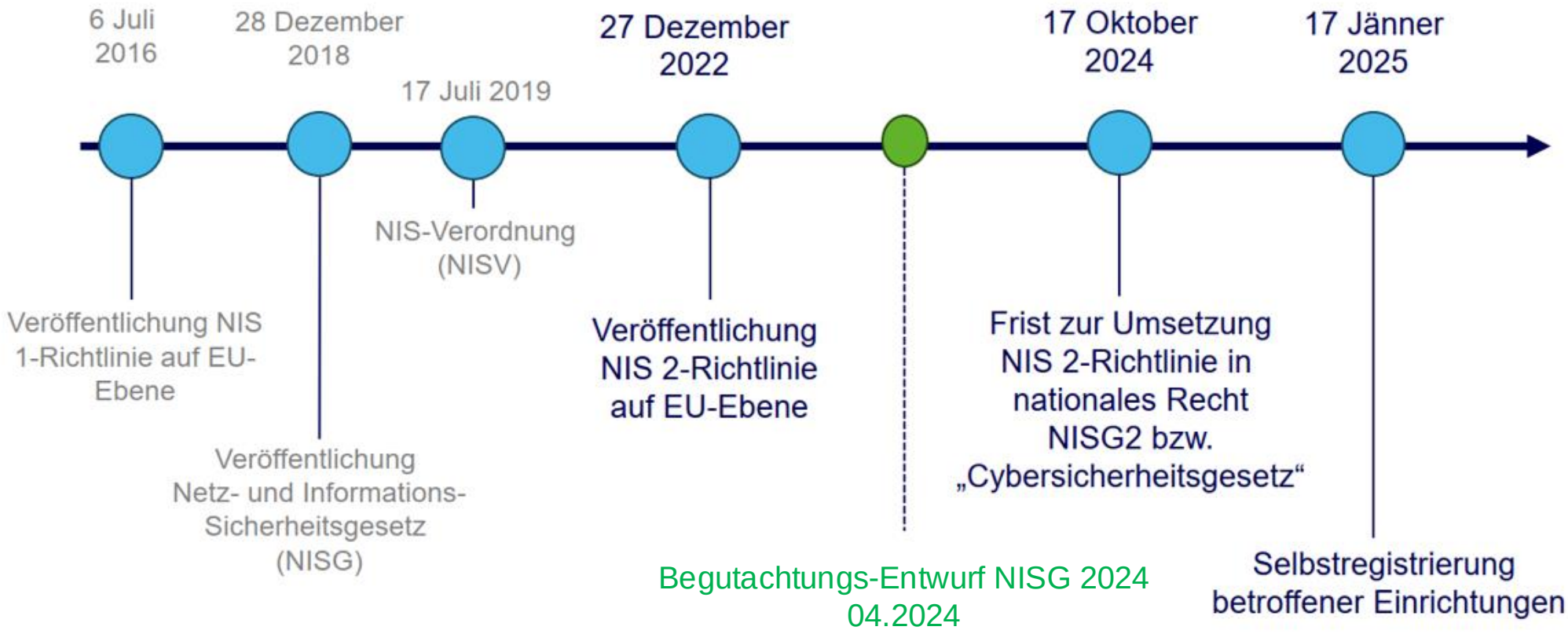
NIS 2

Grundsatzinformationen und Betroffenheit der öffentlichen Verwaltung

ADV eGovernment-Konferenz 2024
20.6.2024 Linz

Stadt
Wien

Zeitleiste NIS1 – NIS2 (NISG 2024) - Entwicklung und Ausblick



Stadt Wien

Wesentliche Änderungen zu NIS-1 (Auswahl)

Keine bescheidmäßige Ermittlung mehr

⇨Alle Firmen des Sektors fallen in den Anwendungsbereich (Ausnahme: Kleinst- und Kleinunternehmen)

