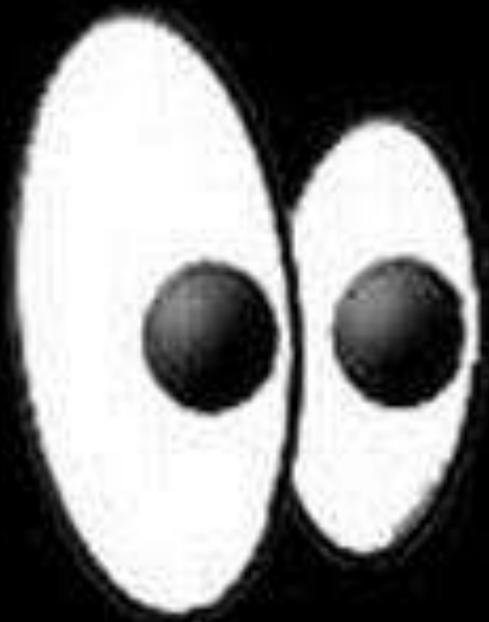
Hosted by: WKO WIRTSCHAFTSKAMMER ÖSTERREICH

Cybersicherheit: Startklar für NIS2
Ready for take off ?

St. Pölten, 11. März 2024

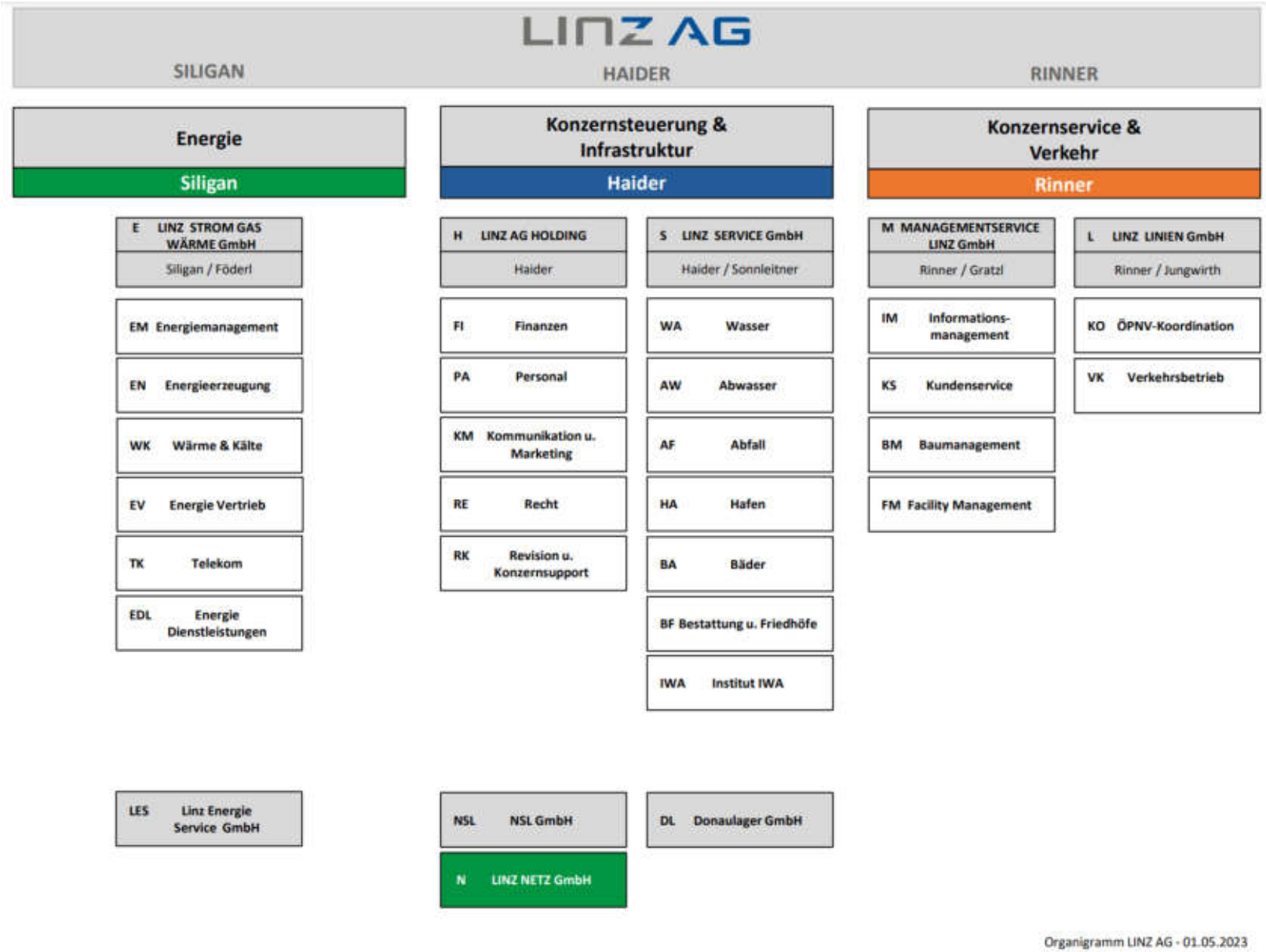
LINZ NETZ
Ein Unternehmen der LINZ AG


sicherheitsbewusstsein
incident-management
netzwerksicherheit
response
sicherheitsbewusstsein
incident
incident-management
schutzmaßnahmen
authentifizierung
sicherheitsrichtlinien
schwachstelle
nis-richtlinie
sicherheitsbewusstsein
sicherheitsaudit
penetrationstest
zugriffskontrolle
netzwerksicherheit
cybersecurity
datenintegrität
informationssicherheit
firewall
cybersecurity
virenschutz
nisg
angriff
vulnerability
nisg
response
verschlüsselung
netzwerksicherheit
nisg
penetrationstest
bedrohung
incident-management
bedrohung
risikomanagement
schwachstelle
bedrohung
incident
schutzmaßnahmen
nis-richtlinie
authentifizierung
management
nis-richtlinie
compliance
response
vulnerability
sicherheitslücken
angriff
sicherheitsaudit
angriff
verschlüsselung
firewall
management
vulnerability
nisg
risikomanagement
sicherheitslücken
datenintegrität
sicherheitsrichtlinien
zugriffskontrolle
nis-richtlinie
bedrohung
virenschutz
datenintegrität
firewall
vulnerability
virenschutz
schutzmaßnahmen
compliance
risikomanagement
incident
compliance
penetrationstest
angriff
incident
cybersecurity
management
zugriffskontrolle
firewall
incident
schwachstelle
authentifizierung
sicherheitsaudit
verschlüsselung
sicherheitslücken
netzwerksicherheit
virenschutz
bedrohung
management
vulnerability



