DER INFOR Anwenderverein

NIS2-Einführung

SACHVERSTÄNDIGENBÜRO MÜLOT

Claus Wissing (Geschäftsführer SVB Mülot GmbH)

- Geschäftsführer und externer Datenschutzbeauftragter für sehr viele Organisationen
- Freier Sachverständiger in den Bereichen Datenschutz, Datensicherheit und Informationssicherheit
- Langjährige Erfahrung im Bereich der Telekommunikations- und IT-Technik
- Zertifizierter Datenschutzbeauftragter und Datenschutzauditor (TÜV-Rheinland)
- Compliance Officer (TÜV-Rheinland)

Fachgebiete

- Planung u. Aufbau von DSM-Systemen, ISMS-Systemen
- Datenschutz u. Informationssicherheit
- Schulungen
- Konzerndatenschutz

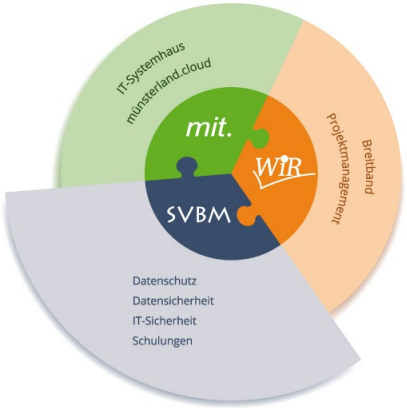
Spezialkompetenz(en)

- Telekommunikation
- Kirchlicher Datenschutz und soziale Einrichtungen

Sachverständigenbüro Mülot GmbH

Wo kommen wir her?

- 1999 von Dirk-Michael Mülot als Einzelunternehmen gegründet
- 2018 Übergang in die Sachverständigenbüro Mülot GmbH mit Claus Wissing als Geschäftsführer
- Standorte in Greven und Langenberg



Was können wir?

- Über 20 Jahre Erfahrung in Datenschutz- und Datensicherheitsthemen nach DSGVO und kirchlichen Datenschutzgesetzen
- Starke Unternehmensgruppe für IT-Projektmanagement, Digitalisierung, Prozessautomatisierung, sichere Systemhauslösungen
- Insgesamt > 50 Beschäftigte mit Fachkompetenz (Ingenieure, Projektmanager, Rechtsanwälte, Planer, IT-Sicherheitsexperten, …)

25 Jahre Erfahrung und Lösungsorientierung

2024

- Ausweitung der innovativen Datenschutz-Dienste (Institut.com, VVT-Easy, DSMS-Dienste)
- Informationssicherheit (ISO 27001, Tisax, KRITIS, NIS2), Hinweisgeberschutz für verschiedenste Branchen
- Exzellente Dienstleistungen durch ausgebautes professionelles Datenschutz-Team
- Datenschutz- und Datensicherheitsthemen nach DSGVO und kirchlichen Datenschutzgesetzen

2018

- Übergang in die Sachverständigenbüro Mülot GmbH und weiterer Ausbau des Datenschutz-Teams
- Claus Wissing übernimmt die Geschäftsführung

1999-2018

- Stetige Erweiterung der Branchenberatung und Lehraufträge TÜV Rheinland sowie Fortbildungsakademie des Deutschen Caritasverbandes
- Tätigkeiten als „Freier Sachverständiger“ und Zertifizierung als Datenschutzbeauftragter und Datenschutzauditor
- Gegründet als Einzelunternehmen/Freiberufler durch Dirk-Michael Mülot

Über die Landesgrenzen hinaus tätig

Bisheriger Radius

EU-weit

- Für Unternehmen in Deutschland und deren Schwestergesellschaften

Europaweit/außerhalb der EU:

- Als Datenschutzvertretung nach Art. 27 DSGVO für Unternehmen außerhalb der EU, welche innerhalb der EU am Markt tätig sind
- In Zusammenarbeit mit Schwesterfirmen und Partner:innen wie der WiR Projects GmbH oder der datenschutzguide.ch GmbH in der Schweiz

International:

- Für international aufgestellte Mandant:innen, die z. B. Geschäftsbereiche oder Konzernmuttergesellschaften in den USA oder in anderen Drittländern haben

Typische Branchen unserer Kunden/Mandanten

Herstellende Industrie:

- Automobilindustrie (incl. Prototypenbau)
- Industrielle Fertigung, Maschinenbau
- Logistik, Reedereien, Distribution

Konsumgüter:

- Bekleidung und Mode
- Lebensmittel und Getränkeindustrie

Gesundheitswesen:

- Versicherungen, Kliniken, Arztpraxen
- Pflegeeinrichtungen

Finanzwesen:

- Versicherungen, Banken, Immobilien

Soziale Organisationen:

- Kirchliche Träger: Bistümer, Kirchliche Gemeinden, Caritasverbände
- Sportverbände, Sportvereine

Bildungseinrichtungen:

- Große Träger der Erwachsenenbildung zur Sensibilisierung

Willkommen zum heutigen Stammtisch

Infos zur Durchführung

Regeln

- Die Mikrofone sind bitte ausgeschaltet, können aber von bei Bedarf eingeschaltet werden.
- Meldungen bitte über Handzeichen.
- Fragen – auch zur Technik – bitte in den Chat schreiben.

Unterlagen

- Foliensatz steht am Ende zur Verfügung.
- Feedback steht anschließend zur Verfügung.

Zwischendurch werden wir kurze Umfragen durchführen:
https://www.menti.com/ald1najkiko9

Hinweis:
Das Web-Seminar wird **nicht** aufgezeichnet. Aufzeichnungen durch die Teilnehmenden sind **nicht** erlaubt!

Agenda

1 Einführung

2 Die NIS-2 Richtlinie und ihre Inhalte

3 Informationssicherheit und die Pflichten

4 Aufgaben der Aufsichtsbehörde

5 Konsequenzen für Unternehmen

1 Einführung

Einleitung

Gründe und Rahmenregelungen für NIS-2

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

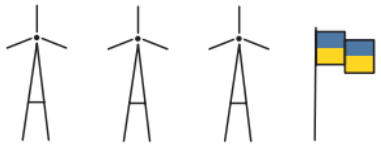
116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden

nach Angriff auf Satelliten-kommunikation



20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schad-programm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

neue Webseiten wurden wegen enthal-tener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

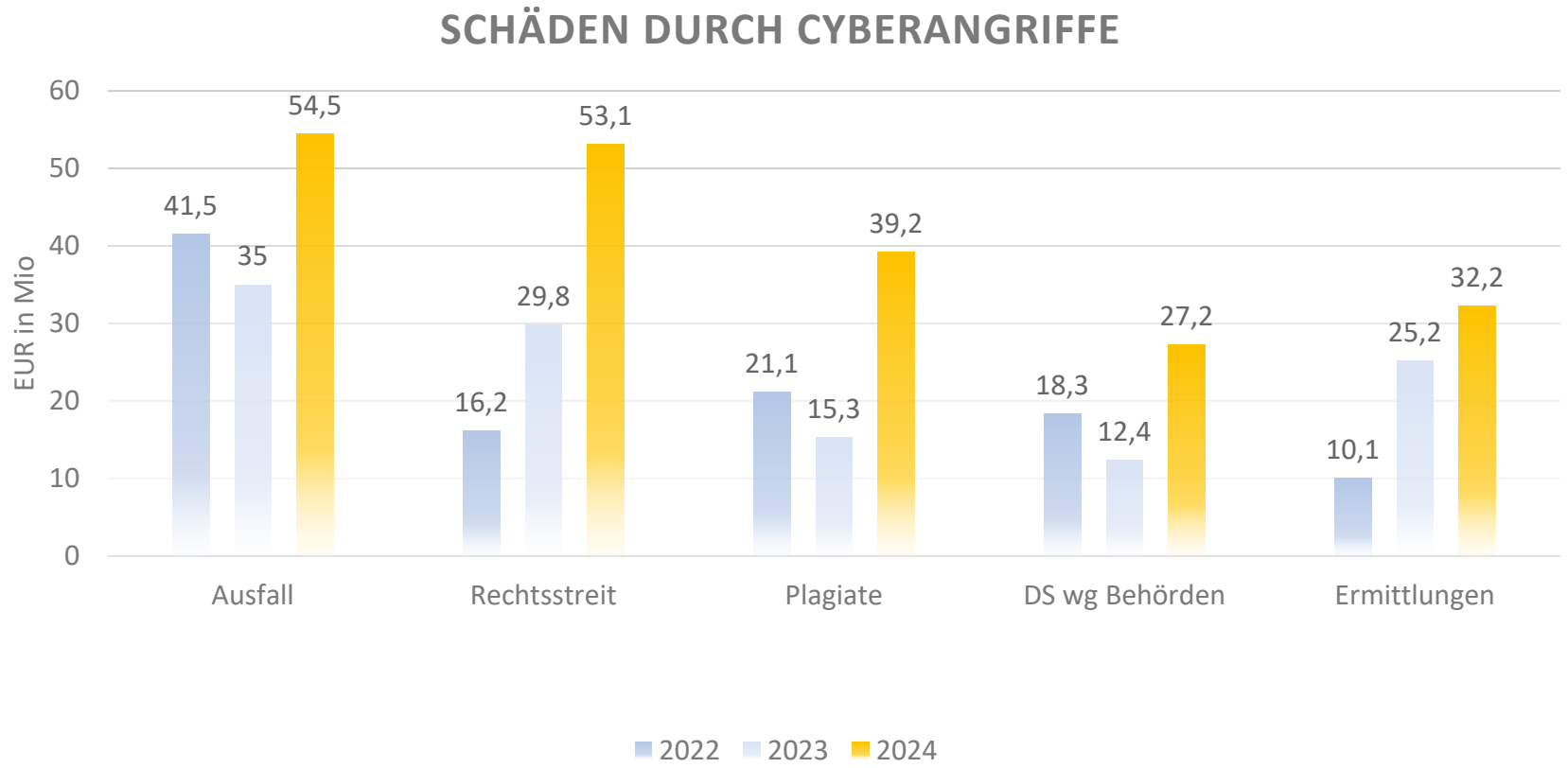
aller Spam-Mails im Berichts-zeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Quellen: Lage der IT-Sicherheit in Deutschland 2022 (BSI)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022-Doppelseite.html?nn=129410 (letzter Zugriff: 23.07.2024)

Bedeutung für den Wirtschaftsstandort



Quelle: Studie „Wirtschaftsschutz 2024“ des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) e.V.

2 Die NIS-2 Richtlinie und Ihre Inhalte

NIS2-Richtlinie

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)

Die NIS2-Richtlinie ist eine **Weiterentwicklung** der ursprünglichen NIS-Richtlinie (Netz- und Informationssicherheitsrichtlinie), die 2016 eingeführt wurde. Die NIS-Richtlinie war die **erste EU-weite Gesetzgebung zur Cybersicherheit**, die darauf abzielte, ein **hohes gemeinsames Sicherheitsniveau** für Netz- und Informationssysteme in der EU zu schaffen.

Die NIS2-Richtlinie wurde entwickelt, um **auf die neuen Bedrohungen und Herausforderungen der Cybersicherheit zu reagieren**, die seit der Einführung der NIS-Richtlinie aufgetreten sind. Sie baut auf den Erfahrungen der Mitgliedstaaten mit der Umsetzung der ursprünglichen NIS-Richtlinie auf und **zielt darauf ab, Schwächen und Lücken zu schließen**.

Während die ursprüngliche NIS-Richtlinie auf bestimmte Sektoren beschränkt war, **erweitert die NIS2-Richtlinie den Geltungsbereich auf zusätzliche Sektoren und Unternehmen**, um den Schutz kritischer Infrastrukturen zu stärken.

Ziele der NIS2-Richtlinie

Erhöhung der Cybersicherheit

Ein zentrales Ziel ist es, das allgemeine Sicherheitsniveau in der EU zu erhöhen, indem Unternehmen dazu verpflichtet werden, strengere Sicherheitsmaßnahmen umzusetzen und regelmäßige Risikobewertungen durchzuführen.

Harmonisierung der Vorschriften

Die NIS2-Richtlinie strebt eine Harmonisierung der Cybersicherheitsvorschriften in allen EU-Mitglied-staaten an, um ein gleichmäßiges Schutzniveau zu gewährleisten und Wettbewerbsverzerrungen zu vermeiden.

Ziele der NIS2-Richtlinie

Stärkung der Resilienz

Unternehmen sollen widerstandsfähiger gegen Cyberangriffe und andere Sicherheitsvorfälle werden, indem sie proaktive Maßnahmen zur Erkennung, Prävention und Reaktion auf Bedrohungen ergreifen.

Erhöhung der Transparenz und Rechenschaftspflicht

Die Richtlinie führt strengere Meldepflichten ein, um sicherzustellen, dass Sicherheitsvorfälle schnell und effizient an die zuständigen Behörden gemeldet werden.

Überblick über die Änderungen

- **Erweiterter Anwendungsbereich**
  - Die NIS2-Richtlinie gilt für eine breitere Palette von Sektoren und Unternehmen, einschließlich mittelgroßer Unternehmen, die von wesentlicher Bedeutung für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Aktivitäten sind.
- **Strengere Meldepflichten**
  - Unternehmen müssen Sicherheitsvorfälle innerhalb kürzerer Fristen melden, und die Richtlinie legt fest, welche Arten von Vorfällen gemeldet werden müssen.
- **Verstärkte Durchsetzung**
  - Die NIS2-Richtlinie enthält strengere Durchsetzungs- und Sanktionsmechanismen. Aufsichtsbehörden haben mehr Befugnisse zur Durchführung von Audits und zur Verhängung von Bußgeldern bei Nichteinhaltung.
- **Erhöhte Anforderungen an die Unternehmensführung**
  - Unternehmen müssen sicherstellen, dass ihre Führungsebene in die Cybersicherheitsstrategie eingebunden ist und die Verantwortung für die Einhaltung der NIS2-Anforderungen übernimmt.

Umsetzung in Deutschland

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

- Frist zur Umsetzung: 17.10.2024
- Regierungsentwurf: 22.07.2024
- Änderungen: u.a. BSI-Gesetz, BND-Gesetz, TDDDG, HinSchG, EnWG, SGB V, SGB VI, SGB XI, TKG
- -> Insgesamt 32 Änderungen

Anwendungsbereich

Besonders wichtige Einrichtungen (§ 28 I BSIG)

Größenunabhängig

- Betreiber kritischer Anlagen (KRITIS)
- qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter

Größenabhängig

- Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, wenn
  - **mindestens 50 Mitarbeitende beschäftigt oder (!)**
  - **Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro**
- Große Unternehmen
  - mindestens 250 Mitarbeitende beschäftigt oder (!)
  - Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro

    und

  - Einrichtung aus **Anlage 1** (Energie, Transport/Verkehr, Finanzwesen, Gesundheit, Wasser/Abwasser, Digitale Infrastruktur, Weltraum)

Anwendungsbereich

Wichtige Einrichtungen (§ 28 II BSIG)

Größenunabhängig

- Vertrauensdiensteanbieter

Größenabhängig

- Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, wenn
  - weniger als 50 Mitarbeitende **und (!)**
  - Jahresumsatz und eine Jahresbilanzsumme von jeweils unter 10 Millionen Euro
- Mittlere und große Unternehmen (=mindestens 50 Mitarbeitende oder Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro)

  und

  - Einrichtung aus **Anlage 1** (Energie, Transport/Verkehr, Finanzwesen, Gesundheit, Wasser/Abwasser, Digitale Infrastruktur, Weltraum) oder
  - Einrichtung aus **Anlage 2** (Post/Kurier, Siedlungsabfallentsorgung, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung)

Nicht betroffen? Aber: Sind Sie Teil einer Lieferkette? Dann bitte dranbleiben.

Exkurs: Berechnung Mitarbeiterzahl/Jahresumsatz

Mitarbeiterzahl

- Berechnung in Vollzeitäquivalenten
- Einbezogen werden:
  - Angestellte
  - Personen, die für das Unternehmen arbeiten und in einem Unterordnungsverhältnis stehen (leih- und Zeitarbeit)
  - Eigentümer-Unternehmer
  - Teilhaber, die eine regelmäßige Tätigkeit ausüben
- Nicht einbezogen werden:
  - Auszubildende oder Studenten in der Berufsausbildung
  - Mitarbeiter im Mutterschafts- oder Elternurlaub

Art. 5 der Empfehlung der Kommission 2003/361/EG

Jahresumsatz

- Berechnung auf Jahresbasis
- Bezieht sich auf den Verkauf von Produkten und die Erbringung von Dienstleistungen
- Ohne Mehrwertsteuer und sonstige indirekte Steuern

Jahresbilanzsumme

- Bezieht sich auf die Hauptvermögenswerte

Art. 4 der Empfehlung der Kommission 2003/361/EG

Schwellenwerte

Berechnungsmethodik

Art. 4 der Empfehlung der Kommission 2003/361/EG	Die Mitarbeiterzahl wird als Jahresdurchschnitt berechnet
	Bei Über-/Unterschreitung der Schwellenwerte verändert sich der Status nach Abweichungen in zwei aufeinanderfolgenden Geschäftsjahren

Schwellenwerte

Querverbund

Bei der Bestimmung der maßgeblichen Mitarbeiterzahlen und des Umsatzes sind nur diejenigen Teile der Einrichtung einzubeziehen, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind, Querschnittsaufgaben wie beispielsweise Personal, Buchhaltung etc. sind hierbei anteilig zu berücksichtigen.

Hierdurch wird sichergestellt, dass Einrichtungen, die insgesamt die Größenschwelle für Mitarbeiteranzahl, Jahresumsatz oder Jahresbilanzsumme überschreiten, deren hauptsächliche Geschäftstätigkeit jedoch nicht einer Einrichtungskategorie gemäß Anlage 1 oder 2 dieses Gesetzes zuzuordnen ist, nicht in unverhältnismäßiger Weise erfasst werden.

Anwendungsbereich

Sektoren

KRITIS

- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Finanzwesen
- Gesundheit
- Wasser
- Ernährung
- Staat und Verwaltung
- Energie
- Siedlungsabfallentsorgung

besonders wichtige Einrichtungen I

- Qualifizierte Vertrauensdienste
- TLD-Registries
- DNS-Dienste
- Bundesverwaltung

Anwendungsbereich

Sektoren

wichtige Einrichtungen (Anhang 2)

Besonders wichtige Einrichtungen II (Anhang 1)

Energie	Transport und Verkehr	Finanzwesen
Gesundheit	Wasser	Digitale Infrastruktur
Große Unternehmen	Weltraum	

Post- und Kurierdienste	Abfallbewirtschaftung	Produktion, Herstellung und Handel mit chemischen Stoffen
Produktion, Verarbeitung und Vertrieb von Lebensmitteln	Verarbeitung und Herstellung von Waren	Anbieter digitaler Dienste
Forschung	Öffentliche TK-Netze und TK-Dienste	Vertrauensdienste

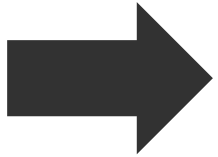
Große und mittlere Unternehmen

Besonders relevante Sektoren

Bereich „industrielle Produktion“

Wichtige Einrichtungen

Post- und Kurierdienste	Abfallbewirtschaftung	Produktion, Herstellung und Handel mit chemischen Stoffen
Produktion, Verarbeitung und Vertrieb von Lebensmitteln	Verarbeitung und Herstellung von Waren	Anbieter digitaler Dienste
Forschung	Öffentliche TK-Netze und TK-Dienste	Vertrauensdienste



a) Herstellung von Medizinprodukten und In-vitro-Diagnostika
b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
c) Herstellung von elektrischen Ausrüstungen
d) Maschinenbau
e) Herstellung von Kraftwagen und Kraftwagenteilen
f) sonstiger Fahrzeugbau

Besonders relevante Sektoren

Bereich „industrielle Produktion“

5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates (4) herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates (5) herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektrischen Ausrüstungen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

Beispiele aus den Untersektoren

„Verarbeitung/Herstellung von Waren“

Untersektor „Maschinenbau“

Verweis auf Abschnitt C Abteilung 28 der Statistische Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev.2):

- Herstellung von nicht wirtschaftszweigspezifischen Maschinen
- Herstellung von Verbrennungsmotoren und Turbinen (ohne Motoren für Luft- und Straßenfahrzeuge)
- Herstellung von hydraulischen und pneumatischen Komponenten und Systemen
- Herstellung von Pumpen und Kompressoren a. n. g.
- Herstellung von Armaturen a. n. g.
- Herstellung von Lagern, Getrieben, Zahnrädern und Antriebselementen
- Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen Herstellung von Öfen und Brennern
- Herstellung von Hebezeugen und Fördermitteln
- Herstellung von handgeführten Werkzeugen mit Motorantrieb
- Herstellung von kälte- und lufttechnischen Erzeugnissen, nicht für den Haushalt
- Herstellung von sonstigen nicht wirtschaftszweigspezifischen Maschinen
- Herstellung von land- und forstwirtschaftlichen Maschinen
- Herstellung von Werkzeugmaschinen
- Herstellung von Werkzeugmaschinen für die Metallbearbeitung
- Herstellung von sonstigen Werkzeugmaschinen
- Herstellung von Maschinen für sonstige bestimmte Wirtschaftszweige
- Herstellung von Maschinen für die Metallerzeugung, von Walzwerkseinrichtungen und Gießmaschinen
- Herstellung von Bergwerks-, Bau- und Baustoffmaschinen

Beispiele aus den Untersektoren

“Verarbeitung/Herstellung von Waren”

Untersektor „Herstellung von elektronischen Ausrüstungen“

Verweis auf Abschnitt C Abteilung 27 der Statistische Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev.2):

- Herstellung von Elektromotoren, Generatoren, Transformatoren, Elektrizitätsverteilungs- und -schalteinrichtungen
- Herstellung von Batterien und Akkumulatoren
- Herstellung von Kabeln und elektrischem Installationsmaterial
- Herstellung von Glasfaserkabeln
- Herstellung von sonstigen elektronischen und elektrischen Drähten und Kabeln
- Herstellung von elektrischem Installationsmaterial
- Herstellung von elektrischen Lampen und Leuchten
- Herstellung von elektrischen Lampen und Leuchten
- Herstellung von Haushaltsgeräten
- Herstellung von elektrischen Haushaltsgeräten
- Herstellung von nichtelektrischen Haushaltsgeräten
- Herstellung von sonstigen elektrischen Ausrüstungen und Geräten a. n. g.
- Herstellung von sonstigen elektrischen Ausrüstungen und Geräten a. n. g.

Beispiele aus den Untersektoren

“Verarbeitung/Herstellung von Waren”

Untersektor „Herstellung von Kraftwagen und Kraftwagenteilen“

Verweis auf Abschnitt C Abteilung 29 der Statistische Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev.2):

Herstellung von Kraftwagen und Kraftwagenteilen

- Herstellung von Kraftwagen und Kraftwagenmotoren
- Herstellung von Karosserien, Aufbauten und Anhängern
- Herstellung von Teilen und Zubehör für Kraftwagen
- Herstellung elektrischer und elektronischer Ausrüstungsgegenstände für Kraftwagen
- Herstellung von sonstigen Teilen und sonstigem Zubehör für Kraftwagen

.

Ausnahmen

Sektorspezifische Regulierungen

- **Finanzsektor (§ 28 V BSIG)**
  - Teile des Finanzsektors unterfallen zwar dem Sektor Finanzwesen, werden aber von den Pflichten (außer Registrierung) befreit, wenn sie DORA (Digital Operational Resilience Act) unterfallen.
- **Betreiber öffentlicher TK-Netze und TK-Dienste (§ 28 IV Nr. 1 BSIG)**
  - Die Sicherheitsmaßnahmen aus § 30 BSI werden analog nach §165 II a TKG überführt.
- **Betreiber von Energieversorgungsnetzen oder Energieanlagen**
  - Die Sicherheitsmaßnahmen aus § 30 BSIG werden analog nach § 5c EnWG überführt.
- **DNS, TLD, Cloud, Rechenzentren, CDNs, Managed Services und Security Services, Online-Marktplätze und Suchmaschinen, soziale Netzwerke und Vertrauensdienste**
  - Die digitalen Dienste sollen vorrangig durch Implementing Acts gem. § 30 III BSIG reguliert werden.

Ausnahmen

Die Lieferkette

NIS2

- Muss NIS2-Pflichten erfüllen
  - Sicherheit der Lieferkette verpflichtend
  - Zulieferer müssen Pflichten erfüllen

Zulieferer

- Muss NIS2-Pflichten erfüllen (Meldepflichten etc.), damit Auftraggeber NIS2-Pflichten erfüllt
  - Sicherheit der Lieferkette verpflichtend
  - Zulieferer müssen Pflichten erfüllen

Zulieferer

- Muss ebenfalls NIS2-Pflichten, damit Auftraggeber und dessen Auftraggeber NIS2-Pflichten erfüllt
- usw.

3 Informationssicherheit und die Pflichten

Pflichten für Unternehmen

Allgemein

	Risiko-management § 30 BSIG	Besondere Anforderungen § 31 BSIG	Meldepflichten § 32 BSIG	Registrierung §§ 33, 34 BSIG	Unterrichtungs-pflichten § 35 BSIG	Governance § 38 BSIG	Nachweispflicht § 39 BSIG
Kritische Anlagen	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Besonders wichtig	Ja	Nein	Ja	Ja	Ja	Ja	Nein
wichtig	Ja	Nein	Ja	Ja	Ja	Ja	Nein

Pflichten für Unternehmen

Risikomanagement § 30 II BSIG

- Risikoanalyse
- ISMS
- Incident Management
- Lieferkettensicherheit
- Business Continuity
- Schulungen
- Zugangs- und Zugriffskontrolle
- Weitere Verordnungen möglich

Meldepflichten § 32 BSIG

- 3stufiges Meldesystem
- 24h/72h/1 Monat
- Meldestelle: BSI

Registrierung §§ 33, 34 BSIG

- Registrierungsstelle von BSI & BBK
- spätestens 3 Monate nach Inkrafttreten
- Name und Rechtsform
- Anschrift inkl. IP-Adressbereich
- Sektor oder Branche
- **Kritis zusätzlich**:
- Spätestens zum 1. Tag
- Versorgungskennzahl
- Standort
- Kontaktstelle

Unterrichtungspflichten § 35 BSIG

- BSI kann Regulierungsbehörden anderer Mitgliedstaaten und Öffentlichkeit informieren

Pflichten für Unternehmen

Governance § 38 BSIG	Nachweispflichten § 39 BSIG	Besondere Anforderungen	Kritische Komponenten § 41 BSIG
• Verpflichtung, Risikomanagement umzusetzen • Verpflichtung, Risikomanagement zu überwachen • Haftung für schuldhaft verursachten Schaden • Schulungsverpflichtung	• Überprüfungen stichprobenartig möglich -> Dokumentationspflicht	• § 31 BSIG grds. nur Kritis	• grds. nur Kritis • Anzeigepflicht kritische Komponenten • Untersagungsbefugnis BMI vor und während des Einsatzes

4

Aufgaben der Aufsichtsbehörde

Gründe für Bussgelder

- **Nichteinhaltung von Sicherheitsmaßnahmen**
  - Fehlende oder unzureichende technische und organisatorische Maßnahmen
- **Verletzung der Meldepflicht**
  - Verspätete oder unterlassene Meldung von Sicherheitsvorfällen
- **Unzureichendes Krisenmanagement und Notfallvorsorge**
  - Geschäftskontinuität
  - Wiederherstellung von Diensten
  - Unzureichende Kommunikation
- **Verantwortung des Managements**
  - Verletzung der Pflichten durch das Management
- **Behinderung der Aufsichtsbehörde**
  - Unzureichende Zusammenarbeit mit der Aufsichtsbehörde

Aufsicht: Befugnisse

- Überwachungs- und Kontrollrechte
- Notfallbefugnisse
- Maßnahmen gegen das Management
- Durchsetzungsrechte
- Kooperation und Koordination
- Veröffentlichung von Informationen

Aufgaben der Aufsichtsbehörde

Wirksame Beaufsichtigung der Einhaltung

- Das BSI ist die zuständige Aufsichtsbehörde für *besonders wichtige* und *wichtige* Einrichtungen mit Niederlassung in Deutschland, für Betreiber kritischer Anlagen auf deutschem Hoheitsgebiet und Einrichtungen der Bundesverwaltung gemäß § 59 BSIG und § 62 BSIG.
- Abweichend von § 62 (1) BSIG ist die Bundesnetzagentur für Betreiber von Kommunikationsnetzen oder Anbieter von Telekommunikationsdiensten zuständig, die ihre Dienste in Deutschland erbringen.
- Im Sektor öffentliche Verwaltung ist das BSI nur für solche *wichtigen* und *besonders wichtigen* Einrichtungen zuständig, die von der Bundesrepublik Deutschland eingerichtet sind.

Aufgaben der Aufsichtsbehörde

Sanktionen / Bußgelder

Höhe	Verstöße z.B.
10 Mio. Euro 7 Mio. Euro 2 Mio. Euro	• Nachweise über Erfüllung der Anforderungen werden nicht richtig oder nicht vollständig erbracht. § 39 (1) Satz BSIG 1 i.V.m. VO § 58 (4) Satz 1 • Nachweise über Erfüllung der Anforderungen werden nicht erbracht. § 39 (1) Satz 1 BSIG i.V.m. VO nach § 58 (4) Satz 1
500.000 Euro	• Meldungen werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt. § 32 (1) BSIG
100.000 Euro	• geeigneter Nachweis über die erfolgte Mängelbeseitigung wird nicht vorgelegt § 39 (1) Satz 6 BSIG

5 Konsequenzen für Unternehmen

Risikomanagement

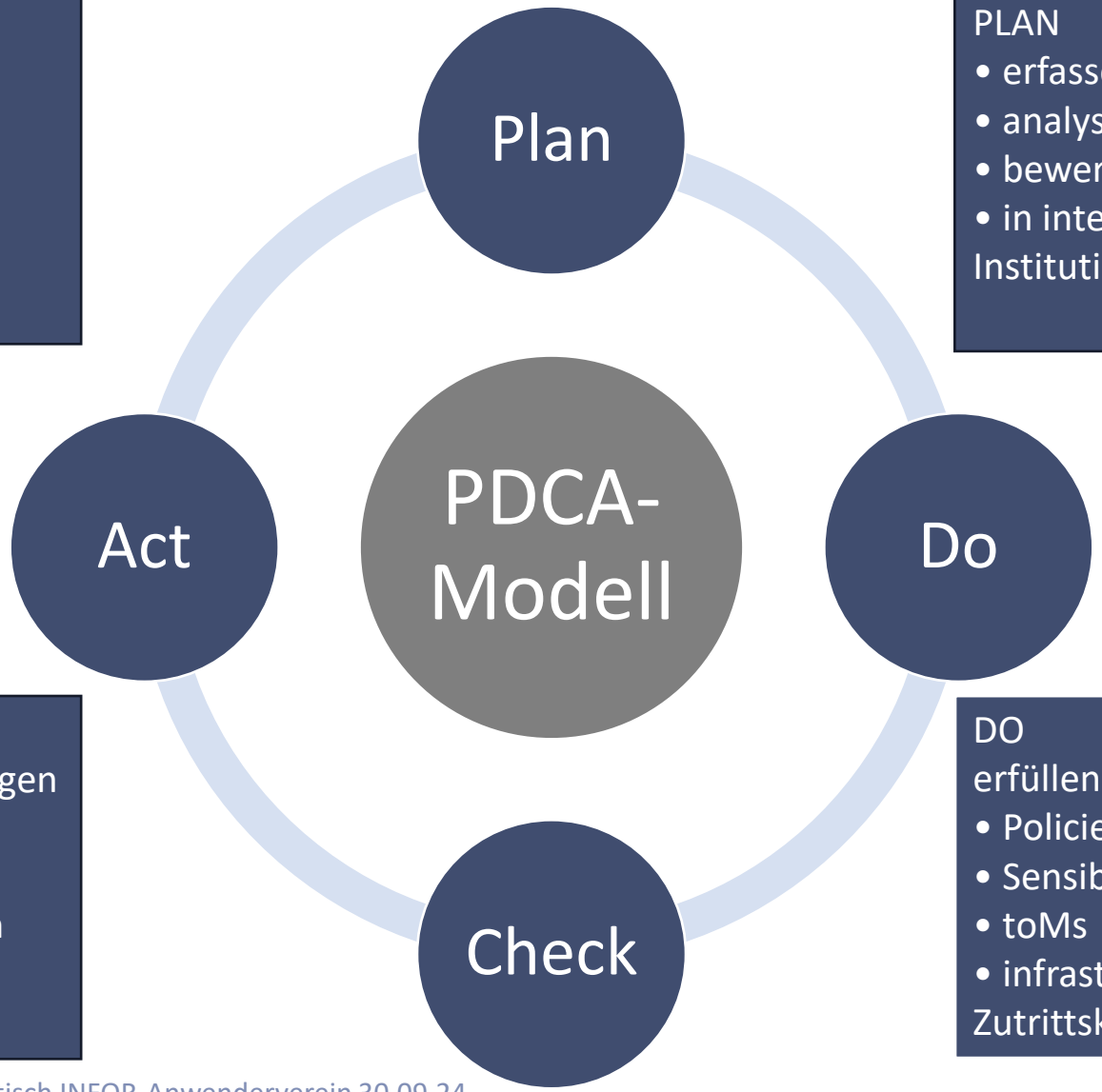
Faktisch erfordert NIS2 die Einführung eines ISMS

Ein Informationssicherheitsmanagementsystem (ISMS) ist ein systematischer Ansatz zur Verwaltung sensibler Unternehmensinformationen, um deren Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Merkmale eines ISMS:

- Durchführung einer umfassenden Risikoanalyse des Unternehmens.
- Regelmäßige Überprüfung und Aktualisierung der Risikoeinschätzung als kontinuierlicher Verbesserungsprozess (PDCA-Zyklus).
- Entwicklung einer Risikomanagement-Strategie unter Berücksichtigung technischer, organisatorischer und personeller Aspekte.
- Identifizierung und Dokumentation kritischer Systeme und Daten.
  - Umfassende Dokumentation von Richtlinien, Verfahren und Prozessen.
  - Nachweisbarkeit der Umsetzung von Sicherheitsmaßnahmen.
  - Asset-Management = Inventarisierung und Klassifizierung von Informationsassets und Festlegung von Schutzmaßnahmen basierend auf der Assetklassifizierung.
- Verantwortlichkeiten und Organisationsstruktur klar zugewiesen.
- Incident Management als Etablierung von Prozessen zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen.
- Business Continuity Management.
- Lieferanten- und Drittanbieter-Management: Einbeziehung von Lieferanten und Dienstleistern in das ISMS und Sicherstellung der Einhaltung von Sicherheitsstandards in der Lieferkette.

Anforderungsmanagement

ACT
• Korrekturmaßnahmen umsetzen und ihre Wirksamkeit überprüfen
• Verbesserung kommunizieren.



PLAN
• erfassen,
• analysieren,
• bewerten und
• in interne (Sicherheits-) Vorgaben für die Institution umwandeln

CHECK
• Indikatoren und Parameter abfragen
• Defizite (in Interaktion mit den Stakeholdern) erkennen
• Korrekturmaßnahmen definieren

DO
erfüllen:
• Policies, Richtlinien
• Sensibilisierung, Weiterbildung
• toMs
• infrastrukturellen Maßnahmen Zutrittskontrolle, Sicherheitszonen

Sicherheit der Lieferkette

- NIS2 legt einen verstärkten Fokus auf die Sicherheit der gesamten Lieferkette (Lieferanten § 30 II Nr. 4 u. 5 BSIG und Einkauf § 30 II Nr. 5 BSIG). Unternehmen müssen nicht nur ihre eigene Cybersicherheit gewährleisten, sondern auch die Sicherheitsmaßnahmen ihrer Zulieferer und Dienstleister berücksichtigen:

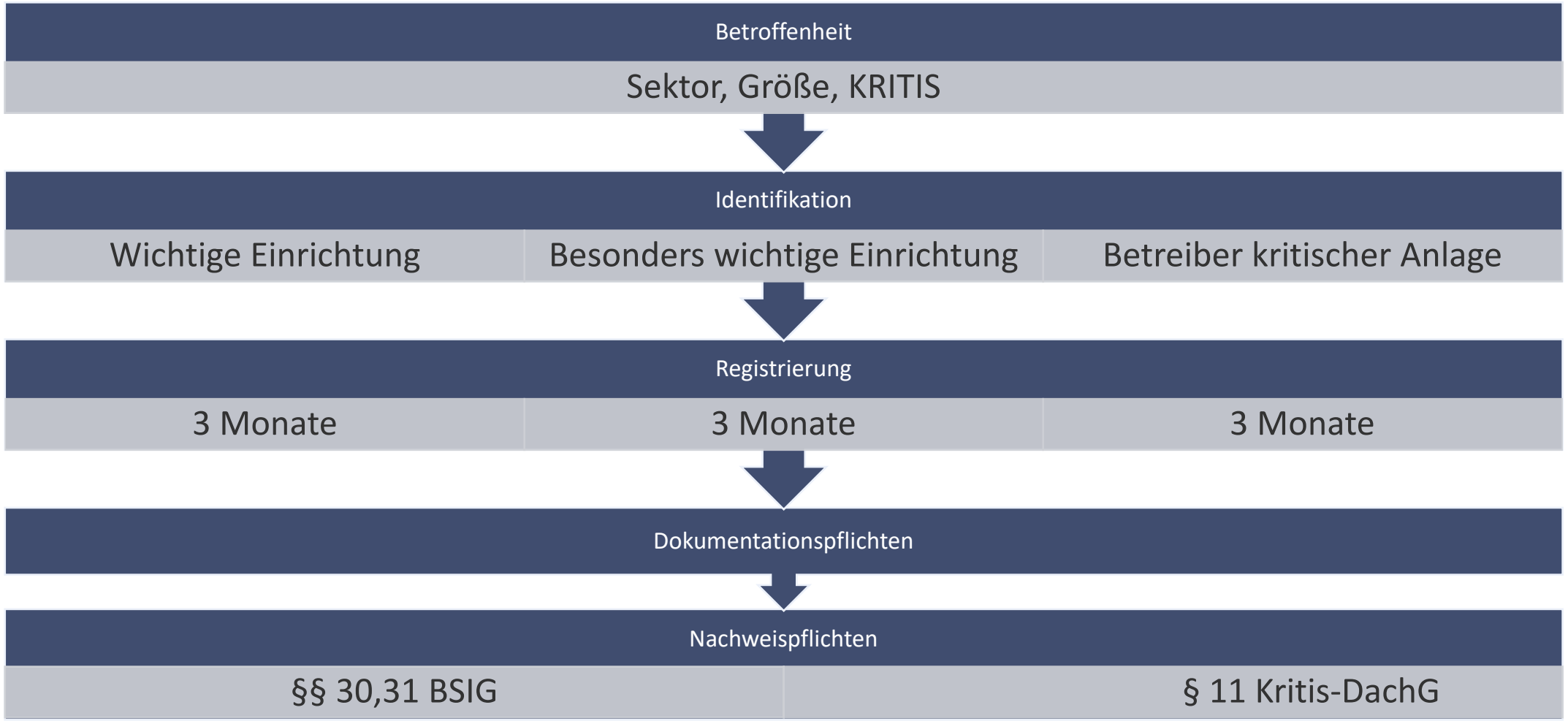
  § 30 (2) S.2 BSIG: *Die Maßnahmen müssen zumindest Folgendes umfassen: […]*
  4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
  5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen

Konsequenzen

- Unternehmen müssen eine umfassende Risikoanalyse ihrer Lieferkette durchführen
- Überprüfung bestehender Lieferanten auf Einhaltung von Sicherheitsstandards (Audits, Zertifizierung etc.)
- Implementierung von Cybersicherheitskriterien bei der Auswahl neuer Lieferanten
- Aufnahme von Cybersicherheitsklauseln in Verträge mit Lieferanten und Dienstleistern und Anpassung bestehender Verträge
- Vereinbarung von Meldepflichten bei Sicherheitsvorfällen in der Lieferkette
- Einbeziehung von Lieferkettenszenarien in Incident-Response-Pläne
- Dokumentation aller Maßnahmen zur Sicherung der Lieferkette
- Fortlaufende Überwachung, Bewertung und Dokumentation der Lieferkette

Registrierung §§ 33, 34 BSIG

Identifizierung und Dokumentation



Meldepflichten § 32 BSIG

Erheblicher Sicherheitsvorfall

Erheblicher Sicherheitsvorfall

- der schwerwiegende Betriebsstörungen oder finanzielle Verluste für den betreffenden Betreiber öffentliche Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste verursacht hat oder verursachen kann, oder
- der andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Meldepflichten § 32 BSIG

Dreistufiges Meldesystem

>24 Std.
frühe Erstmeldung

- Verdacht rechtswidriger Handlung
- oder Verdacht böswilliger Handlung
- oder grenzüberschreitende Auswirkung

- § 12 KRITIS-DachG
- Anzahl Betroffene
- Voraussichtliche Dauer
- Gebiet
- Informationen zu Art, Ursache

72 Std.
Bestätigung/Aktualisierung der Erstmeldung

- Erste Bewertung einschließlich Schweregrad und Auswirkungen
- Ggf. Komprimittierungsindikatoren

1 Monat
Abschlussmeldung

- Ausführliche Beschreibung des Vorfalls einschließlich Schweregrad und Auswirkungen
- Angaben zur Art bzw. Ursache
- Angaben zu Abhilfemaßnahmen
- Ggf. Angaben zu grenzüberschreitender Auswirkung

§ 12 III KRITIS-DachG
- Ausführlicher Bericht

Dokumentations- und Berichtspflichten

Dokumentations- und Berichtspflichten (§ 35 BSIG Unterrichtung und § 39 BSIG Dokumentation), allg. Pflicht gem. § 30 I S. 2 BSIG.

(3) Das Bundesamt kann auch gegenüber anderen besonders wichtigen Einrichtungen frühestens drei Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen.

-> Die Überprüfungen erfolgen gem. § 60 IV BSIG risikobasiert.

- Weitere Nachweispflichten für besonders wichtige Einrichtungen nach § 62 i.V.m. § 61 BSIG

-> Die Überprüfungen erfolgen gem. § 61 BSIG anlassbezogen.

Governance

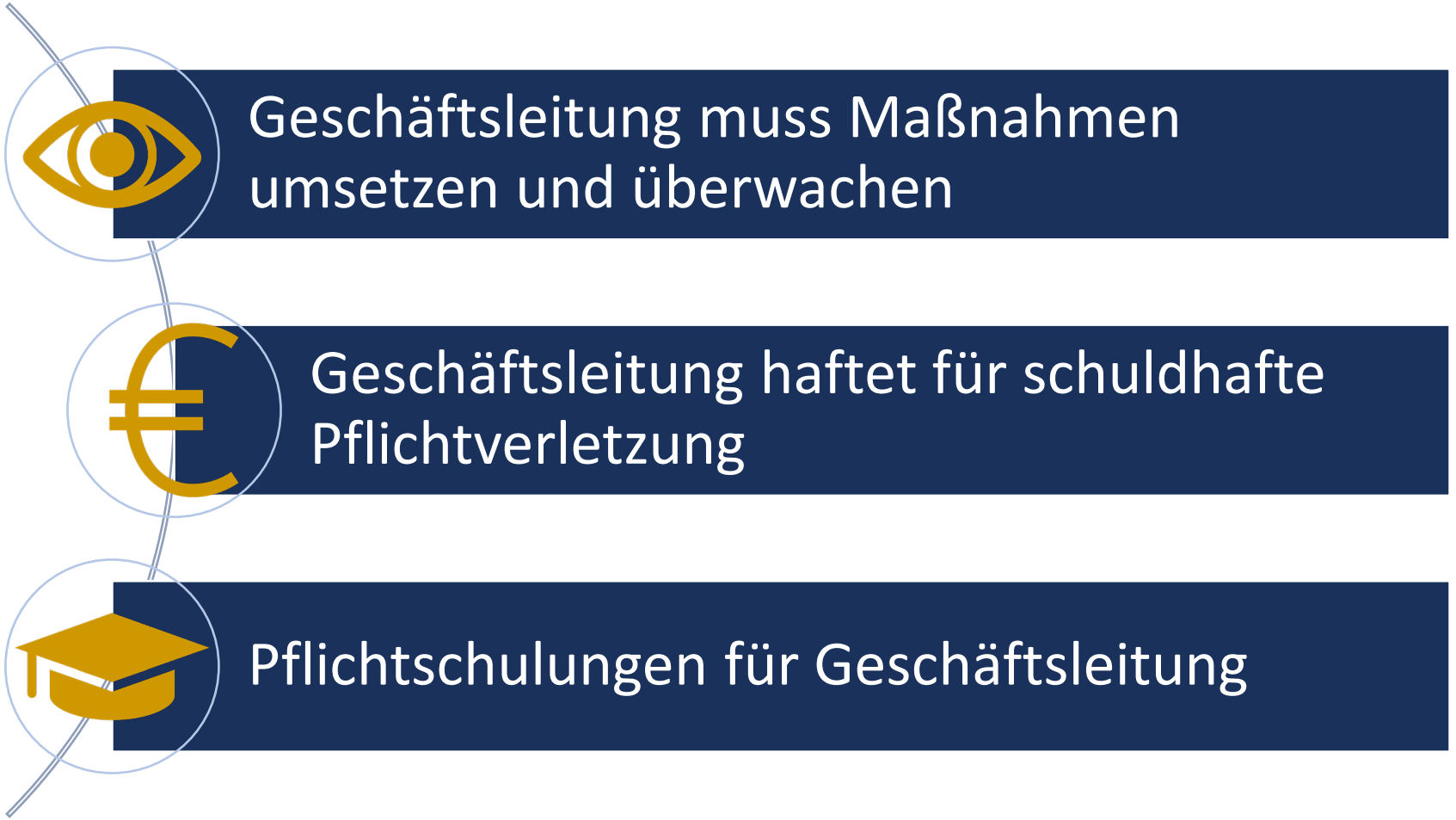
Verantwortlichkeit der Unternehmensführung (§ 38 BSIG)

Die Unternehmensleitung muss aktiv in die Cybersicherheitsstrategie eingebunden sein und die Einhaltung der gesetzlichen Anforderungen sicherstellen:

> *(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts.*
>
> *(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.*

Governance

Gem. § 38 BSIG



Compliance


Risikoanalyse
Risikomanagement
Sicherheitsrichtlinien
toM
Supply Chain
Security
Incident-Response-
Prozess
Schulung und
Sensibilisierung
Business Continuity
Disaster Recovery
Überwachung
Dokumentation
Faktoren

NIS2 und Datenschutz

Schnittmengen identifizieren und nutzen 1/2

- Kernziele identisch
  - CIA: Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit)

- Risikobasierter Ansatz
  - Beide Regelwerke erfordern eine Bewertung der spezifischen Risiken
  - Maßnahmen sollen an die identifizierten Risiken angepasst werden
  - Sowohl die DSGVO als auch die NIS2-Richtlinie betonen, dass Sicherheitsmaßnahmen angemessen und verhältnismäßig zu den identifizierten Risiken sein müssen.
  - Beide Regelungen erfordern eine kontinuierliche Überprüfung und Anpassung der Sicherheitsmaßnahmen, um neue Bedrohungen und Schwachstellen zu adressieren.

NIS2 und Datenschutz

Schnittmengen identifizieren und nutzen 2/2

DSGVO

- Datenschutz-Folgenabschätzung für risikobehaftete Verarbeitungen (Art. 35)
- toM sollen dem Risiko angemessen sein (Art. 24; 25; 32)
- Meldepflichten (Art. 33)

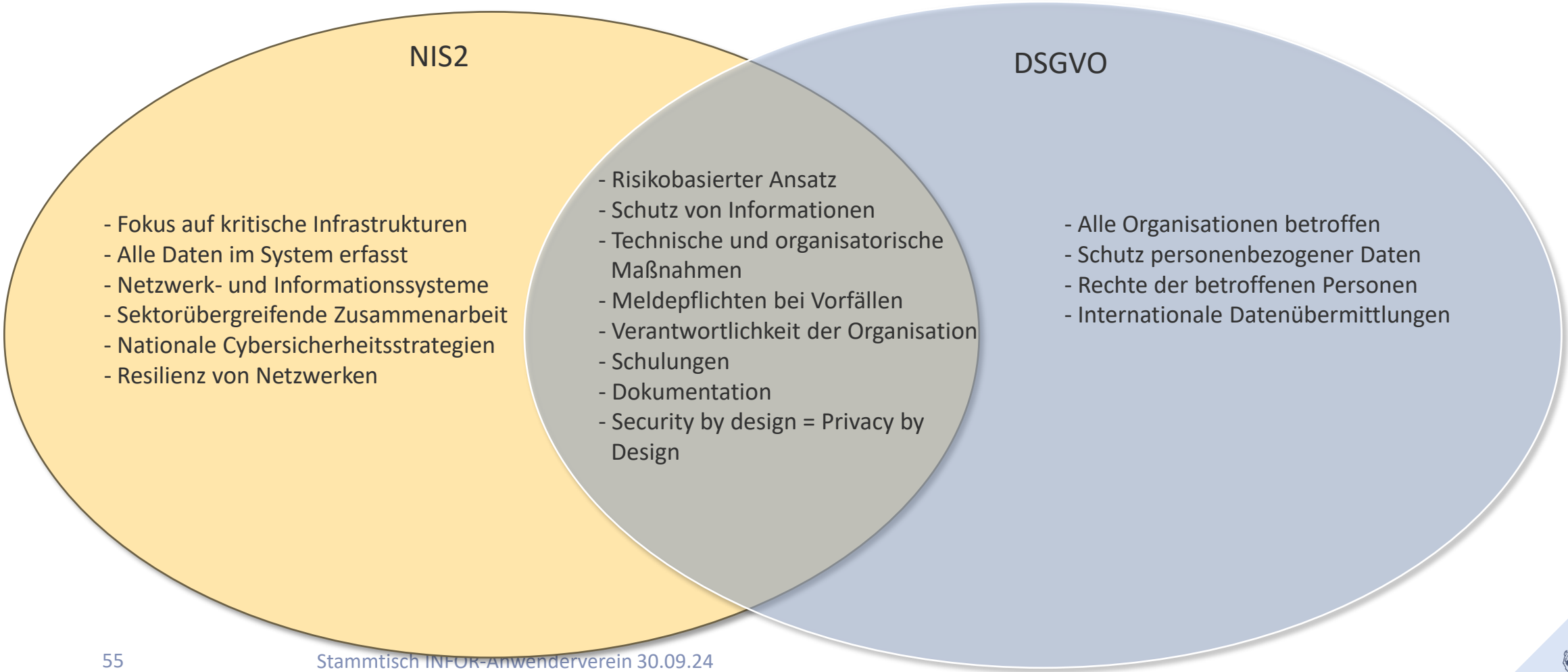
NIS2

- Risikoanalysen für Netzwerk- und Informationssysteme (§ 30 II BSIG)
- Risikomanagementmaßnahmen=toM (§§ 30 I 2, 31 BSIG)
- Meldepflichten (§ 32 BSIG)

- Diese Parallelen verdeutlichen die Notwendigkeit eines integrierten Ansatzes zur Datensicherheit und Cybersicherheit, da beide Regulierungen ähnliche Prinzipien verfolgen, um den Schutz von Daten und die Sicherheit von Systemen zu gewährleisten

NIS2 und Datenschutz

Schnittmengen identifizieren und nutzen



NIS2 und Datenschutz

Schnittmengen identifizieren und nutzen

Risikoanalyse und -management: Bestehende DSGVO-Risikoanalysen können als Basis für NIS2-Bewertungen dienen. Gemeinsame Methodik für Risikobewertung und -behandlung.

Sicherheitsmaßnahmen: Viele technische und organisatorische Maßnahmen der DSGVO sind auch für NIS2 relevant. Gemeinsame Sicherheitsstandards und Best Practices.

Incident Response und Meldepflichten: Bestehende Prozesse können angepasst werden, um beiden Regelwerken zu entsprechen.

Lieferantenmanagement: DSGVO-Verträge mit Auftragsverarbeitern können um NIS2-Anforderungen erweitert werden. Gemeinsame Audits und Überprüfungen von Dienstleistern.

Dokumentation und Nachweise: Bestehende Dokumentationen können um NIS2-relevante Aspekte ergänzt werden. Gemeinsame Compliance-Nachweise für beide Regelwerke.

Schulungen und Sensibilisierung: Datenschutz- und IT-Sicherheitsschulungen können kombiniert werden.

Governance und Verantwortlichkeiten: Eine enge Zusammenarbeit zwischen Datenschutz- und IT-Sicherheitsverantwortlichen ist sinnvoll.

Bundesratssitzung am 27.09.

1. Authentifizierung mittels europäischer Identität auf Vertrauensniveau „hoch“
2. Neben Schwellenwerten aus KRITIS-DachG andere Kriterien, damit Krankenhäuser reguliert werden
3. Domainregistrierung nur nach Identitätsfeststellung (gegen Fake-Shops)
4. Meldungen nach § 32 BSIG zeitgleich auch für Meldung nach Art. 34 DSGVO, dann Weiterleitung an Aufsicht
5. IT-Aufsicht meldet jeden Verstoß gegen Risikomanagement oder Berichtspflichten , der eine Datenschutzverletzung zur Folge haben kann, an Datenschutzaufsicht

Muss das alles sein?

Spoiler: Ja

„Beim Sicherheitsthema geht es wirklich um die Wurst.“

Martin Wansleben, Geschäftsführer der Deutschen Industrie- und Handelskammer (DIHK)

- Cybersecurity sollte wie Datenschutz nicht als „aufgezwungene“ Maßnahme begriffen werden.
- Es werden die eigenen Assets im eigenen Interesse geschützt.
- Wertschöpfung durch Sicherheit als vertrauensbildende Maßnahme.

-> Sicherheit und Datenschutz sollten nicht nur auf dem Papier (für die Aufsicht) bestehen, sondern auch gelebt werden.

Kurzer Ausblick

Nach der Umsetzung ist vor der Umsetzung

- Ab 2027 findet der Cyber Resilience Act (CRA) Anwendung
- Regelt die Cybersicherheit für Produkte (NIS2 die betriebsbezogene Cybersicherheit)
- Security by Design
- Fortlaufende Risikobewertung für 5 Jahre ab Inverkehrbringens

- Betroffen:
  - Produkte, die miteinander oder mit dem Internet verbunden werden können
  - Hersteller, Händler, Einführer (ohne Schwellenwerte)
  - Keine Differenzierung zwischen B2B und B2C

NIS2 und Datenschutz

Unser NIS2-Beratungsangebot

- Erstgespräch zur NIS2-Orientierung
  - Analyse der NIS2-Anwendbarkeit für Ihr Unternehmen
  - Identifikation der nächsten wichtigen Schritte
  - Überblick über relevante Anforderungen
  - Besprechung von Herausforderungen und Lösungsansätzen
- Sonder-Konditionen!
  - Pauschale: 10 € zzgl. MwSt.
  - Dauer: 60 Minuten
- Kontakt
  - Tel: +49 2571-5402-0
  - Mail: sales@svb-muelot.de
  - Web: www.svb-muelot.de

Newsletter-anmeldung

Noch Fragen?

SACHVERSTÄNDIGENBÜRO MÜLOT GMBH

Datenschutz | Datensicherheit | Forensische Informatik

Risikomanagement | ISO27001

Grüner Weg 80
48268 Greven

Tel.: 02571/5402 0
info@svb-muelot.de

www.svb-muelot.de