Wegfall des Fokus auf den „wesentlicher Dienst“

⇨Gesamte IT/OT fällt in den Anwendungsbereich

Vereinheitlichung der minimalen Maximalstrafhöhen

⇨10 Mio EUR bzw. 2 % des weltweiten Jahresumsatzes

Zusätzliche (Teil-)Sektoren

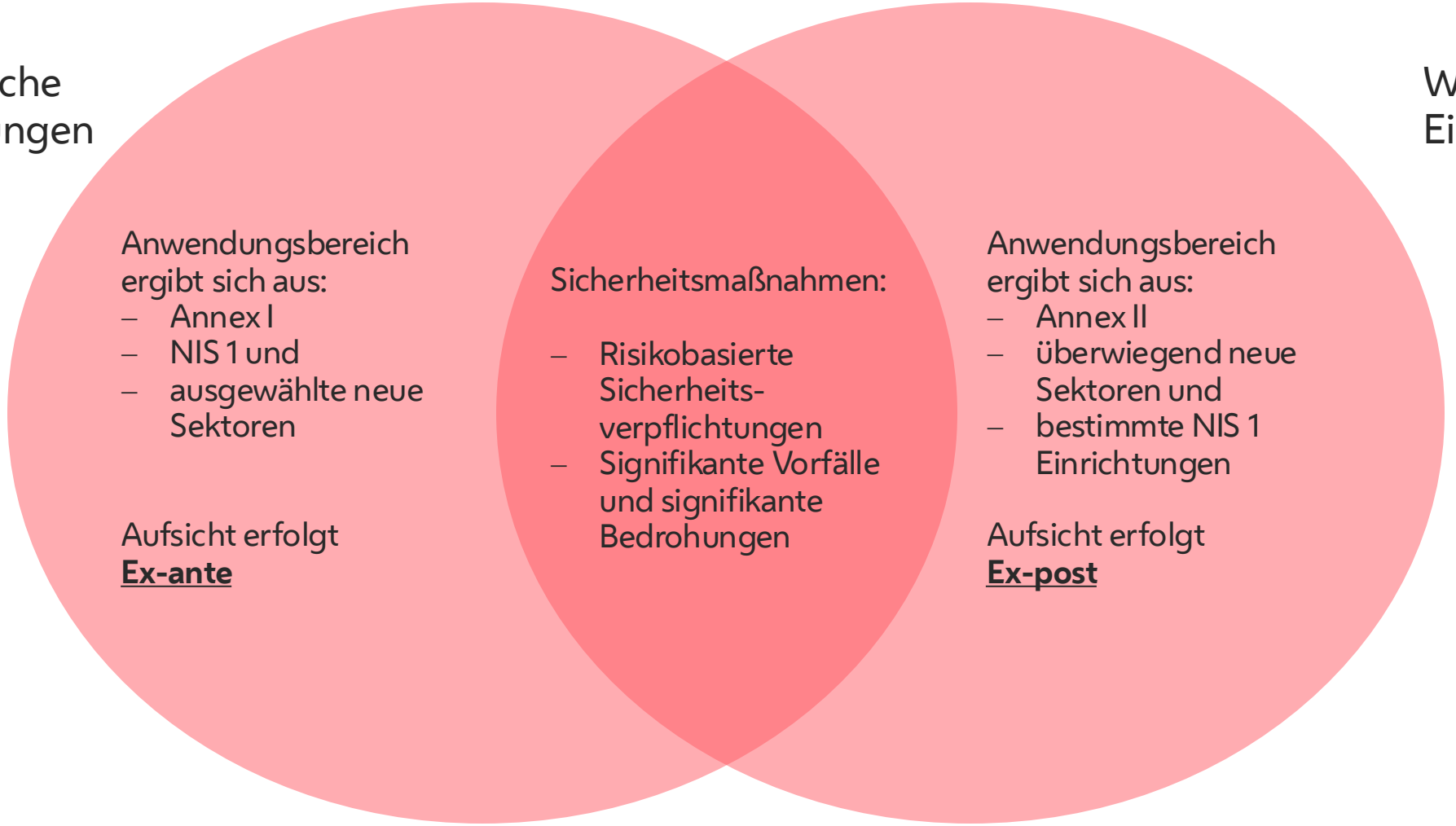
⇨z.B. Fernwärme/-kälte, Rechenzentren, öff. Verwaltung bis Länderebene (NUTS2)

Verstärkung der Management-Verantwortung

⇨Geschäftsführerhaftung

⇨Verpflichtende Fortbildungen für Management

Wesentliche Einrichtungen und wichtige Einrichtungen



Berichtspflichten

Unternehmen müssen erhebliche Sicherheitsvorfälle unverzüglich an das Computer-Notfallteam (CERT/CSIRT) melden

Frühwarnung

Frist: Unverzüglich bis max. 24 Stunden nach Kenntnisnahme	**Inhalt:** Verdacht, ob Sicherheitsvorfall auf rechtswidriger oder böswilliger Handlung beruht und ob grenzüberschreitend.