LICHT INS DUNKEL

Quelle: Standard.at


LINZ AG
SILIGAN
HAIDER
RINNER
Energie
Siligan
Konzernsteuerung & Infrastruktur
Haider
Konzernservice & Verkehr
Rinner
E LINZ STROM GAS WÄRME GmbH
Siligan / Föderl
EM Energiemanagement
EN Energieerzeugung
WK Wärme & Kälte
EV Energie Vertrieb
TK Telekom
EDL Energie Dienstleistungen
H LINZ AG HOLDING
Haider
FI Finanzen
PA Personal
KM Kommunikation u. Marketing
RE Recht
RK Revision u. Konzernsupport
S LINZ SERVICE GmbH
Haider / Sonnleitner
WA Wasser
AW Abwasser
AF Abfall
HA Hafen
BA Bäder
BF Bestattung u. Friedhöfe
IWA Institut IWA
M MANAGEMENTSERVICE LINZ GmbH
Rinner / Gratzl
IM Informations-management
KS Kundenservice
BM Baumanagement
FM Facility Management
L LINZ LINIEN GmbH
Rinner / Jungwirth
KO ÖPNV-Koordination
VK Verkehrsbetrieb
LES Linz Energie Service GmbH
NSL NSL GmbH
N LINZ NETZ GmbH
DL Donaulager GmbH
Organigramm LINZ AG - 01.05.2023

Dienstleistungen der LINZ AG in 105 Gemeinden:

Strom:
82 Gemeinden

Erdgas:
30 Gemeinden

Fernwärme:
27 Gemeinden

Wasser:
22 Gemeinden

Abwasser:
41 Gemeinden

Abfall:
58 Gemeinden

Verkehr:
11 Gemeinden

Stromnetz

Netzgebiet

- Linz und 81 Gemeinden
- 1.651 km² versorgte Fläche

Netzanlagen

- 8.177 km Leitungslänge
  (110 kV, 25 kV, 10 kV, 6 kV, 0,4 kV)
- 27 Umspannwerke
- rd. 2.870 Trafostationen

Kundenanlagen

- rd. 284.583 Zählpunkte, davon rd. 180.000 Smart Meter
- rd. 2.230 GWh Netzabgabe
- rd. 416 MW Netzhöchstlast

Gasnetz

- Linz und 29 Gemeinden
- 2.053 km Hauptrohrleitungen
- 56.086 Kunden
- 2.825 GWh Netzabgabe

