

NIS-PRÜFSTELLE

NIS-2 kommt

INFORMATIONSVVERANSTALTUNG

23.04.24

Campus V - Hintere Achmühlerstraße 1 . 6850 Dorbirn

Allgemeines

NIS-PRÜFSTELLE

NIS-2 kommt

INFORMATIONSVERANSTALTUNG

23.04.24 | Campus V - Hintere Achmühlerstraße 1, 6850 Dornbirn

VORTRAGENDE:

- DR.TECH WOLFGANG PRENTNER
- DR. CHRISTINE KNECHT-KLEBER
- ING. PETER SAGMEISTER, MSC
- KASPER HORST, MBA CMC

MODERATION:

- MATTHIAS NEUSTÄDTER / ORF

ANMELDESEITE
Event



Link in Bio



NIS-2 . Prüfstelle informiert CYBER-Sicherheit

PROGRAMM

16:00

- Empfang: Dr.tech Wolfgang Prentner / ZTP.digital
- Moderation: Matthias Neustädter / ORF

VORTRAG

16:10

- Kasper Horst, MBA CMC
- UBIT/WKO - Wie unterstützt die WKÖ zur NIS-2?

VORTRAG

16:20

- Ing. Peter Sagmeister, MAS / VBG Landeskrankenhäuser
- Praxisbericht: Gesetzliches NIS-Audit 2023

VORTRAG

16:50

- Dr. Christine Knecht-Kleber / Rechtsanwältin
- Rechtliche Grundlagen zu NIS-2

VORTRAG

17:20

- Dr.tech Wolfgang Prentner / NIS-Prüfer
- Wie arbeitet eine Prüfstelle nach NIS-2

18:00

- Diskussion mit Fragen und Antworten

Ende: 18:30 Uhr

Management Board

von ZTP.digital



Wolfgang Prentner

Lehre und HTL in Vorarlberg (Josef Otten)

Informatiker (TU-Wien)

IT-Ziviltechniker . staatlich befugt und beeidet seit 1998

Gerichtssachverständiger seit 2005

Vorsitzender der Bundesfachgruppe IT in der ZT-Kammer

E-GOV Beauftragter „Die Freien Berufe Österreich“ seit 2003

Mitglied „Plattform Digitales Österreich“ im BKA/BMDW seit 2004

Mitglied „Executive Board Unternehmensserviceportal“ im BMF seit 2013



Das Unternehmen



Gründung: 1998



Mitarbeiter: 15



Standorte in Österreich
Wien, NÖ, VBG



Umsatz 2023
€ 2 Mio überschritten



Kunden: 30



Kundenstruktur

Österreichweite Unternehmen,
Behörden und internationale
Konzerne

Zertifizierte

Cyber-Security

Technologie



ZfP 
DIGITAL . SICHER

IT-Ziviltechniker

Unabhängig.

Planen.
Prüfen.

