NIS2 Umsetzung/NISG2024

Was muss gemeldet werden, welche Risikomanagementmaßnahmen müssen getroffen werden?

Mag. Gernot Goluch
Bundesministerium für Inneres, Gruppe IV/NCSZ – Nationales Cybersicherheitszentrum
Bereich – Aufsicht und Durchsetzung

St. Pölten, 29. Mai 2024

Agenda / Themen

- Aktueller Stand NIS2 Umsetzung/NISG2024
- NIS2 Meldungen
- NIS2 Risikomanagementmaßnahmen und „Prüfregime“

Aktueller Stand NIS2 Umsetzung/NISG2024

NIS 2 in a nutshell 1/3

- Bis 17. Oktober 2024 in nationales Recht umzusetzen
- Anwendungsbereich durch Größenschwellenwert („**size cap rule**“) bestimmt **Mittlere** und **große** Einrichtungen / Kleine nur in bestimmten Ausnahmefällen **Öffentliche** oder **private** Einrichtungen

Fähigkeiten der Mitgliedstaaten	Kooperation und Informationsaustausch	Risikomanagement
Nationale Behörden	NIS-Kooperationsgruppe Peer-Review	Verantwortlichkeit des Top-Managements
Computer-Notfallteams (CERTs/CSIRTs)	CSIRTs-Netzwerk	Schulungen für Top-Management
Cyber-Krisenmanagement	EU-Cyberkrisennetzwerk (CyCLONe)	Unterscheidung wesentliche und wichtige Einrichtungen
Nationale Strategien	ENISA Cybersecurity Reports	Risikomanagementmaßnahmen
Rahmen für CVD (Coordinated Vulnerability Disclosure)	Europäisches Schwachstellenregister	Berichtspflichten

NIS 2 in a nutshell 2/3

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
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 soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

NIS 2 in a nutshell 3/3

- **Aufsichtsmaßnahmen und Befugnissen** (bspw. regelmäßige & gezielte Audits, Vor-Ort- & Off-Site-Kontrollen, Sicherheitsscans, Ersuchen um Informationen & Zugang etc.)
  - Vollwertige Aufsicht (**ex ante & ex post**) für wesentliche Einrichtungen
  - Abgeschwächte Aufsicht (**ex post**) für wichtige Einrichtungen

- **Verwaltungssanktionen und Durchsetzungsmaßnahmen** (z. B. verbindliche Anweisungen, Verwaltungsstrafen, Veröffentlichung von Verstößen, Überwachungsbeauftragter etc.)
- Maximale **Bußgeldhöhe**:
  - mind. 10.000.000 EUR oder 2% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres für wesentliche Einrichtungen
  - mind. 7.000.000 EUR oder 1,4% für wichtige Einrichtungen
- Natürliche Personen (leitende Angestellte) können für Pflichtverletzungen haftbar gemacht werden