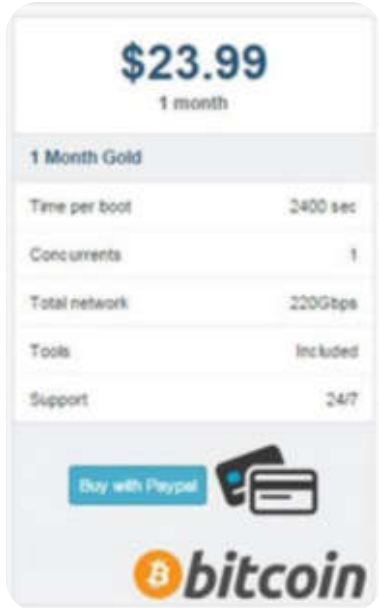
Telekomnetz

- 910 km Signalkabel
- 1818 km Lichtwellenleiterkabel

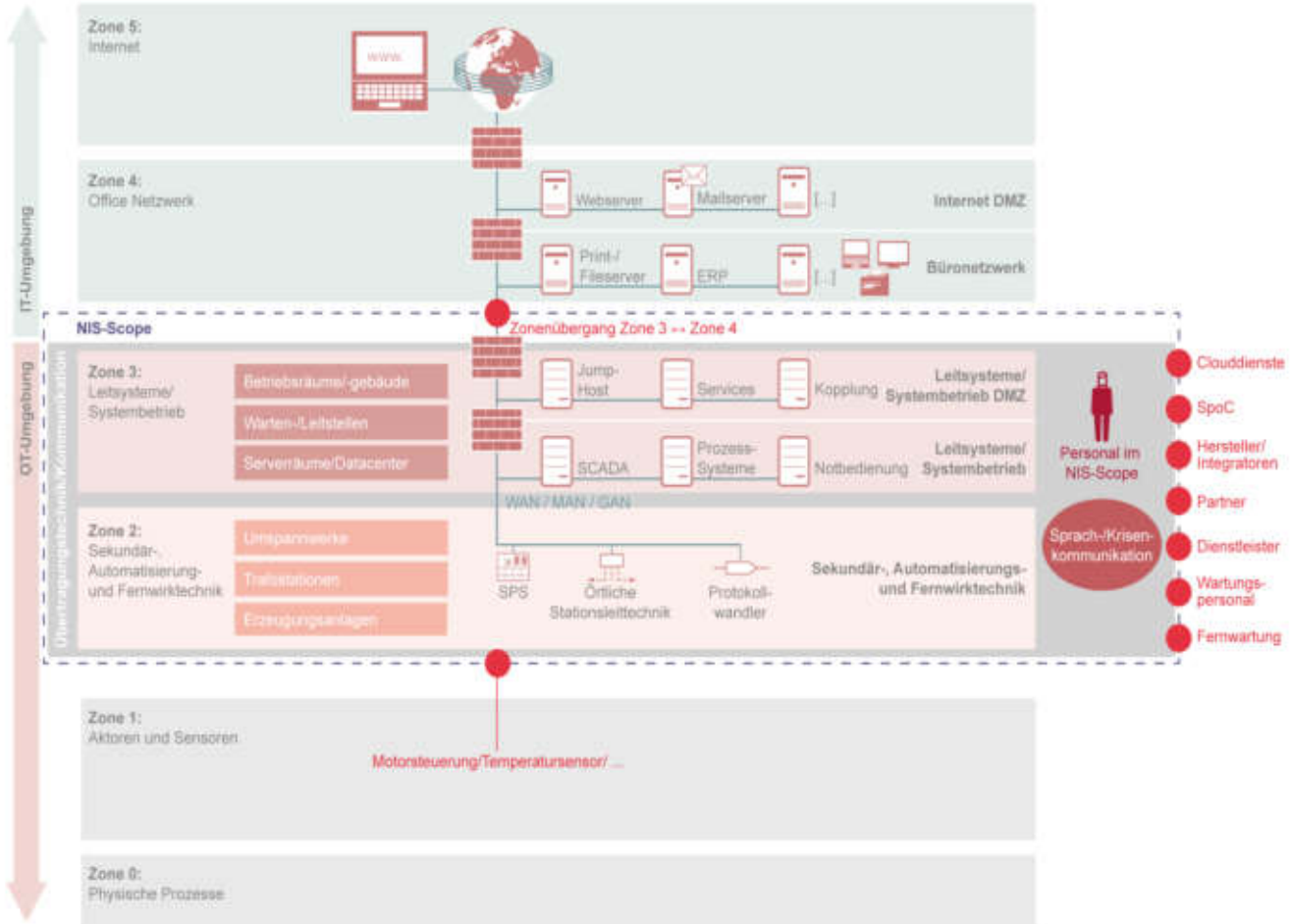
Mehr Information oder für eine DDoS-Attack

https://www.linzag.at

https://www.linznetz.at



AT-3SV-Elektrizität



Leitsysteme/ Systembetrieb	**Systeme, die der Netzsteuerung und -überwachung oder der Steuerung von Erzeugungsanlagen dienen, sowie die hierzu notwendigen unterstützenden Systeme, Anwendungen und zentralen Infrastrukturen.** **Beispiele:** **- Netzleit- und Netzführungssysteme für Energieübertragung und -verteilung,** **- Warten zur Steuerung von Erzeugungsanlagen,** **- Zentrale Messwerterfassungssysteme,** **- Zentrale Parametrier-, Konfigurations- und Programmiersysteme.**
Übertragungstechnik/ Kommunikation	**Die in der Steuerung von Netzen oder Erzeugungsanlagen zur Kommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik.** **Beispiele:** **- Router, Switches und Firewalls,** **- Fernwartungssysteme,** **- Übertragungstechnische Netzelemente,** **- Management-, Konfigurations- und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik,**
Sekundär-, Automatisierungs- und Fernwirktechnik	**Die prozessnahe Steuerungs- und Automatisierungstechnik, die zugehörigen Schutz- und Sicherheitssysteme, fernwirktechnische Komponenten sowie die Automatisierungstechnik** **Beispiele:** **- örtliche Stations- oder Wartenleittechnik** **- Steuerungs- und Automatisierungskomponenten,** **- Leit- und Feldgeräte,** **- Controller und SPSen inklusive digitaler Sensor- und Aktorelemente,** **-Schutzgeräte und Sicherheitskomponenten,** **-Fernwirkgeräte,** **-Mess- und Zählvorrichtungen; mit Ausnahme jener, welche für Verrechnungen des Energieverbrauches dezentral bei juristischen oder natürlichen Personen installiert sind,** **- Parametrierungs- und Programmierwerkzeuge**

AT-3SV-Elektrizität

oesterreichs energie.

AT-3SV-Elektrizität

Sektorenspezifische Sicherheitsvorkehrungen für den Sektor Energie (AT-3SV-Elektrizität) im Sinne des § 17 Abs. 2 NISG mit Einschränkung auf den Teilsektor Elektrizität im Sinne des § 4 Abs. 1 Z 1 NISV

Versionsnummer: 1.4
Ausstellungsdatum: 24. Juni 2021
Österreichs E-Wirtschaft

oesterreichs energie.