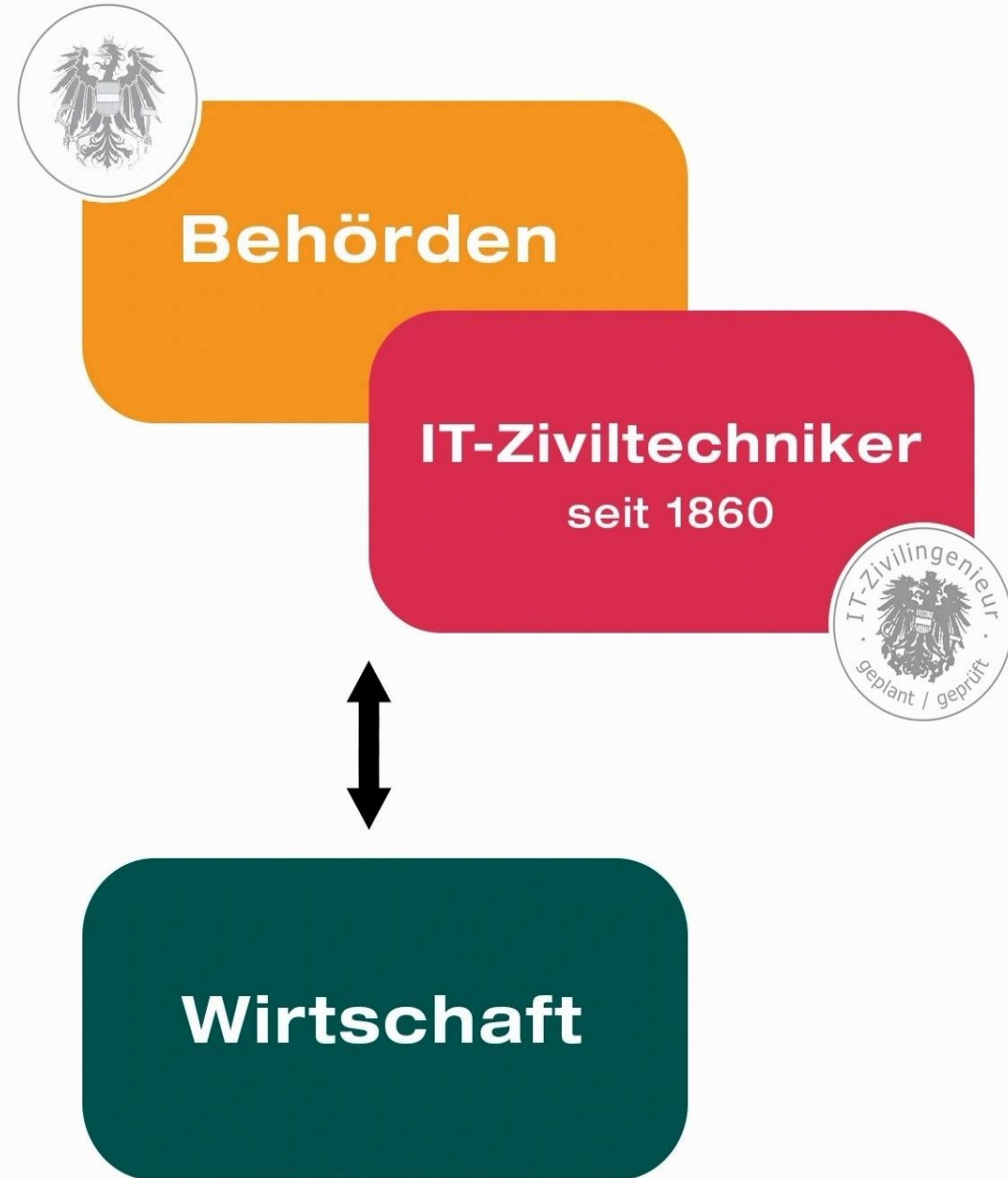
Nur sicher mit dem Siegel.

Ihre ZiviltechnikerInnen.



zt:

Ziviltechniker



Vorträge

NIS-2 . Prüfstelle informiert CYBER-Sicherheit

PROGRAMM

16:00

- Empfang: Dr.tech Wolfgang Prentner / ZTP.digital
- Moderation: Matthias Neustädter / ORF

VORTRAG

16:10

- Kasper Horst, MBA CMC
- UBIT/WKO - Wie unterstützt die WKÖ zur NIS-2?

VORTRAG

16:20

- Ing. Peter Sagmeister, MAS / VBG Landeskrankenhäuser
- Praxisbericht: Gesetzliches NIS-Audit 2023

VORTRAG

16:50

- Dr. Christine Knecht-Kleber / Rechtsanwältin
- Rechtliche Grundlagen zu NIS-2

VORTRAG

17:20

- Dr.tech Wolfgang Prentner / NIS-Prüfer
- Wie arbeitet eine Prüfstelle nach NIS-2

18:00

- Diskussion mit Fragen und Antworten

Ende: 18:30 Uhr

Vortrag

Wie arbeitet eine Prüfstelle nach NIS

Dr.tech Wolfgang Prentner / NIS-Prüfer

Inhalt

- Allgemeines „Ersten Überblick verschaffen“
- Gesetzesgrundlage NISG 2024 „Begutachtungsentwurf“
- Definition von Cyber-Sicherheit, Netz- und Informationssystemen
- Inhalt: Wie arbeitet eine Prüfstelle nach NIS
- Unterlage und Informationen
- Zusammenfassung

Bundesgesetz: NISG 2024

Bundesgesetz
zur
Gewährleistung eines hohen Cybersicherheitsniveaus
von
Netz- und Informationssystemen
(NISG 2024)

Rechtliches aus dem BKA zur NIS2

09.04.2024

NIS-2 Business Breakfast: Es gilt keine Zeit zu verlieren!