NISG2024 – aktueller Stand

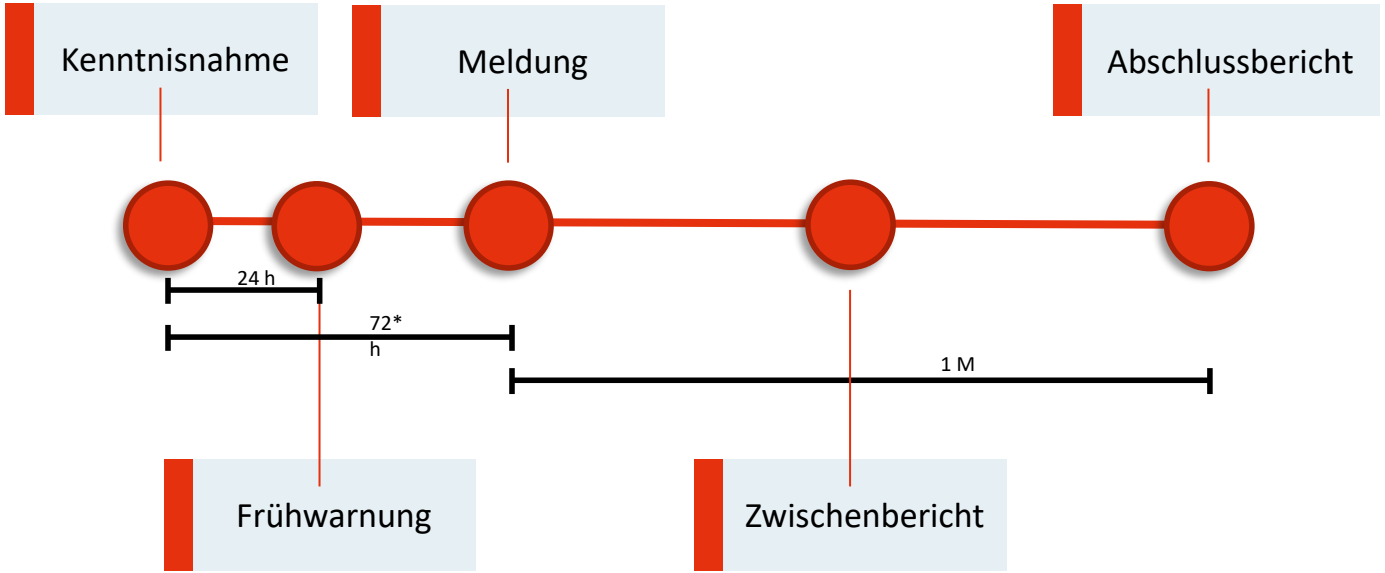
- **Begutachtung** für NISG2024 ist erfolgt
  - vgl. https://www.parlament.gv.at/gegenstand/XXVII/ME/326
- **BMI** wird alleinige **NIS Behörde** (strategische Agenden wandern von BKA zu BMI)
- Neben bereits laufender Abstimmungen und Kommunikation (CSP, KSÖ…) werden bereits **breitflächigere Abstimmungen und Einbindungen** unterschiedlicher Stakeholder durchgeführt, insb. Länder & Wirtschaft (WKÖ, IV, IOÖ etc.) via CSP (PPP Platform im BKA)
- **Öffentliche Verwaltung**: BMI, BMLV, BMJ sowie Gemeinden (regionale Ebene gem. NIS2-RL optional) gem aktuellen Entwurf nicht im Anwendungsbereich
- **Strafbehörden** gem. aktuellen Entwurf: BVBs
- Aktuelle Erhebungen (resultierend aus Kooperation mit Statistik Austria) deuten auf **zumindest 3000 Normunterworfene Einrichtungen** in Österreich hin