A Änderungshistorie

Version	Datum	Bearbeiter	Kommentar
V1.0	31.08.2020	AS & TP	Version für Einreichung beim BM.I
V1.0.5	07.04.2021	AS & TP	Einarbeitung und Überarbeitung basierend auf Zwischenbericht vom 11. Feb 2021 des BVT
V1.1	07.04.2021	AS & TP	Überarbeitete abgestimmte Fassung
V1.2	21.04.2021	TP	Überarbeitung Tabelle ANHANG I
V1.3	22.04.2021	AS	Finale Version zur Rückmeldung an BVT
V1.4	24.06.2021	AS & TP	Finalisierte Version zur Übermittlung an BVT

B Projektteam

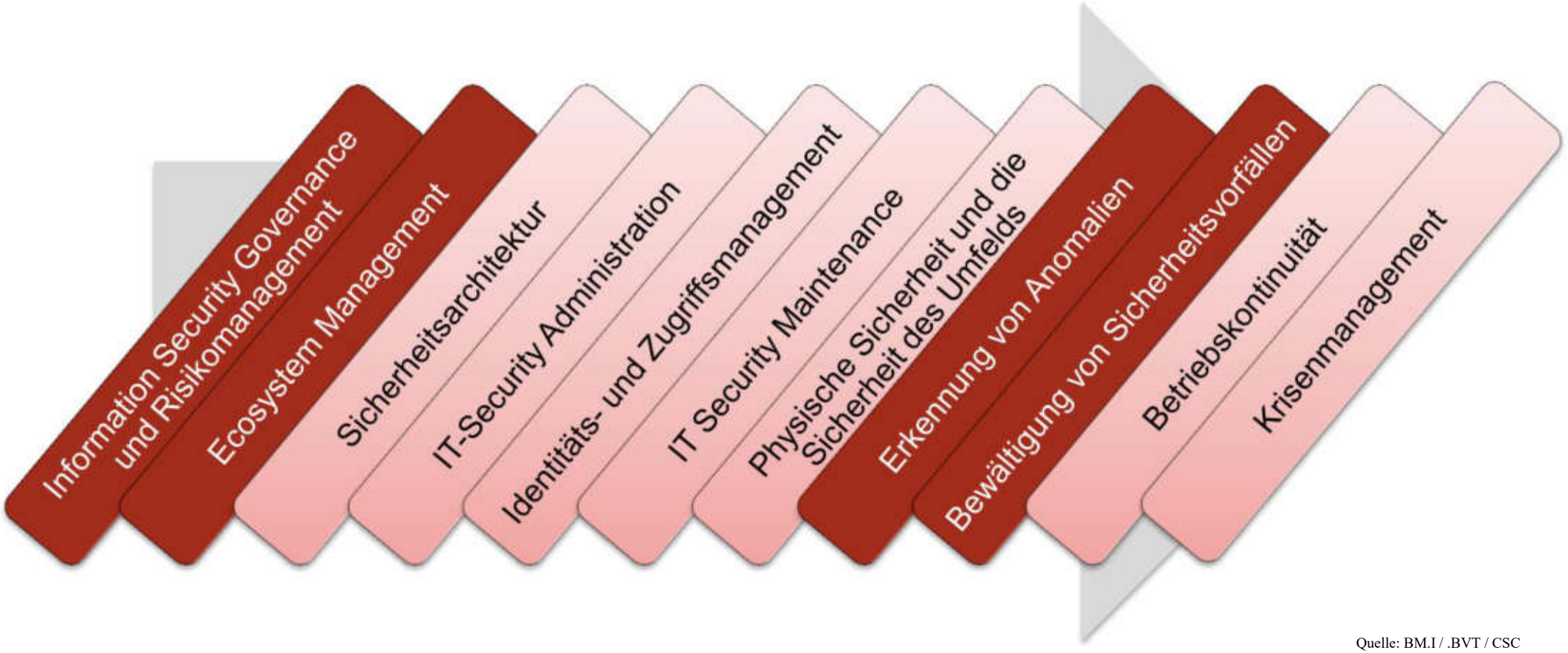
Ansprechpartner
Dipl.-Ing. Armin Selhofer, MSc (Österreichs E-Wirtschaft)

Projektleitung
Thomas Pfeiffer, BSc MSc (LINZ NETZ GmbH, Linz)

Mitwirkende
Mitarbeiter Oesterreichs Energie, Projektmitglieder Oesterreichs Energie und Ansprechpartner in den Unternehmen des Sektors Energie.