Mag. Arno Spiegel
Leiter NIS Büro
Bundeskanzleramt, Abteilung I/8
Krisenrechenzentrum)
Wien, 08.04.2024
NIS2-Vortrag im Anhang

Definition

Cyber-Sicherheit, Netz- und Informationssystemen

Definition Netz- und Informationssystem

NISG §3 Abs 1

Netz- und Informationssystem

- a) Kommunikationsnetz im Sinne des § 4 Z 1 des Telekommunikationsgesetzes 2021 (TKG 2021), BGBl. I Nr. 190/2021,
- b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder
- c) digitale Daten, die von den in den Buchstaben a) und b) genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

Definition: Cyber-Sicherheit

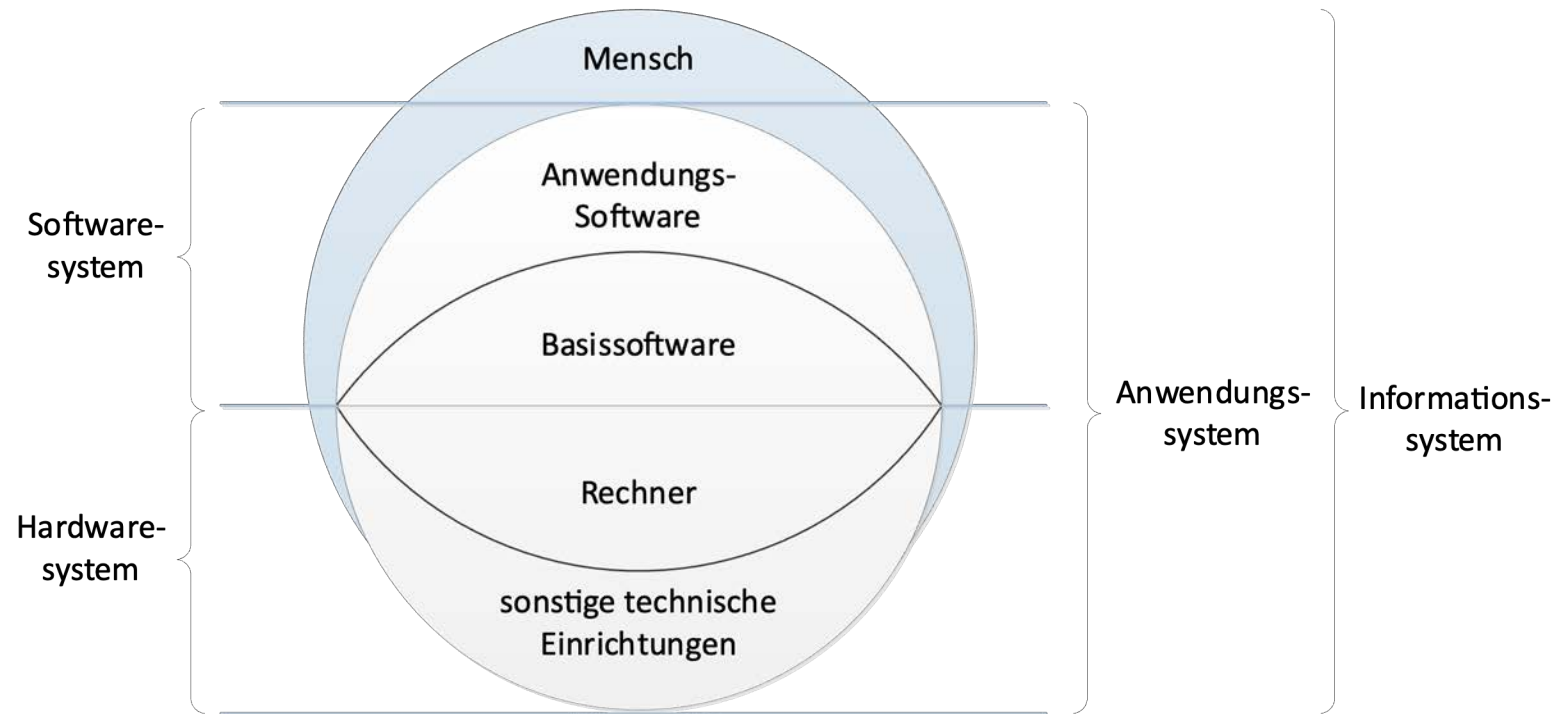
NISG §3 Abs 2 . VAIV

„Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten **Vertrauensniveau** alle Ereignisse abzuwehren, die die

1. Verfügbarkeit,
2. Authentizität,
3. Integrität oder
4. Vertraulichkeit

gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können

2. Informationssysteme



Risikomanagementmaßnahmen

nach Anlage 3

Anlage 3

Risiko-Managementmaßnahmen-Bereiche

Kontroll-Punkte (13/49 vormals 11) für Einzelnachweise und Dokumente

1. Leitungsorgane (1)
2. Sicherheitsrichtlinien (2)
3. Risikomanagement (4)
4. Verwaltung von Vermögenswerten (5)
5. Personalwesen (4)
6. Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen (2)
7. Sicherheit von Lieferketten (2)
8. Zugangssteuerung (7)
9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung (10)
10. Kryptographie (1)
11. Umgang mit Cybersicherheitsvorfällen (6)
12. Betriebskontinuitäts- und Krisenmanagement (3)
13. Umgebungsbezogene und physische Sicherheit (2)

Zu 8. Zugangssteuerung (7 Kontroll-Punkte)

Zugangssteuerung (7)

1. Zugangssteuerungsrichtlinie
2. Verwaltung von Zugriffsberechtigungen
3. Privilegierte und administrative Zugänge
4. Systeme und Anwendungen zur Systemadministration
5. Identifikation
6. Authentifikation
7. Multi-Faktor-Authentifikation

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.	Bewusstseins-schaffung und Cyberhygiene
b.	Cybersicherheitsschulungen
7.	Sicherheit von Lieferketten
a.	Richtlinie zur Sicherheit von Lieferketten
b.	Lieferantenverzeichnis
8.	Zugangssteuerung
a.	Zugangssteuerungsrichtlinie
b.	Verwaltung von Zugriffsberechtigungen
c.	Privilegierte und administrative Zugänge
d.	Systeme und Anwendungen zur Systemadministration
e.	Identifikation
f.	Authentifikation
g.	Multi-Faktor-Authentifikation
9.	Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
a.	Konfigurationsmanagement
b.	Änderungsmanagement und Wartung
c.	Umgang mit Schwachstellen und deren Offenlegung
d.	Sicherheitstests
e.	Patchmanagement
f.	Sicherheit bei der Beschaffung von Dienstleistungen, Systemen und Produkten
g.	Sichere Softwareentwicklung
h.	Netzwerksegmentierung
i.	Netzwerksicherheit
j.	Schutz vor bösartiger und unautorisierter Software
10.	Kryptographie
a.	Kryptographierichtlinie
11.	Umgang mit Cybersicherheitsvorfällen
a.	Richtlinie zum Umgang mit Cybersicherheitsvorfällen
b.	Überwachung und Protokollierung
c.	Meldung von Ereignissen
d.	Erhebung und Klassifikation von Ereignissen
e.	Reaktion auf Cybersicherheitsvorfälle
f.	Erkenntnisse nach Cybersicherheitsvorfällen

12.	Betriebskontinuitäts- und Krisenmanagement
a.	Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne
b.	Backup-, Redundanz- und Wiederherstellungsmanagement
c.	Krisenmanagement
13.	Umgebungsbezogene und physische Sicherheit
a.	Sicherheitsperimeter und physische Zutrittskontrollen
b.	Schutz vor umgebungsbezogenen Gefährdungen
c.	Versorgungseinrichtungen

NIS2 Gesetz

Anlage 3: Kontroll-Punkte

Wie arbeitet eine Prüfstelle nach NIS1

Risikomanagementmaßnahmen im Bereich der Cybersicherheit NISG §32 (TOO)

Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige, ein dem Risiko angemessenes Cybersicherheitsniveau (TOO) auf

1. technischer,
2. operativer und
3. organisatorischer

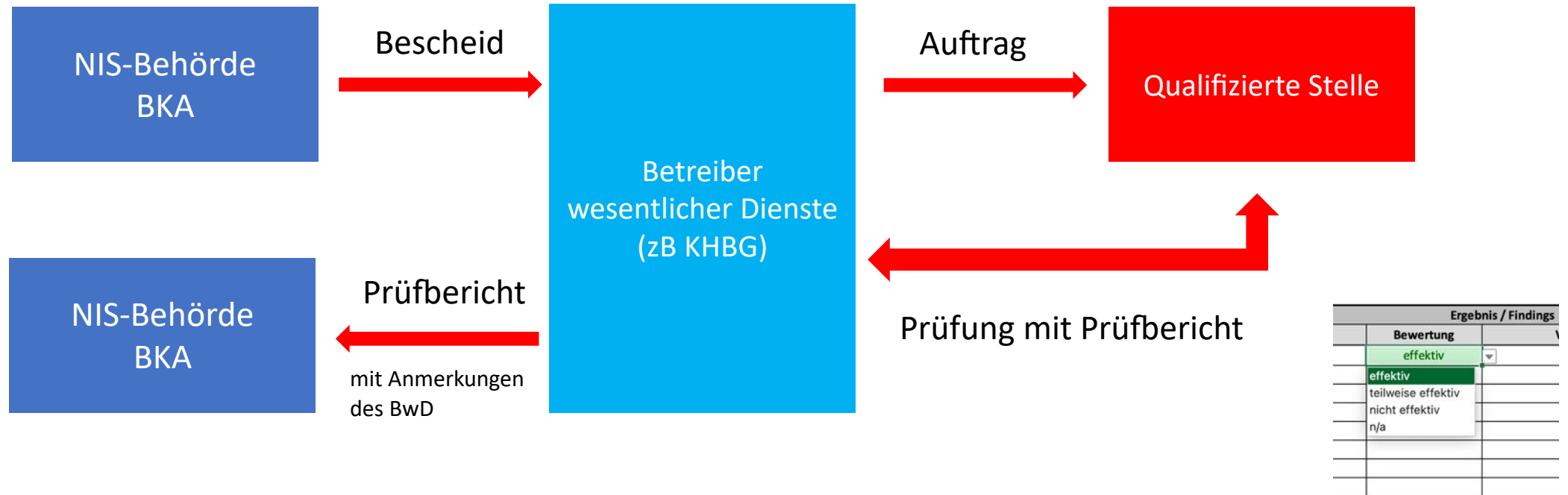
siehe Anlage 3, nach dem

1. Stands der Technik
2. Normen
3. Best-Practices sowie unter dem
4. Aspekt der Kosten

umzusetzen

Ablauf einer NIS1 Prüfung

Qualifizierte Stelle nach QuaSte VO



Hilf-Material Fact-Sheets

Qualifizierte Stellen

NIS Fact Sheet 7/2019 – Version 3

Inhalt

Inhalt.....	2
1 Einleitung.....	3
1.1 Rahmen.....	3
1.2 Anwendungsbereich.....	3
1.3 Zuständigkeit und Kommunikation.....	4
1.4 Arten der Überprüfung von Betreibern wesentlicher Dienste.....	5
2 Ablauf der Feststellung einer qualifizierten Stelle	7
2.1 Antragschreiben.....	7
2.2 Übermittlung der Nachweise.....	8
2.3 Prüfung der Nachweise und Erledigung mittels Bescheid.....	11
3 Prüfer.....	12
3.1 Prüfertypen.....	12
3.2 Bekanntgabe von Prüfern.....	16
3.3 Anforderungen an Prüfer.....	18
4 Jährlicher Statusbericht	21
4.1 Durchgeführte Überprüfungen.....	21
4.2 Weiterbildungsmaßnahmen.....	21
5 Exkurs Sicherheitsüberprüfungen	24
5.1 Überblick.....	24
5.2 Vorgehensweise bei Prüfern.....	25
6 Versionshistorie	27
Impressum.....	28

Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

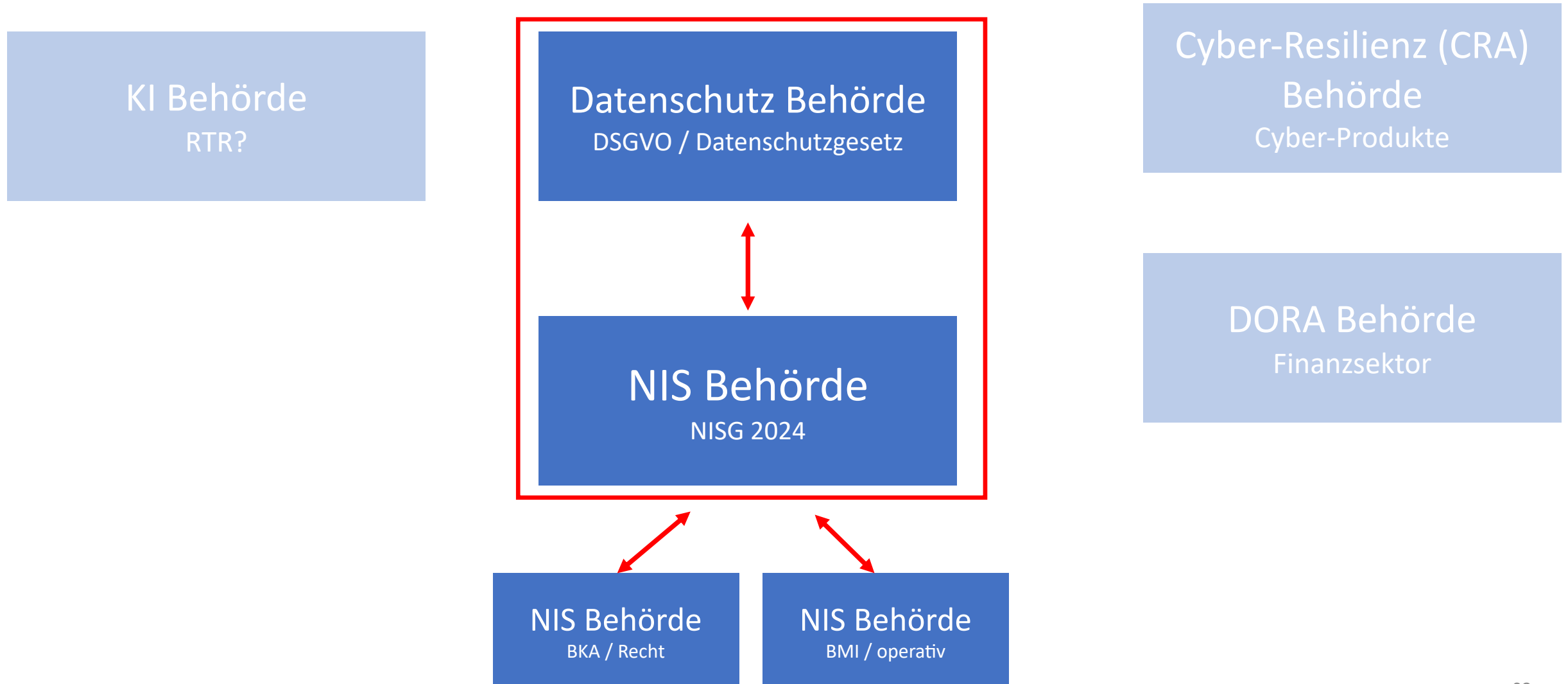
NIS Fact Sheet 9/2022

Inhalt

Inhalt.....	2
Einleitung	3
Hintergrund	3
Anwendbarkeit	3
NIS-Kooperationsgruppe	4
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
Versionshistorie	30
Impressum.....	31

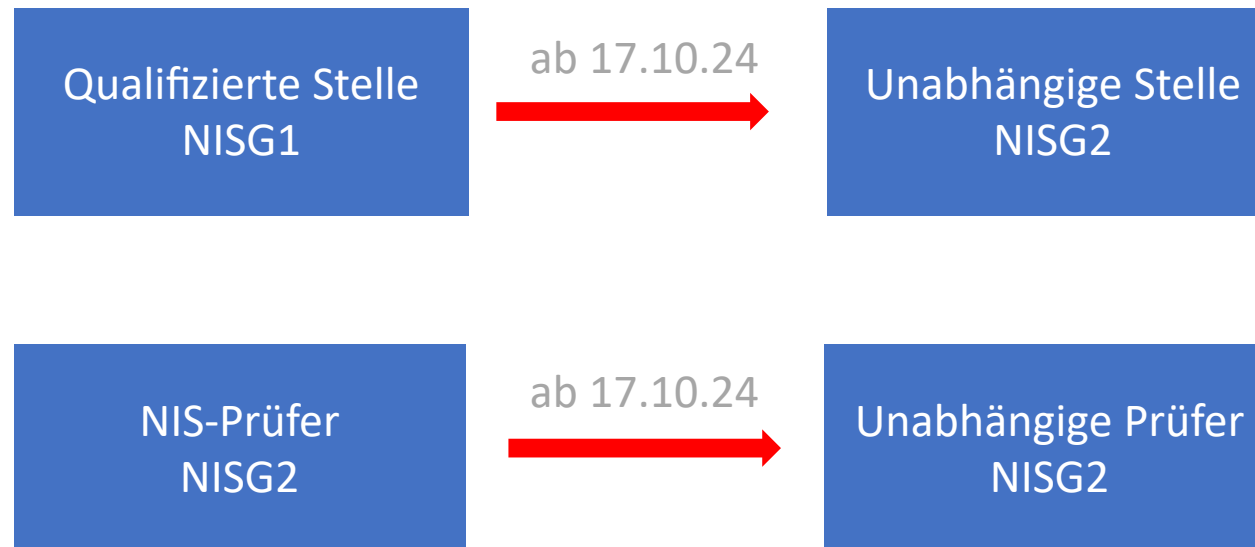
Informationen und Kontakte

Architektur der Gesetze und Cyber-Organisationen



NISG1 zu NISG2

im Bereich Prüfstellen und Prüfer



Wichtige Links

- Gesetzesentwurf NISG 2
 - Parlament: <https://www.parlament.gv.at/gegenstand/XXVII/ME/326>
 - RIS-BKA: <https://shorturl.at/hkvW3>
- NIS-Behörde
 - BKA (rechtlich): <https://shorturl.at/GPVW5>
 - BMI (operativ): <https://www.nis.gv.at/>
- Melde-Stellen
 - Datenschutzbehörde:
 - BM Inneres:
- Sonstiges
 - Fact-Sheets des BMI: <https://www.nis.gv.at/rechtliches-und-dokumente.html>
 - WKO: <https://ratgeber.wko.at/nis2/>

Kontakt

Strategische NIS-Behörde

Bundeskanzleramt

E-Mail: NIS@bka.gv.at

Operative NIS-Behörde

Bundesministerium für Inneres

E-Mail: post@nis.gv.at

S/MIME & PGP: securemail.bmi.gv.at

Telefon: +43 591 33-989480

BMI-Cryptshare: cryptshare.bmi.gv.at

Vorfallsmeldungen

- nis.govcert.gv.at: NISG Plattform für Meldungen aus der Öffentlichen Verwaltung
- nis.cert.at: NISG Plattform für Meldungen von Betreibern und Anbietern
- nis.energy-cert.at: NISG Plattform für Meldungen für Sektor Energie (AEC).

Zentrale

Millennium Tower,
Handelskai 94-96, Office 2319,
1200 Wien

office@ztp.digital
www.ztp.digital
+43 1 5324686

Niederlassung

J. Kinclgasse 1
2201 Gerasdorf
bei Wien

office@ztp.digital
www.ztp.digital
+43 1 5324686

Niederlassung

CAMPUS V .
Hintere Achmühlerstraße 1,
6850 Dornbirn

office@ztp.digital
www.ztp.digital
+43 1 5324686



Besten Dank
für die Zusammenarbeit!

Haben Sie noch Fragen?



Kunden

in Vorarlberg und darüber hinaus



Wolfgang Hartmann, Geschäftsleitung CFO beim Roten Kreuz Vorarlberg | Dr.tech Wolfgang Prentner, CEO bei ZTP.digital | Erwin Mangeng, Bereichsleiter IT beim Roten Kreuz Vorarlberg



Dr.tech Wolfgang Prentner, CEO bei ZTP.digital | Ing. Peter Sagmeister, MAS, IT-Manager bei VLKH



Mag. Raimund Wachter, CEO bei Vorarlberg Milch | Dr.tech Wolfgang Prentner, CEO bei ZTP.digital | Richard Schwaninger, EDV-Leiter bei Vorarlberg Milch



Dr.tech Wolfgang Prentner, CEO bei ZTP.digital | DI Andreas Huber MBA, Leitung Digitalisierung & IT bei Doppelmayr Seilbahnen

Österreichweite Kunden



Raiffeisen Software GmbH



REWE Group



CYBERDOC GmbH & Co KG



Voest Alpine



Vorarlberger Krankenhausbetriebsges.mbH



Wiener Linien GmbH & Co KG