NIS2 Meldungen

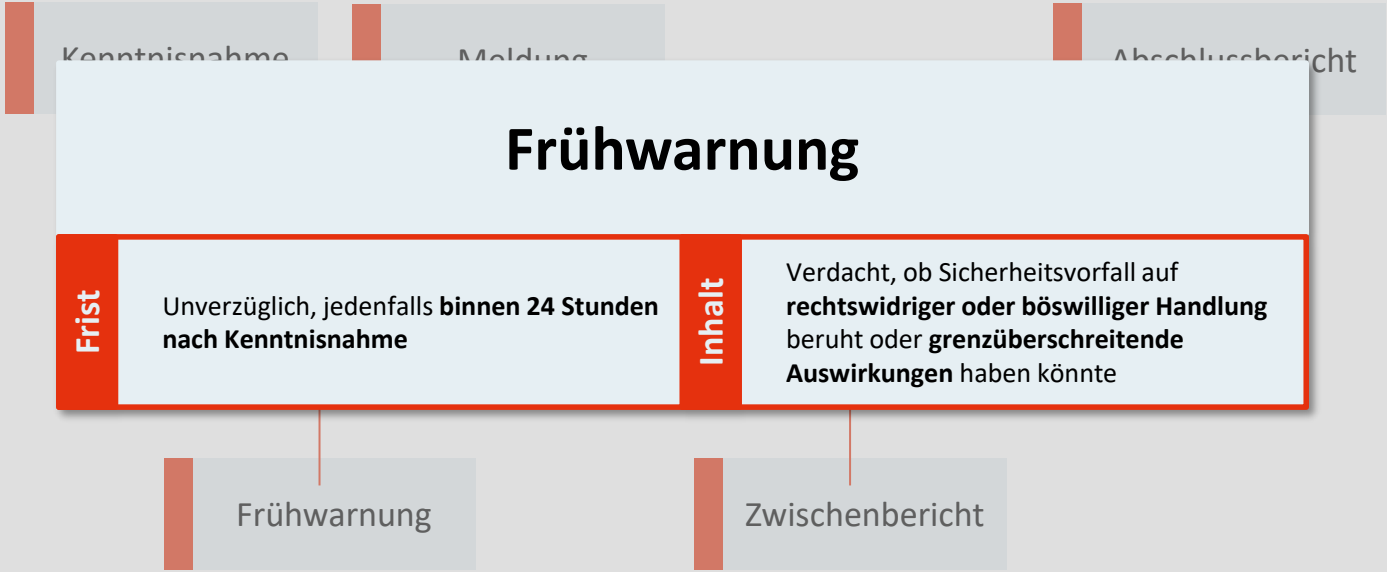
Pflicht- vs. Freiwillige Meldung

<table>
<tr><th></th><th>Wesentliche Einrichtungen</th><th>Wichtige Einrichtungen</th><th>Einrichtungen außerhalb des AWB</th></tr>
<tr><td>Erheblicher Sicherheitsvorfall
Art 23 Abs 3</td><td colspan="2">Pflichtmeldung</td><td rowspan="4">Freiwillige Meldung</td></tr>
<tr><td>Beinahe-Vorfall
Art 6 Z 5</td><td colspan="2" rowspan="3"></td></tr>
<tr><td>Cyberbedrohung
Art 6 Z 10</td></tr>
<tr><td>Sicherheitsvorfall
Art 6 Z 6</td></tr>
</table>