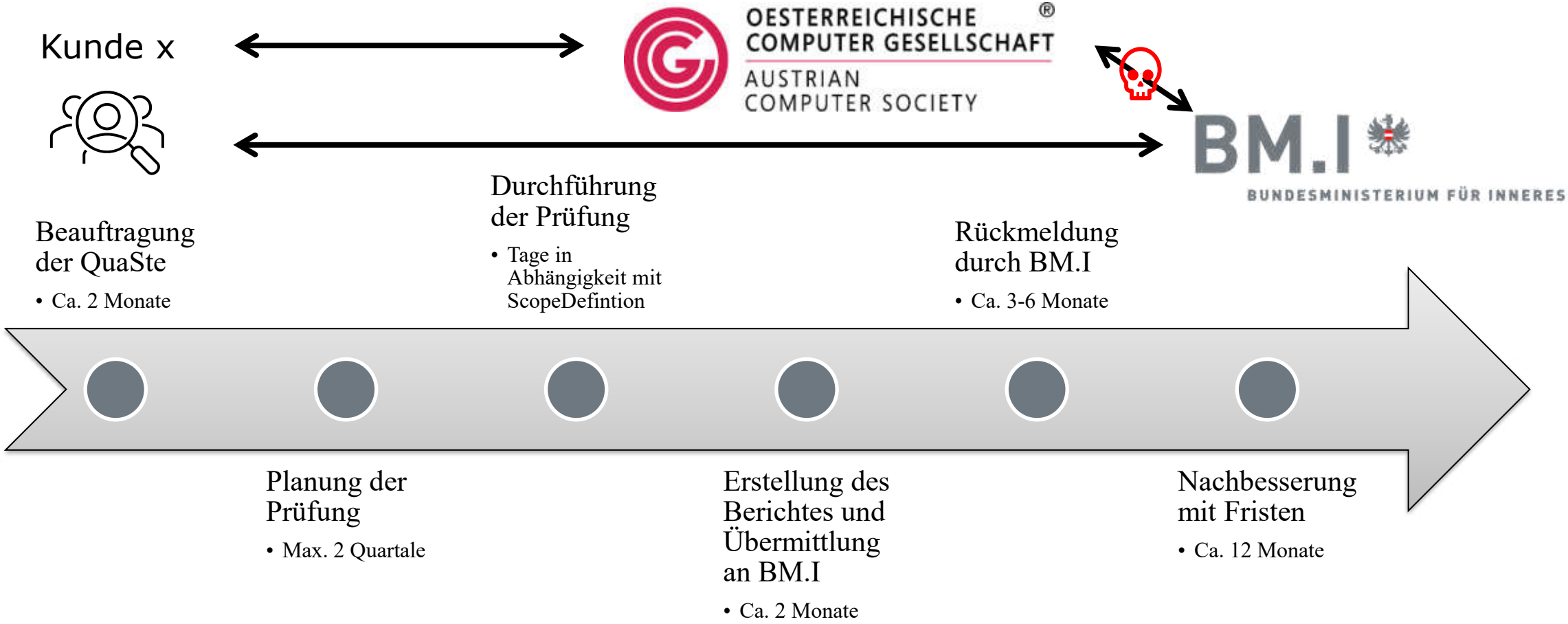
https://oesterreichsenergie.at/
→ Publikationsdatenbank

Mindestsicherheitsvorkehrungen



Quelle: BM.I / .BVT / CSC

Zeitachse Prüfung aus der Praxis



12 Monate bis Berichtübermittlung an BM.I
24 Monate bis „Vollständiger Prozess" abgeschlossen !!!!

KombiAudit – ISO/IEC 27001 und NISG

Timeline

- Bescheid……11.11.2019
- PreAudit……28.02.2022
- Stage I……10.03.2022
- Stage II und NISG……17. - 20.05.2022 und 23. - 25.05.2022
- Abgabe Bericht……10.11.2022

Arbeitsaufwand für 8,5 Audit/Prüftage (2 Prüfer)?

Prüfungsgrundlagen

- NISG - Kontaktstelle
- §11 iVm Anlage 1 NISV – technische und organisatorische Sicherheitsvorkehrungen
- NIS Fact Sheets iVm mit Anlage 1 NISV und Sektorenspezifische Sicherheitsvorkehrungen
- Standards, Normen, Good Practices laut NIS-Fact Sheet
- Empfehlungen von Herstellern für technische Maßnahmen
- Erfahrungen der Prüfer:innen von Sicherheitsvorfällen in Bezug auf die Sicherheitsvorkehrungen
- Interne Compliance-Vorgaben der Kundin
- LIEFERKETTE !!!!!

Arbeitsaufwand nur für Audit/Prüfung

343 Stunden

25 Mitarbeiter:innen

Ohne Vorbereitung und Nachbereitung

FINDINGS

https://pixabay.com - Génesis Gabriella

1. **Unzureichende Passwortsicherheit:** Schwache Passwörter oder die Verwendung desselben Passworts für verschiedene Konten sind häufige Fehler. Starken, einzigartigen Passwörtern und der Verwendung von Passwortmanagern sollte Priorität eingeräumt werden.
2. **Mangelnde Aktualisierung und Patching:** Das Versäumnis, Systeme, Anwendungen und Geräte regelmäßig zu aktualisieren und Sicherheitspatches einzuspielen, öffnet Schwachstellen für potenzielle Angriffe.
3. **Fehlende Awareness und Schulung:** Mangelndes Bewusstsein für Cyberbedrohungen und fehlendes Wissen über Sicherheits-Best-Practices sind häufige Fehler. Die Schulung von Mitarbeitern in Bezug auf Phishing, Social Engineering und andere Angriffsmethoden ist entscheidend.
4. **Unzureichende Zugriffskontrolle:** Übermäßige Berechtigungen, unzureichende Zugriffskontrollen und das Fehlen einer strengen Authentifizierung können dazu führen, dass unbefugte Personen Zugriff auf sensible Daten erhalten.
5. **Fehlende Datensicherung:** Das Fehlen einer regelmäßigen Datensicherung erhöht das Risiko von Datenverlust bei Cyberangriffen, Hardwarefehlern oder anderen Störungen.
6. **Vernachlässigung von Sicherheitslücken:** Das Ignorieren oder Verzögern der Behebung bekannter Sicherheitslücken kann dazu führen, dass Angreifer leicht auf Systeme zugreifen und diese kompromittieren können.
7. **Fehlende Netzwerksegmentierung:** Das Fehlen einer angemessenen Segmentierung von Netzwerken und Systemen kann dazu führen, dass sich Angriffe leicht über das gesamte Netzwerk ausbreiten können.
8. **Schwachstellen in Drittanbieter-Software:** Das Nicht-Überprüfen der Sicherheit von Drittanbieter-Software und das Verwenden von unsicheren oder veralteten Anwendungen erhöht das Risiko von Schwachstellen.
9. **Fehlende Incident Response Planung:** Das Fehlen eines gut durchdachten Incident Response Plans kann zu Verzögerungen bei der Reaktion auf Sicherheitsvorfälle und zur Eskalation von Schäden führen.
10. **Fehlende regelmäßige Sicherheitsüberprüfung:** Das Vernachlässigen von regelmäßigen Sicherheitsprüfungen und Penetrationstests führt dazu, dass Schwachstellen und Sicherheitslücken unentdeckt bleiben.