Meldung

Frist: Unverzüglich bis max. 72 Stunden nach Kenntnisnahme	**Inhalt:** Erste Bewertung des Sicherheitsvorfalls (inkl. Schweregrad, Auswirkungen, ggf Kompromittierungsindikatoren)

Abschlussmeldung

Frist: 1 Monat nach Meldung	**Inhalt:** Ausführliche Beschreibung, Angaben zur Art der Bedrohung, Ursachen, Abhilfemaßnahmen

Aufsicht durch Behörde

Aufsichtsmaßnahmen und Befugnisse

- Mindestliste an Aufsichtsmaßnahmen (regelmäßige & gezielte Audits, Vor-Ort- &, Sicherheitsscans) und Mittel, die den zuständigen Behörden zur Verfügung stehen (Ersuchen um Informationen & Zugang zu Beweismitteln).

2 Aufsichtssysteme (!)

- Vollwertige Aufsicht (**ex ante & ex post**) für wesentliche Einrichtungen
- Abgeschwächte Aufsicht (**ex post**) für wichtige Einrichtungen

Durchsetzung

Mindestliste von **Verwaltungssanktionen** (z. B. verbindliche Anweisungen, Verwaltungsstrafen)

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

Bei der **Messung der Strafe** werden unter anderem folgende Kriterien beachtet:

- Art, Schwere und Dauer des Verstoßes
- Verstöße mit Verletzungen des Schutzes personenbezogener Daten
- Alle getroffenen Sicherheitsmaßnahmen nach dem Stand der Technik
- Durchgeführte Prüfungen und Dokumentation der Sicherheitsmaßnahmen
- Nachgekommene Meldepflicht
- Nachweis von allfälligen Zertifizierungen
- Durchgeführte Prüfung durch eine qualifizierte Stelle

Grundregel Anwendungsbereich Anhang I u II

Sektoren	Große Unternehmen	Mittlere Unternehmen	Klein-unternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktinfrastrukturen / Gesundheitswesen / Trinkwasser / Abwasser / Verwaltung von IKT-Diensten / Öffentliche Verwaltung/ Weltraum	wesentlich	wichtig	
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / Verarbeitendes Gewerbes bzw. Herstellung von Waren / Anbieter digitaler Dienste / Forschung	wichtig	wichtig	

Wesentliche und wichtige Einrichtungen in den Sektoren

1. Energie,
2. Verkehr,
3. Bankwesen,
4. Finanzmarktinfrastrukturen,
5. Gesundheitswesen,
6. Trinkwasser,
7. Abwasser,
8. Digitale Infrastruktur,
9. Verwaltung von IKT-Diensten (Business-to-Business),
10. öffentliche Verwaltung,
11. Weltraum,
12. Post- und Kurierdienste,
13. Abfallbewirtschaftung,
14. Produktion, Herstellung und Handel mit chemischen Stoffen,
15. Produktion, Verarbeitung und Vertrieb von Lebensmitteln,
16. Verarbeitendes Gewerbe/Herstellung von Waren,
17. Anbieter digitaler Dienste,
18. Forschung,

Betroffene Einrichtungen im Magistrat?

1. Energie,
2. **Verkehr,**
3. Bankwesen,
4. Finanzmarktinfrastrukturen,
5. **Gesundheitswesen,**
6. **Trinkwasser,**
7. **Abwasser,**
8. Digitale Infrastruktur,
9. Verwaltung von IKT-Diensten (Business-to-Business),
10. **öffentliche Verwaltung,**
11. Weltraum,
12. Post- und Kurierdienste,
13. **Abfallbewirtschaftung,**
14. Produktion, Herstellung und Handel mit chemischen Stoffen,
15. Produktion, Verarbeitung und Vertrieb von Lebensmitteln,
16. Verarbeitendes Gewerbe/Herstellung von Waren,
17. Anbieter digitaler Dienste,
18. Forschung,

§ 32 Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige **technische**, **operative** und **organisatorische Risikomanagementmaßnahmen** in den Bereichen der **Anlage 3** umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

(4) Der Bundesminister für Inneres **hat mit Verordnung Risikomanagementmaßnahmen** in den Bereichen der Anlage 3 hinsichtlich technischer, operativer und organisatorischer Anforderungen festzulegen. Ferner kann der Bundesminister für Inneres sektorspezifische Anforderungen an diese Risikomanagementmaßnahmen mit Verordnung festlegen.

Die Risikomanagement-Bereiche der Anlage 3 im Überblick

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

Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024)

- Erster nationaler Gesetzesentwurf wurde im November 2023 ausgesendet
- Mehrere **Verhandlungsrunden** zwischen Vertreter*innen des BMI und BKA mit Vertreter*innen der Länder (→ mehrere Überarbeitungen des Entwurfs)
- Begutachtungs-Entwurf wurde schließlich mit 4. April 2024 zur Stellungnahme übermittelt

Was ist neu ?

