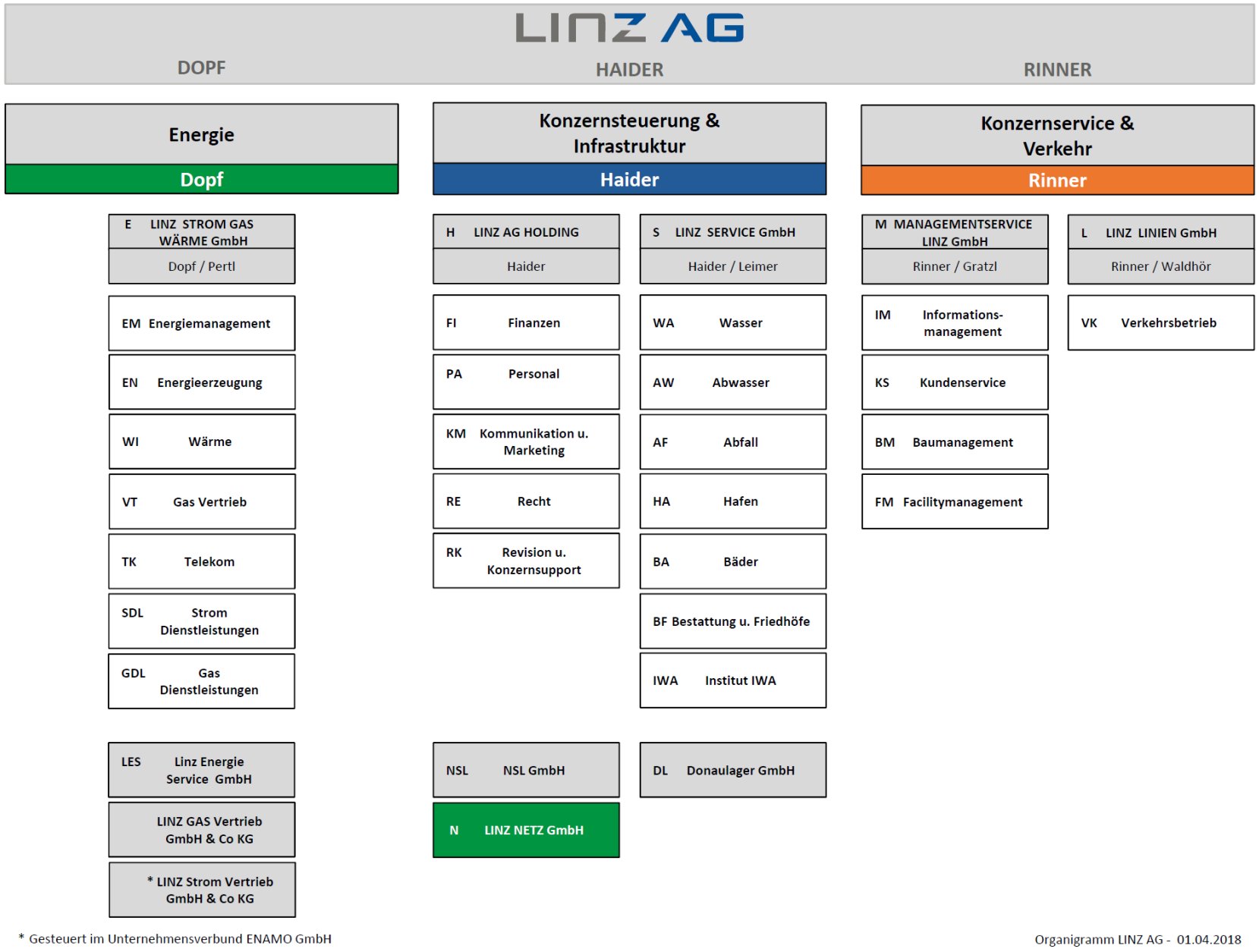
Thomas Pfeiffer


LINZ AG
DOPF
HAIDER
RINNER
Energie
Dopf
Konzernsteuerung & Infrastruktur
Haider
Konzernservice & Verkehr
Rinner
E LINZ STROM GAS WÄRME GmbH
Dopf / Pertl
EM Energiemanagement
EN Energieerzeugung
WI Wärme
VT Gas Vertrieb
TK Telekom
SDL Strom Dienstleistungen
GDL Gas Dienstleistungen
LES Linz Energie Service GmbH
LINZ GAS Vertrieb GmbH & Co KG
* LINZ Strom Vertrieb GmbH & Co KG
H LINZ AG HOLDING
Haider
FI Finanzen
PA Personal
KM Kommunikation u. Marketing
RE Recht
RK Revision u. Konzernsupport
NSL NSL GmbH
N LINZ NETZ GmbH
S LINZ SERVICE GmbH
Haider / Leimer
WA Wasser
AW Abwasser
AF Abfall
HA Hafen
BA Bäder
BF Bestattung u. Friedhöfe
IWA Institut IWA
DL Donaulager GmbH
M MANAGEMENTSERVICE LINZ GmbH
Rinner / Gratzl
IM Informations-management
KS Kundenservice
BM Baumanagement
FM Facilitymanagement
L LINZ LINIEN GmbH
Rinner / Waldhör
VK Verkehrsbetrieb
* Gesteuert im Unternehmensverbund ENAMO GmbH
Organigramm LINZ AG - 01.04.2018

Dienstleistungen der LINZ AG in 105 Gemeinden:

Strom:
82 Gemeinden

Erdgas:
30 Gemeinden

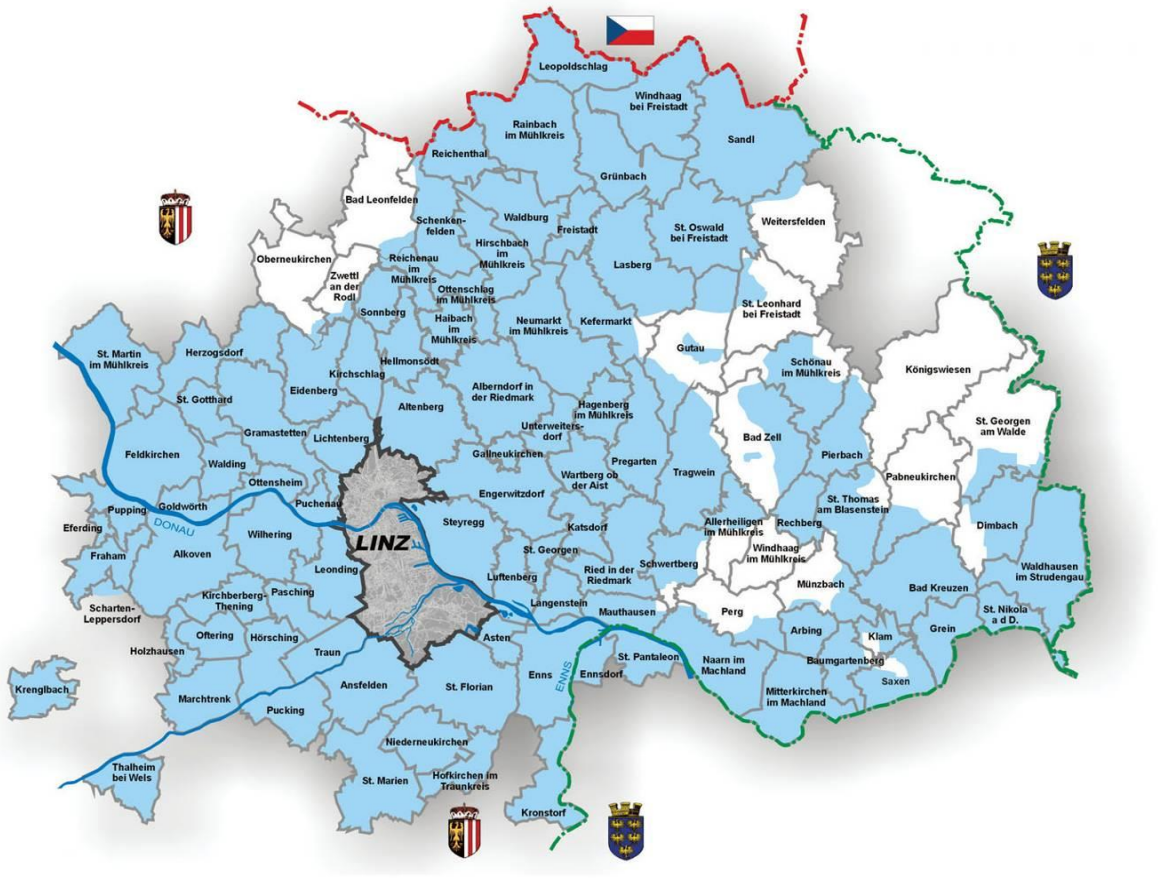
Fernwärme:
27 Gemeinden

Wasser:
22 Gemeinden

Abwasser:
41 Gemeinden

Abfall:
58 Gemeinden

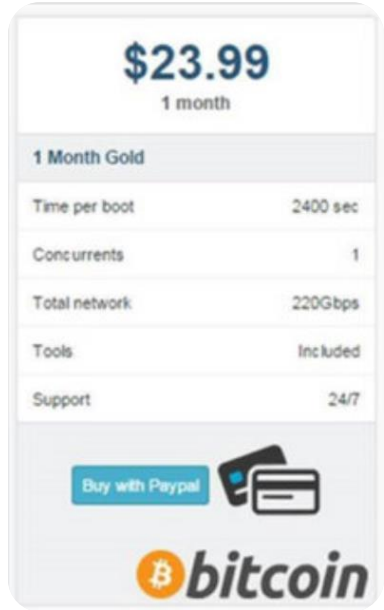
Verkehr:
11 Gemeinden



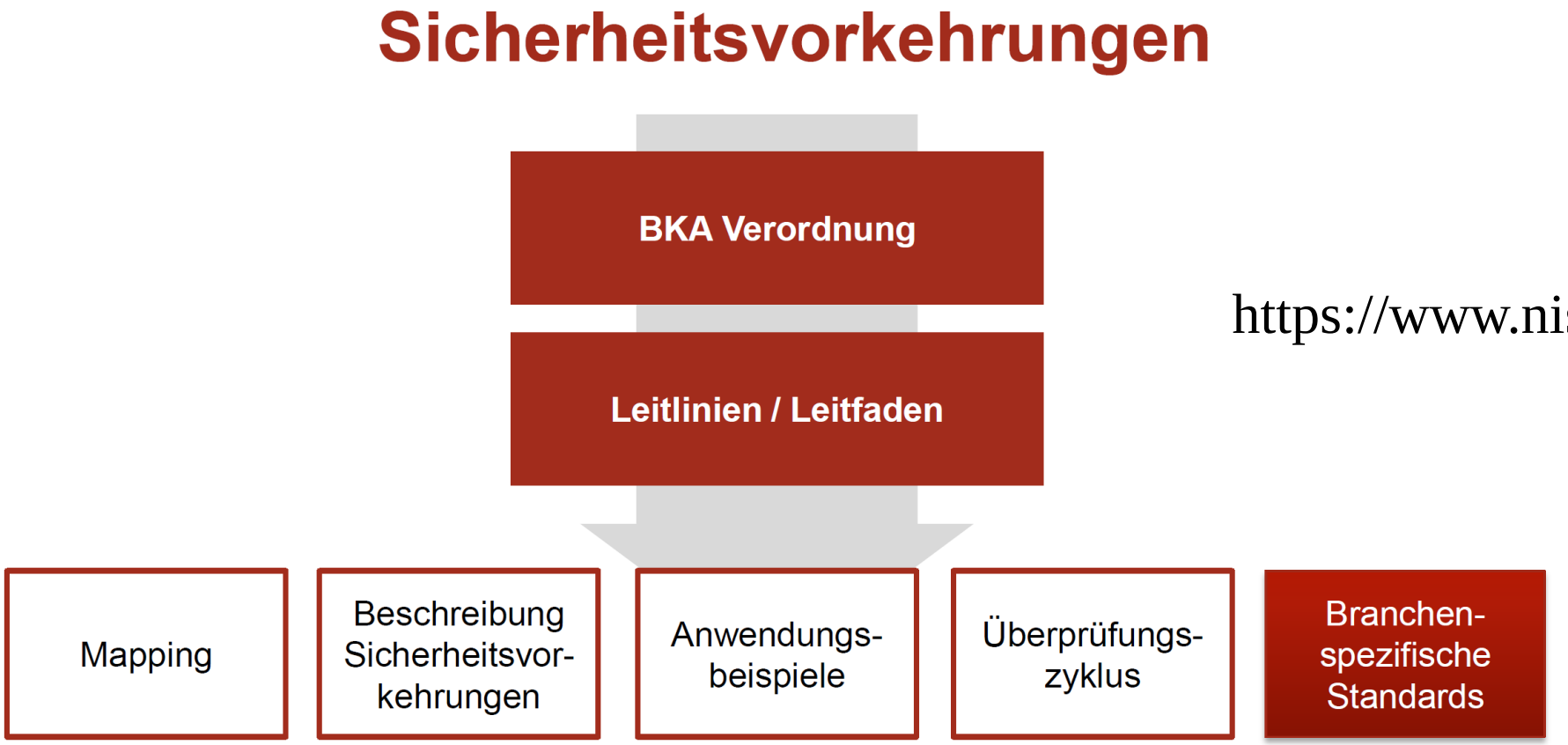
Mehr Information oder für eine DDoS-Attack

https://www.linzag.at

https://www.linznetz.at

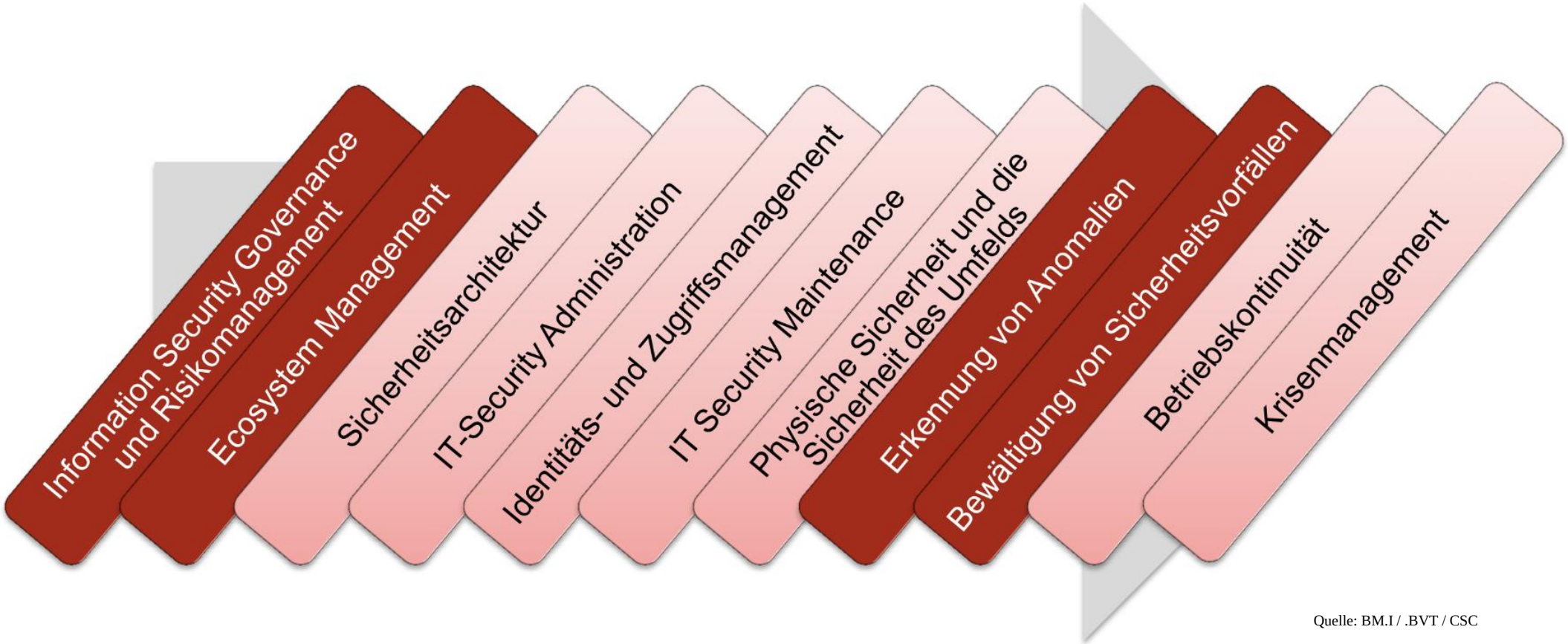


Mindestsicherheitsmaßnahmen



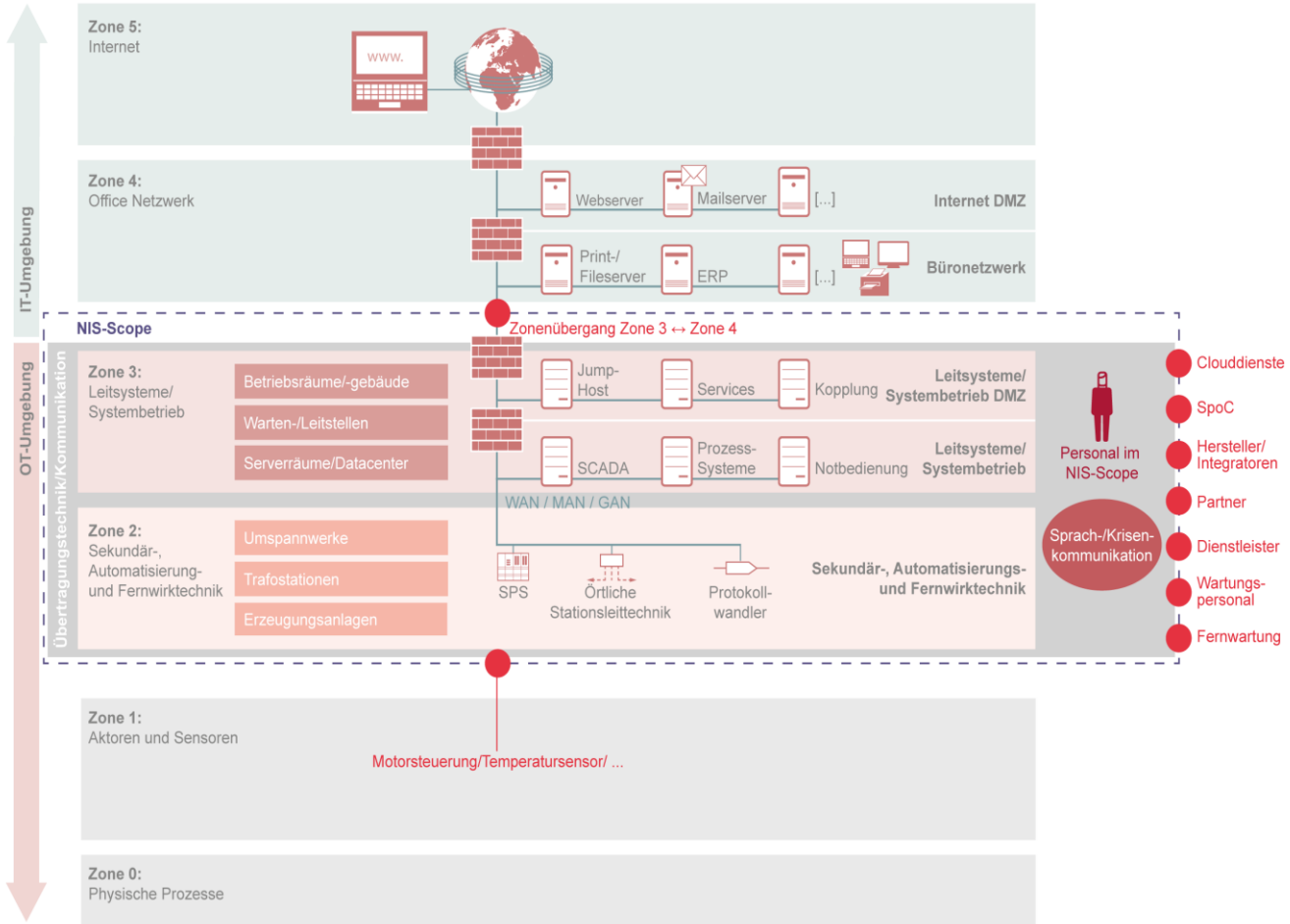
https://www.nis.gv.at

Mindestsicherheitsvorkehrungen



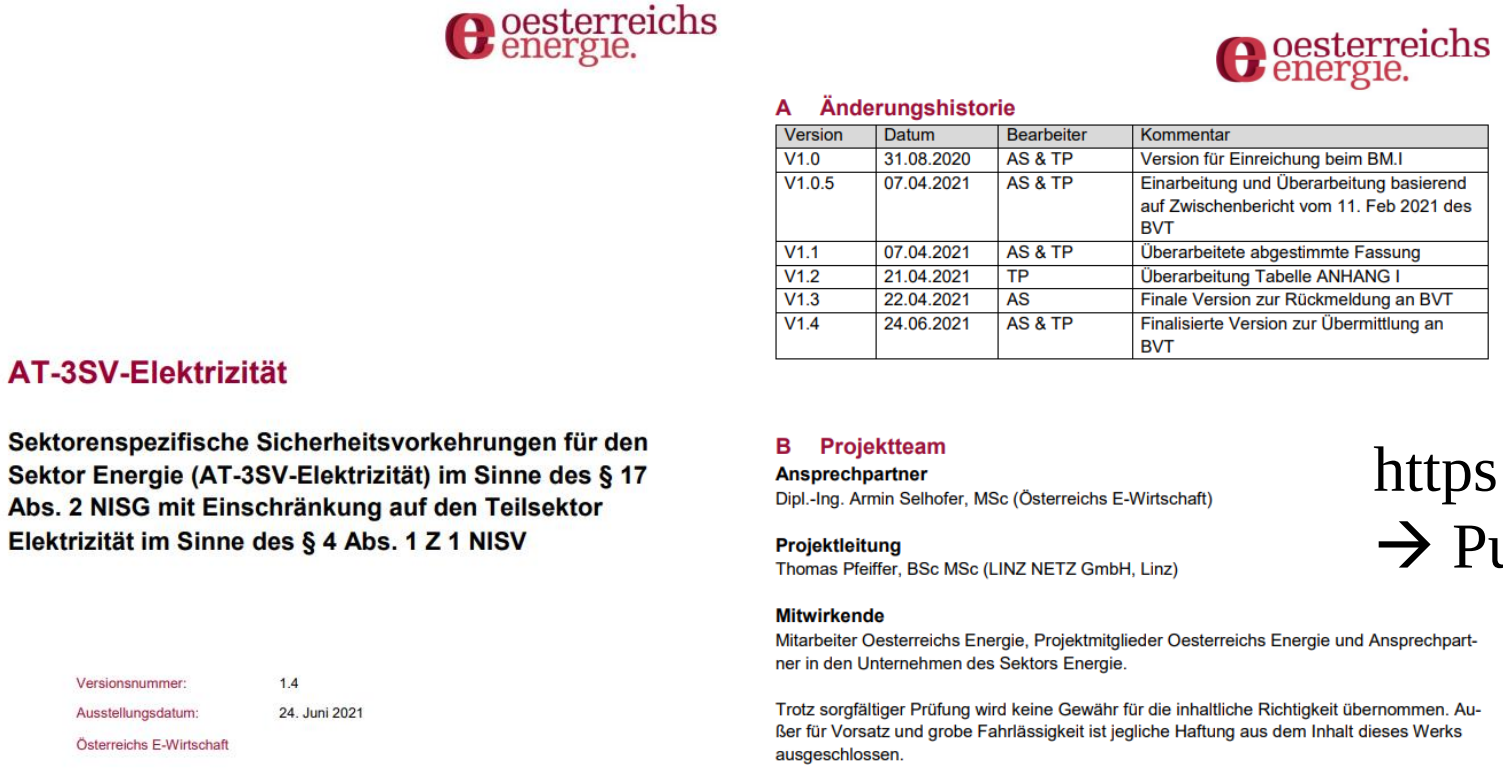
Quelle: BM.I / .BVT / CSC

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



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

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.

Trotz sorgfältiger Prüfung wird keine Gewähr für die inhaltliche Richtigkeit übernommen. Außer für Vorsatz und grobe Fahrlässigkeit ist jegliche Haftung aus dem Inhalt dieses Werks ausgeschlossen.

https://oesterreichsenergie.at/
→ Publikationsdatenbank

KombiAudit – ISO/IEC 27001 und NISG

OESTERREICHISCHE COMPUTER GESELLSCHAFT ®
AUSTRIAN COMPUTER SOCIETY

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)?

Arbeitsaufwand nur für Audit/Prüfung

343 Stunden

25 Mitarbeiter:innen

Ohne Vorbereitung und Nachbereitung

NIS-RL 2.0

- 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/HTML/?uri=CELEX:32022L2555&qid=1673182593331&from=en

- Veröffentlicht im Europäischen Amtsblatt am 27.12.2022

- *„Bis zum 17. Oktober 2024 erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis. Sie wenden diese Vorschriften ab dem 18. Oktober 2024 an.“*[vgl. Artikel 41 NIS-2 Richtlinie]

NIS 2.0 – Die drei Säulen und Neuerungen

Mitgliedstaaten	Kooperation und Informationsaustausch	Risikomanagement
Nationale Behörden	NIS-Kooperationsgruppe Peer-Review	Verantwortlichkeit des Top-Managements
CSIRTs	CSIRTs-Netzwerk	Trainings für Top-Managements
Krisenmanagement	CyCLONe	Unterscheidung wesentliche und wichtige Einrichtungen
Nationale Strategien	Biennial ENISA Cybersecurity Reports	Einrichtungen sind verpflichtet, Sicherheitsmaßnahmen zu ergreifen
Rahmen für CVD (coordinated vulnerability disclosure)	Europäisches Schwachstellenregister	Einrichtungen sind verpflichtet, Bedrohungen und Vorfälle zu melden

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	

Schwellwerte „SIZE CAP RULE“

- **Empfehlung 2003/361/EG der EU-Kommission:**
  - **Großunternehmen**: Alle Unternehmen, sofern kein KMU
  - **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
  - **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.

Artikel 34 - Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

*(4) Die Mitgliedstaaten stellen sicher, dass gegen wesentliche Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens **10 000 000 EUR** oder mit einem Höchstbetrag von mindestens **2 %** des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.*

*(5) Die Mitgliedstaaten stellen sicher, dass gegen wichtige Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens **7 000 000 EUR** oder mit einem Höchstbetrag von mindestens **1,4 %** des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.*

(6) Die Mitgliedstaaten können die Befugnis vorsehen, Zwangsgelder zu verhängen, um eine wesentliche oder wichtige Einrichtung zu zwingen, einen Verstoß gegen diese Richtlinie gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen.

Artikel 20 - Governance

(1) Die Mitgliedstaaten stellen sicher, dass die ***Leitungsorgane wesentlicher und wichtiger Einrichtungen*** *die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen* ***verantwortlich gemacht werden*** *können.*

Die Anwendung dieses Absatzes lässt die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

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 - LINZ NETZ

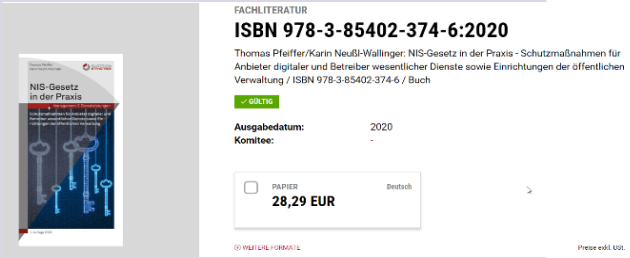
- GAP-Analyse NIS1 zu NIS 2
- Scope-Erweiterung
- ISO/IEC 27001f:2022 und ISO/IEC 27019:yyyy
- EU-RL 2022/2557 (Resilienz kritischer Einrichtungen)
- Network Code on Cybersecurity – cross-border-Security ! (ENTSOe.eu)
- Erneuerbare Energie (Ladestationen, Wärmepumpen, Photovoltaik, …)
- LINZ AG intern - Lieferkette ;-)

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
- Buchautor
- Founder & CEO Council.at GmbH
- CyberKabarettist – in progress
- Advisory Board Member (https://www.ares-ci.com/)

council.at



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