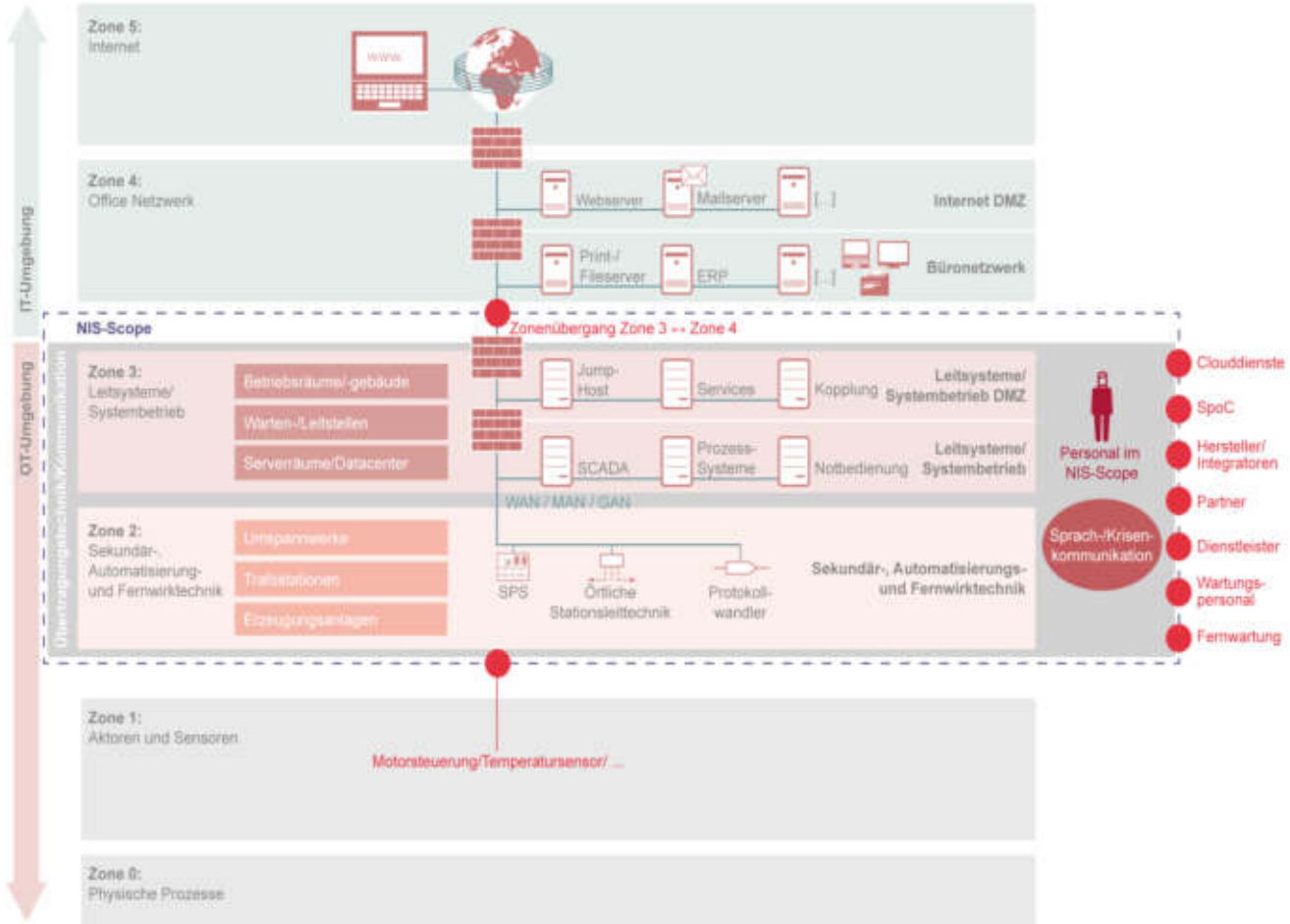
Es ist wichtig, diese Fehler zu vermeiden und eine umfassende Sicherheitsstrategie zu implementieren, um die Sicherheit von Systemen, Daten und Netzwerken zu gewährleisten.

