NIS umsetzen

Wie kann Zertifizierung helfen?

Mag. Vinzenz Heußler, LL.M.
Bundeskanzleramt, Abteilung I/8
OCG, 5. Dezember 2019

Inhalt

- Überblick NIS-Regelungssystematik (NISG, NISV, QuaSteV)
- Generelle Vorgaben und Sektorenspezifika
- Anforderungen für Anbieter digitaler Dienste
- Rolle der Zertifizierung

Zentrale Akteure des NISG

- Adressaten
  - Anbieter digitaler Dienste
  - Betreiber wesentlicher Dienste
  - Einrichtungen der öffentlichen Verwaltung
- Vollzugsbehörden („NIS-Behörden“)
  - Bundeskanzler (strategisch)
  - Bundesminister für Inneres (operativ)
- Computer-Notfallteams
- Qualifizierte Stellen

Zentrale Pflichten aus dem NISG

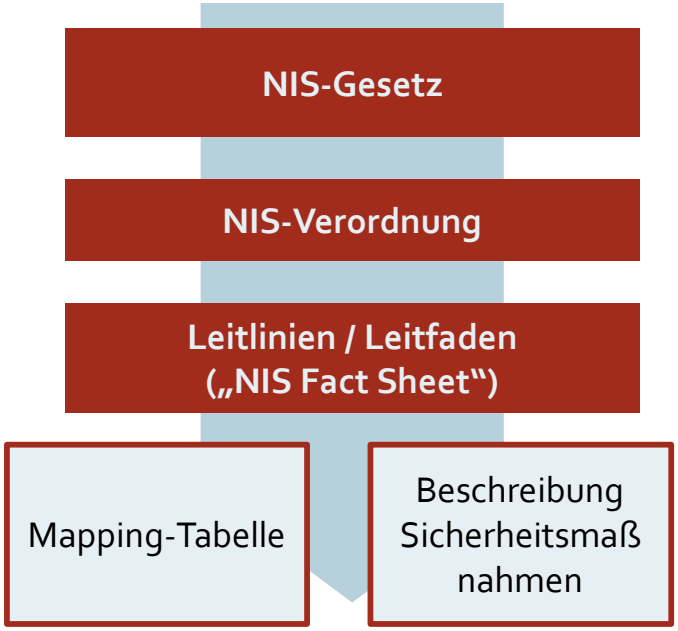
Meldepflicht bei Sicherheitsvorfällen

Implementierung von Sicherheitsvorkehrungen

Regulierungssystematik der Sicherheitsvorkehrungen - Generelle Vorgaben und Sektorenspezifika

Sicherheitsvorkehrungen

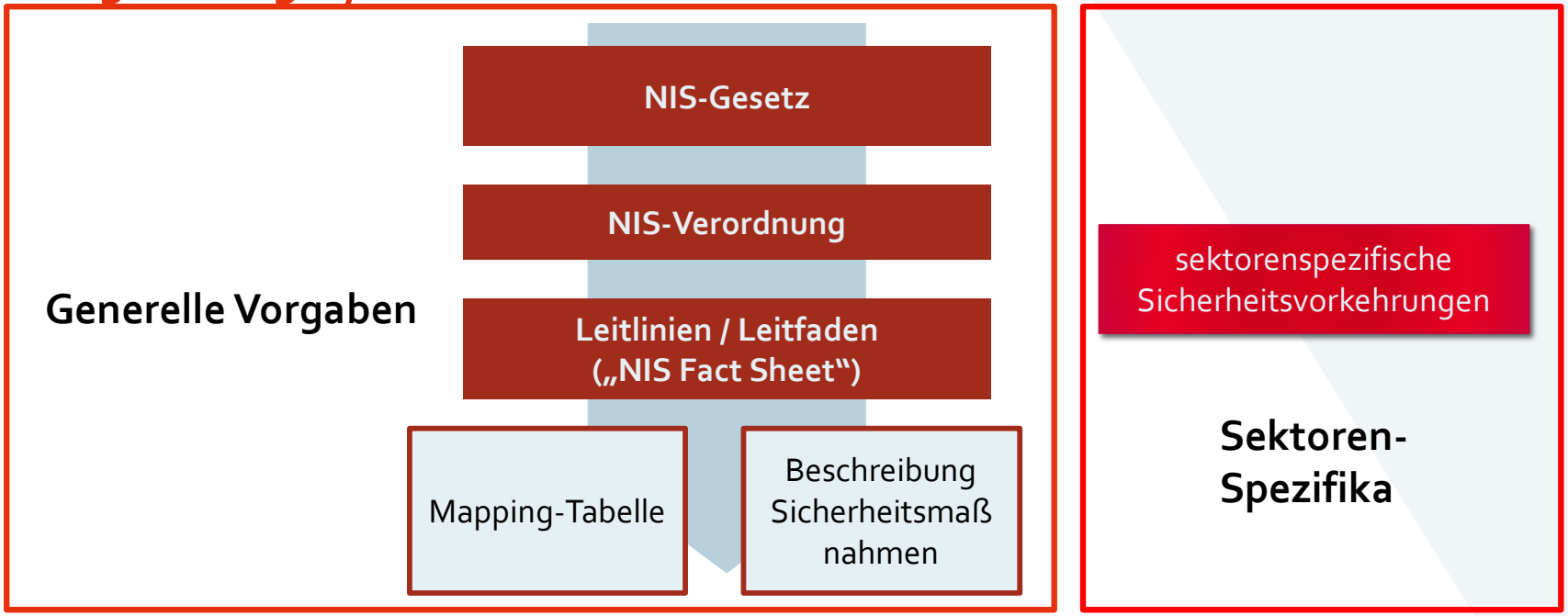
Regulierungssystematik I



sektorenspezifische Sicherheitsvorkehrungen

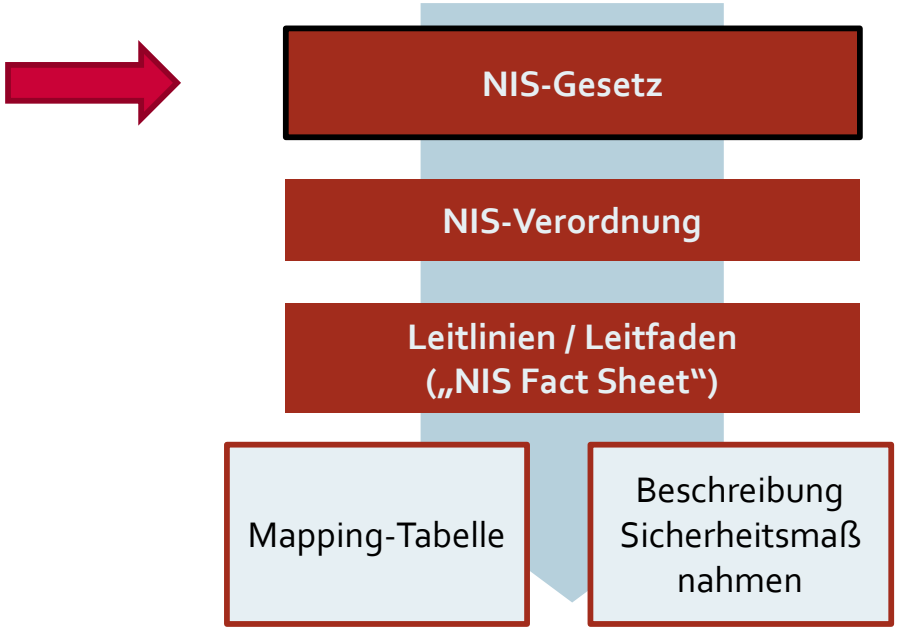
Sicherheitsvorkehrungen

Regulierungssystematik II



Sicherheitsvorkehrungen

Regulierungssystematik III



sektorenspezifische Sicherheitsvorkehrungen

Sicherheitsvorkehrungen

Regulierungssystematik IV

- **§ 17.** (1) NISG
  - Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

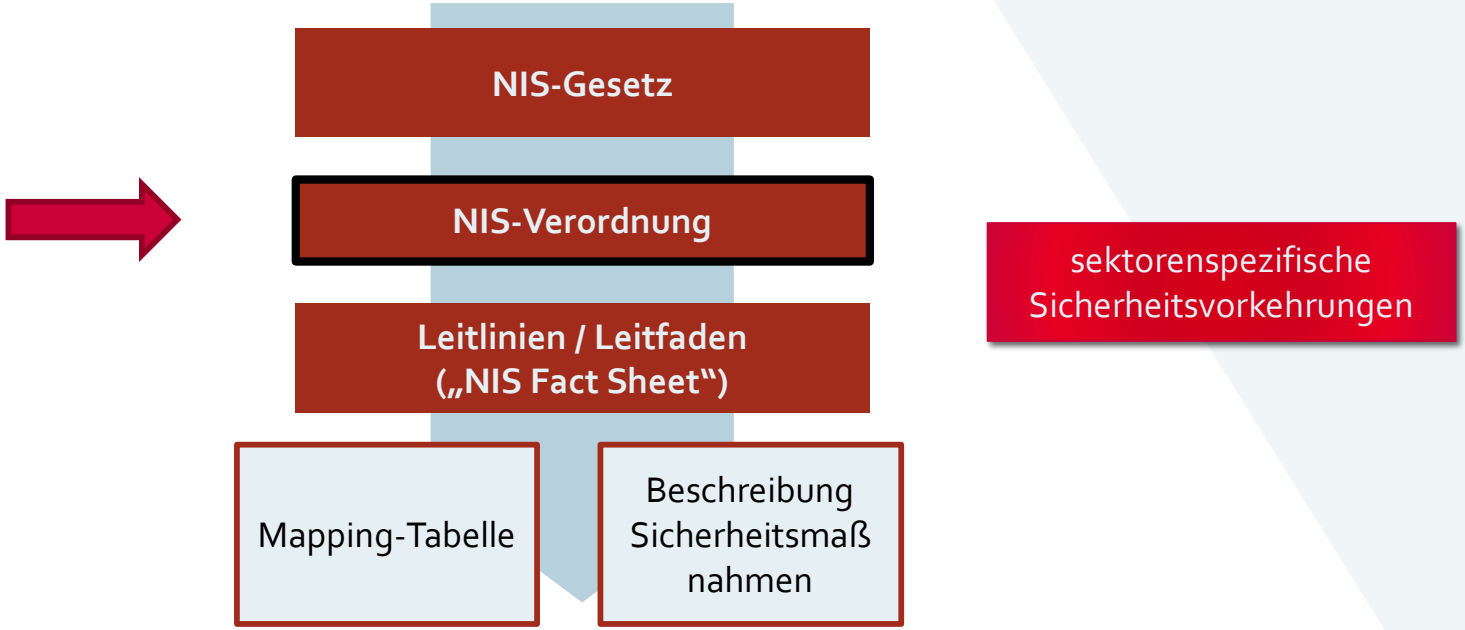
Sicherheitsvorkehrungen

Regulierungssystematik V

- **§ 17.** (1) NISG
  - Zweck: Gewährleistung der Netz- und Informationssystemsicherheit
  - Gegenstand: Netz- und Informationssysteme
    - die für die Bereitstellung des wesentlichen Dienstes genutzt werden
  - Anforderungen an Sicherheitsvorkehrungen
    - geeignet & verhältnismäßig
    - technischer & organisatorischer Natur
    - berücksichtigen Stand der Technik
    - angemessen zu Risiko, das mit vernünftigem Aufwand feststellbar ist

Sicherheitsvorkehrungen

Regulierungssystematik VI



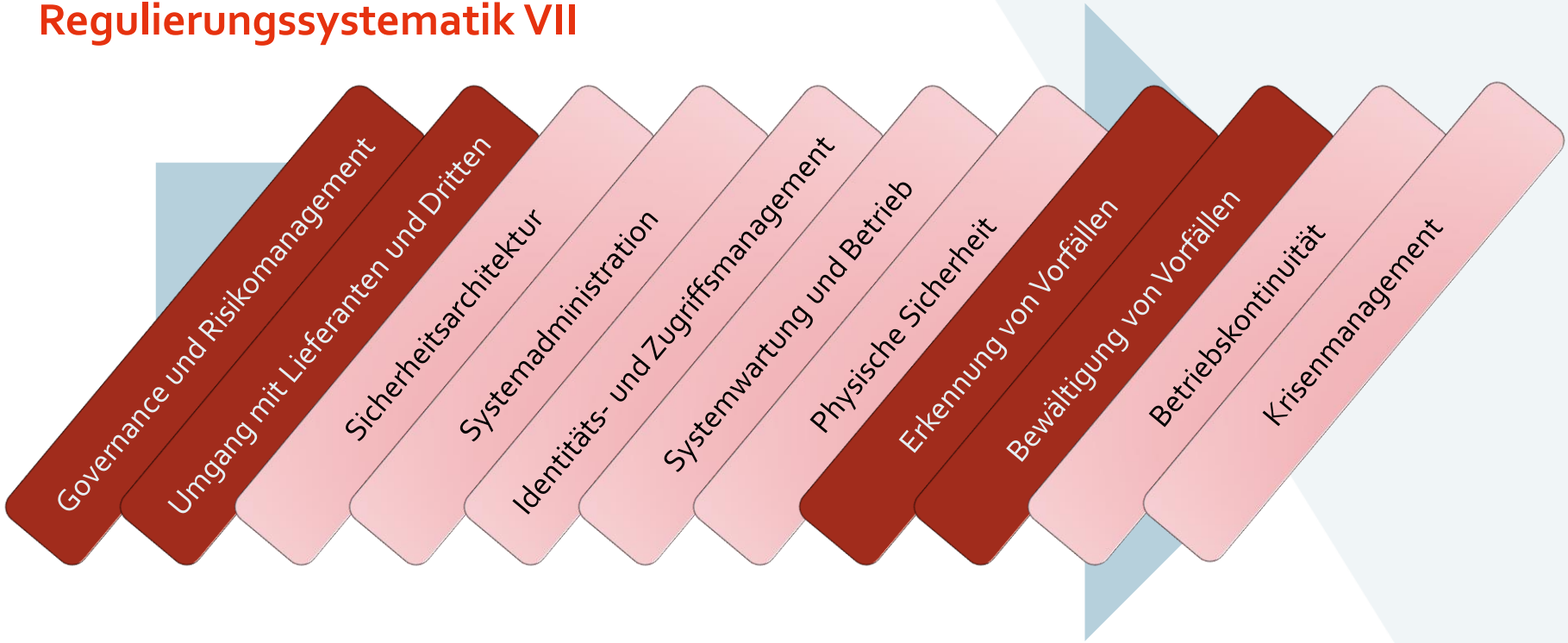
NISV – Gegenstand

- Gegenstand der NISV ist die Festlegung

1. von Kriterien für die Parameter zu Sicherheitsvorfällen gemäß § 3 Z 6 lit. a bis d NISG (Meldeschwellenwerte)
2. näherer Regelungen zu den in § 2 NISG genannten Sektoren gemäß § 16 Abs. 2 NISG (wesentliche Dienste)
3. von Sicherheitsvorkehrungen nach § 17 Abs. 1 NISG (**Sicherheitsmaßnahmen**)
4. von Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste gemäß § 20 Abs. 1 NISG (lex specialis)

Sicherheitsvorkehrungen

Regulierungssystematik VII



Sicherheitsvorkehrungen

Regulierungssystematik VIII

	Sicherheitsmaßnahmen
1.	Governance und Risikomanagement
1.1.	Risikoanalyse: Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.
1.2.	…

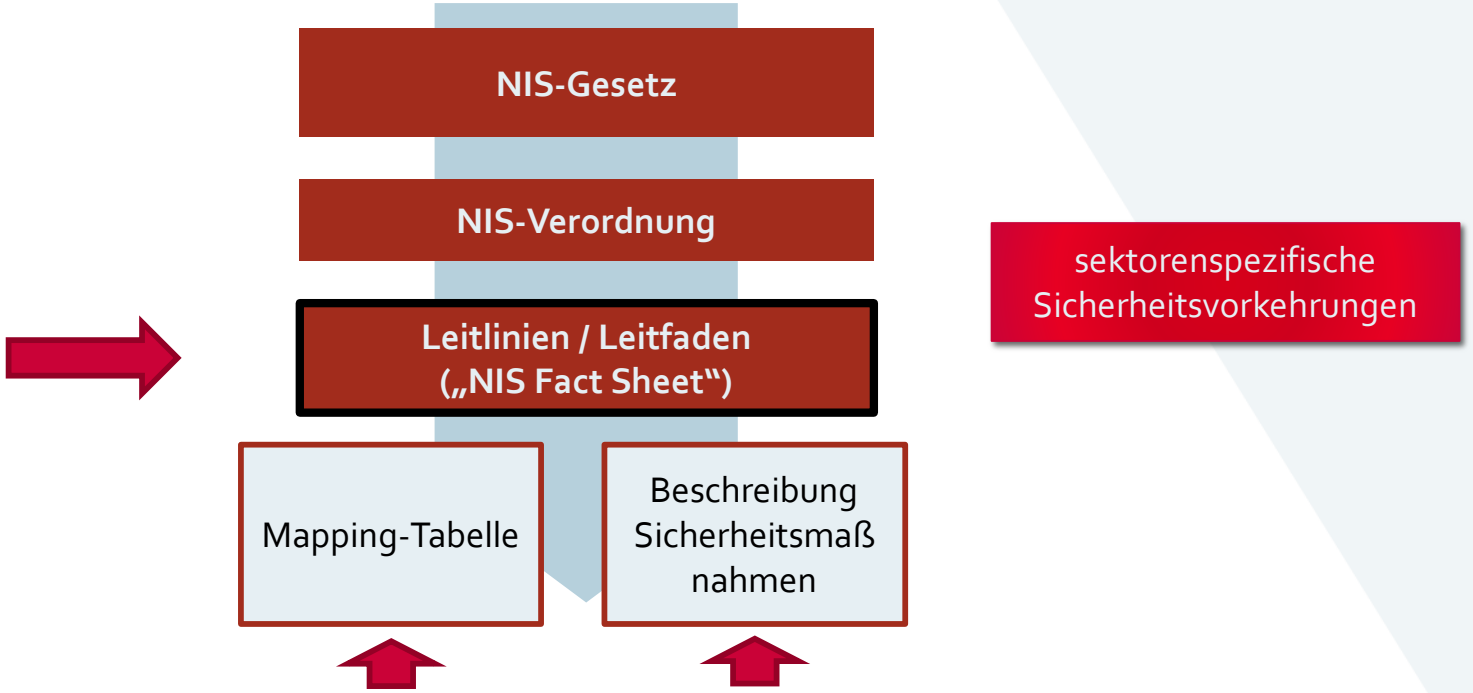
Sicherheitsvorkehrungen

Regulierungssystematik IX

- § 11 Abs 2 NISV:
  - Die Umsetzung jeder Sicherheitsmaßnahme hat, soweit möglich, in technischer und organisatorischer Hinsicht auf Basis der […] Risikoanalyse zu erfolgen.

Sicherheitsvorkehrungen

Regulierungssystematik X



Sicherheitsvorkehrungen

Regulierungssystematik XI

Mapping-Tabelle (NIS Fact Sheet 8/2018)

2.2.1 Governance und Ökosystem

#	Kategorie	Sicherheits-maßnahme	Ö. Informations-sicherheits-handbuch Version 4.0.1	BSI IT-Grundschutz[5]	ISO 27001:2013	ISA/IEC 62443 3-3	CIS CSC Version 6.0	CIS CSC Version 7.0	NIST CYBER SECURITY FRAMEWORK
1	Governance und Risikomanagement	Risikoanalyse	4 Risikoanalyse	*BSI-Standard 100-2, Kapitel 3, 4, 5, BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz*	8.2 Information security risk assessment 8.3 Information security risk treatment	SR 5.1, 5.2, 5.3	1, 2, 4, 13, 14, 17	1, 2, 3, 13, 14, 17	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2

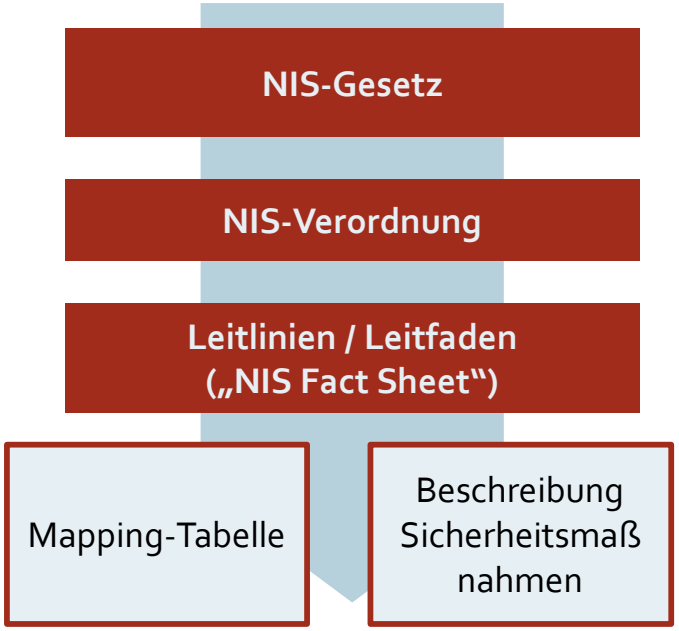
Sicherheitsvorkehrungen

Regulierungssystematik XII

- Beschreibung Sicherheitsmaßnahmen (NIS Fact Sheet 8/2019)
- Auszug zu Risikoanalyse:
  - Der Betreiber führt eine Risikoanalyse durch und **aktualisiert sie regelmäßig**.
  - Die Durchführung der Risikoanalyse beinhaltet die oben erwähnte laufende **Aktualisierung** im Rahmen eines **kontinuierlichen Verbesserungsprozesses (KVP)**.
  - Bei der **Aktualisierung** der Analyse werden insbesondere neue Bedrohungen, der Effektivitätsverlust umgesetzter Maßnahmen sowie Änderungen der Risikosituation, beispielsweise durch Änderungen in der Systemarchitektur, berücksichtigt.

Sicherheitsvorkehrungen

Regulierungssystematik XIII



sektorenspezifische Sicherheitsvorkehrungen

Berücksichtigung von Sektorenspezifika I

- im Rahmen von sektorenspezifische Sicherheitsvorkehrungen
  - Betreiber wesentlicher Dienste können sektorenspezifische Sicherheitsvorkehrungen vorschlagen
  - Gemeinsam mit Sektorenverbänden
  - Bundesminister für Inneres stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen zu erfüllen

Berücksichtigung von Sektorenspezifika II

- Im Rahmen der generellen Vorgaben auch möglich.
- Auszug Einleitung NIS Fact Sheet 8/2019:
  - „Wenn aus technischen oder betrieblichen Gründen die Umsetzung der […] Ausführungen nicht gänzlich möglich ist, sind die dadurch bedingten Abweichungen […] durch risikominimierende und/oder kompensierende Maßnahmen auszugleichen und dies entsprechend in den zu erbringenden Nachweisen (Prüfbericht) darzustellen und glaubhaft zu begründen."

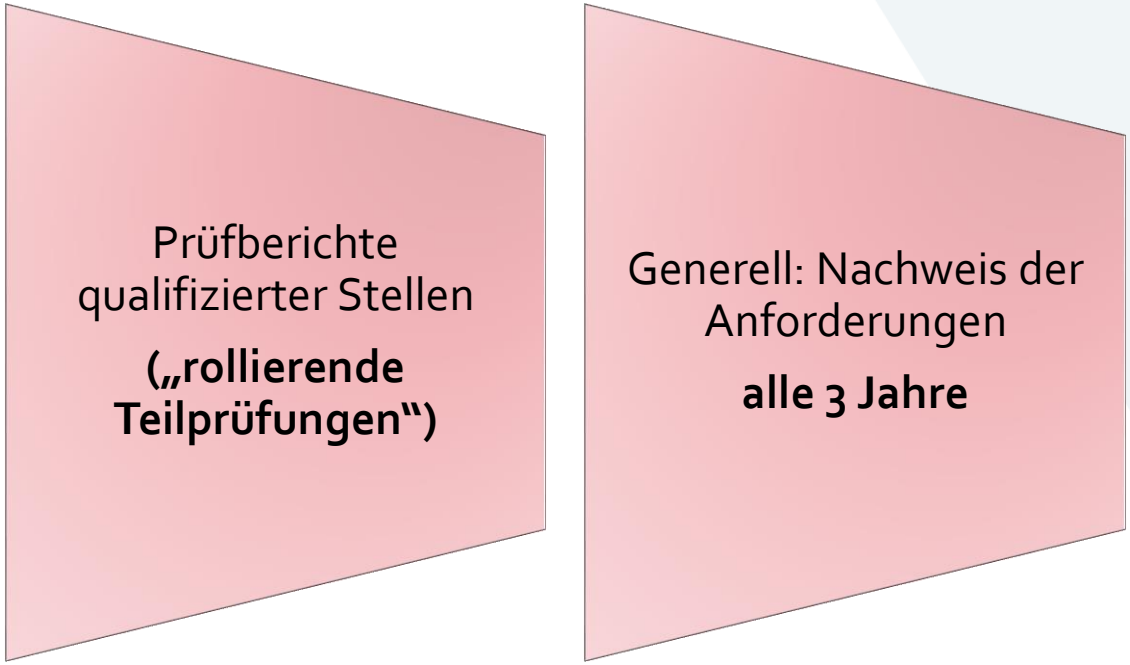
Nachweiserbringung

- Betreiber müssen haben mindestens alle drei Jahre die Erfüllung der Anforderungen gegenüber dem BMI nachzuweisen
- Frist läuft ab Zustellung des Bescheides
- Betreiber übermitteln eine Aufstellung der vorhandenen Sicherheitsvorkehrungen
  - durch den Nachweis von **Zertifizierungen** oder durchgeführten Überprüfungen durch **qualifizierte Stellen**

Qualifizierte Stellen

Sicherheitsvorkehrungen

Überprüfung



Überprüfung der Sicherheitsvorkehrungen

Qualifizierte Stellen – Voraussetzungen

„befähigte **Mitarbeiter**"

„adäquate **Zertifizierungen**"

„dem Stand der Technik entsprechende **Werkzeuge**"

„geeigneter **Prüfungsprozess**"

Anbieter digitaler Dienste

Digital Service Provider (DSP)

Definition

Ein Anbieter digitaler Dienste ist:

1. eine juristische Person
2. mit Hauptniederlassung in Österreich
   - oder: ohne Hauptniederlassung in der EU, die einen Vertreter namhaft gemacht hat,
3. die einen digitalen Dienst in Österreich anbietet
4. die kein Kleinstunternehmen oder kleines Unternehmen ist

- „provider driven approach"

Digitaler Dienst

Ein digitaler Dienst ist

- ein Dienst iSd § 3 Z 1 E-Commerce-Gesetz
  - Dienst der Informationsgesellschaft: ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst
- bei dem es sich handelt um
  - einen Online-Marktplatz
  - eine Online-Suchmaschine
  - einen Cloud-Computing-Dienst

Sicherheitsvorkehrungen

- NISG macht DSP idente Vorgabe im Vergleich zu Betreibern
- Aber Folgendem ist Rechnung zu tragen:
  a) Sicherheit der Systeme und Anlagen
  b) Bewältigung von Sicherheitsvorfällen
  c) Betriebskontinuitätsmanagement
  d) Überwachung, Überprüfung und Erprobung
  e) Einhaltung der internationalen Normen

Sicherheitsvorkehrungen

- DSP unterliegen auf europäischer Ebene stärker harmonisiertem Konzept
- Durchführungsverordnung (EU) 2018/151 der Kommission zur NIS-Richtlinie

Artikel 2

Sicherheitselemente

(1) Die Sicherheit der Systeme und Anlagen gemäß Artikel 16 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/1148 bezeichnet die Sicherheit von Netz- und Informationssystemen und ihrer physischen Umgebung und umfasst die folgenden Elemente:

a) das systematische Management von Netz- und Informationssystemen, d. h. eine Erfassung und Abbildung der Informationssysteme und die Einführung einer Reihe von geeigneten Maßnahmen für das Management der Informationssicherheit, einschließlich Risikoanalyse, Humanressourcen, Betriebssicherheit, Sicherheitsarchitektur, Lebenszyklus-Management gesicherter Daten und Systeme sowie gegebenenfalls Verschlüsselung und Verschlüsselungsmanagement;

b) die physische Sicherheit und die Sicherheit der Umgebung, d. h. das Vorhandensein einer Reihe von Vorkehrungen zum Schutz der Sicherheit der Netz- und Informationssysteme von Anbietern digitaler Dienste vor Schäden anhand eines risikobasierten Allgefahrenansatzes, der beispielsweise Systemversagen, menschliche Fehler, böswillige

Durchsetzung der Pflichten

- Überprüfung nur im Anlassfall (ex-post)
- BMI kann verlangen, dass DSP Nachweise über Sicherheitsvorkehrungen erbringt
  - nur wenn BMI Umstände bekannt werden, dass DSP Pflichten nicht nachkommt
  - DSP hat Aufstellung der vorhandenen Sicherheitsvorkehrungen zu übermitteln
  - Verantwortungsbereich des DSP, welche Maßnahmen er ergreift, die er für die Bewältigung der Risiken für die NIS für angemessen hält

Cybersecurity Act

Cybersecurity Act

- Zweiter EU-Rechtsakt über Cybersicherheit
- 13.09.2017 vorgelegt
  - Cybersecurity Act/Rechtsakt zur Cybersicherheit, COM(2017) 477 final
- 07.06.2019 Veröffentlichung im Amtsblatt der EU
- 27.06.2019 In Kraft getreten

Cybersecurity Act

- Zwei Kerninhalte:
  - „**EU-Cybersicherheitsagentur**" (ENISA)
  - **Zertifizierungsrahmen**
- ENISA
  - ENISA erhält neues, stärkeres und permanentes Mandat
  - ENISA wird finanziell und personell aufgestockt
  - Benennung als Agentur der EU für Cybersicherheit

Cybersecurity Act – Zertifizierungsrahmen

- Mehrere IKT-Zertifizierungssysteme und -initiativen in MS
- Marktfragmentierung und Interoperabilitätsprobleme
- Mehrere Zertifizierungsverfahren für Unternehmen in verschiedenen MS
- CSA schafft einen Rahmen für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozesse

Cybersecurity Act – Zertifizierungsrahmen

- Was bedeutet der Zertifizierungsrahmen?
  - „Werkzeugkasten"
    - CSA führt keine unmittelbar operativen Zertifizierungssysteme ein
    - Zertifizierungsschemata werden von der Kommission als Durchführungsrechtsakte erlassen
    - Zertifizierungsschemata werden durch ENISA vorbereitet unter Beteiligung der Stakeholder und MS

Cybersecurity Act – Zertifizierungsrahmen

- Prinzip der Freiwilligkeit
  - sofern im Unionsrecht oder im Recht der MS nicht anders bestimmt
  - Kommission muss sich regelmäßig (spätestens bis Ende 2023) fragen, ob ein bestimmtes europäisches Cybersicherheitszertifizierungsschema verbindlich vorgeschrieben werden soll
  - Fokus auf NIS-Sektoren

Cybersecurity Act – Schritte auf EU-Ebene

- Kommission erstellt Arbeitsprogramm
- Kommission hat ECCG einberufen
- Kommission baut mit ENISA die SCCG auf
- ENISA baut Strukturen auf
- ENISA bereit erstes Zertifizierungsschema vor
  - ENISA hat dazu ad hoc Working Group aufgesetzt

Danke für Ihre Aufmerksamkeit!

Mag. Vinzenz Heußler, LL.M.,
Abteilung I/C/8 – Cyber Security, GovCERT, NIS-Büro und ZAS
vinzenz.heussler@bka.gv.at