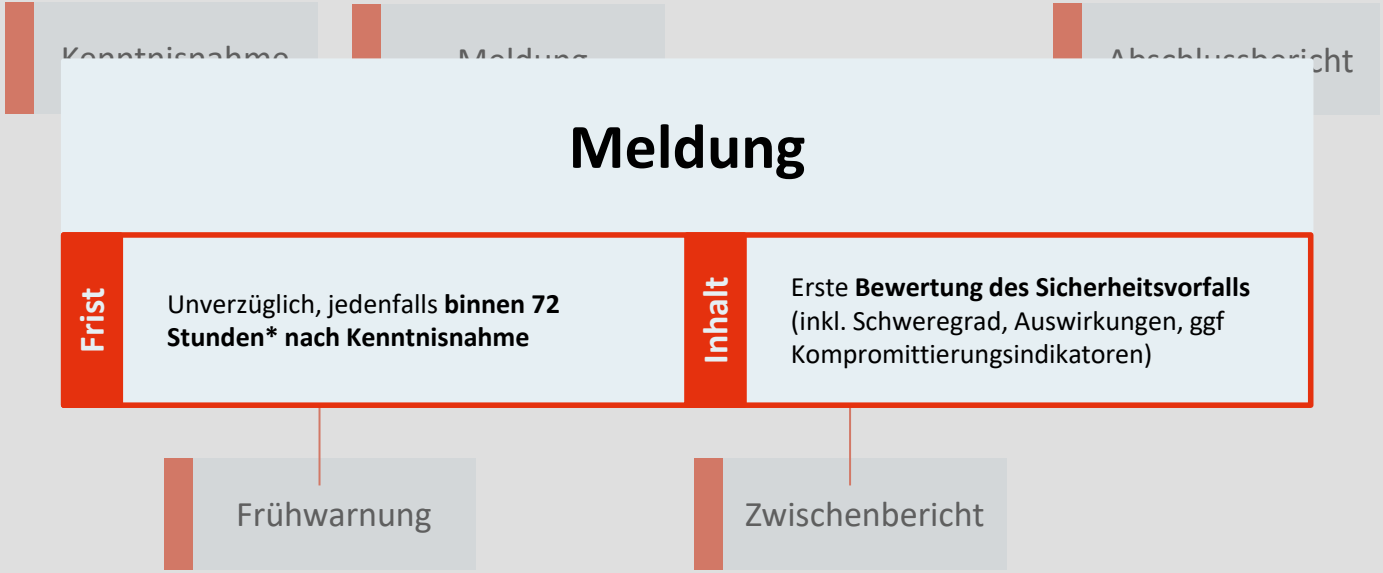
Meldevorgang



Meldevorgang



Meldevorgang



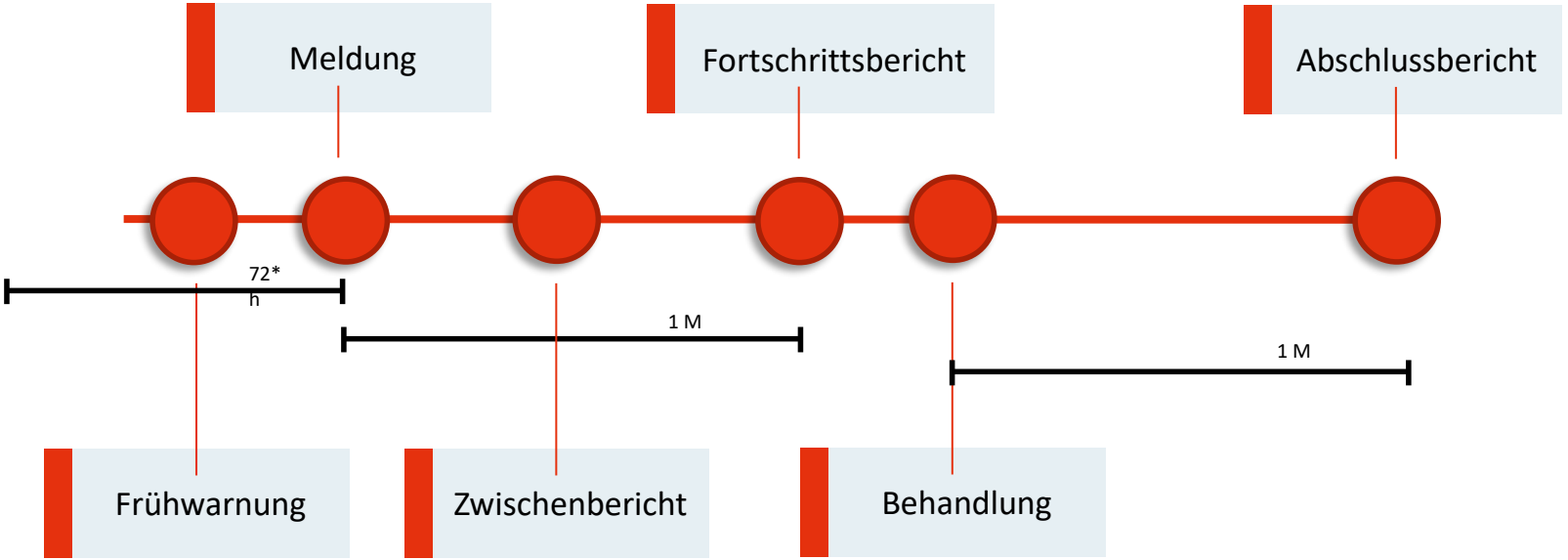
*** Vertrauensdiensteanbieter**

binnen **24** Stunden nach Kenntnisnahme

Meldevorgang

Meldevorgang

Sonderfall: andauernder Sicherheitsvorfall



NIS2 Risikomanagementmaßnahmen und „Prüfregime“

NIS2-RL Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

NIS2-RL Artikel 21

(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.

Problematiken:

- Rechtssicherheit
- Wirksamkeit
- Interpretationsspielräume

Aktueller Stand Anlage 3 Risikomanagementmaßnahmen-Bereiche

- Rollen und Verantwortlichkeiten der Leitungsorgane
- Sicherheitsrichtlinien
- Funktionen, Aufgaben und Verantwortlichkeiten
- Risikomanagementrichtlinie und –prozess
- Beurteilung der Effektivität von Risikomanagementmaßnahmen
- Überwachung der Einhaltung von Vorgaben
- Unabhängige Überprüfungen
- Klassifikation von Vermögenswerten
- Handhabung von Vermögenswerten
- Umgang mit Wechseldatenträgern
- Inventarisierung von Vermögenswerten
- Rücknahme oder Löschung von Vermögenswerten

Aktueller Stand Anlage 3 Risikomanagementmaßnahmen-Bereiche

- Sicherheit im Personalwesen
- Hintergrundüberprüfung
- Verfahren bei Beendigung oder Wechsel eines Beschäftigungsverhältnisses
- Umgang mit Verstößen gegen die Sicherheitsrichtlinie
- Vermittlung von Cybersicherheitskompetenzen
- Cybersicherheitsschulungen
- Richtlinie zur Sicherheit von Lieferketten
- Lieferantenverzeichnis
- Zugangssteuerungsrichtlinie
- Verwaltung von Zugriffsberechtigungen
- Privilegierte und administrative Zugänge
- Systeme und Anwendungen zur Systemadministration
- Identifikation
- Authentifikation
- Multi-Faktor-Authentifikation

Aktueller Stand Anlage 3 Risikomanagementmaßnahmen-Bereiche

- Konfigurationsmanagement
- Änderungsmanagement
- Umgang mit Schwachstellen und deren Offenlegung
- Sicherheitstests
- Patchmanagement
- Sicherheit bei der Beschaffung von IKT-Diensten und IKT-Produkten
- Sichere Softwareentwicklung
- Netzwerksicherheit
- Netzwerksegmentierung
- Schutz vor bösartiger und unautorisierter Software
- Kryptographierichtlinie
- Richtlinie zum Umgang mit Cybersicherheitsvorfällen
- Überwachung und Protokollierung
- Meldung von Ereignissen
- Korrelation und Analyse von Ereignissen
- Reaktion auf Cybersicherheitsvorfälle
- Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne
- Backup-, Redundanz- und Wiederherstellungsmanagement
- Krisenmanagement

Weitere Risikomanagementmaßnahmen

- Werden im Rahmen von CSP Arbeitsgruppen diskutiert
  - Beitritt möglich nach E-Mail Registrierung unter csp@bka.gv.at
  - 2 CSP-Termine betreffend der Risikomanagementmaßnahmen-VO finden noch statt
  - Nächster CSP-Termin ist der 03.06.2024

Problematik „Skalierung aktuelles Prüfregime“

- Aktuelles NISG/QuaSteV Prüfregime für ca. 100 BwD wird nicht auf NIS 2 Anwendungsbereich skalieren für:
  - **Wesentliche** Einrichtungen **Ex-Ante** Aufsicht (Art. 32 Abs. 2 Lit b NIS2-RL):

> regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

  - **Wichtige** Einrichtungen **Ex-Post** Aufsicht (Art. 33 Abs. 2 Lit b NIS2-RL):

> gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

  - sowohl bzgl. Aufwände bei Einrichtungen, Unabhängigen Stellen / Prüfer und Behörde nicht

Artikel 31 NIS2-RL:
Allgemeine Aspekte der Aufsicht und Durchsetzung

(2) Die Mitgliedstaaten können ihren zuständigen Behörden gestatten, Aufsichtsaufgaben zu priorisieren. Diese Priorisierung beruht auf einem risikobasierten Ansatz. Zu diesem Zweck können die zuständigen Behörden bei der Wahrnehmung ihrer in den Artikeln 32 und 33 aufgeführten Aufsichtsaufgaben Aufsichtsmethoden festlegen, die eine Priorisierung dieser Aufgaben auf der Grundlage eines risikobasierten Ansatzes ermöglichen.

- Priorisierungsmöglichkeiten /-werkzeuge
  - Nutzung einer Form von Selbstassessment als Basis (**Selbstdeklaration**)
  - **Prüfungen** durch unabhängige **Stellen** / unabhängige **Prüfer**
  - Nutzung (stark erweiterter) **Aufsichts- und Durchsetzungsmaßnahmen** seitens **Behörde**

Danke für Ihre Aufmerksamkeit!

BMI, Gruppe IV/NCSZ – Nationales Cybersicherheitszentrum
Bereich – Aufsicht und Durchsetzung
St. Pölten, 29.05.2024