Quelle:chatGPT

NIS 2.0 – WESENTLICHE UND WICHTIGE EINRICHTUNGEN

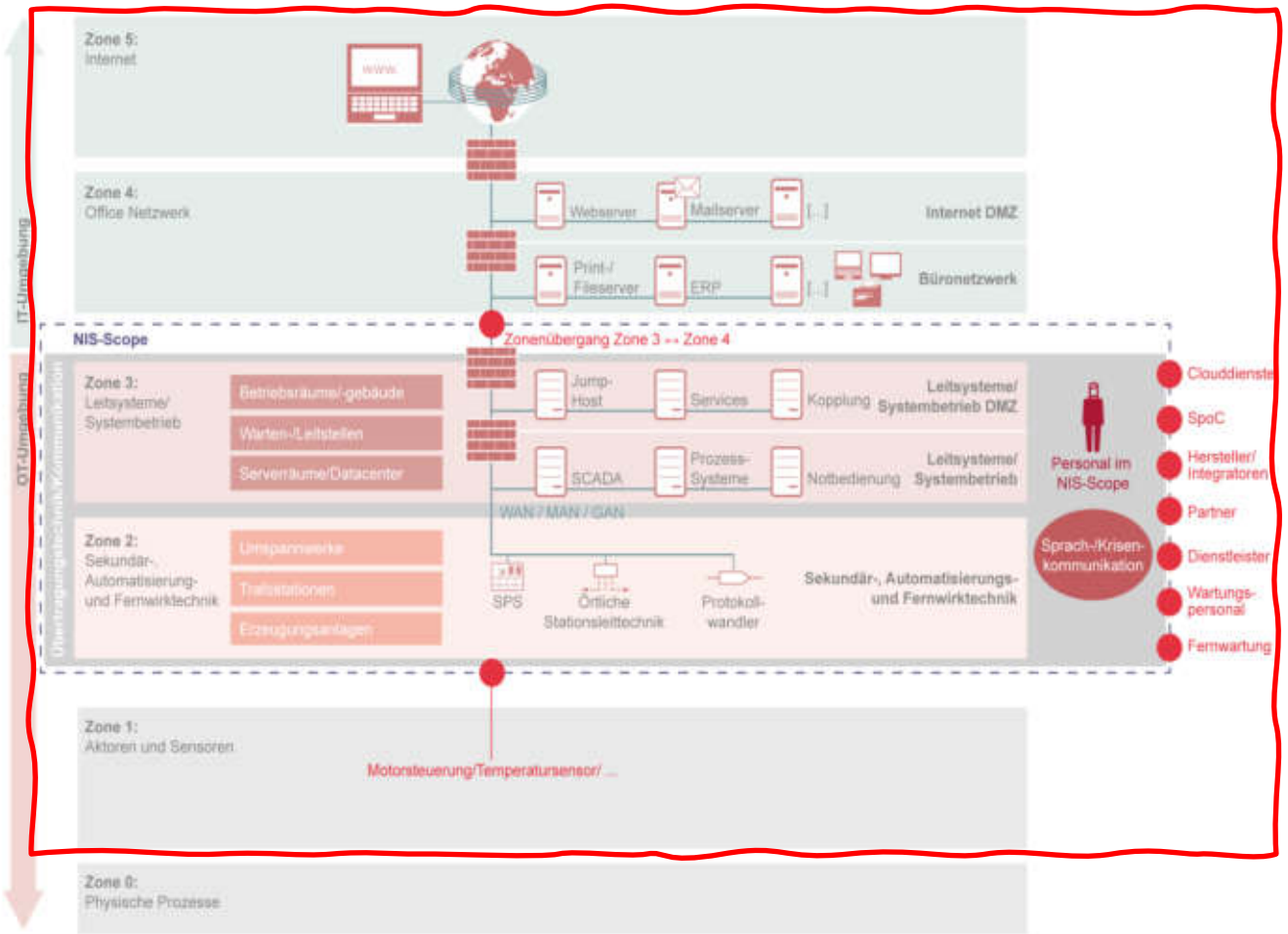
Wesentliche/Wichtige Einrichtungen (Anhang I)	Wichtige/Wesentliche Einrichtungen (Anhang II)
Energie (Elektrizität*, Fernwärme/Kälte , Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft , Schiene , Schifffahrt , Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister , EU Referenzlaboratorien , Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste Suchmaschinen , online Marktplätze und Plattformen für Dienste sozialer Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud Computing, Rechenzentren, Inhaltszustellnetzen (CDN), Vertrauensdiensteanbieter und öffentliche elektronische Kommunikationsnetze)	
IKT-Service Management	
Öffentliche Verwaltung	
Weltraum	

NIS2 – Scope ???



Leitsysteme/ Systembetrieb	**Systeme, die der Netzsteuerung und -überwachung oder der Steuerung von Erzeugungsanlagen dienen, sowie die hierzu notwendigen unterstützenden Systeme, Anwendungen und zentralen Infrastrukturen.** **Beispiele:** **- Netzleit- und Netzführungssysteme für Energieübertragung und -verteilung,** **- Warten zur Steuerung von Erzeugungsanlagen,** **- Zentrale Messwerterfassungssysteme,** **- Zentrale Parametrier-, Konfigurations- und Programmiersysteme.**
Übertragungstechnik/ Kommunikation	**Die in der Steuerung von Netzen oder Erzeugungsanlagen zur Kommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik.** **Beispiele:** **- Router, Switches und Firewalls,** **- Fernwartungssysteme,** **- Übertragungstechnische Netzelemente,** **- Management-, Konfigurations- und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik,**
Sekundär-, Automatisierungs- und Fernwirktechnik	**Die prozessnahe Steuerungs- und Automatisierungstechnik, die zugehörigen Schutz- und Sicherheitssysteme, fernwirktechnische Komponenten sowie die Automatisierungstechnik** **Beispiele:** **- örtliche Stations- oder Wartenleittechnik** **- Steuerungs- und Automatisierungskomponenten,** **- Leit- und Feldgeräte,** **- Controller und SPSen inklusive digitaler Sensor- und Aktorelemente,** **-Schutzgeräte und Sicherheitskomponenten,** **-Fernwirkgeräte,** **-Mess- und Zählvorrichtungen; mit Ausnahme jener, welche für Verrechnungen des Energieverbrauches dezentral bei juristischen oder natürlichen Personen installiert sind,** **- Parametrierungs- und Programmierwerkzeuge**