- Von funktionalem (NIS1) zu organisationalem (NIS2) Ansatz - viel breiterer Anwendungsumfang, Haftung der Leitungsorgane, sehr hohe Strafen, Lieferkettensicherheit…..

- Neu für Wien: Abwasser, Abfall, insb **Öffentliche Verwaltung** – auf Landesebene

- → Verhandlungen Bund / Länder mit folgenden Ergebnissen

Ergebnisse der Verhandlungsrunden (1)

- § 1 **(Verfassungsbestimmung)**

  (3) Bundesgesetze, mit denen §§ 17, 24 Abs. 2 Z 2, Abs. 3 und 5, § 44 Abs. 1, § 45 Abs. 5 und § 46 geändert werden, sofern sie sich jeweils auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, beziehen, dürfen nur mit Zustimmung der Länder kundgemacht werden.

  → **Abänderungen** der Bestimmungen über Wesentliche und wichtige Einrichtungen; Bestimmung über die Einschränkung der Betroffenheit der öffentlichen Verwaltung auf die Einrichtungen der Regionalverwaltung (=Landesverwaltung), Strafbestimmungen **bedürfen der Mitwirkung der Länder**

Ergebnisse der Verhandlungsrunden (2)

- **§ 24 Wesentliche und wichtige Einrichtungen**

  (1) Als **wesentliche Einrichtungen** gelten,

  …

  3. Einrichtungen der in **Anlage 1 dieses Gesetzes** genannten Art, die ein großes Unternehmen gemäß § 25 Abs. 2 betreiben. → **Anlage 1: Definition der Sektoren**

  (2) Als **wichtige Einrichtung** gelten,

  …

  2. Einrichtungen im **Sektor der öffentlichen Verwaltung auf Landesebene** gemäß Abs. 5

  (5) Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene sind die **Ämter der Landesregierungen** und die **Bezirkshauptmannschaften** sowie Einrichtungen gemäß Abs. 3, die zudem **zur Besorgung von Angelegenheiten der Landesverwaltung** berufen sind und Rechtspersönlichkeit besitzen.

Ergebnisse der Verhandlungsrunden (3)

- **§ 44. Strafbestimmungen**

  (1) Den **Bezirksverwaltungsbehörden obliegt die Verhängung von Verwaltungsstrafen** gemäß § 45. Der Bundesminister für Inneres hat der zuständigen Bezirksverwaltungsbehörde den Verdacht einer Verwaltungsübertretung gemäß § 45 Abs. 1 oder 4 anzuzeigen. Die Bezirksverwaltungsbehörde hat dem Bundesminister für Inneres einen jährlichen Bericht über eingeleitete Verwaltungsstrafverfahren sowie die Gründe für die Nichteinleitung oder Einstellung von Verwaltungsstrafverfahren nach standardisierten Vorgaben bis zum 31. März des Folgejahres zu übermitteln.

Ergebnisse der Verhandlungsrunden (4)

- **§ 45 Verwaltungsstrafbestimmungen**

  (5) Auf **Behörden, Organe sowie Einrichtungen** und sonstige Stellen der öffentlichen Verwaltung, **unabhängig** davon, **ob sie hoheitlich oder im Rahmen der Privatwirtschaftsverwaltung eingerichtet** oder tätig sind, findet diese Bestimmung **keine Anwendung**.

Umsetzungsschritte – Abwicklung als Programm

Magistratsweites Programm wurde aufgesetzt

(Vorbereitende) Schritte der Dienststellen für NISG 2024

1. Klärung der Betroffenheit
   im Hinblick auf § 24 Abs. 2 und 5 NISG 2024 (→ wer sind die Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene bzw. wer nimmt Aufgaben der Landesverwaltung wahr?)

2. Businesskritische Services im NISG-Kontext festhalten (→ BIA!)

3. Verantwortlichkeiten wahrnehmen (→ Umsetzung der Risikomanagementmaßnahmen gem. § 32 NISG 2024)

D.I.in Sandra Heissenberger, MBA
Gruppenleiter-Stellvertreterin

Magistratsdirektion der Stadt Wien
Geschäftsbereich Organisation und Sicherheit
Gruppe Prozessmanagement und IKT-Strategie
Rathausstraße 8, 1010 Wien
Mailto: Sandra.Heissenberger@wien.gv.at
Tel.: +43 1 4000 75038
Fax: +43 1 4000 99 75038
Mobil: +43 676 8118 75038