Kritische
INFRASTRUKTUR

Vom Rechenzentrum bis zum Outdoor-Schrank

Roadshow

council.at

LINZ NETZ
Ein Unternehmen der LINZ AG

Energie CISO und NIS-Prüfer als Einbrecher

Graz, 23. September 2025

FATH® | DATWYLER

council.at

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

LINZ NETZ
Ein Unternehmen der LINZ AG

LINZ AG

SILIGAN | HAIDER | RINNER

Energie

Siligan

- E LINZ STROM GAS WÄRME GmbH — Siligan / Föderl
- EM Energiemanagement
- EN Energieerzeugung
- WK Wärme & Kälte
- EV Energie Vertrieb
- TK Telekom
- EDL Energie Dienstleistungen

- LES Linz Energie Service GmbH

Konzernsteuerung & Infrastruktur

Haider

- 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

- NSL NSL GmbH
- N LINZ NETZ GmbH

- DL Donaulager GmbH

Konzernservice & Verkehr

Rinner

- 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

LINZ NETZ
Ein Unternehmen der LINZ AG

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

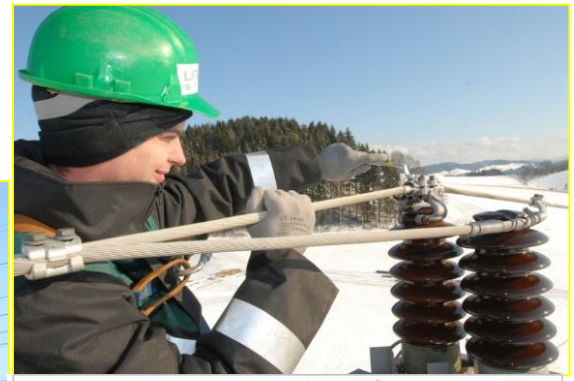
Stromnetz

Netzgebiet

- Linz und 81 Gemeinden
- 1.651 km² versorgte Fläche

Netzanlagen

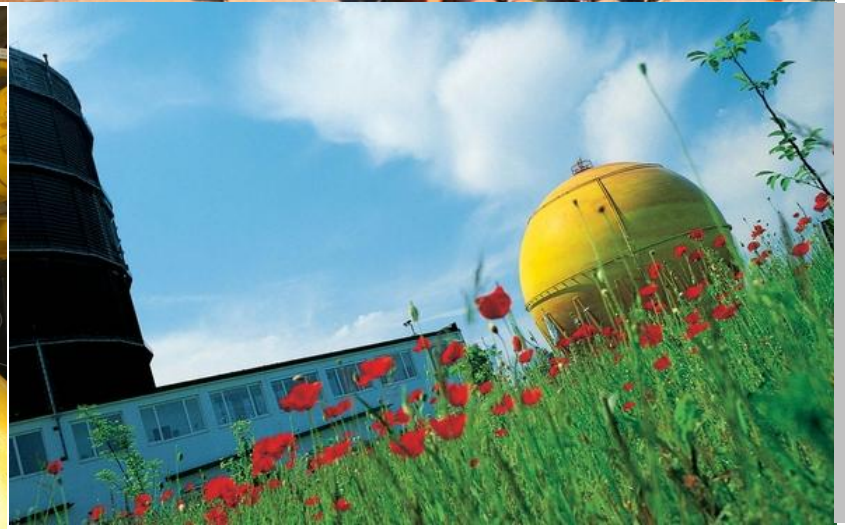
- 8.177 km Leitungslänge
  (110 kV, 25 kV, 10 kV, 6 kV, 0,4 kV)
- 27 Umspannwerke
- rd. 2.870 Trafostationen



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

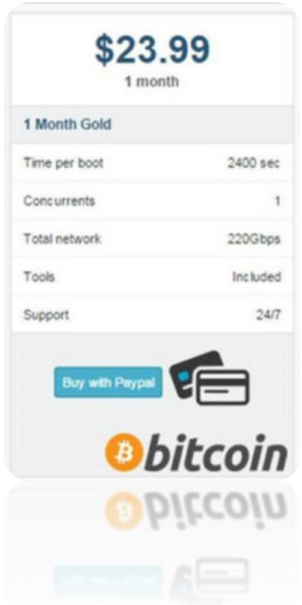
Telekomnetz

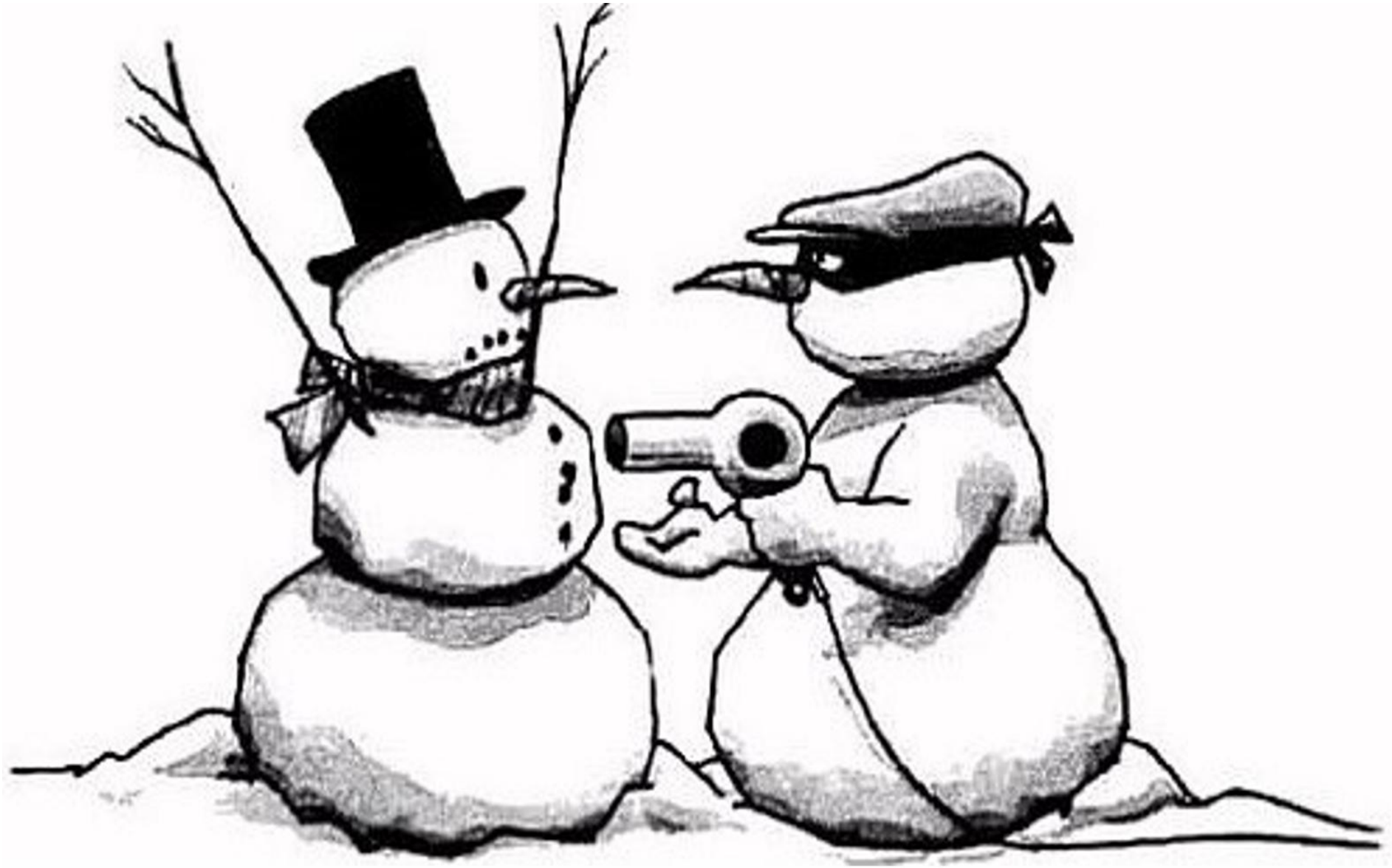
- **910 km Signalkabel**
- **1.818 km Lichtwellenleiterkabel**

Mehr Informationen oder für eine DDoS-Attack

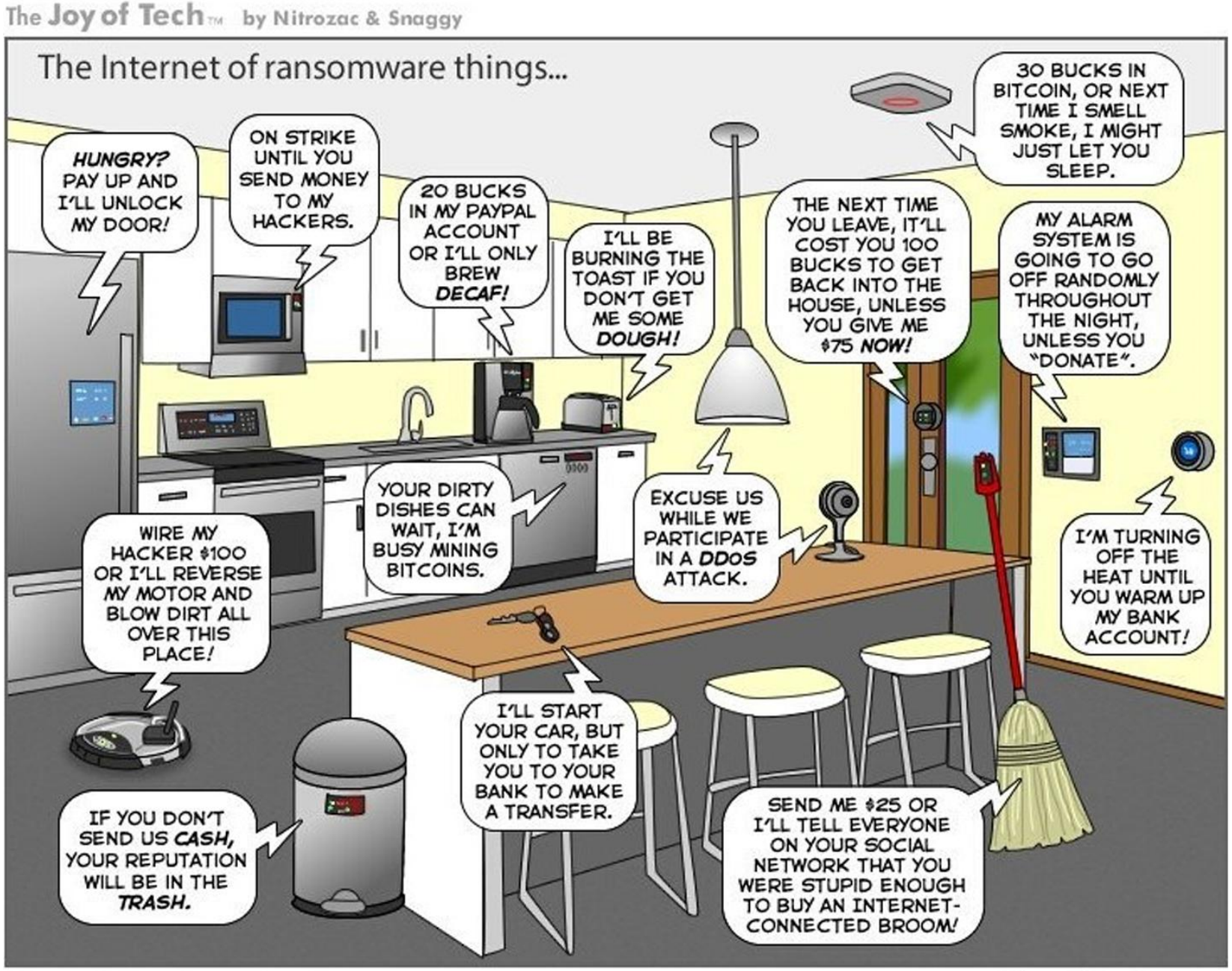
https://www.linzag.at

https://www.linznetz.at



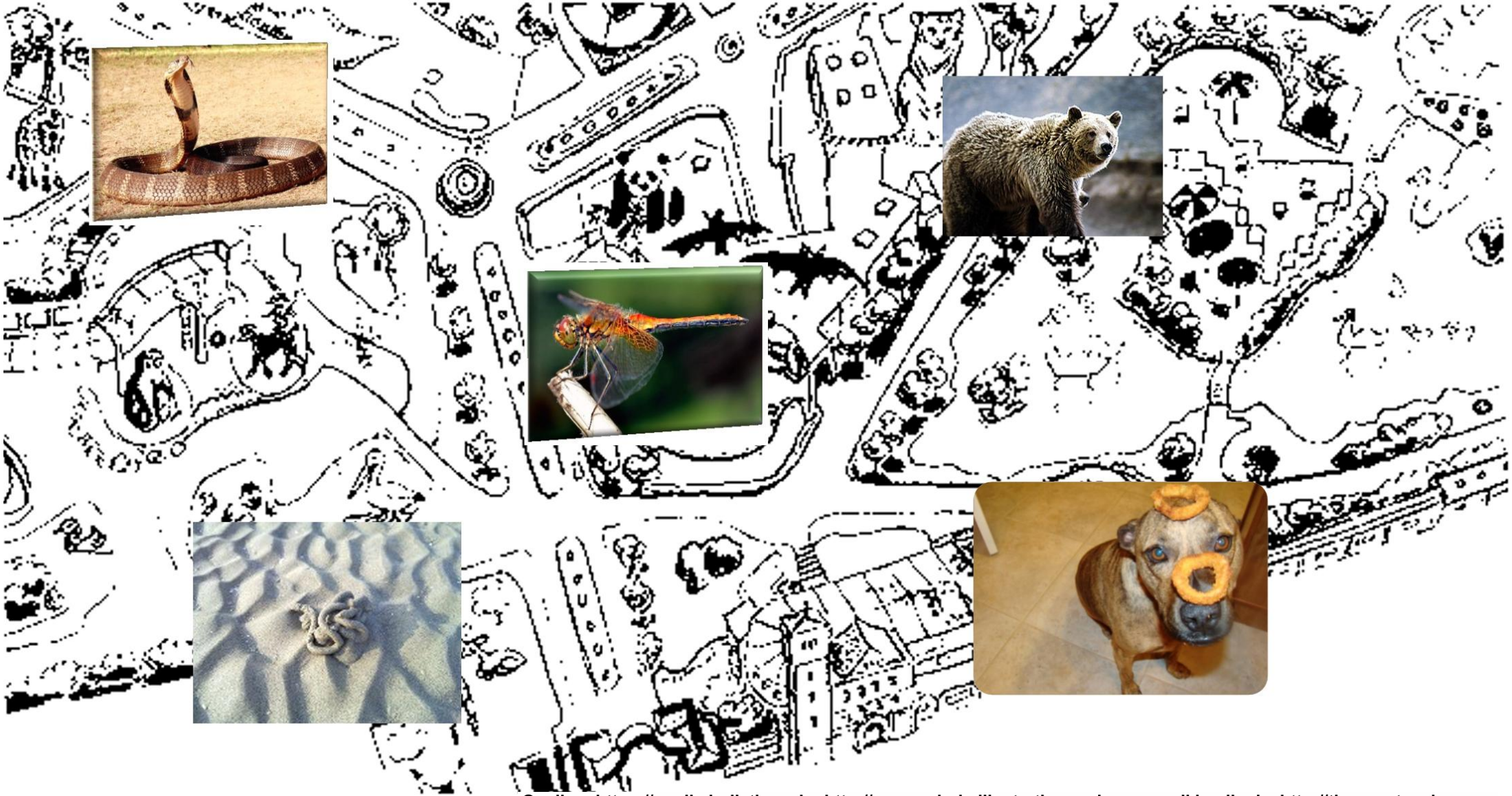


Quelle: blog.de


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

council.at

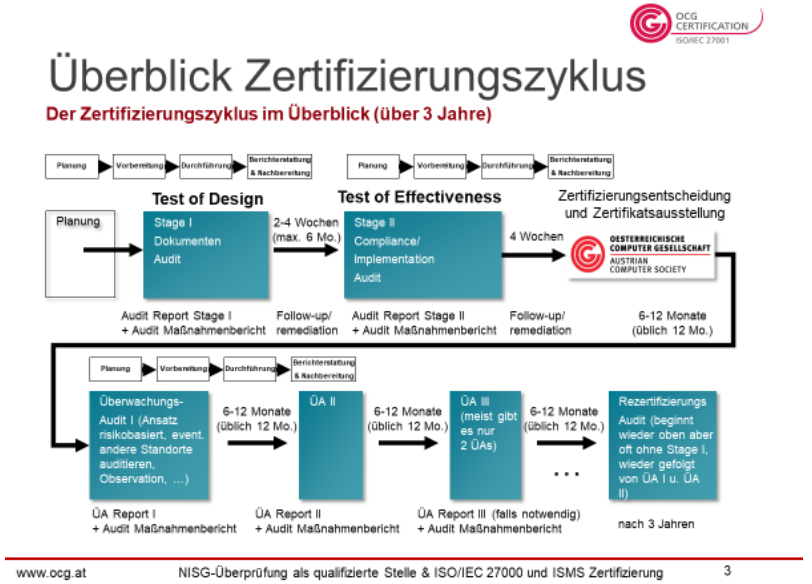
Quellen: https://media.indiatimes.in; http://www.schulz-illustrationen.de; www.wikipedia.de; http://thesmartcanine.com



Quellen: https://media.indiatimes.in; http://www.schulz-illustrationen.de; www.wikipedia.de; http://thesmartcanine.com

ISO/IEC 27001

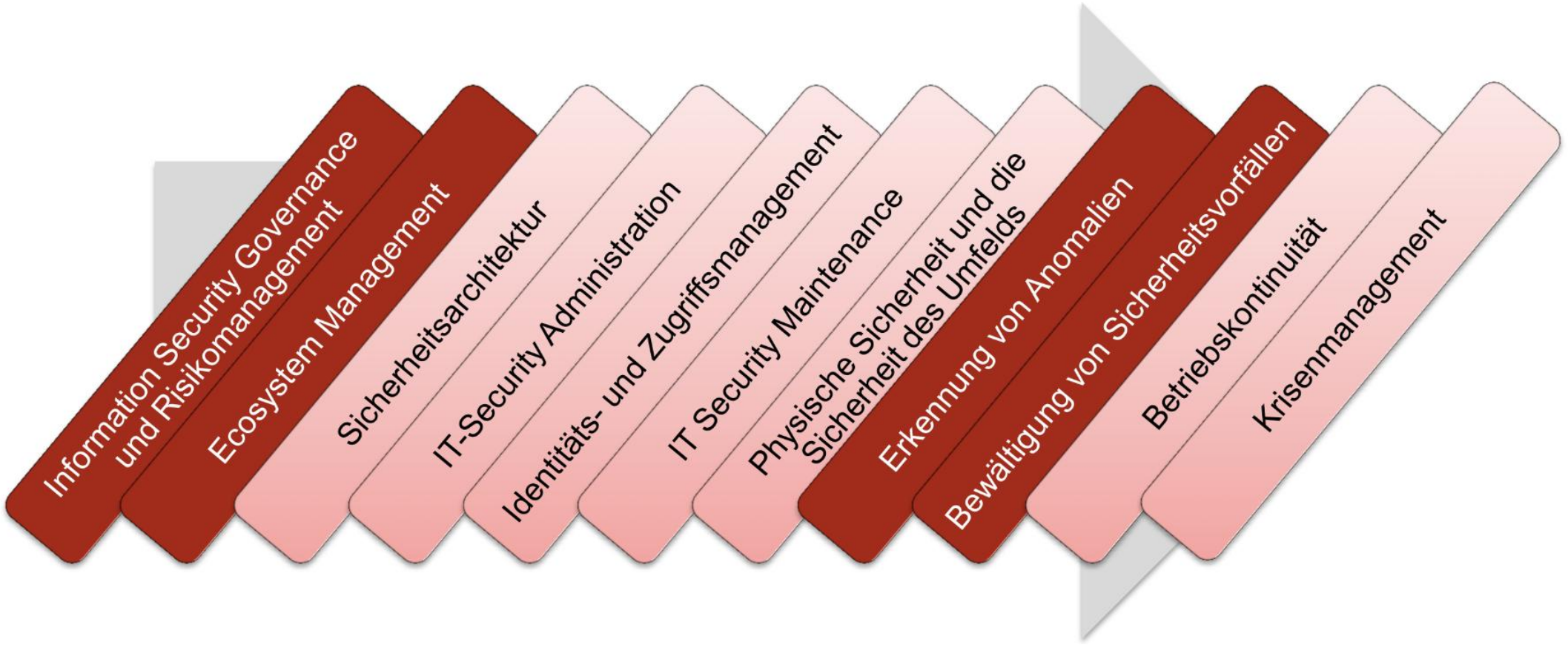
Dieser internationale Standard kann als „Mutter aller Normen und Standards" von Informationssicherheitsmanagementsystemen bezeichnet werden.



Entsprechend dieses Standards besteht die Möglichkeit, sich von externen Auditoren überprüfen zu lassen. Durch die Verleihung eines Zertifikats im definierten Anwendungsbereich (Scope) kann die Effektivität des überprüften Managementsystems bestätigt werden. Ein solches Zertifikat hat die Gültigkeit von drei Jahren und muss durch eine Re-Zertifizierung erneuert werden. In diesem dreijährigen Zyklus erfolgt die Überprüfung mittels zwei Überwachungsaudits durch unabhängige Auditoren von Zertifizierungsstellen (das kann z. B. die Österreichische Computergesellschaft (OCG) sein). Bei diesen Überprüfungen wird ein funktionierendes Informationssicherheitsmanagementsystem erwartet. [1, p.62]

[1] NIS-Gesetz in der Praxis, Thomas Pfeiffer, et.al, ISBN: 978-3-85402-374-6

MINDESTSICHERHEITSVORKEHRUNGEN



Quelle: BM.I / .BVT / CSC

NIS-FACT-SHEET 9/2022

council.at

Bundeskanzleramt

Bundesministerium
Inneres

Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

NIS Fact Sheet 9/2022

Kategorien und Sicherheitsmaßnahmen der NISV 6
1. Governance und Risikomanagement 6
2. Umgang mit Dienstleistern, Lieferanten und Dritten 10
3. Sicherheitsarchitektur 12
4. Systemadministration 16
5. Identitäts- und Zugriffsmanagement 18
6. Systemwartung und Betrieb 20
7. Physische Sicherheit 22
8. Erkennung von Vorfällen 23
9. Bewältigung von Vorfällen 25
10. Betriebskontinuität 27
11. Krisenmanagement 28

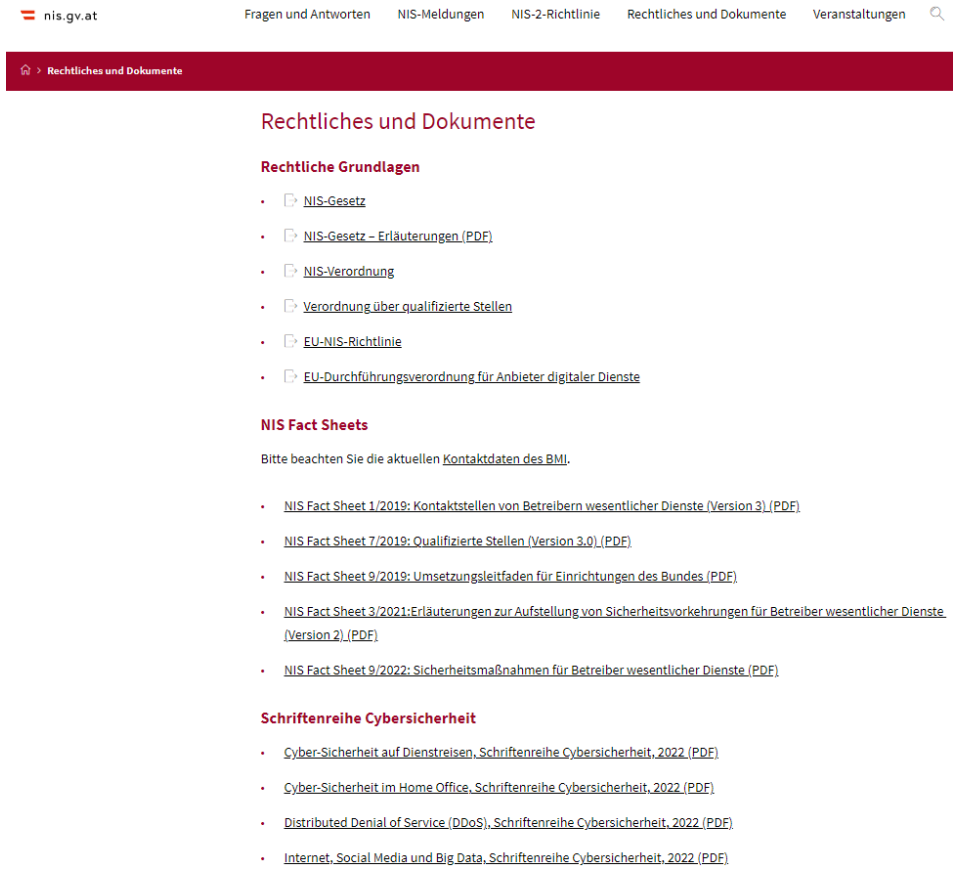
Mapping internationaler Informationssicherheitsstandards und Best Practises

Die NIS-Richtlinie gibt vor, dass die Mitgliedstaaten bei der Umsetzung die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen zu fördern haben, um eine einheitliche Anwendung der Richtlinie zu gewährleisten.[3] Auf Basis dessen wurde innerhalb des Work Streams „Security measures for Operators of Essential Services (OES)“ eine Grundlage für ein Mapping erarbeitet und für die Mitgliedstaaten zur Verfügung gestellt. Dieses Mapping wurde mit nationalen Informationssicherheitsstandards erweitert und enthält demnach folgende Informationssicherheitsstandards und Best Practises:

- IEC 62443 Teil 3-3 („System security requirements and security levels”, edition 1.0, 2013-08)
- IEC 62443 Teil 2-1 (“Security program requirements for IACS asset owners”, draft - CDV, 2019-08)
- ÖNORM A 7700-4 (Ausgabe vom 2019-10-01)
- Österreichisches Informationssicherheitshandbuch – Version 4.3.0 (ÖISHB)
- ISO 27001
- CIS CSC 8.0
- KSÖ Cyber Risk Rating
- EN 50600

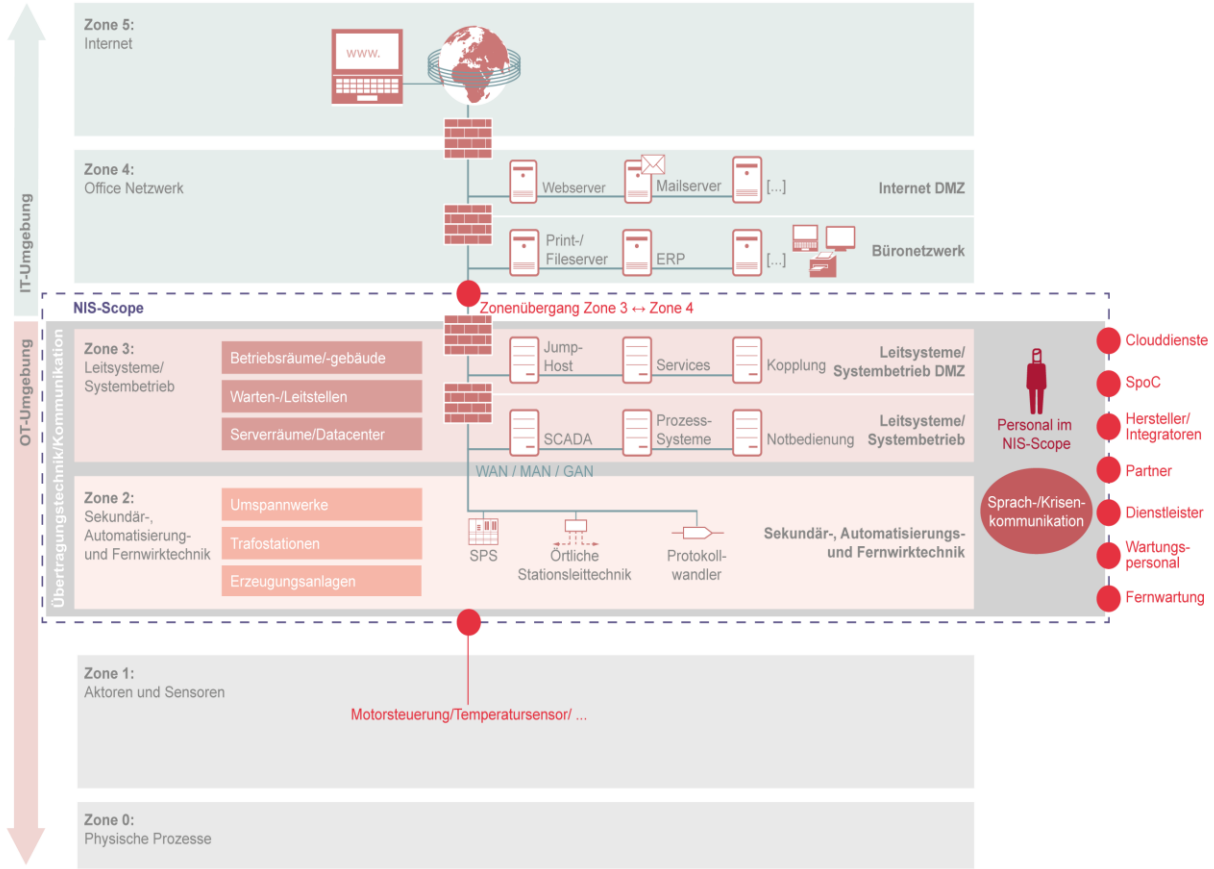
WO FINDE ICH INFORMATIONEN ?

- https://www.nis.gv.at
  - EU-Richtlinien
  - Nationale Gesetze und Verordnungen
  - NIS-Fact-Sheets
  - Schriftenreihe



council.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

council.at

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.

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.

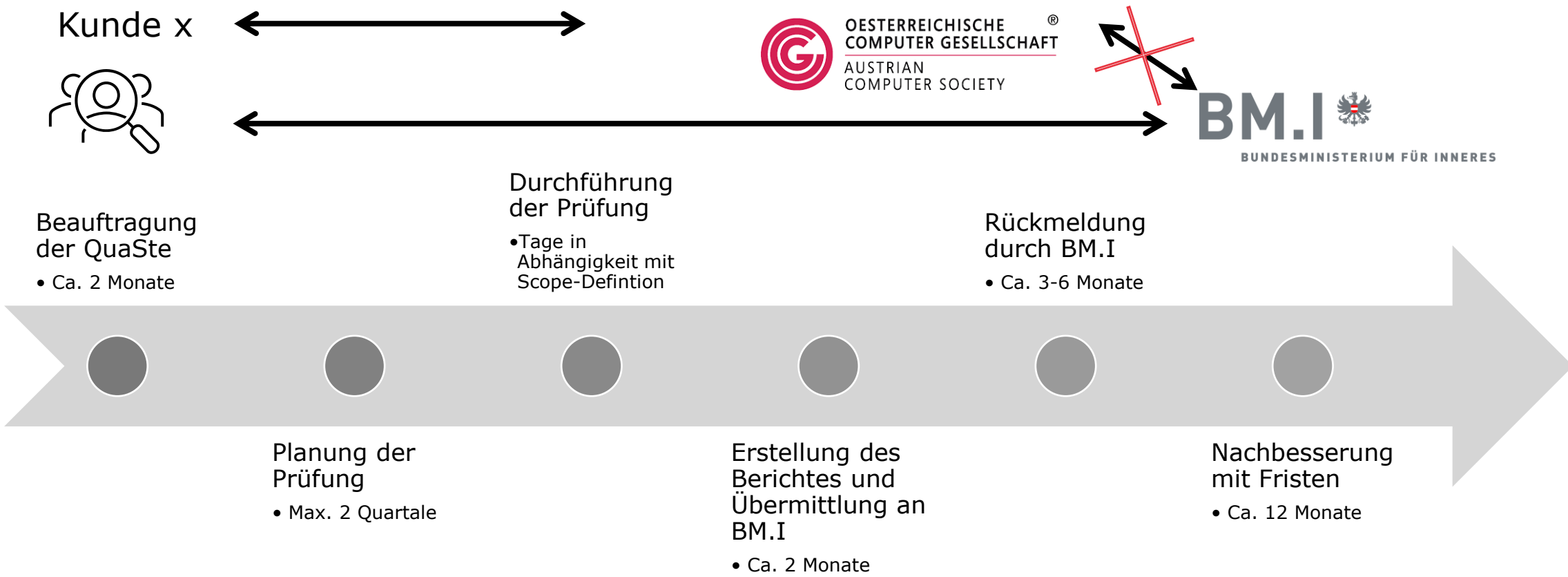
Diese Publikation ist urheberrechtlich geschützt.

Alle Rechte vorbehalten. © Wien 2021

→ Publikationsdatenbank
https://oesterreichsenergie.at/

council.at

ZEITACHSE PRÜFUNG AUS DER PRAXIS



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

KOMBIAUDIT – ISO/IEC 27001 UND NISG

LINZ NETZ
Ein Unternehmen der LINZ AG

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

6.2 Fernzugriff

NIS-Verordnung:
Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.

Der Betreiber etabliert Prozesse zur Verwaltung von Fernzugriffen. Insbesondere stellt er Techniken zur Verfügung, die Fernzugriffe auf Netz- und Informationssysteme nur nach dem Minimalrechtsprinzip autorisiert und zeitlich beschränkt ermöglichen.

Die Authentifizierung im Rahmen des Fernzugriffs wird mittels Zwei-Faktor-Authentifizierung umgesetzt. Jeglicher unautorisierte Zugriff wird unterbunden.

Für Wartungsarbeiten, die über Fernzugriffe erfolgen, stellt der Betreiber sicher, dass alle Tätigkeiten und Operationen aufgezeichnet und dokumentiert werden. Alle Zugriffe externer Personen können nur unter Kontrolle der Systemverantwortlichen erfolgen.

Der Einsatz von sog. „Jumpservern“/„Jumphosts“, bspw. für die Durchführung administrativer Tätigkeiten, ist durchaus möglich. Die Konfiguration der Jumpserver/Jumphosts für die Nutzung durch MitarbeiterInnen, welche sich aus einem Netzwerkabschnitt mit geringerem Schutzbedarf von einem Gerät verbinden bzw. der Einsatz von Sicherheitsmaßnahmen bei ebenjenen, hat den Vorgaben zur Fernwartung von Externen zu entsprechen.

PRÜFUNG! WIE?

Substantive (Nomen)
Fernzugriff, Minimalrechtsprinzip, Periodisch, …

Verben
Eingeschränkt, zu überprüfen, Anzupassen, …

Adjektive
Zeitlich

PRÜFUNGSBEISPIEL

council.at

Kategorie lt. NISV	**Systemwartung und Betrieb**
Sicherheitsmaßnahme lt. NISV	**Fernzugriff**
Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.	
Verwendete Werkzeuge gem. § 2 Z 10 QuaSteV getrennt mit ";"	n/a
Geprüfte Systemkomponenten ID aus "Systemkomponenten" - getrennt mit ";"	19; 30
Aggregierte Effektivitätsbewertung der Sicherheitsmaßnahme	nicht effektiv
Gefährdungsbewertung	hoch

Prüfgegenstand	**Prüfungshandlung**							**Ergebnis / Findings**	
Beschreibung	**Standort**	**Prüfer**	**Vorgehensweise**	**Überprüfungsart**	**Durchgeführte Prüfungshandlungen**	**Evidenzen / Ref.**	**Feststellungen**	**Effektivitätsbewertung**	**Verbesserungsmöglichkeit(en)**
Fernzugriffe sind geregelt und werden sicher betrieben # Der Betreiber stellt Verfahren zur Verfügung, die Fernzugriffe auf Netz- und Informationssysteme nur nach dem Minimalrechtsprinzip autorisiert und zeitlich beschränkt ermöglichen. #	[redacted]	[redacted]	Befragung	tech.	Werden MFAs verwendet?	n/a	Aussagegemäß wird für client-2-site Verbindungen [redacted] verwendet. Der Dienstleister ist die [redacted] und verwendet aussagegemäß wahrscheinlich RSA SecureID. Die Aufzeichnung von allen Operationen und Tätigkeiten konnte nicht nachgewiesen werden.	teilweise effektiv	Der Betreiber wesentlicher Dienste soll dem Risiko angemessen und mit vernünftigtem Aufwand feststellbar die Fernzugriffsberechtigungen in einem periodischem Zyklus iSd NISG überprüfen und eine durchgängige MFA umsetzen.
Fernzugriffe sind geregelt und werden sicher betrieben #	[redacted]	[redacted]	Befragung/Überprüfung	org./tech.	Wie können Fernzugriffe angefordert werden und ist dafür ein Prozess definiert?	Screenshot_Fernzugriff_Genehmigung1 Screenshot_Fernzugriff_Genehmigung2	In Kapitel 3 [ID30] ist definiert, wie ein Fernzugriff angefordert werden kann. Dieser Prozess gilt für interne und externe und läuft über das Serviceportal [ID19]	effektiv	n/a
Für Wartungsarbeiten, die über Fernzugriffe erfolgen, stellt der Betreiber sicher, dass alle Tätigkeiten und Operationen aufgezeichnet und dokumentiert werden. #	[redacted]	[redacted]	Befragung	org./tech.	Werden interne Zugriffe nach den Vorgaben des NIS-Fact-Sheets behandelt?	n/a	Interne Sessions mit Zugriffen Netzwerkabschnitten mit unterschiedlichen Schutzbedarf werden aussagegemäß nicht aufgezeichnet.	nicht effektiv	Auszug aus NIS-Fact-Sheet 9/2022: *Der Einsatz von sog. „Jumpservern"/„Jumphosts", bspw. für die Durchführung administrativer Tätigkeiten, ist durchaus möglich. Die Konfiguration der Jumpserver/Jumphosts für die Nutzung durch MitarbeiterInnen, welche sich aus einem Netzwerkabschnitt mit geringerem Schutzbedarf von einem Gerät verbinden bzw. der Einsatz von Sicherheitsmaßnahmen bei ebenjenen, hat den Vorgaben zur Fernwartung von Externen zu entsprechen.* *... Für Wartungsarbeiten, die über Fernzugriffe erfolgen, stellt der Betreiber sicher, dass alle Tätigkeiten und Operationen aufgezeichnet und dokumentiert werden*
									Der Betreiber wesentlicher Dienste soll dem Risiko angemessen und

Nr.	Sicherheitsmaßnahme lt. NISV	Effektivitätsbewertung	Gefährdungsbewertung
1.	**Governance und Risikomanagement**		
1.1	Risikoanalyse	teilweise effektiv	niedrig
1.2	Sicherheitsrichtlinie	teilweise effektiv	niedrig
1.3	Überprüfungsplan der Netz- und Informationssysteme	teilweise effektiv	mittel
1.4	Ressourcenmanagement	teilweise effektiv	niedrig
1.5	Informationssicherheitsmanagementsystemprüfung	teilweise effektiv	mittel
1.6	Personalwesen	teilweise effektiv	niedrig
2.	**Umgang mit Dienstleistern, Lieferanten und Dritten**		
2.1	Beziehungen mit Dienstleistern, Lieferanten und Dritten	teilweise effektiv	niedrig
2.2	Leistungsvereinbarungen mit Dienstleistern und Lieferanten	teilweise effektiv	niedrig
3.	**Sicherheitsarchitektur**		
3.1	Systemkonfiguration	effektiv	niedrig
3.2	Vermögenswerte	teilweise effektiv	niedrig
3.3	Netzwerksegmentierung	teilweise effektiv	hoch
3.4	Netzwerksicherheit	teilweise effektiv	hoch
3.5	Kryptographie	nicht effektiv	mittel
4.	**Systemadministration**		
4.1	Administrative Zugangsrechte	teilweise effektiv	niedrig
4.2	Systeme und Anwendungen zur Systemadministration	teilweise effektiv	mittel
5.	**Identifikations- und Zugriffsmanagement**		
5.1	Identifikation und Authentifikation	teilweise effektiv	niedrig
5.2	Autorisierung	teilweise effektiv	niedrig
6.	**Systemwartung und Betrieb**		
6.1	Systemwartung und Betrieb	teilweise effektiv	niedrig
6.2	Fernzugriff	nicht effektiv	hoch
7.	**Physische Sicherheit**		
7.1	Physische Sicherheit	nicht effektiv	hoch
8.	**Erkennung von Vorfällen**		
8.1	Erkennung	teilweise effektiv	mittel
8.2	Protokollierung und Monitoring	teilweise effektiv	niedrig
8.3	Korrelation und Analyse	teilweise effektiv	niedrig
9.	**Bewältigung von Vorfällen**		
9.1	Vorfallsreaktion	teilweise effektiv	niedrig
9.2	Vorfallsmeldung	teilweise effektiv	niedrig
9.3	Vorfallsanalyse	effektiv	niedrig
10.	**Betriebskontinuität**		
10.1	Betriebskontinuitätsmanagement	effektiv	niedrig
10.2	Notfallmanagement	teilweise effektiv	mittel
11.	**Krisenmanagement**		
11.1	Krisenmanagement	teilweise effektiv	niedrig

ÜBERSICHT

Effektiv – Wahrscheinlich OK

Teilweise effektiv – ToDo Deadline

Nicht effektiv – ToDo Deadline – Strafandrohung

Gefährdungsbewertung als Zusatz Parameter zur Einschätzung für die Behörde

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

FEUERWEHRZUFAHRT FREIHALTEN!
Achtung
Haupttor sperren
Secret
Secret
Secret
Secret
Secret
Graz 23.09.2025

council.at

council.at

Brandmelderzentrale
Graz 23.09.2025

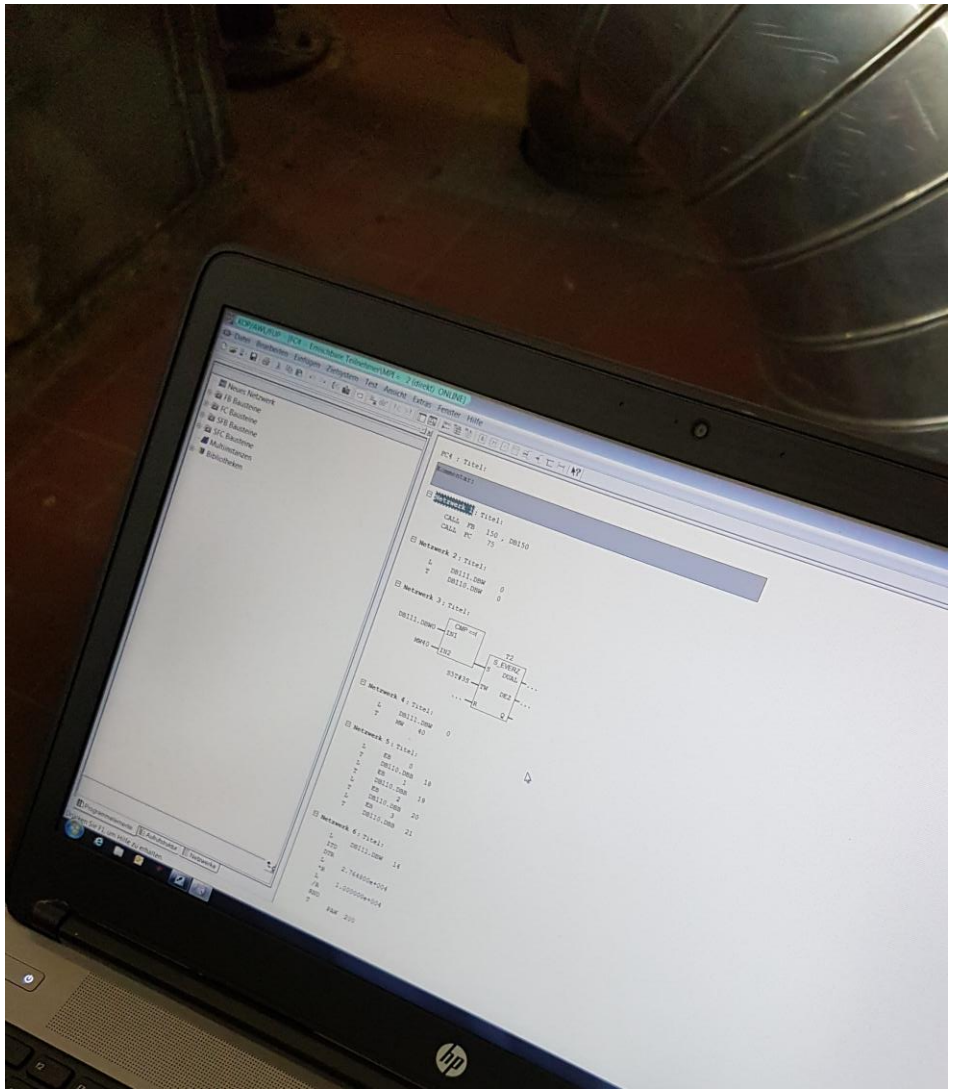
SIEMENS
SF
DC5V
FRCE
RUN
STOP
PUSH
RUN
STOP
MRES
SIMATIC
S7-300

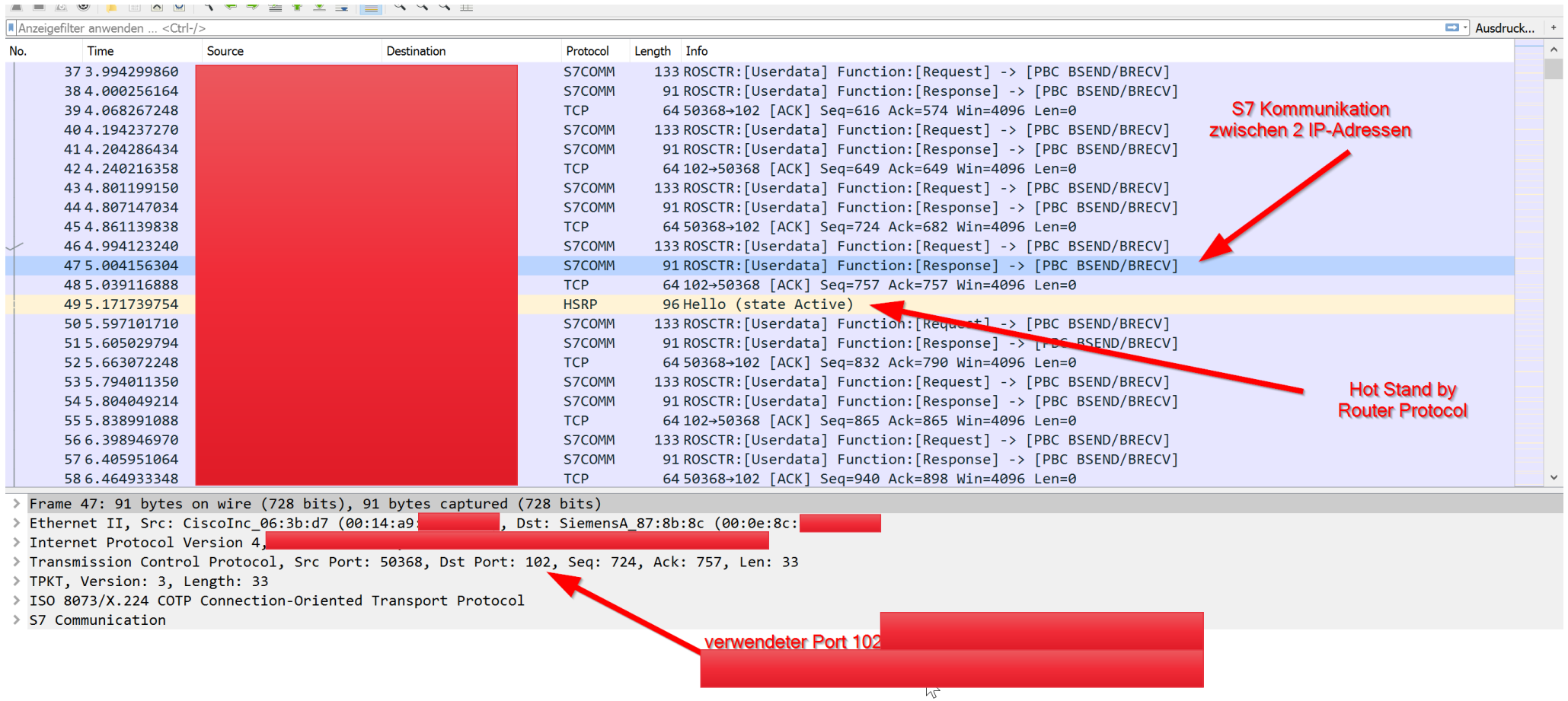
council.at

Netzumwälz-
pumpe 1
Saugschieber

SIEMENS
SIMATIC
S7-300
RUN
STOP
MRES
PUSH

Netzumwälz-
pumpe 1
Saugschieber




Anzeigefilter anwenden ... <Ctrl-/>
Ausdruck...
No. Time Source Destination Protocol Length Info
37 3.994299860 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
38 4.000256164 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
39 4.068267248 TCP 64 50368→102 [ACK] Seq=616 Ack=574 Win=4096 Len=0
40 4.194237270 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
41 4.204286434 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
42 4.240216358 TCP 64 102→50368 [ACK] Seq=649 Ack=649 Win=4096 Len=0
43 4.801199150 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
44 4.807147034 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
45 4.861139838 TCP 64 50368→102 [ACK] Seq=724 Ack=682 Win=4096 Len=0
46 4.994123240 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
47 5.004156304 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
48 5.039116888 TCP 64 102→50368 [ACK] Seq=757 Ack=757 Win=4096 Len=0
49 5.171739754 HSRP 96 Hello (state Active)
50 5.597101710 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
51 5.605029794 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
52 5.663072248 TCP 64 50368→102 [ACK] Seq=832 Ack=790 Win=4096 Len=0
53 5.794011350 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
54 5.804049214 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
55 5.838991088 TCP 64 102→50368 [ACK] Seq=865 Ack=865 Win=4096 Len=0
56 6.398946970 S7COMM 133 ROSCTR:[Userdata] Function:[Request] -> [PBC BSEND/BRECV]
57 6.405951064 S7COMM 91 ROSCTR:[Userdata] Function:[Response] -> [PBC BSEND/BRECV]
58 6.464933348 TCP 64 50368→102 [ACK] Seq=940 Ack=898 Win=4096 Len=0
S7 Kommunikation zwischen 2 IP-Adressen
Hot Stand by Router Protocol
Frame 47: 91 bytes on wire (728 bits), 91 bytes captured (728 bits)
Ethernet II, Src: CiscoInc_06:3b:d7 (00:14:a9:
, Dst: SiemensA_87:8b:8c (00:0e:8c:
Internet Protocol Version 4,
Transmission Control Protocol, Src Port: 50368, Dst Port: 102, Seq: 724, Ack: 757, Len: 33
TPKT, Version: 3, Length: 33
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
S7 Communication
verwendeter Port 102
0000 00 0e 8c 87 8b 8c 00 14 a9 06 3b d7 08 00 45 00 ....;...E.
0010 00 49 ef b4 00 00 19 06 1d b9 0a 06 00 0f 0a 20 .I..... ..... .
0020 80 0d c4 c0 00 66 09 e9 76 3e 09 7c d6 da 50 18 .....f.. v>.|..P.
0030 10 00 33 a0 00 00 03 00 00 21 02 f0 80 32 07 00 ..3..... .!...2..
0040 00 b1 41 00 0c 00 04 00 01 12 08 12 86 01 44 00 ..A..... ..... D.
0050 00 00 00 0a 00 00 00 c7 44 bf 89 ..... D..

council.at

Fluchtweg
nicht
versperren!
Wasser
ZS 50
0,5
6,2

ÖSTERREICH
MONTAG, 29. AUGUST 2016
Heute mit dem besten Gesund-Magazin
MIT GESUND & FIT:
Fitness für Kids
gesund&fit
Heute:
Obers
Sport-
Extra
Nur 2,50 Euro

Quellen: https://media.indiatimes.in; http://www.schulz-illustrationen.de; www.wikipedia.de; http://thesmartcanine.com

NIS 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]

WAS WILL NIS 2.0 BESSER MACHEN?

1. Stärkung der Cyberresilienz eines alle relevanten Sektoren umfassenden Spektrums von Unternehmen,
   - alle öffentlichen und privaten Einrichtungen im gesamten Binnenmarkt, die wichtige Funktionen für die Wirtschaft und die Gesellschaft als Ganzes erfüllen, sollen verpflichtet werden, angemessene Cybersicherheitsmaßnahmen zu ergreifen

2. Förderung einer gleich starken Resilienz bei den bereits unter die Richtlinie fallenden Sektoren im Binnenmarkt , durch weitere Angleichung
   (1) des De facto Anwendungsbereichs,
   (2) der Sicherheitsanforderungen und Meldepflichten bei Sicherheitsvorfällen,
   (3) der Bestimmungen für die nationale Aufsicht und Durchsetzung sowie,
   (4) der Kapazitäten der zuständigen Behörden in den Mitgliedstaaten.

WAS WILL NIS 2.0 BESSER MACHEN?

3. Verbesserung der gemeinsamen Lageerfassung und der kollektiven Vorsorge und Reaktionsfähigkeit
   (1) Maßnahmen zur Stärkung des Vertrauens zwischen den zuständigen Behörden
   (2) verstärkten des Informationsaustauschs
   (3) Festlegung von Regeln und Verfahren im Falle weitreichender Sicherheitsvorfälle oder Krisen

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	

ANWENDUNGSBEREICH

- **NIS1:**
  - Mitgliedstaaten hatten großen Ermessensspielraum bei der Ermittlung der Betreiber wesentlicher Dienste.

- **NIS2:**
  - Anwendungsbereich durch „size cap rule" vorgegeben.
  - NIS2 gilt für alle öffentliche oder private wesentliche und wichtige Einrichtungen der in Anhang I und Anhang II genannten Art, die ihre Dienstleistungen in der EU erbringen oder ihre Tätigkeiten in der EU ausüben und die den Schwellenwert für mittlere Unternehmen iSd Empfehlung 2003/361/EG der EU-Kommission erreichen oder überschreiten
  - Kleinunternehmen nur in bestimmten Fällen umfasst.

NIS 2.0 – WESENTLICHE UND WICHTIGE EINRICHTUNGEN

	Wesentliche / Wichtige	Wichtige / Wesentliche
Anwendungsbereich	Annex I NIS 1 + ausgewählte neue Sektoren	Annex II Überwiegend neue Sektoren + bestimmte NIS1 Einrichtungen
Sicherheitsmaßnahmen	Risikobasierte Sicherheitsverpflichtungen	
Meldepflichten	Signifikante Vorfälle und signifikante Bedrohungen	
Aufsicht	Ex-ante	Ex-post

- Kein Ermittlungsverfahren mehr
- Kleinunternehmen ausgenommen (aber: Gegenausnahmen)

RISIKOMANAGEMENTMAßNAHMEN IS NISG 2024 ENTWURF IVM ANLAGE 3

council.at

- 50 Stück AT versus 10 Stück EU 2022/2555 Artikel 21
- ISO/IEC 27001 Zertifizierung unterstützt Sorgfaltspflicht
- Was ist mit Unternehmen außerhalb Österreichs?

1 von 2

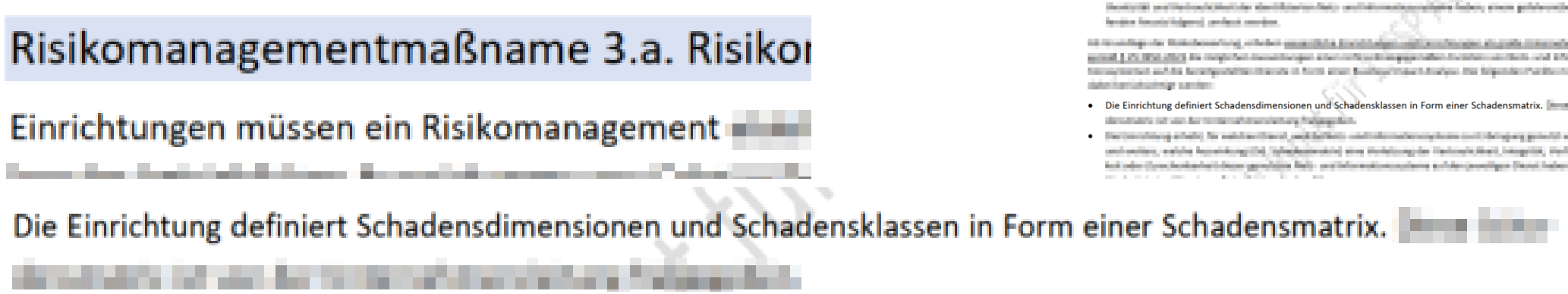
Anlage 3

Risikomanagementmaßnahmen-Bereiche	
1.	Leitungsorgane
a.	Rollen und Verantwortlichkeiten der Leitungsorgane
2.	Sicherheitsrichtlinien
a.	Sicherheitsrichtlinien
b.	Funktionen, Aufgaben und Verantwortlichkeiten
3.	Risikomanagement
a.	Risikomanagementrichtlinie und -prozess
b.	Beurteilung der Effektivität von Risikomanagementmaßnahmen
c.	Überwachung der Einhaltung von Vorgaben
d.	Unabhängige Überprüfungen
4.	Verwaltung von Vermögenswerten
a.	Inventarisierung von Vermögenswerten
b.	Klassifikation von Vermögenswerten
c.	Handhabung von Vermögenswerten
d.	Umgang mit Wechseldatenträger
e.	Rücknahme oder Löschung von Vermögenswerten
5.	Personalwesen
a.	Sicherheit im Personalwesen
b.	Hintergrundüberprüfung
c.	Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses
d.	Disziplinarmaßnahmen
6.	Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
a.	Bewusstseinsschaffung und Cyberhygiene
b.	Cybersicherheitsschulungen

council.at

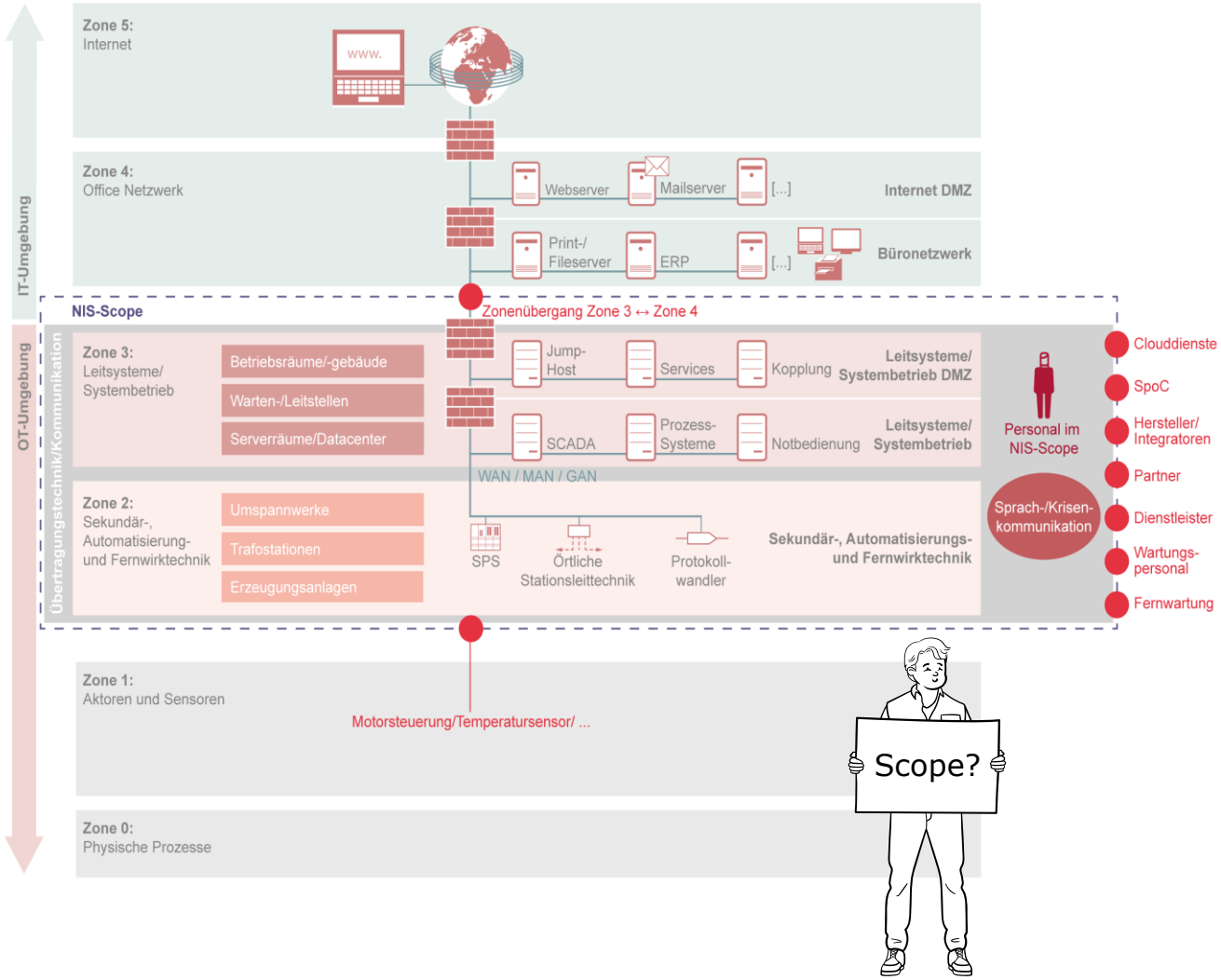
WAS MUSS ICH UMSETZEN?

- Durchführungsverordnung (nat. BM.I notwendig / digital EU erledigt)
- Cybersicherheitsplattform (CSP) – PPP-Modell
- Anpassung von möglichen neuen NIS-Fact-Sheet
- Na dann warte ich darauf
- Reifegrad voraussichtlich ca. 2 Jahre



RISIKOBASIERTER ALL-HAZARD-APPROACH ANSATZ

council.at



- Generische Risikoanalyse für die Einrichtung
- Business Impact Analyse
- Assetdeklaration/-definition
- Risikomanagement auf Ziele, Prozesse, Assets, Lieferkette, …
- Maßnahmendefinition nach NISG 2024 Anlage 3, ISO/IEC 27001, DSG-VO, […]

RCE UND CRA – DIE ZUKUNFT DER CYBERSICHERHEIT?

council.at

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 GEGENWÄRTIGE CYBERSICHERHEIT

council.at

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;

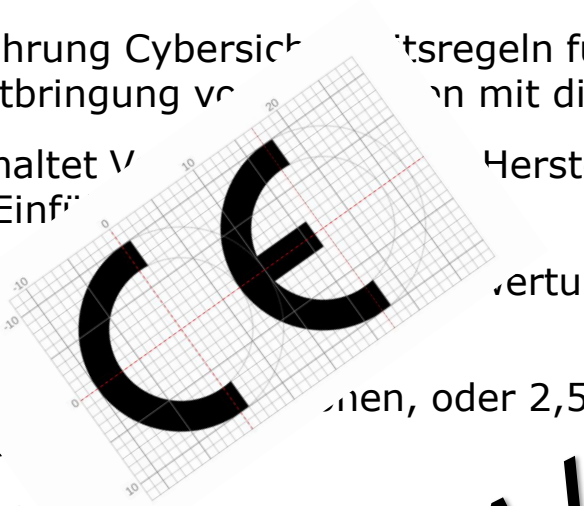
e) ein angemessenes Sicherheitsmanagement […].

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 Cybersich[illegible]tsregeln für die auf-den-Marktbringung v[illegible]n mit digitalen Elementen
- Beinhaltet V[illegible] Hersteller, Distributoren und Einf[illegible]
- Ver[illegible]ertungen je nach [illegible]
- Str[illegible]nen, oder 2,5% des weltweiten Ums[illegible]
- Risikor[illegible]:
  - 90% aller Produkte (default category): Self-Assessment
  - 10% entweder
    - Critical „Class I" (Standard oder Third-Party Assessment)
    - Critical „Class II" (Third-Party Assessment)



EU 2024/2847

MASCHINENVERORDNUNG (EU 2023/1230)

TRITT IM JÄNNER 2027 IN KRAFT

- Die neue Maschinenverordnung betrifft Unternehmen, die Maschinen entwerfen, herstellen, in Verkehr bringen oder in Betrieb nehmen. Hersteller, Bevollmächtigte, Importeure und Händler von Maschinen und verwandten Produkten. Die Verordnung gilt für alle Maschinen sowie für die mit diesen Maschinen verbundenen Sicherheitskomponenten. Neu ist, dass die Verordnung auch explizit Software für sicherheitskritische Anwendungen in Maschinen reguliert, was insbesondere im Zusammenhang mit digitaler Sicherheit und Cybersicherheit relevant wird.
- Was muss umgesetzt werden?
  - CE-Kennzeichnung: Maschinen müssen weiterhin eine CE-Kennzeichnung erhalten, um anzuzeigen, dass sie den Sicherheitsanforderungen entsprechen.
- Technische Dokumentation:
  - Detaillierte technische Unterlagen müssen erstellt und bereitgestellt werden, insbesondere zu sicherheitskritischen Softwarekomponenten.
  - Risikobeurteilung: Es ist eine vollständige Risikobeurteilung der Maschinen erforderlich, die nun auch Cyberrisiken einbezieht. Es geht also nicht nur um mechanische Sicherheit, sondern auch um die Sicherheit der Steuerungssoftware und deren Schutz vor Cyberangriffen.
  - Digitaler Zugang zu Dokumenten: Ein großer Unterschied zur alten Richtlinie besteht darin, dass die technische Dokumentation auch digital zugänglich gemacht werden kann.

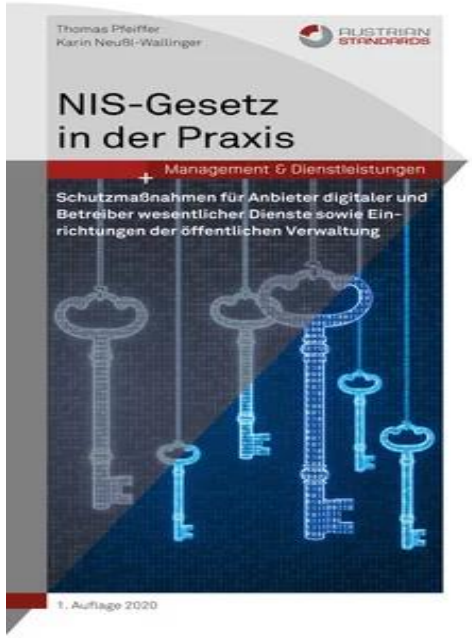
WENN MAN EINMAL WEIß, WIE MAN ETWAS FALTET, DANN KANN AUS EINEM WEIßEN BLATT PAPIER VIEL ENTSTEHEN.

[…] FALTEN WIR GEMEINSAM

https://pixabay.com/ -jolanta waniowska

WHO AM I ?

council.at



NIS-Gesetz in der Praxis

Schutzmaßnahmen für Anbieter digitaler und Betreiber wesentlicher Dienste sowie Einrichtungen der öffentlichen Verwaltung

ISBN:	978-3-85402-374-6
Verlag:	Austrian Standards plus GmbH
Land des Verlags:	Österreich
Erscheinungsdatum:	13.03.2020
Autoren:	Pfeiffer Thomas, Neußl-Wallinger Karin
Reihe:	QuickInfo
Format:	Softcover
Seitenanzahl:	154

Thomas Pfeiffer, BSc MSc

- Chief Information Security Officer (CISO)
- Chairman a.D. Österreichs Energie
- Lecturer
  - Security Department – FH Hagenberg
- ISO/IEC 27001 Auditor und Qualifizierter Prüfer iS NISG iVm QuaSteV
  - Österreichische Computer Gesellschaft
- Buchautor
- Founder & CEO Council.at GmbH
- Cyber-Kabarettist
- Advisory Board Member (https://www.ares-ci.com/)

Kontakt:

t.pfeiffer@council.at
Thomas Pfeiffer

FRAGEN?

COUNCIL.AT GMBH
PROMENADE 25 / TOP 7
4020 LINZ
INFO@COUNCIL.AT
council.at

Q&A