NIS2 - Scope



Leitsysteme/ Systembetrieb	**Systeme, die der Netzsteuerung und -überwachung oder der Steuerung von Erzeugungsanlagen dienen, sowie die hierzu notwendigen unterstützenden Systeme, Anwendungen und zentralen Infrastr…** **Beispiele:** **- Netzleit- und Netzführungssysteme für …-verteilung,** **- Warten zur Steuerung von Erzeugun…** **- Zentrale Messwerterfassungssysten…** **- Zentrale Parametrier-, Konfigurs…rsysteme.**
Übertragungstechnik/ Kommunikation	**Die in der Steuerun… Erzeugungsanlagen zur Kommunikation eing…, Telekommunikations- und Netzwerktechnik.** **Beispiele:** **- Router, Swit…** **- Fernwartu…** **- Übertrag…nente,** **- Manag… und Überwachungssysteme der Übert…kations- und Netzwerktechnik,**
Sekundär-, Automatisierun… und Fernwirkte…	**…ahe Steuerungs- und Automatisierungstechnik, die Schutz- und Sicherheitssysteme, fernwirktechnische …ten sowie die Automatisierungstechnik** **…ele:** **…che Stations- oder Wartenleittechnik** **…euerungs- und Automatisierungskomponenten,** **…Leit- und Feldgeräte,** **- Controller und SPSen inklusive digitaler Sensor- und Aktorelemente,** **-Schutzgeräte und Sicherheitskomponenten,** **-Fernwirkgeräte,** **-Mess- und Zählvorrichtungen; mit Ausnahme jener, welche für Verrechnungen des Energieverbrauches dezentral bei juristischen oder natürlichen Personen installiert sind,** **- Parametrierungs- und Programmierwerkzeuge**

!!! ALLE NETZ- UND INFORMATIONSSYSTEME !!!

Artikel 21 und 23 iVm Artikel 20

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

- *a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;*
- *b) Bewältigung von Sicherheitsvorfällen;*
- *c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;*
- *d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;*
- *e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;*
- *f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;*
- *g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;*
- *h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;*
- *i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;*
- *j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.*

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

- *a) er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;*
- *b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.*

ToDo`s für zukünftige Betroffene

- Prüfung, ob Betroffen
  - SIZE CAP RULE
  - ANHANG I oder II
- GAP-Analyse der Sicherheitsmaßnahmen
- Umsetzen der Maßnahmen iVm mit ISO/IEC 27001:2022 → Zertifikat ?
- Vorbereitung auf technische Prüfungen
  - Systemkonfiguration
  - Vermögenswerte
  - Netzwerksicherheit und -segmentierung
  - Kryptografie
  - Fernzugriff

RCE und CRA – Die Zukunft der Cybersicherheit ?

Resilience of criticial entities (RCE)

a) das Auftreten von Sicherheitsvorfällen zu verhindern, unter gebührender Berücksichtigung von Katastrophenvorsorge und Maßnahmen zur Anpassung an den Klimawandel;

b) einen angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten, […] Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen;

c) auf Sicherheitsvorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen, […];

d) nach Sicherheitsvorfällen die Wiederherstellung zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen;

e) ein angemessenes Sicherheitsmanagement […].

f) das entsprechende Personal für die unter den Buchstaben a bis e genannten Maßnahmen unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen zu sensibilisieren.

Cyber Resilience Act (CRA)

- Einführung Cybersicherheitsregeln für die auf-den-Marktbringung von Produkten mit digitalen Elementen
- Beinhaltet Verpflichtungen für Hersteller, Distributoren und Einführer
- Verpflichtende Konformitätsbewertungen je nach Risikoniveau
- Strafen bis zu 15 Millionen, oder 2,5% des weltweiten Umsatzes.
- Risikoniveaus:
  - 90% aller Produkte (default category): Self-Assessment
  - 10% entweder
    - Critical „Class I“ (Standard oder Third-Party Assessment)
    - Critical „Class II“ (Third-Party Assessment)

RCE und CRA – Die Zukunft der Cybersicherheit ?

Resilience of criticial entities (RCE)

a) das Auftreten von Sicherheitsvorfällen zu verhindern, unter gebührender Berücksichtigung von Katastrophenvorsorge und Maßnahmen zur Anpassung an den Klimawandel;

b) einen angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten, […] Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen;

c) auf Sicherheitsvorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen, […];

d) nach Sicherheitsvorfällen die Wiederherstellung zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen;

e) ein angemessenes Sicherheitsmanagement […].

f) das entsprechende Personal für die unter den Buchstaben a bis e genannten Maßnahmen unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen zu sensibilisieren.

EU 2022/2557

Cyber Resilience Act (CRA)

- Einführung Cyber[…]eitsregeln für die auf-den-Marktbringun[…]rten mit digitalen Elementen
- Beinha[…] Herstel[…] Dist[…]
- […]
- […]es we[…]
- Risi[…]
  - 9[…]efault category): Self-A[…]

„Class I" (Standard oder Third-Party […]ssment)

Critical „Class II" (Third-Party Assessment)

WHO AM I ?

Thomas Pfeiffer, BSc MSc

- Chief Information Security Officer (CISO)
- Chairman Österreichs Energie
- Lecture
  - Security Department – FH Hagenberg
  - Urban renewable Energy Systems – Technikum Wien
- ISO/IEC 27001 Auditor und Qualifizierter Prüfer iS NISG iVm QuaSteV
  - Österreichische Computer Gesellschaft
- Fachbuchautor
- Founder & CEO Council.at GmbH council.at
- CyberKabarettist
- Advisory Board Member (https://www.ares-ci.com/)

Follow or contact

@hackfleisch_007
t.pfeiffer@council.at
t.pfeiffer@linznetz.at
Darknet - Name = maybe u find out ;-)

U can also find me on: