebenszyklus
- Anforderungen an Umgang mit Schwachstellen
- Konformitätsbewertung und CE-Kennzeichnung (abhängig von der Risikoklassifikation des Produkts)
- Meldepflichten

Lernziele 🚀

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



Inhalte 📦

Cyberangriffe

NIS 2 Richtlinie

Datensicherheit

Operationalize Security

HoliSec

Inhalte 📦

Cyberangriffe

NIS 2 Richtlinie

Daten-sicherheit

Operationalize Security

HoliSec

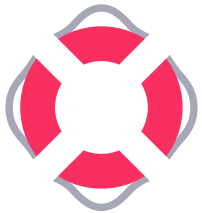
Datenssicherheit 🔒

und die Risikomanagement Maßnahmen der NIS 2

Lernziele 🚀

- Was bedeuten die Risikomanagementmaßnahmen für mein Unternehmen?
- Wie kann ich eine Umsetzung als KMU erreichen?
- Habe ich genügend Know-how im Unternehmen?

Risikomanagament maßnahmen



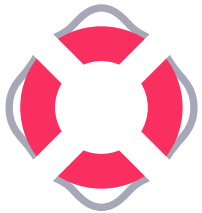
Welche Anforderungen müssen aufgrund der NIS 2 in Organisationen erfüllt werden ?

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



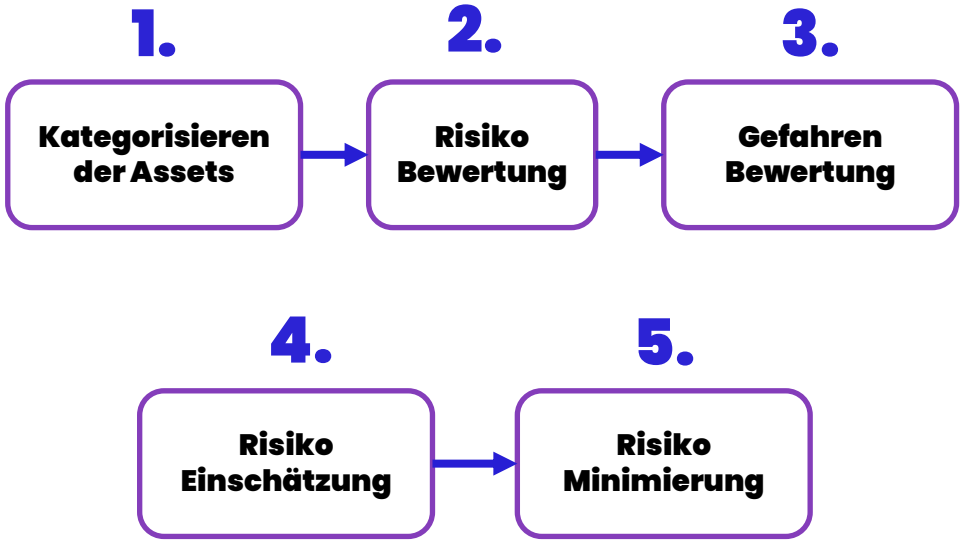
Maßnahmen, die jede Organisation treffen sollte!

HoliSec

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?



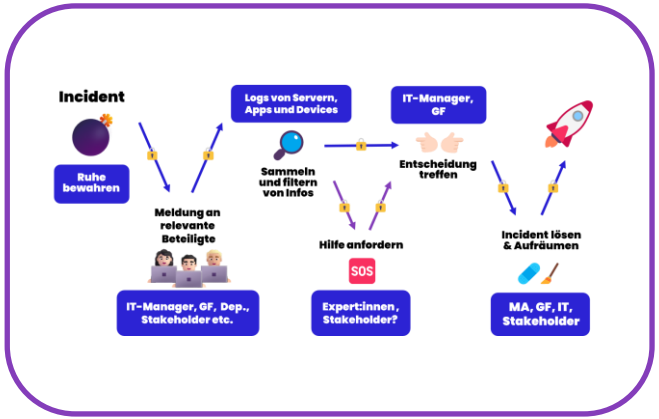
Quelle: https://searchinform.com/

Risikomanagementmaßnahmen

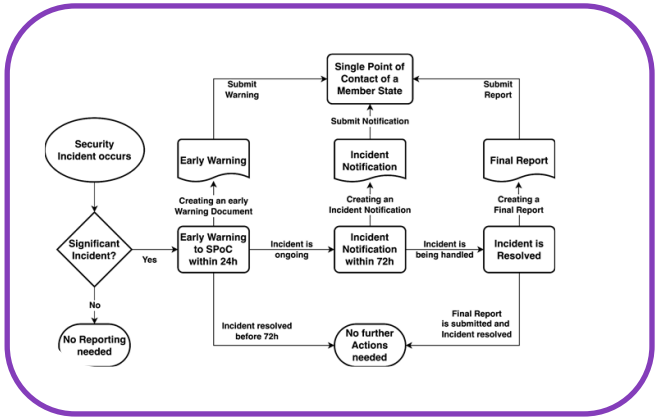
1. **Risikoanalyse und Sicherheitskonzept:** Die Risiken identifizieren, bewerten und dokumentieren.

2. Sicherheitsvorfälle und Meldepflicht

2. Sicherheitsvorfälle und Meldepflicht



Interner Incident Response Plan



NIS 2 Meldeverhalten

HoliSec

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

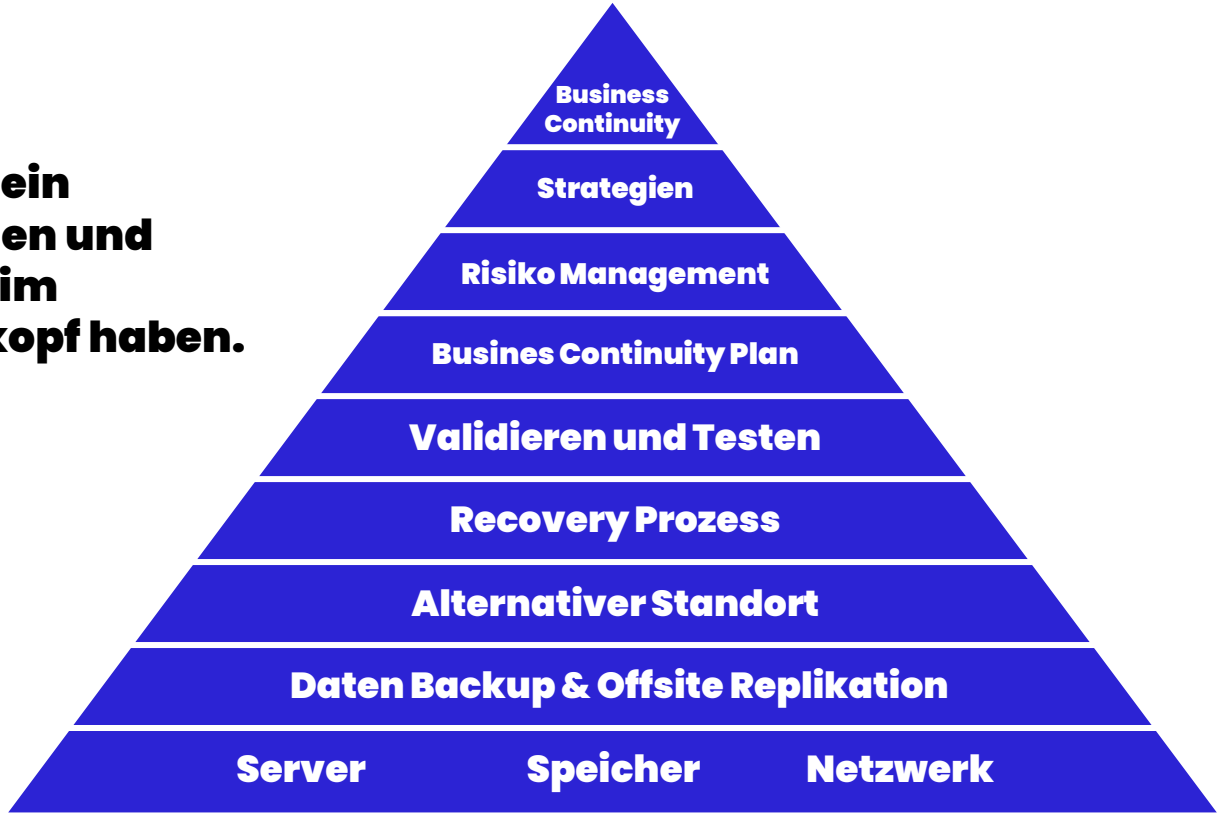
3. Backups, Continuity & Notfallmanagement

💡 **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/

3. Backups, Continuity & Notfallmanagement

Diese Fragen solltet ihr euch stellen:

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

HoliSec

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

Risikomanagementmaßnahmen

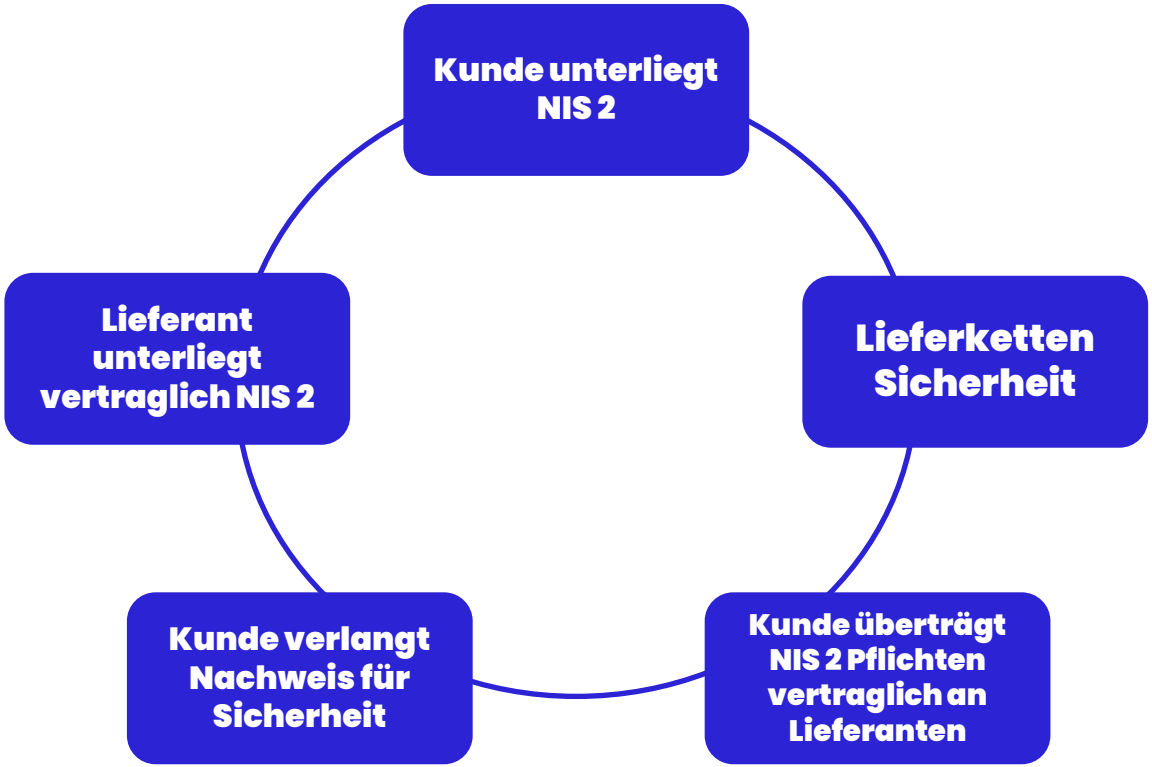
1. **Risikoanalyse und Sicherheitskonzept:** Die Risiken identifizieren, bewerten und dokumentieren.

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

4. Sicherheit in der Lieferkette

Diese Fragen solltet ihr euch stellen:

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

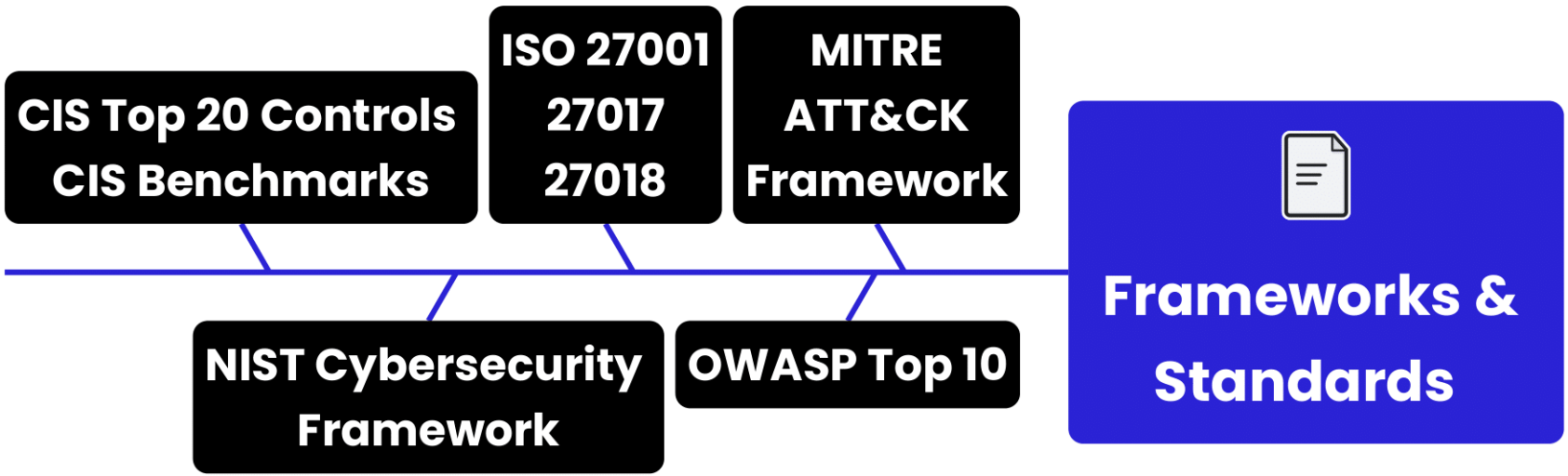
Quelle: https://www.wko.at/it-sicherheit/nis2-uebersicht - Webinar

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

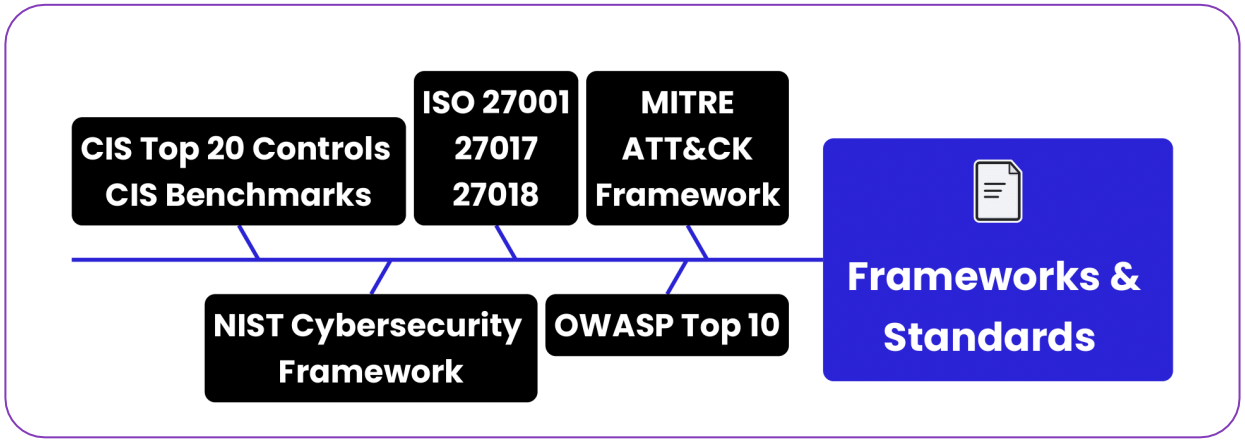
5. Erwerb, Entwicklung und Wartung von ITK



5. Erwerb, Entwicklung und Wartung von ITK

Diese Fragen solltet ihr euch stellen:

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



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 **A**dequate **R**easonable **E**ffective

HoliSec

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

HoliSec

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?

HoliSec

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

7. Awareness und Cyber-Hygiene

WHY

Warum und wofür ist es wichtig ?

HOW

Wie willst du dein Ziel erreichen?

WHAT

was machst du um dein Ziel zu erreichen?

HoliSec

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**

HoliSec

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

Risikomanagementmaßnahmen

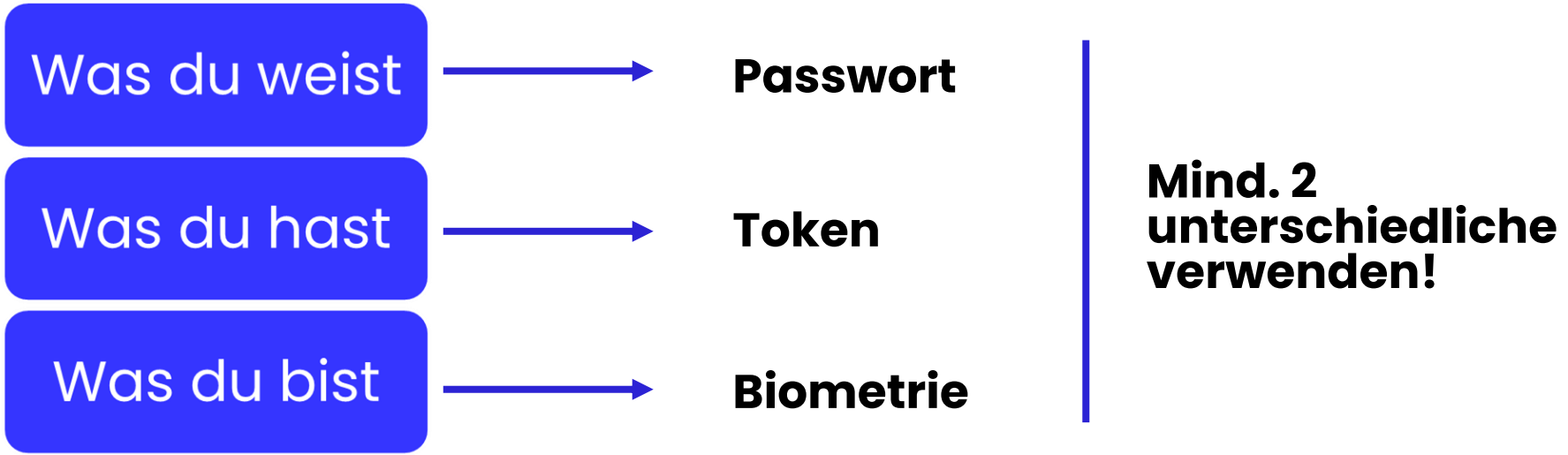
7. Awareness und Cyber-Hygiene:
Alle technischen oder organisatorischen Maßnahmen sind nur dann wirkungsvoll, wenn alle Mitarbeiter*innen sie kennen und umsetzen.

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

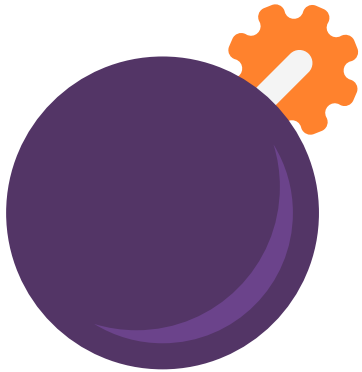
Zeit für ein Quiz! 

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

HoliSec

Ausgangspunkt für alle Maßnahmen ist unser Risikomanagement.

Es geht darum Risken festzustellen und zu verwalten.

Der folgende Prozess skizziert eine mögliche Herangehensweise.

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

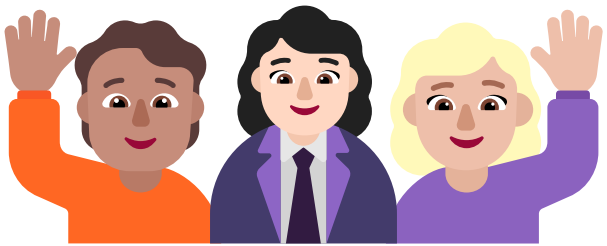
Vision/Mission

Wertschöpfungs kette

Produkte/ Dienstleistung

HoliSec

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

HoliSec

Risikomanagement Prozess

Assets

Welche Assets benötigt man für was?

- Software
- Hardware
- Daten
- Services
- Lieferanten

Risikomanagement Prozess

Ziele der Organisation

Vision/Mission

Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Wertschöpfungs kette

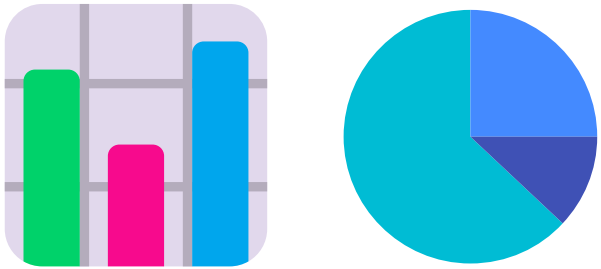
Produkte/ Dienstleistung

Assets

Software/ Hardware

HoliSec

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

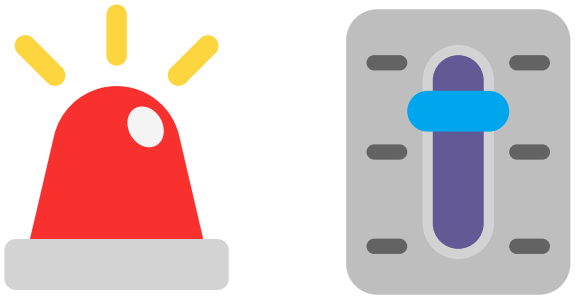
Produkte/ Dienstleistung

Assets

Software/ Hardware

HoliSec

Risikomanagement Prozess



Maßnahmen setzen

- **Adäquat zu den zugewiesenen Einstufungen.**

Leicht **Mittel** **Stark**

Risikomanagement Prozess

Ziele der Organisation

Vision/Mission

Wertschöpfungs kette

Produkte/ Dienstleistung

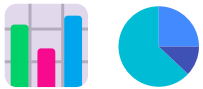
Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Assets

Software/ Hardware

Leicht, Mittel, Stark



Kritikalität zuweisen

Maßnahmen setzen

Entsprechend Kritikalität

HoliSec

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

Wertschöpfungs kette

Produkte/ Dienstleistung

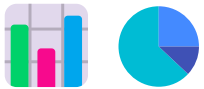
Verantwortlichkeiten/ Ressourcen

Abteilungen &Teams

Assets

Software/ Hardware

Leicht, Mittel, Stark



Kritikalität zuweisen

Maßnahmen setzen

Entsprechend Kritikalität

HoliSec

Blick hinter die Kulissen 

Anhang 3 und NIS Fact Sheets

HoliSec

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

Wie können wir nun nachweißen, dass wir die Maßnahmen umgesetzt haben?

Standards & Normen

Es gibt viele unterschiedliche Cybersecurity Standards.

- **ISO 27001**
- **IEC 62443**
- **NIST SP 800 – CSF**
- **CIS Controls**

Standards & Normen

Problem: Fokus liegt auf Enterprise Level!

- **ISO 27001**
- **IEC 62443**
- **NIST SP 800 – CSF**
- **CIS Controls**

Für ein KMU ist eine solche Umsetzung unrealistisch.

Sitution in KMUs

z. B. indirekte Betroffenheit
- Lieferkette

z.B. Vorlagebericht für
- Cyberversicherung

- **Know-How Mangel**
- **Budget für die Umsetzung klein**
- **Cybersecurity meistens ein neues Thema**
- **Standards sind viel zu Breit**

Wie denkt ihr ist dennoch ein Nachweis möglich?

Eine niederschwellige Zertifizierung mit ausreichender Qualität.

Cyber Risk Rating Österreich

HoliSec

Cyber Risk 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**

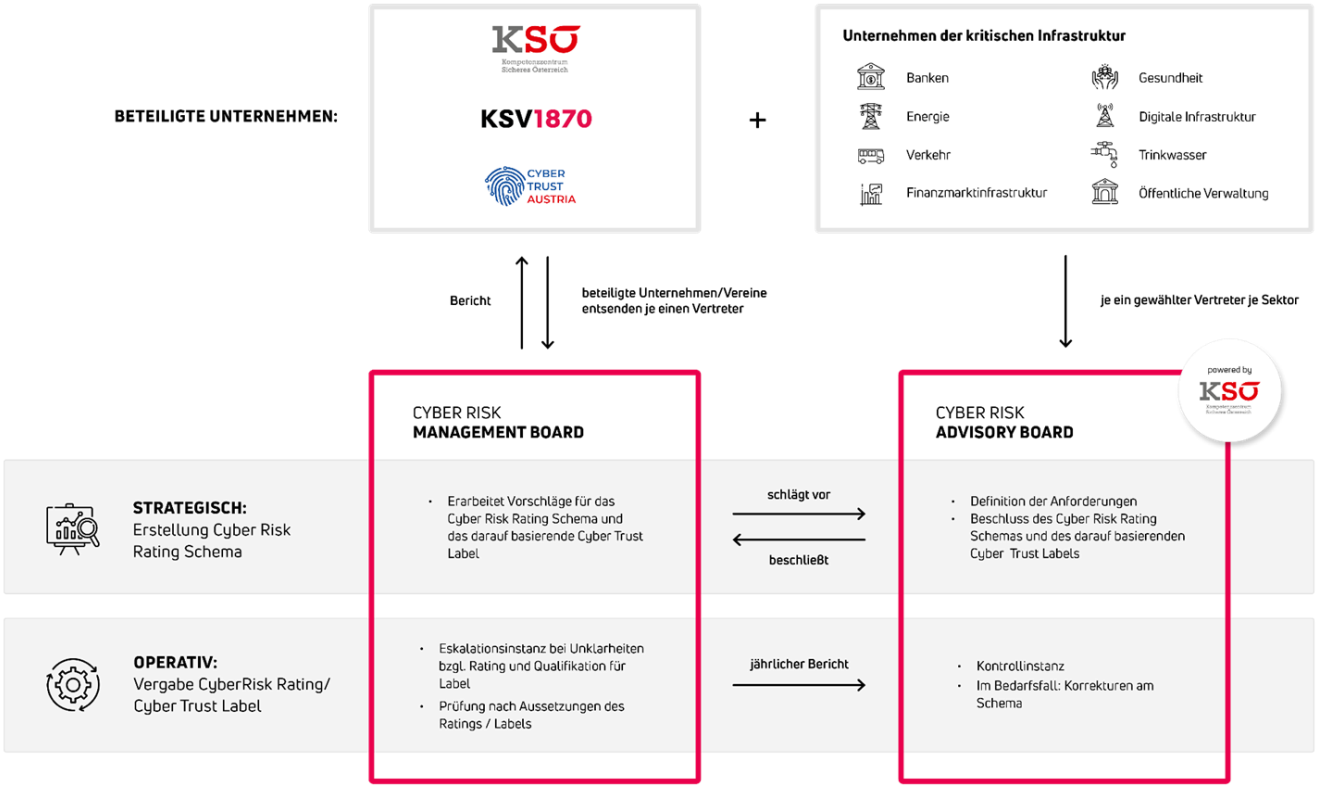
KSÖ
Kompetenzzentrum Sicheres Österreich

CYBER TRUST AUSTRIA

KSV1870

HoliSec

Cyber Risk Rating Österreich



HoliSec

CYBER TRUST AUSTRIA

Wie funktioniert die Zertifizierung?

Cyber Risk Rating Österreich

- 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

HoliSec

Cyber Risk Rating Österreich

- 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

HoliSec

Cyber Risk Rating Österreich

- 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

HoliSec

Cyber Risk Rating Österreich

- 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

HoliSec

Cyber Risk Rating Österreich

- 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

HoliSec

Cyber Risk Rating Österreich

- 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

HoliSec

Cyber Risk Rating Österreich

- 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

HoliSec

B – Rating

Für KMUs & Zulieferer (Anhang 2).

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

HoliSec

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

A - Rating

CYBER TRUST AUSTRIA

Für KMUs & Zulieferer (Anhang 1).

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

A+ Rating

CYBER TRUST AUSTRIA

Für Große & Zulieferer (Anhang 1).

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

Wir gehen jetzt alle Anforderungen Step-by-Step durch.

Parallel könnt ihr direkt euer eigenes Asessment ausfüllen.

demo.cyberrisk-rating.at

HoliSec

B1. Informations-sicherheitsrichtlinie

CYBER TRUST AUSTRIA

Was ist eine Informations-sicherheits Richtlinie?

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.

B1. Informationssicherheitsrichtlinie

- IT-Grundschutz BSI
- DIN SPEC 27076
- ISO 27001 - Control 5.1
- IT Sicherheitshandbuch
- Basismaßnahmen
- KSV 1870 - Snacks
- kmusec

B2. Security Schulungen

B2. Security Schulungen

Anforderung:

Schulen Sie ihre Mitarbeiter regelmäßig in Informationssicherheit?

Anforderungskriterien:

- Sicherer Umgang mit Computern und Informationen
- Sicher im Internet
- Gefährliche Schadprogramme
- Verhalten bei Verdacht auf IT-Sicherheitsvorfall
- Passwörter richtig auswählen und verwalten
- E-Mails, Spam und Phishing

CYBER TRUST AUSTRIA

Macht ihr Schulungen in eurem Unternehmen?

B2. Security Schulungen

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- KSV 1870 - Snacks
- kmusec

B2. Security Verantwortung

CYBER TRUST AUSTRIA

Gibt es bei euch einen oder mehrere Security Verantwortlichen?

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 […].

B3. Security Verantwortung

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- KSV 1870 - Snacks
- kmusec

B4. Assetmanagement & Stakeholder

CYBER TRUST AUSTRIA

Habt ihr im Unternehmen ein Asset Management?

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.**

Praxisübung – Asset Management

Ablauf ⏩

- Findet heraus mit welchen Tools Asset Management umgesetzt werden kann.

Tipps 💡

- Ein gut gepflegtes Tabellenblatt entspricht den Anforderungen.

Dokumentation 📃

- Liste mit Tools
- Vor- und Nachteile unters. Lösungen

Zeit & Format 🕐

- 10 min Recherche
- 5 min Diskussion

B4. Asset Management & Stakeholder

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- KSV 1870 - Snacks
- kmusec

B5. Berechtigungskonzept + Enforcement

Anforderung:

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

Anforderungskriterien:

- **Bei dem Zugang zu den Anwendungen/Dateisystemen muss über Berechtigungen sichergestellt werden, dass nur berechtigte Personen zugreifen können.**
- **Es gibt eine dokumentierte Vorgehensweise zur Vergabe und Entzug von Berechtigungen.**

B5. Berechtigungskonzept + Enforcement

CYBER TRUST AUSTRIA

Wie kann man so ein Konzept umsetzen?

Praxisübung – Access Control Matrix

Ablauf ⏩

- Erstellt eine schematische Access Control Matrix mit den wichtigsten Benutzergruppen & Assets.

Tipps 💡

- Vergesst nicht, dass hier auch der physische Zugriff berücksichtigt werden sollte.

Dokumentation 📄

- Access Control Matrix (z.B mit Excel)

Zeit & Format 🕐

- 10 min Ausarbeitung
- 5 min Diskussion

B5. Berechtigungskonzept + Enforcement

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- KSV 1870 - Snacks
- kmusec

B6. Passwort Richtlinien & Management

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.

CYBER TRUST AUSTRIA

Habt ihr Passwort Regeln definiert?

B6. Passwort Richtlinien & Management

Passwortmanager verwenden & Multi Faktor Authentifizierung aktivieren

B6. Passwort Richtlinien & Management

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- NIS GV Kennwortsicherheit

B7. Empfohlene Sicherheitskonfiguration

B7. Empfohlene Sicherheitskonfiguration

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.

CYBER TRUST AUSTRIA

Sind eure Konfigurationen nach den Sicherheitsempfehlungen der Hersteller gesetzt?

HoliSec

B7. Empfohlene Sicherheitskonfigurationen

- NIST Configuration Checklist
- CISA Service Configuration Best Practices
- Information Security Manual
- Herstellerdokumentationen
  - Security Best Practices
  - Security Hardening Guides
- Doku über Asset Management Items.

B8. Öffentliche Schnittstellen

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.

CYBER TRUST AUSTRIA

Habt ihr solche Software im Einsatz?

B8. Öffentliche Schnittstellen

- NIST - Secure System Applications
- kmusec Ratgeber Pentest
- CISA – Pentest
- NIS 2 & Pentesting

B9. Patch Management

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.**
- **Systeme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden, werden rechtzeitig außer Betrieb genommen.**

CYBER TRUST AUSTRIA

Wie patcht ihr aktuell Server, Applikationen und Endgeräte?

B9. Patch Management

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- kmusec.com

B10. Network Security

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.

CYBER TRUST AUSTRIA

Wie setzt ihr eure Netzwerk Sicherheit um?

B10. Network Security

- BSI Netzwerksicherheit
- CIS Control 12 – Network Infrastructure Managment
- NIST – Network Security
- Network Security - Quick Wins
  - Least Privilege Access
  - Macro and Micro Segmentation
  - Firewall mit VLANs
  - Perimeter Absichern
  - Unterschied zwischen Public und Private Zones

B11. Antivirus

B11. Antivirus

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.

CYBER TRUST AUSTRIA

Welche AV Lösung habt ihr im Einsatz?

B11. Antivirus

Ist diese auch mit dem Asset Management verknüpft?

B11. Antivirus

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- kmusec.com

B12. Verschlüsselte Kommunikation

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.

CYBER TRUST AUSTRIA

Wie kommuniziert ihr mit Kunden?

B12. Verschlüsselte Kommunikation

- 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

B13. Aufbewahrung von Logs

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.**

CYBER TRUST AUSTRIA

Habt ihr einen zentralen Speicherort für Logs?

B13. Aufbewahrung von Logs

- IT-Grundschutz BSI
- DIN SPEC 27076
- IT Sicherheitshandbuch
- Basismaßnahmen
- kmusec.comNIS GV - Log Aufbewahrung

B14. Verhalten im Notfall

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**

CYBER TRUST AUSTRIA

Was ist das wichtigste an der Planung?

B14. Verhalten im Notfall

Testen und Validieren.

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

HoliSec

Lernziele 🚀

- Was bedeuten die Risikomanagementmaßnahmen für mein Unternehmen?
- Wie kann ich eine Umsetzung als KMU erreichen?
- Habe ich genügend Know-how im Unternehmen?

Datenschutz 

anhand der Vorgaben der Datenschutz Grundverordnung

Lernziele 🚀

- Was ist Datenschutz?*
- Was sind personenbezogene Daten und Datenverarbeitung?*
- Wie wird man compliant?*

*Laut Datenschutz Grundverordnung der Europäischen Union

Kennt ihr den Begriff Data Governance?

Data Governance bedeutet buchstäblich die Regierung über Daten.

Data governance helps manage whose data you collect, how you collect and enhance it, and what you do with it after collection.

Quelle: Jarmul, K. (2023). Practical data privacy. O'Reilly Media, Inc.

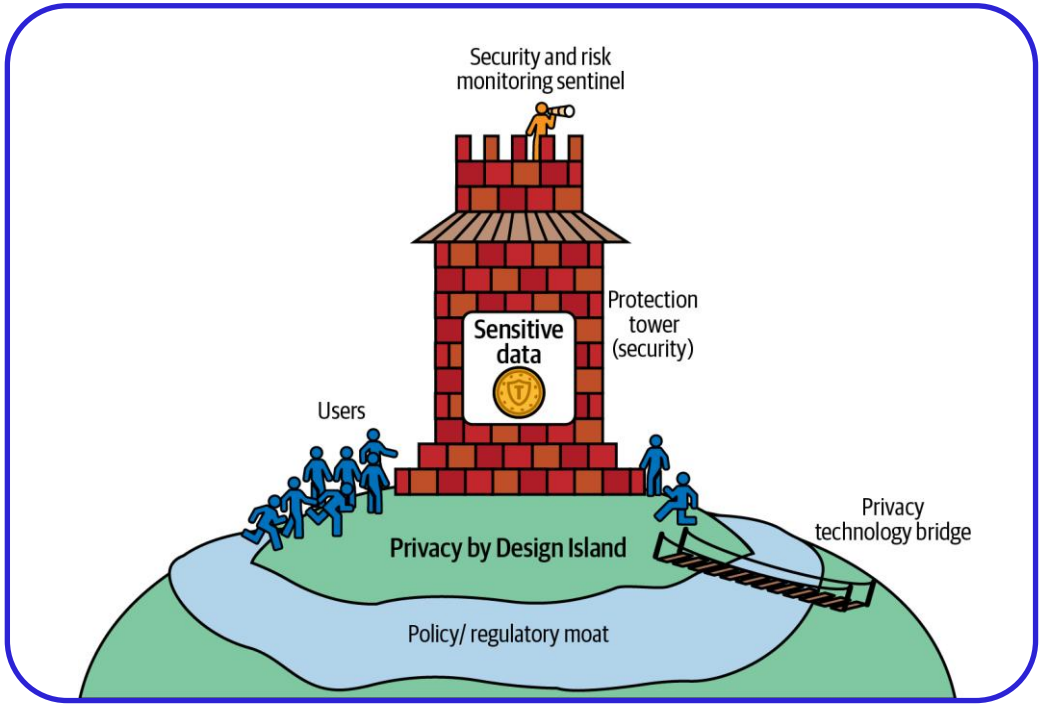
Was ist Data Governance?

"Privacy by Design" sind Prinzipien, die sicherstellen, dass Systeme und Software von Anfang an datenschutzorientiert gestaltet werden.

Quelle: https://noyb.eu/de/privacy-shield-20-erste-reaktion-von-max-schrems

Data Governance vs. Privacy & Security

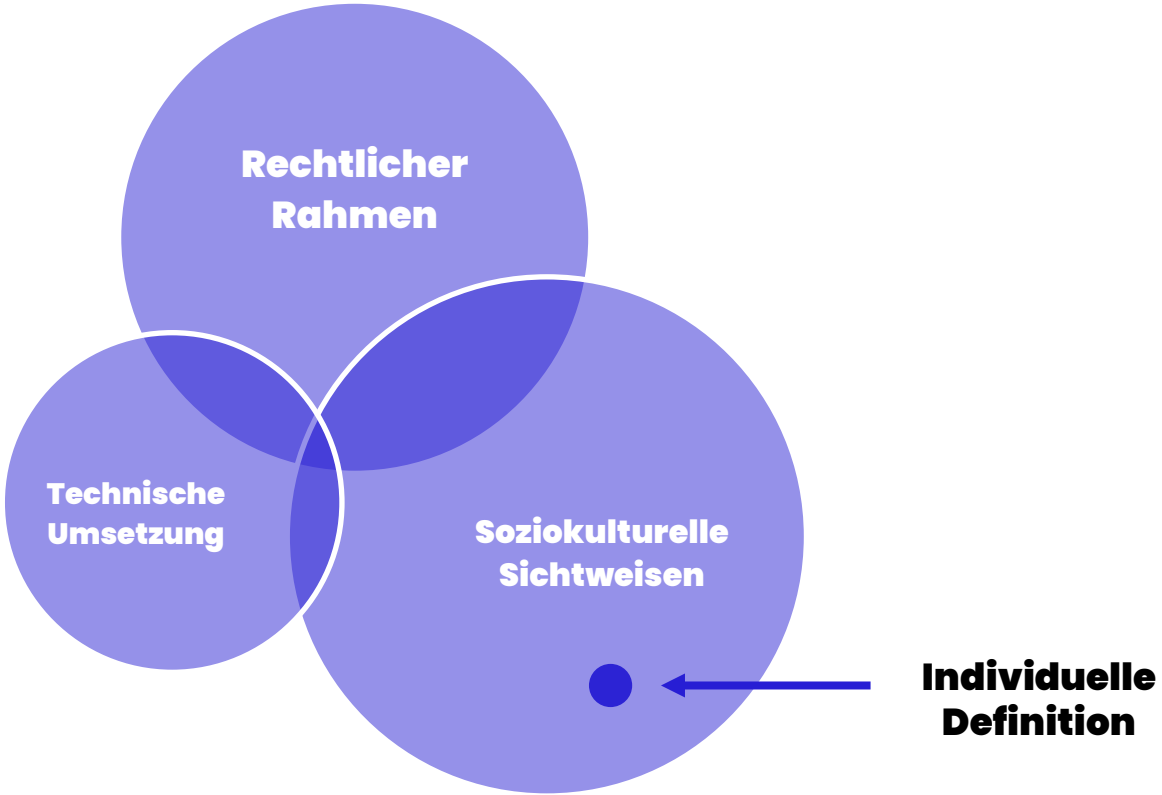
- **Privacy by Design Island**
- **Sicherheitsturm (Security)**
- **Graben & Brücken (Privacy)**



HoliSec

Quelle: Jarmul, K. (2023). Practical data privacy. O'Reilly Media, Inc.

Data Privacy = Datenschutz



HoliSec

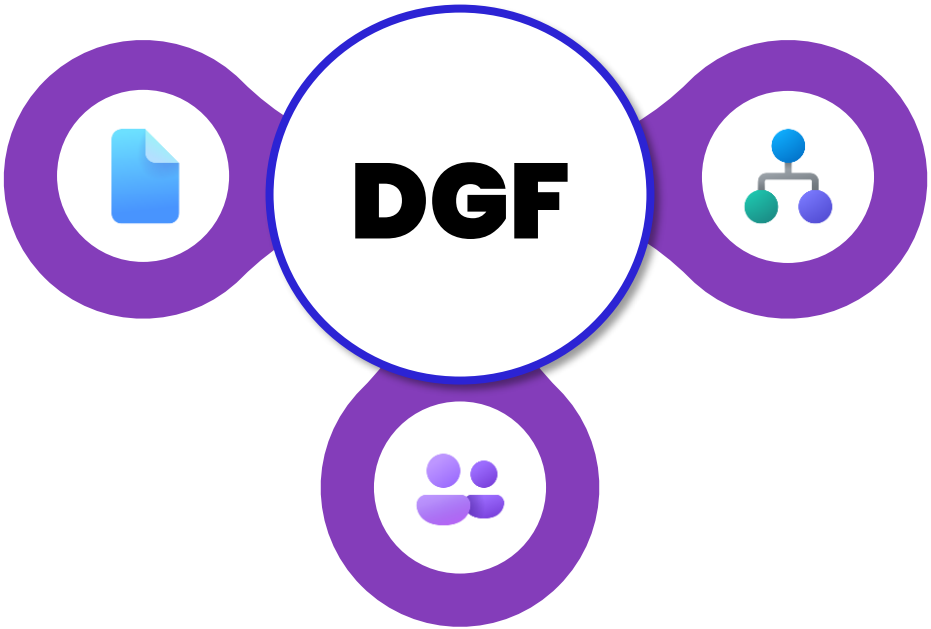
Live Demo 

Datenschutz

Was denkt ihr wie kann man Data Governance in der Praxis umsetzen?

Data Governance Framework

Richtlinie



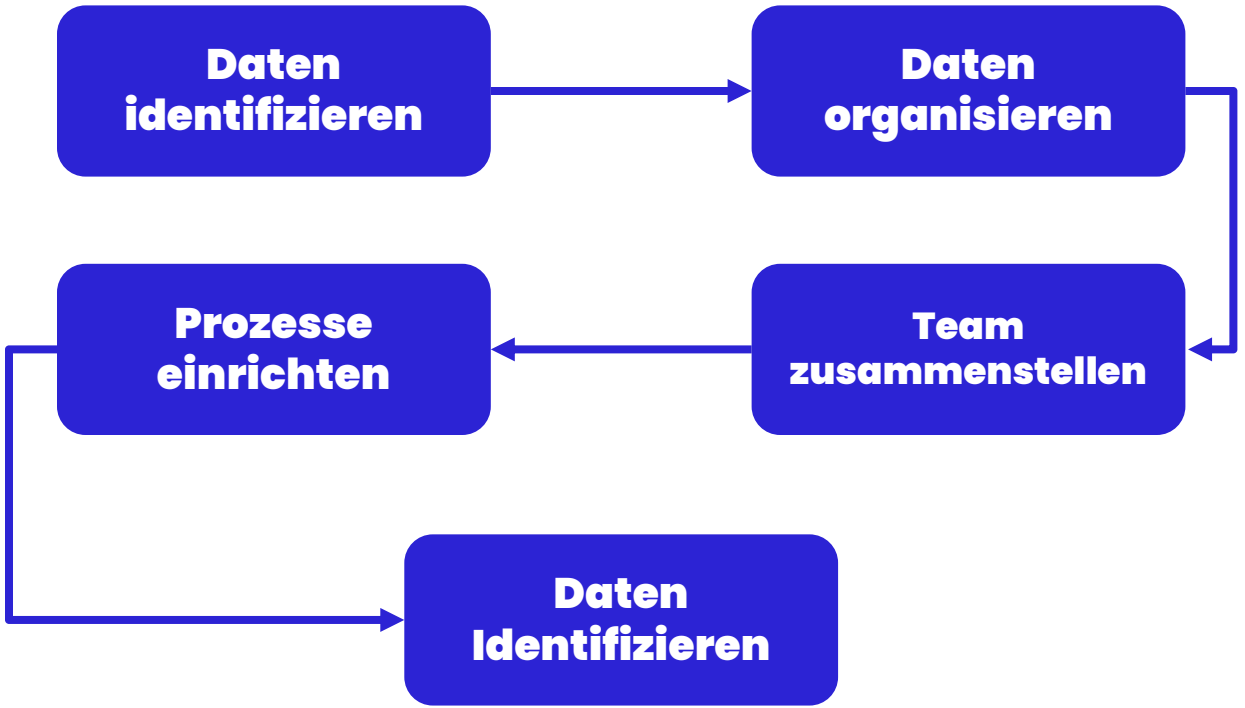
Prozess

Verantwortliche

HoliSec

Wie startet man damit am besten?

Wie startet man mit Data Governance?



HoliSec

Daten identifizieren mittels Daten Klassifizierung.

HoliSec

Daten Kategorien

Öffentliche Daten

Interne Daten

Vertrauliche Daten

Praxisübung – Data Governance

Ablauf ⏩

- Ausarbeitung simplen Datenrichtlinie samt Datenklassifizierung.

Tipps 💡

- Beispiel einer Richtlinie.

Dokumentation 📄

- Grobkonzeption der Datenrichtlinie
- Datenkategorien

Zeit & Format 🕛

- 20 min Recherche
- 5 min Diskussion

HoliSec

Was versteht ihr unter dem Begriff Datenschutz?

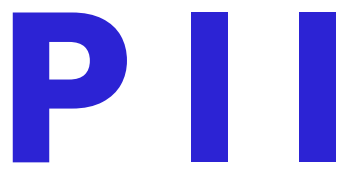
Datenschutz Grundverordnung (DSGVO)

HoliSec

Was ist Datenschutz laut DSGVO ?

Schutz von
personenbezogenen Daten

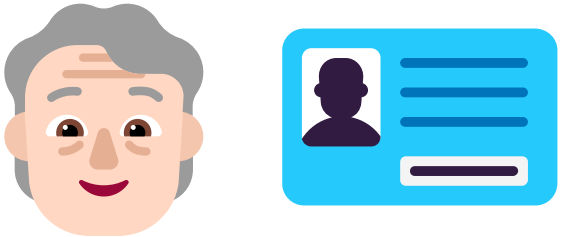
Was sind personenbezogene Daten (PII) ?



Was sind personenbezogene Daten (PII) ?

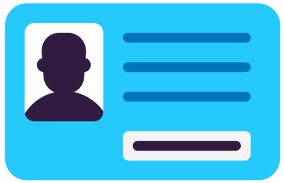
Personally **I**dentifiable **I**nformation

Was sind personenbezogene Daten (PII) ?



alle Informationen, die sich auf identifizierbare Person beziehen

Was sind personenbezogene Daten (PII) ?



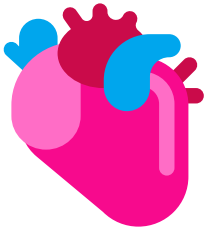
Name

Adresse

Telefonnummer

E-Mail-Adresse

Geburtsdatum



Gesundheitsdaten

Was ist Datenverarbeitung laut DSGVO?

Datenverarbeitung im Sinne der DSGVO bedeutet jegliche Erhebung, Speicherung, Nutzung oder Weitergabe personenbezogener Daten (PII).

Quelle: https://www.wko.at/datenschutz/eu-dsgvo-wichtige-begriffsbestimmungen

Was ist Datenverarbeitung laut DSGVO?

kurz gesagt...

Irgendwas mit PII tun

Gilt die DSGVO auch für mein Unternehmen? 🙈

Gilt die DSGVO auch für mein Unternehmen?

kurz gesagt...

JA!

Gilt die DSGVO auch für mein Unternehmen?

Die DSGVO gilt…

- für **alle** Unternehmen in der **EU**.
- **inhaltlich**, wenn „personenbezogene Daten (**PII**)“ vorliegen und diese „verarbeitet“ werden.

Quelle: https://europa.eu/youreurope/business/dealing-with-customers/data-protection

Was ist das Minimum, das ich tun sollte? 🔽

Was ist das Minimum, das ich tun sollte?

Die Betroffenenrechte einhalten

Jetzt seid Ihr dran! 🚀

Praxisübung - Datenanfrage

Ablauf ⏩

- Stellt eine Auskunftsanfrage über eure persönlichen Daten an das Unternehmen eurer Wahl.

Tipps 💡

- Ihr wollt eine schnelle Antwort? Sendet die Anfrage an Google oÄ., die haben den Prozess automatisiert

Dokumentation 📄

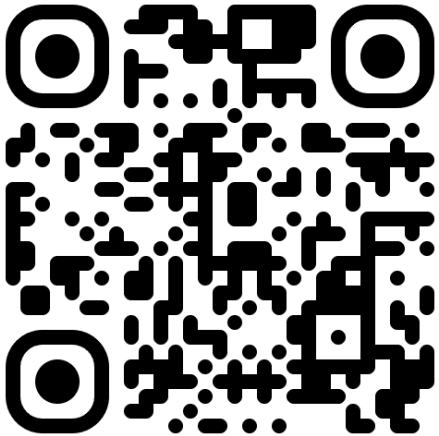
- Bestägigung von Datenanfragen.de

Zeit & Format 🕐

- 5 min Anfrage stellen

HoliSec

Praxisübung - Datenanfrage



www.datenanfragen.de

HoliSec

Was sind die Betroffenenrechte laut DSGVO?

- Recht auf Information
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Einschränkung
- Recht auf Widerspruch
- Recht auf Löschung
- Recht auf Datenübertragbarkeit

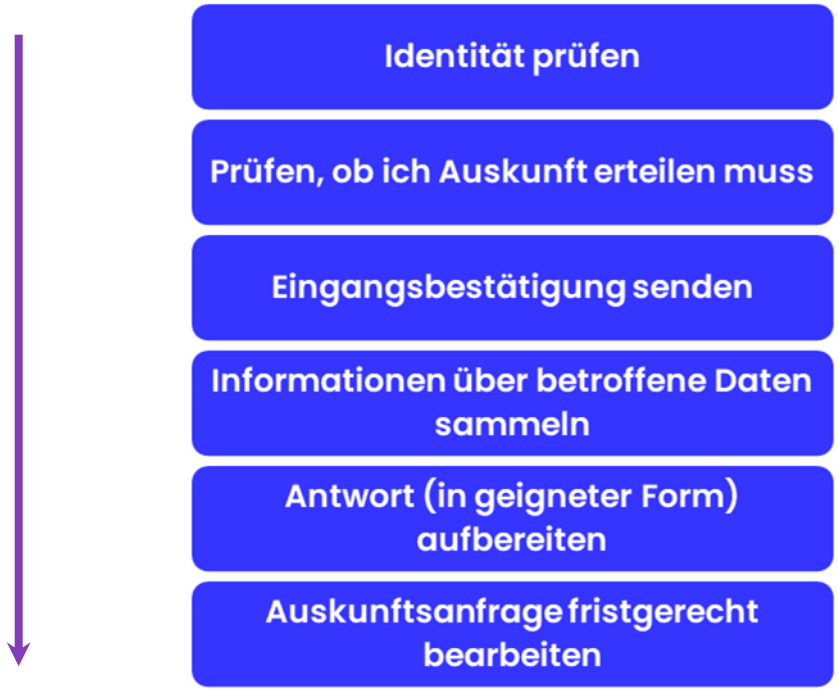
HoliSec

Was muss ich als Unternehmen machen?

Auskunftsanfrage fristgerecht beantworten

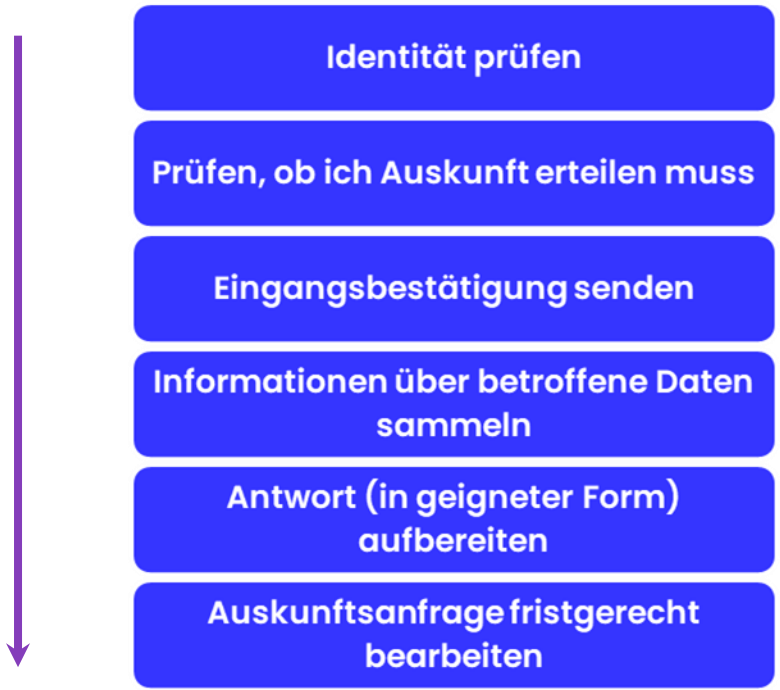
1 Monat

Auskunftsanfrage – der Prozess



HoliSec

Was ist für euch wichtig?



Anfrage rechtzeitig an zuständige Person weitergeben!

Was ist sonst noch zu tun um Compliant zu werden?

Wie wird man DSGVO compliant?

1. **Betroffenenrechte**
2. **Dokumentationspflicht**
3. **Informationspflicht**
4. **Laufender Datenschutz**

HoliSec

Wie wird man DSGVO compliant?

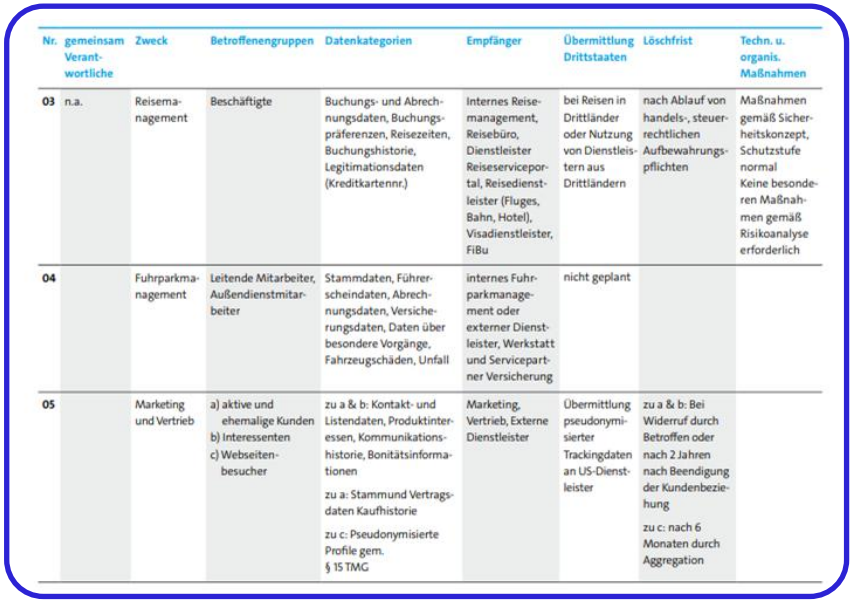
1. **Betroffenenrechte**
2. **Dokumentationspflicht**
3. **Informationspflicht**
4. **Laufender Datenschutz**

HoliSec

Dokumentationspflicht

Verarbeitungstätigkeitsverzeichnis

- Zweckbestimmung der Verarbeitung
- Datenkategorien
- Betroffenenkreis
- Datenempfänger
- Datenübermittlung in Drittländer
- Löschfristen



Nr.	gemeinsam Verant-wortliche	Zweck	Betroffenengruppen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist	Techn. u. organis. Maßnahmen
03	n.a.	Reisema-nagement	Beschäftigte	Buchungs- und Abrech-nungsdaten, Buchungs-präferenzen, Reisezeiten, Buchungshistorie, Legitimationsdaten (Kreditkartennr.)	Internes Reise-management, Reisebüro, Dienstleister Reiseserviceportal, Reisedienst-leister (Fluges, Bahn, Hotel), Visadienstleister, FiBu	bei Reisen in Drittländer oder Nutzung von Dienstleis-tern aus Drittländern	nach Ablauf von handels-, steuer-rechtlichen Aufbewahrungs-pflichten	Maßnahmen gemäß Sicher-heitskonzept, Schutzstufe normal Keine besonde-ren Maßnah-men gemäß Risikoanalyse erforderlich
04		Fuhrparkma-nagement	Leitende Mitarbeiter, Außendienstmitar-beiter	Stammdaten, Führer-scheindaten, Abrech-nungsdaten, Versiche-rungsdaten, Daten über besondere Vorgänge, Fahrzeugschäden, Unfall	internes Fuhr-parkmanage-ment oder externer Dienst-leister, Werkstatt und Servicepart-ner Versicherung	nicht geplant		
05		Marketing und Vertrieb	a) aktive und ehemalige Kunden b) Interessenten c) Webseiten-besucher	zu a & b: Kontakt- und Listendaten, Produktinter-essen, Kommunikations-historie, Bonitätsinforma-tionen zu a: Stammund Vertrags-daten Kaufhistorie zu c: Pseudonymisierte Profile gem. § 15 TMG	Marketing, Vertrieb, Externe Dienstleister	Übermittlung pseudonymi-sierter Trackingdaten an US-Dienst-leister	zu a & b: Bei Widerruf durch Betroffen oder nach 2 Jahren nach Beendigung der Kundenbezie-hung zu c: nach 6 Monaten durch Aggregation	

HoliSec

Beispielverzeichnis

Nr.	gemeinsam Verant-wortliche	Zweck	Betroffenengrup-pen	Datenkategorien	Empfänger	Übermittlung Drittstaaten	Löschfrist	Techn. u. organis. Maßnahmen
01	Muster-mann Vertriebs Inc. Muster-mann Datacenter Inc.	Bewerber-manage-ment	Bewerber	Stammdaten, Daten über Kenntnisse und Fähigkeiten wie Zeugnis-se, Lebenslauf, Beurtei-lungen, Kommunikati-onsdaten	Recruiting, Fachabteilung, FiBu, Mitbe-stimmungsgre-mien, Personal-dienstleister	USA	Bewerbungsunter-langen wie Zeugnisse, Lebenslauf etc.: 4 Monate nach Abschluss des Bewerbungsver-fahrens; mit Einwilligung des Betroffenen: 2 Jahre nach Eingang Bewer-bungsanschreiben, Korrespondenz: 10 Jahre	Maßnahmen gemäß Sicherheitskonzept, Schutzstufe 1

HoliSec

Technische & organisatorische Maßnahmen (TOM)

Verschlüsselung

Identitäten

TOM

Datenprüfung

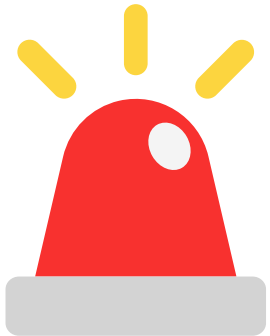
Wiederherstellung

Verfügbarkeit

Datenpanne

jeder Fall, wo personenbezogene Daten…

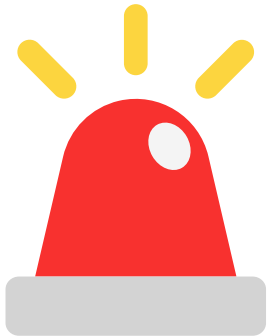
- **in die Hände unbefugter Dritte gelangen**
- **nicht mehr zugreifbar sind**
- **unbefugt verändert wurden**



Datenpanne - Folgen

bei einem Datenschutz Verstoß drohen...

- **hohe Verwaltungsstrafen**
- **Haftung und Schadensersatz**
- **Image Probleme**



Auftragsverarbeiter

Behörde

Betroffene Person

Daten anfragen

Daten Auskünfte

Datenschutz beauftragte

Verantwortliche Organisation

Vertrag

Datenschutz beauftragter

Auftrags-verarbeiter

HoliSec

Datenschutzfolgeabschätzung (DSFA)

1 **Geringes Risiko**

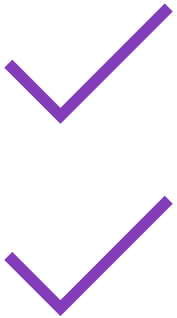
2 **Mittleres Risiko**

3 **Hohes Risiko**

HoliSec

Wie wird man DSGVO compliant?

1. **Betroffenenrechte**
2. **Dokumentationspflicht**
3. **Informationspflicht**
4. **Laufender Datenschutz**



HoliSec

Informationspflicht

Vorabinformation vor einer Datenerhebung

Transparenz schaffen

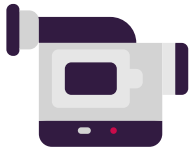
Zweck/ Rechtsgrundlage

Kommunikation

Live Demo 

Datenschutzerklärung

Situationen der Datenerhebung



Videoüberwachung

Verkauf

Internet

Telefon

Fotorechte

Quelle: https://www.lda.bayern.de/de/thema_informationspflichten.html

Wie wird man DSGVO compliant?

1. **Betroffenenrechte**
2. **Dokumentationspflicht**
3. **Informationspflicht**
4. **Laufender Datenschutz**

HoliSec

Laufender Datenschutz

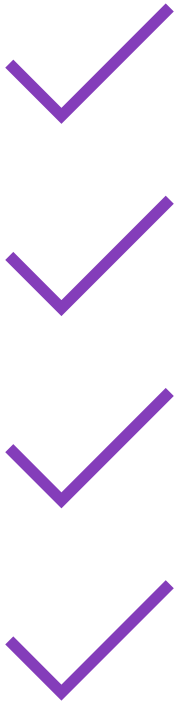
Mitarbeiter Trainings

Datenschutz-beauftragter

Umsetzung der TOMS

Wie wird man DSGVO compliant?

1. **Betroffenenrechte**
2. **Dokumentationspflicht**
3. **Informationspflicht**
4. **Laufender Datenschutz**



HoliSec

Lernziele 🚀

- Was ist Datenschutz?*
- Was sind personenbezogene Daten und Datenverarbeitung?*
- Wie wird man compliant?*

*Laut Datenschutz Grundverordnung der Europäischen Union

Jetzt seid Ihr dran! 🚀

Praxisübung - Detektivarbeit 🔍

Ablauf ⏩

- Versucht möglichst viel über euch und den [Kunde] im Internet herauszufinden
- Überlegt euch wie diese Daten missbraucht werden können

Dokumentation 📃

- Notiert die relevantesten Informationen und zugehörigen Quellen

Zeit & Format 🕐

- 15 min Recherche
- 5 min Diskussion

Inhalte 📦

Cyberangriffe

NIS 2 Richtlinie

Datensicherheit

Operationalize Security

HoliSec

Inhalte 📦

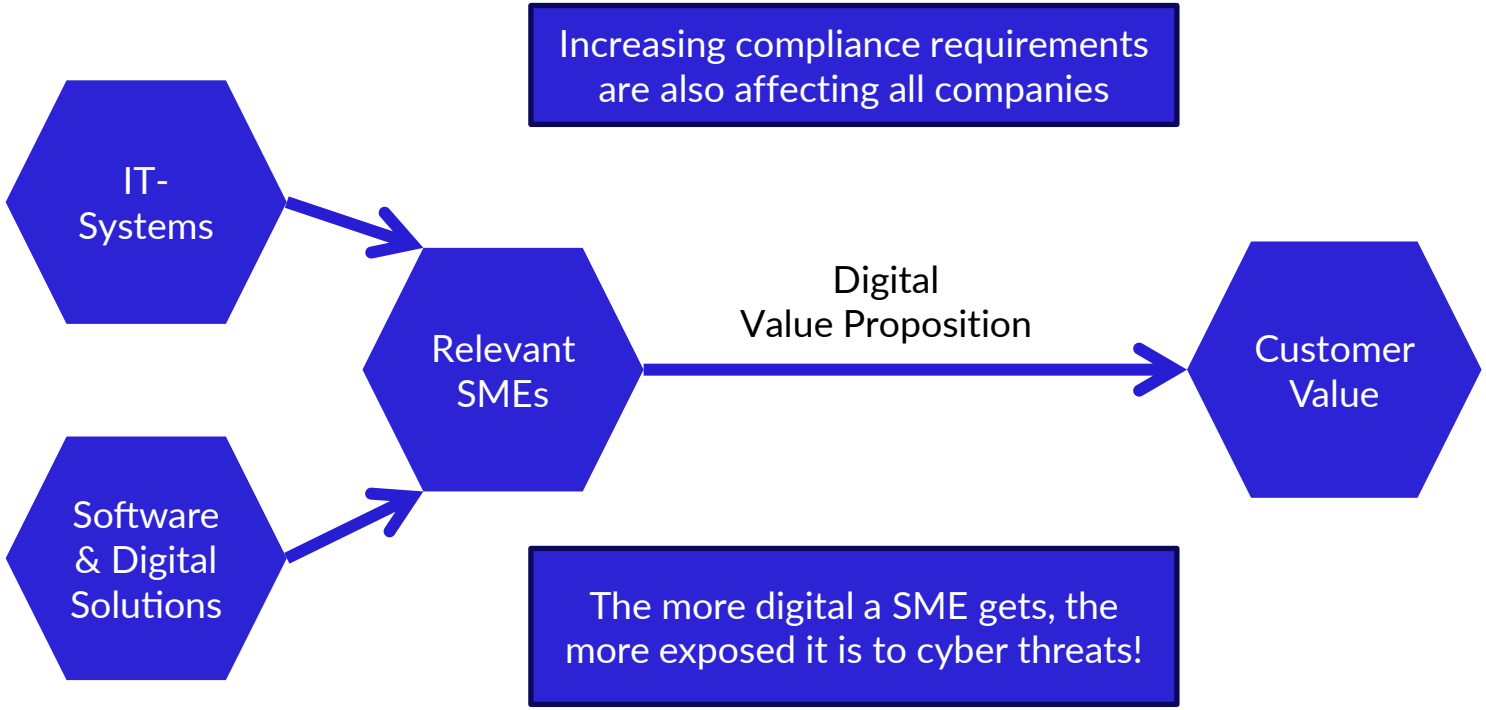
Cyberangriffe

NIS 2 Richtlinie

Datensicherheit

Operationalize Security

Why is Cybersecurity important?



SMEs and Cybersecurity?

Consequently, SMEs often do not assign cybersecurity the necessary strategic importance or lack the financial and human resources to implement appropriate protective measures.

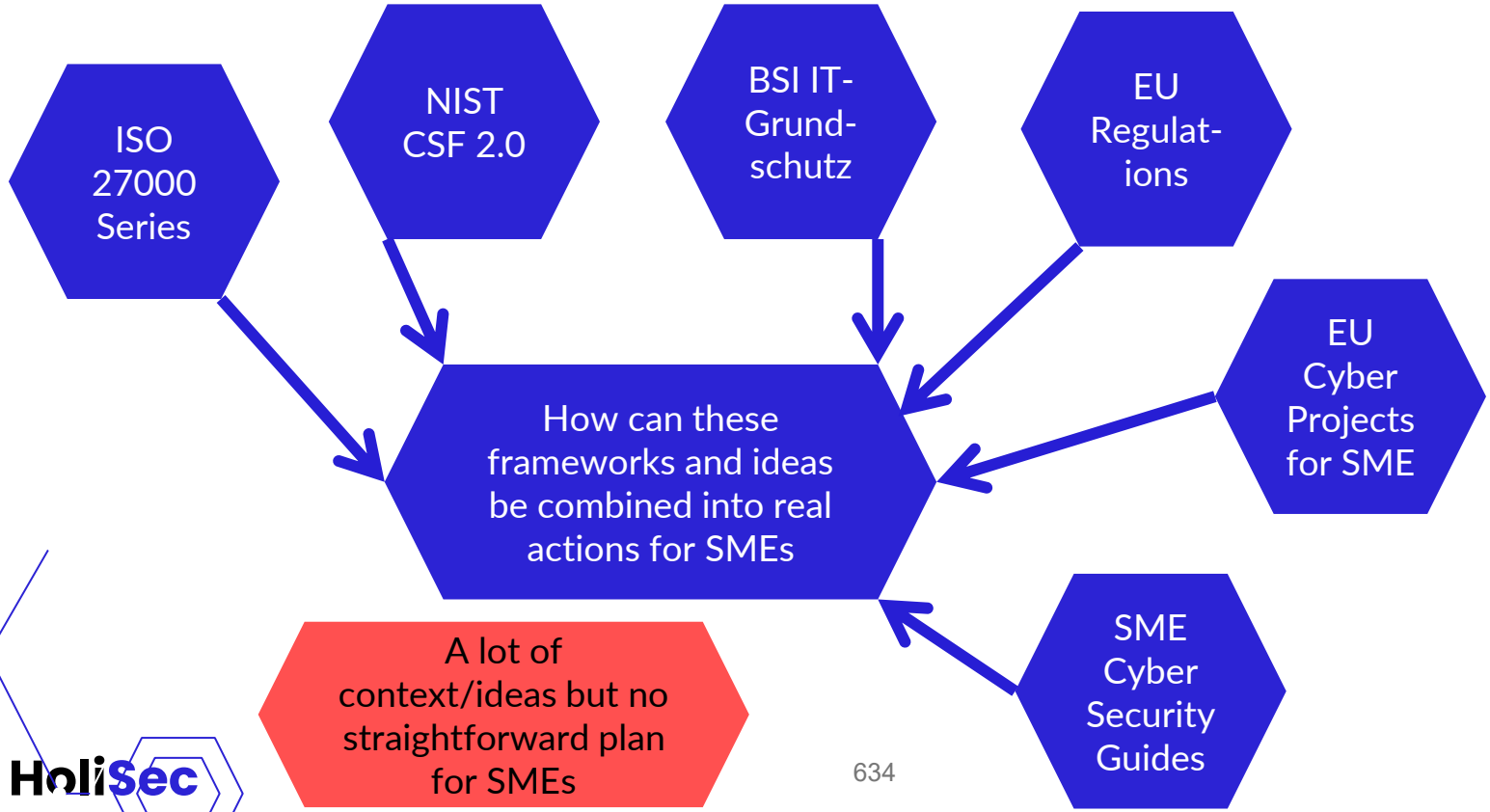
Motivation

- Cybersecurity is still not a priority in many SMEs
- Many lack awareness, structure, and guidance
- Existing standards are too complex and expensive
- SMEs need a simple and actionable approach

Main objective: Bring cybersecurity to SMEs in a practical way and show them how they can achieve that!

Findings & Results

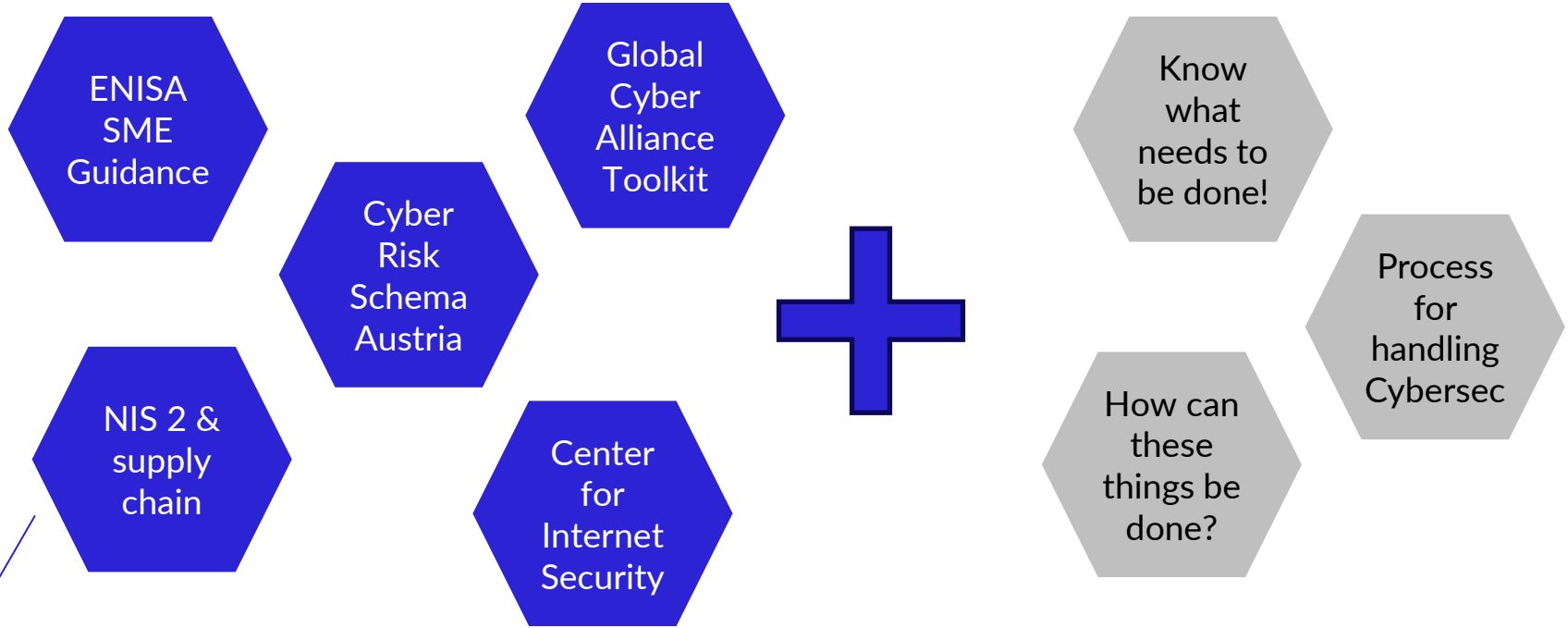
What I wanted to Understand

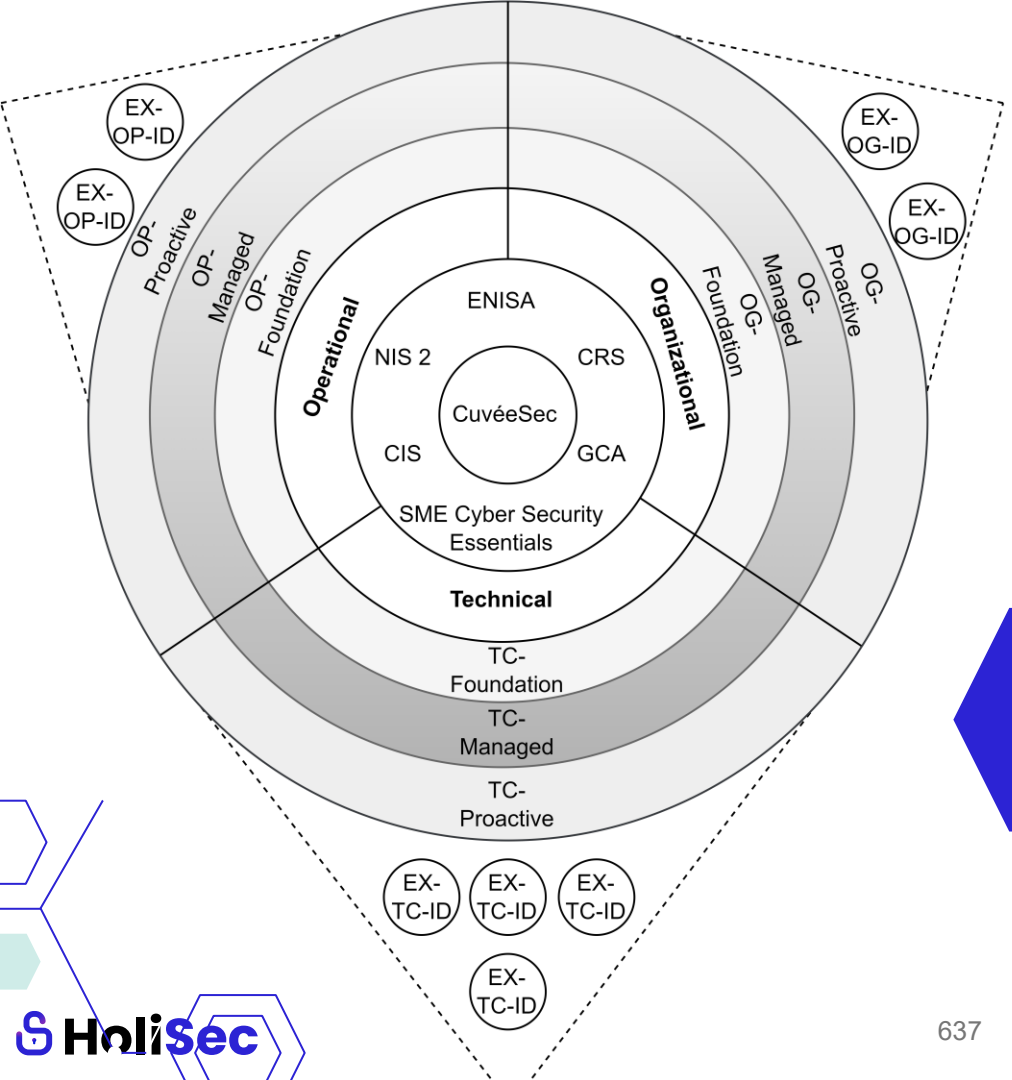


What do SME really need from all these ideas?

HoliSec

Clear Requirements and Guidance





CuvéeSec Framework for SME

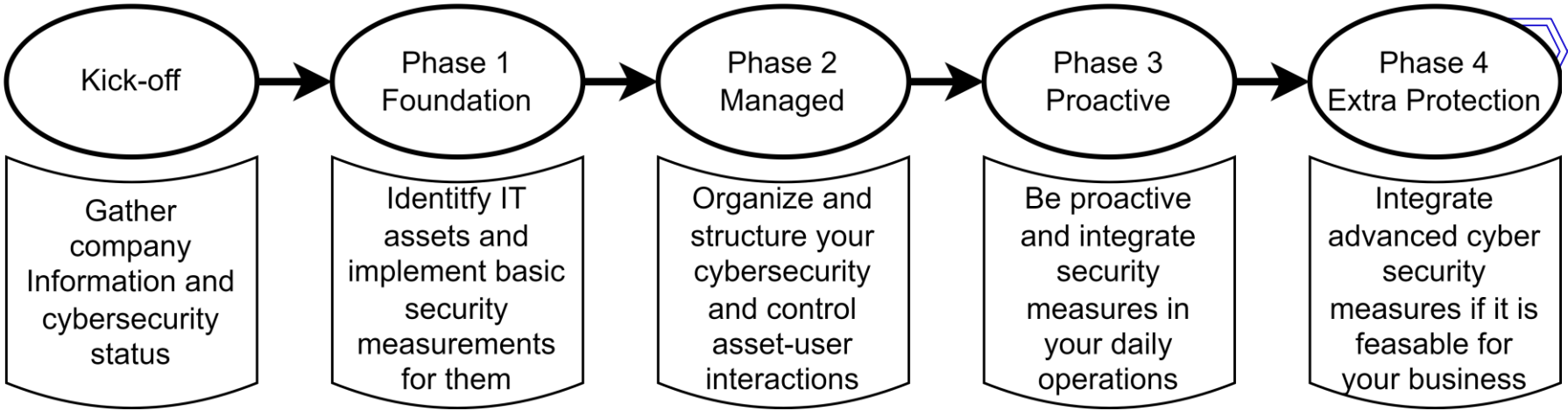
61 Cuvée Sec Actions

+

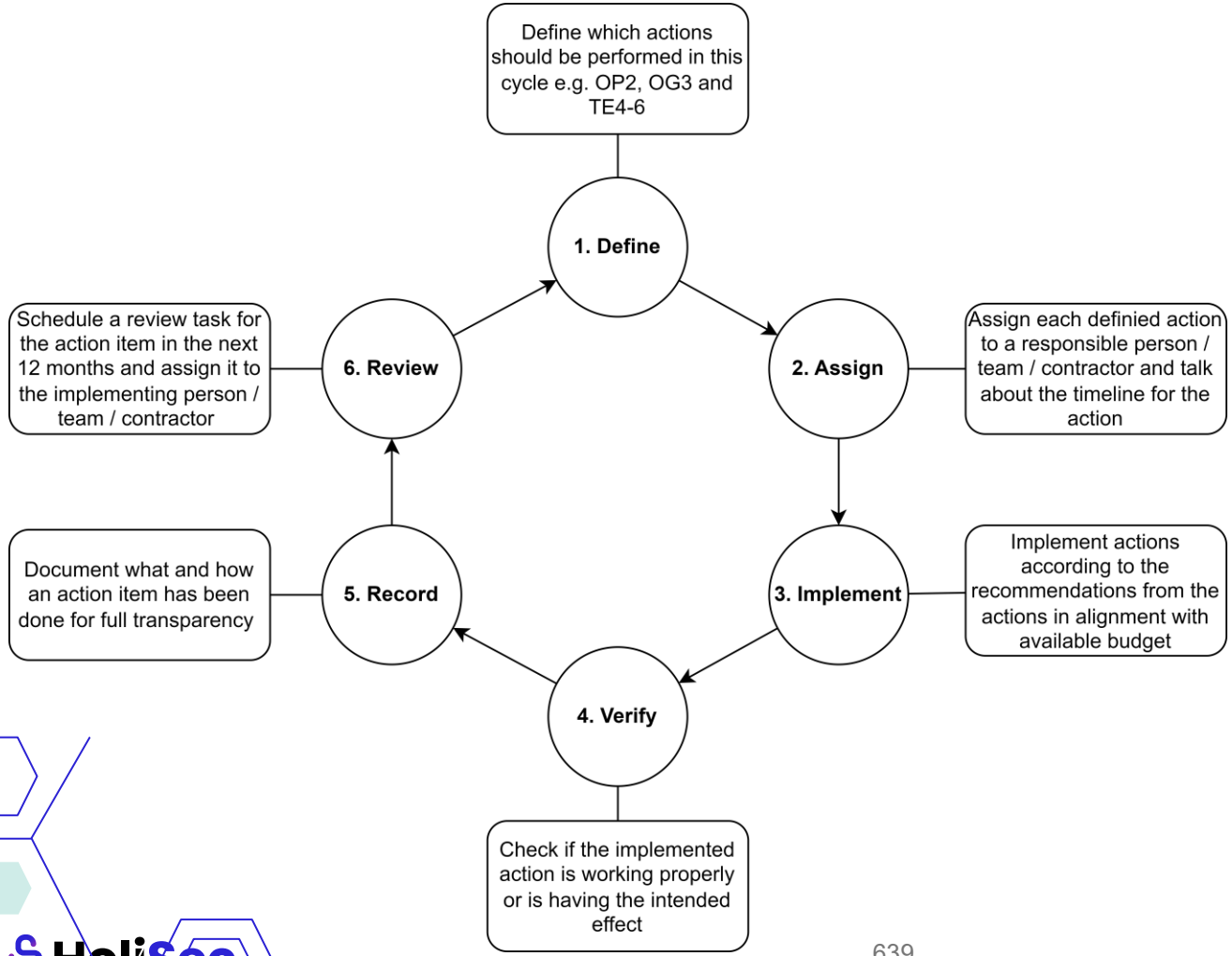
Cuvée Sec Action Cycles

HoliSec

CuvéeSec Process



Plan CuvéeSec Action Cycles



How can framework be put into a tool that SMEs could use?

First Prototype: Requirements

- General Availability/Usability without extra costs
- Ability to plan a Kick-Off for a SME
- Document and reference CuvéeSec Actions
- Plan and organize CuvéeSec Action Cycles
- Ability to perform IT-Asset Management and map it to CuvéeSec Action

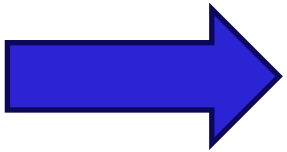
First Prototype: Technology

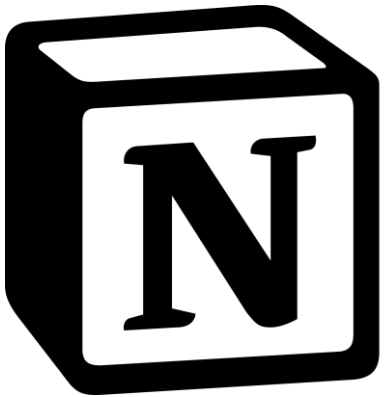
Database Support

Code Logic Support

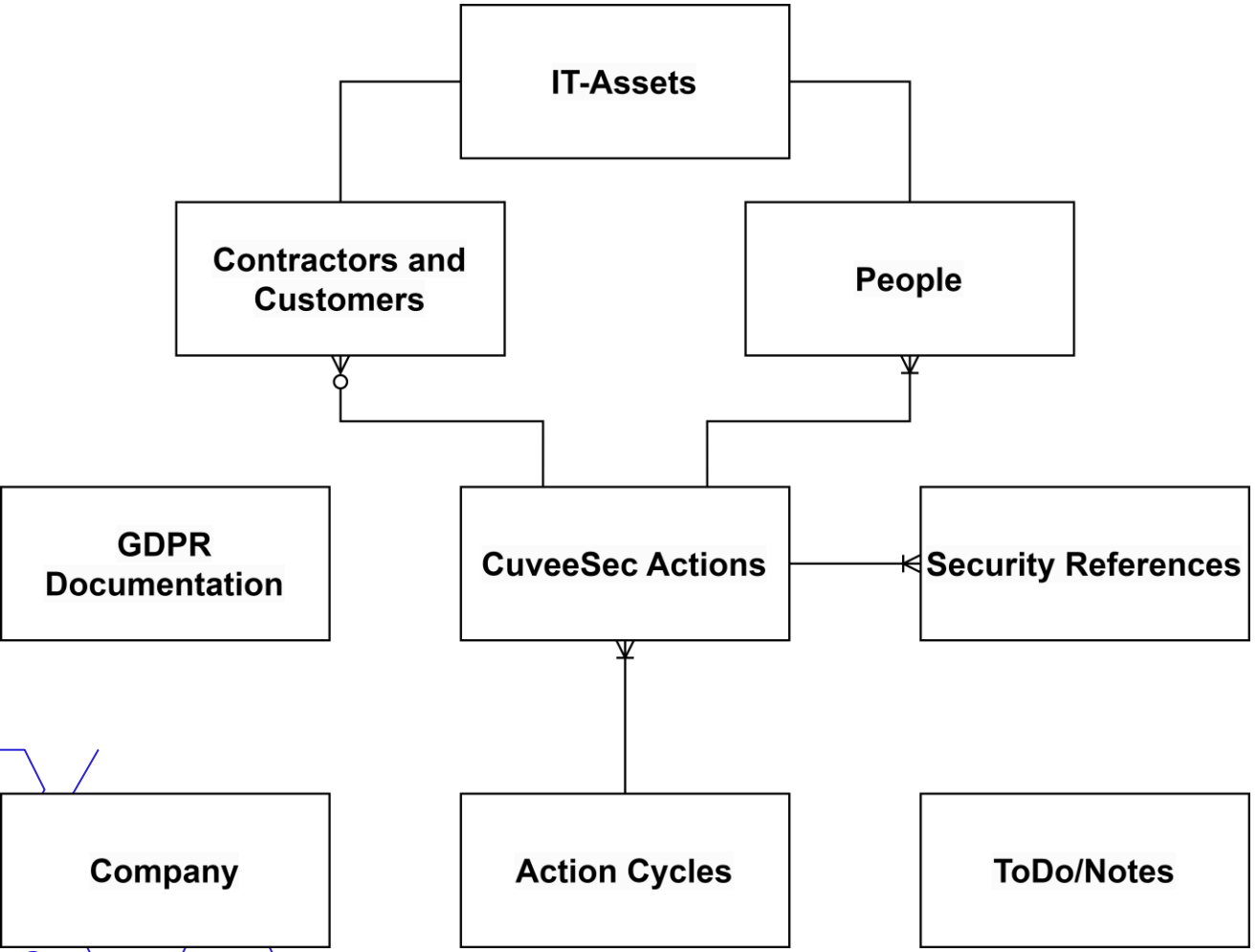
User Experience must be okay

Browser/ Web Based App

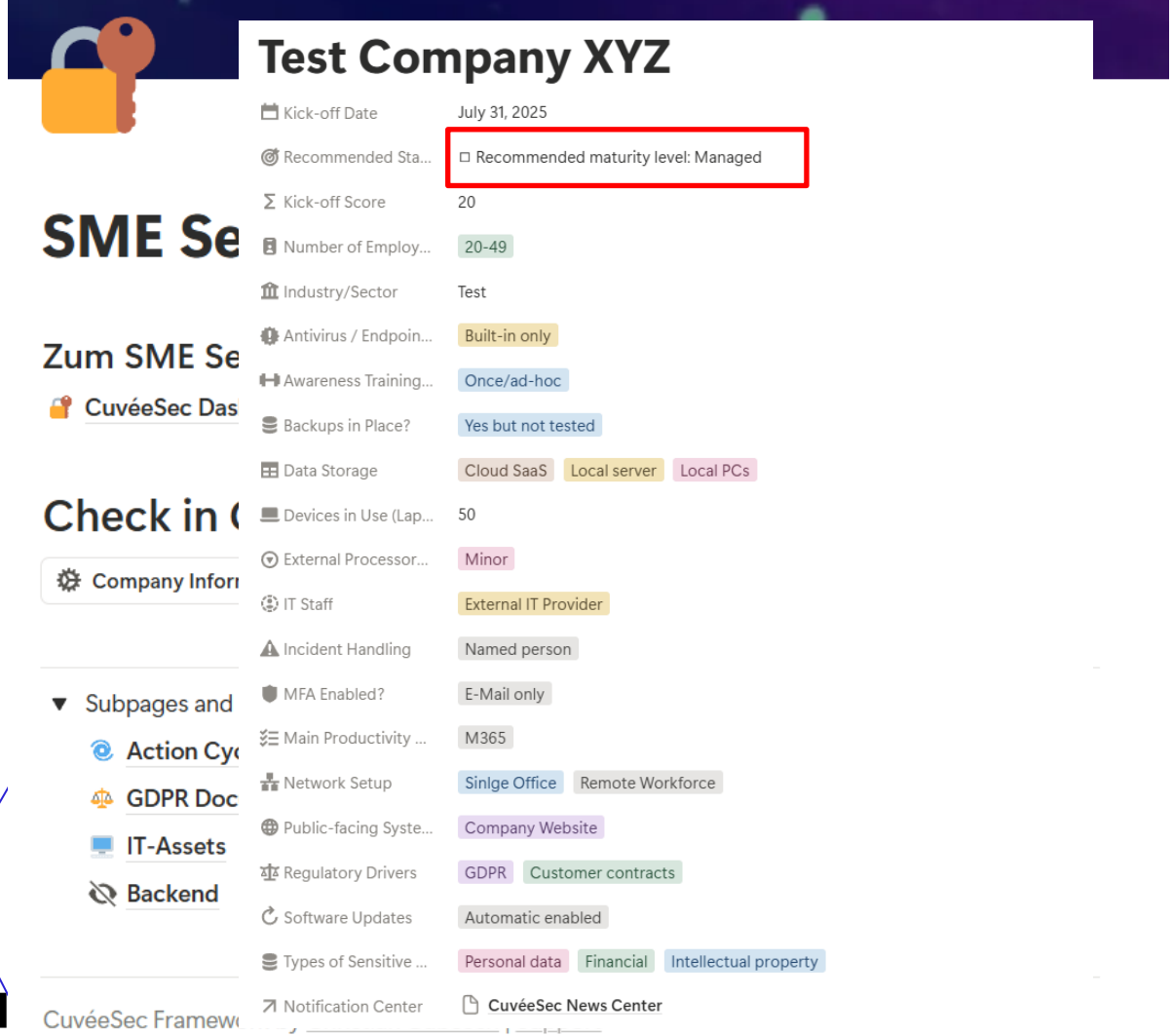




Notion
(productivity software)



First Prototype: Database s



First Prototype: UI

CuvéeSec Dashboard

"There are only two types of companies: those that have been bre

QUICK LINKS

- CuvéeSec Dashboard
- Action Cycle Planner
- GDPR Documents
- IT-Assets

QUICK ACTIONS

- Add IT-Asset
- Plan a new Action Cycle
- Create new Person
- Add a Contractor/Customer
- Create new ToDo

All Imp

Actions

№	Action I
	TC6 - IT
	OG2 - R
	TC5 - B
	OG4 - P
	TC1 - M

OG4 - Password Management

Domain	Organizational
Maturity Level	Foundational
Status	Verified
Assigned To	Max Mustermann
Last Review Date	August 22, 2025
Next Review Date	August 22, 2026
Linked Contractors	1Password
Linked References/...	ENISA SME Guide
Action Cycles	Action-Cycle-01

Add a property

What is this Action?

This action requires SMEs to use a **password manager** for shared accounts or systems with critical access (e.g., cloud services, admin logins, financial tools).

A password manager prevents employees from reusing weak passwords, avoids insecure sharing (email, sticky notes), and ensures access is revoked easily when staff leave.

What needs to be done?

- **Step 1:** Identify shared or critical accounts (e.g., finance, domain registrar, SaaS admin accounts).
- **Step 2:** Choose a password manager that fits the SME's size and budget.
- **Step 3:** Store these credentials in the password manager instead of sharing via email or chat.
- **Step 4:** Train staff on how to use the password manager for retrieving and updating passwords.
- **Step 5:** Review access rights at least annually (or when staff leave).
- **Step 6 (optional):** For external sharing, use secure password sharing features instead of email.

Who can do this?

- **IT Admin / External IT Provider:** set up the password manager, configure secure sharing.

New

ew Date

6
26
26
26
26

Notification

Current Status

New

CuvéeSec News Center

- Good Evening, HoliSec GmbH!
- Today is Thursday, 25 September 2025
- Recommended maturity level: Managed
- Current Action Cycle is: Action-Cycle-02. The current progress is at: 63%

New page

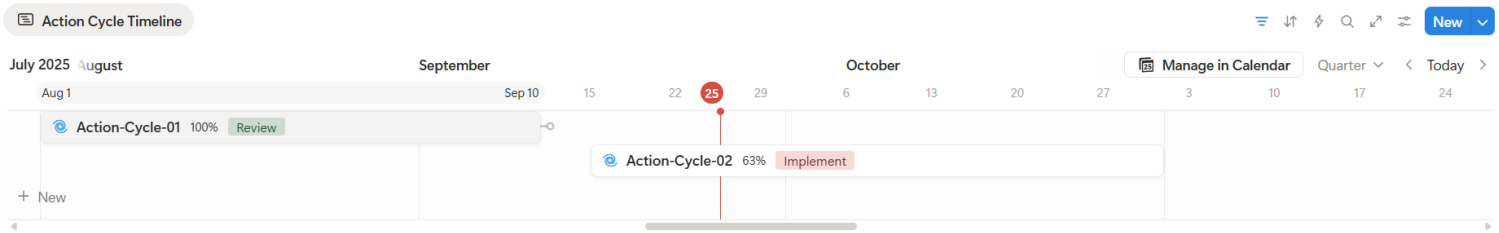
Action Cycle Planner

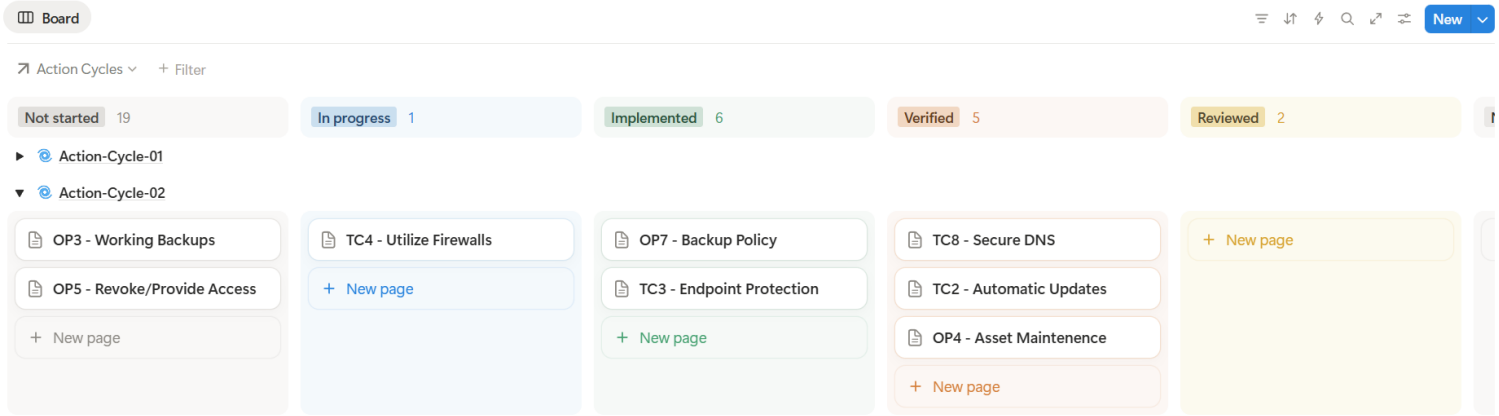
QUICK LINKS

- CuvéeSec Dashboard
- Action Cycle Planner
- GDPR Documents
- IT-Assets

QUICK ACTIONS

- Add IT-Asset
- Plan a new Action Cycle
- Create new Person
- Add a Contractor/Customer
- Create new ToDo





HoliSec

Field Experiment

Goal:

- Identify potential companies (real customers of my company)
- Get them into a testing phase in a collaborative approach
- Gather information on how this framework works for SMEs

Result:

- I performed two experiments with companies based in Graz
  - Software Development company ~ 40 employees
  - Photvoltaics company ~ 10 office employees

- Very time-consuming process because I needed many 1:1 sessions with the companies to run them through.

Conclusion – CuvéeSec

- Action set (61 Actions) could be thinner
- Hard to integrate with existing solutions (e.g Asset Management)
- Additional technical guidance needed
- SaaS concerns/dependency on Notion

Conclusion – Thesis

- The framework and tool are useable and valuable for SMEs
- More Design Science Research cycles would be even better
- Additional information for SMEs is required to use the framework/tool on their own

Future Outlook

- Make the necessary changes to the framework
- Identify what is missing in order to sell the framework and tooling as a product
- Create a funding plan to build it as a software product and qualify a set of companies

Habt ihr noch Fragen? 🚀

HoliSec

Feedback