IT-Sicherheit und Datenschutz – was muss, was darf?

Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein
Universität des Saarlands, 31.03.2026 (online)

Plattform Privatheit

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

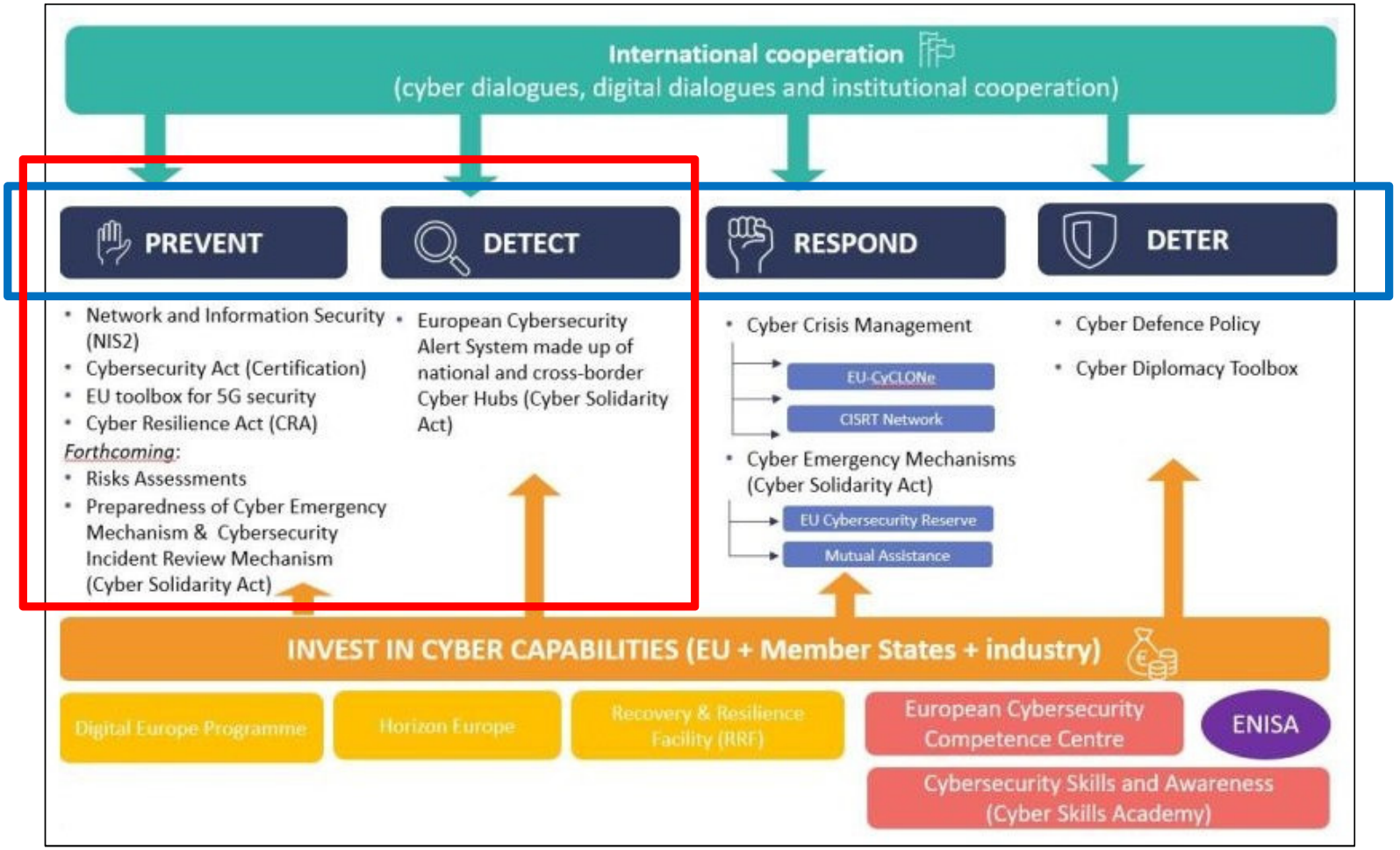
1. Motivation

Datenschutz braucht Sicherheit

1. EU-Cybersicherheitsstrategie

Überblick

1. Motivation
2. Sicherheit und DSGVO
3. Sicherheit und NIS2
4. Sicherheit und CRA
5. Wie geht's zusammen? DSGVO, NIS2 und CRA
6. Fazit und Ausblick



EU Cybersecurity Strategy, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity (2024)

Überblick

2. Sicherheitspflichten: DSGVO

Art. 5 DSGVO – Datenschutzgrundsätze

(1) Personenbezogene Daten müssen

[…]

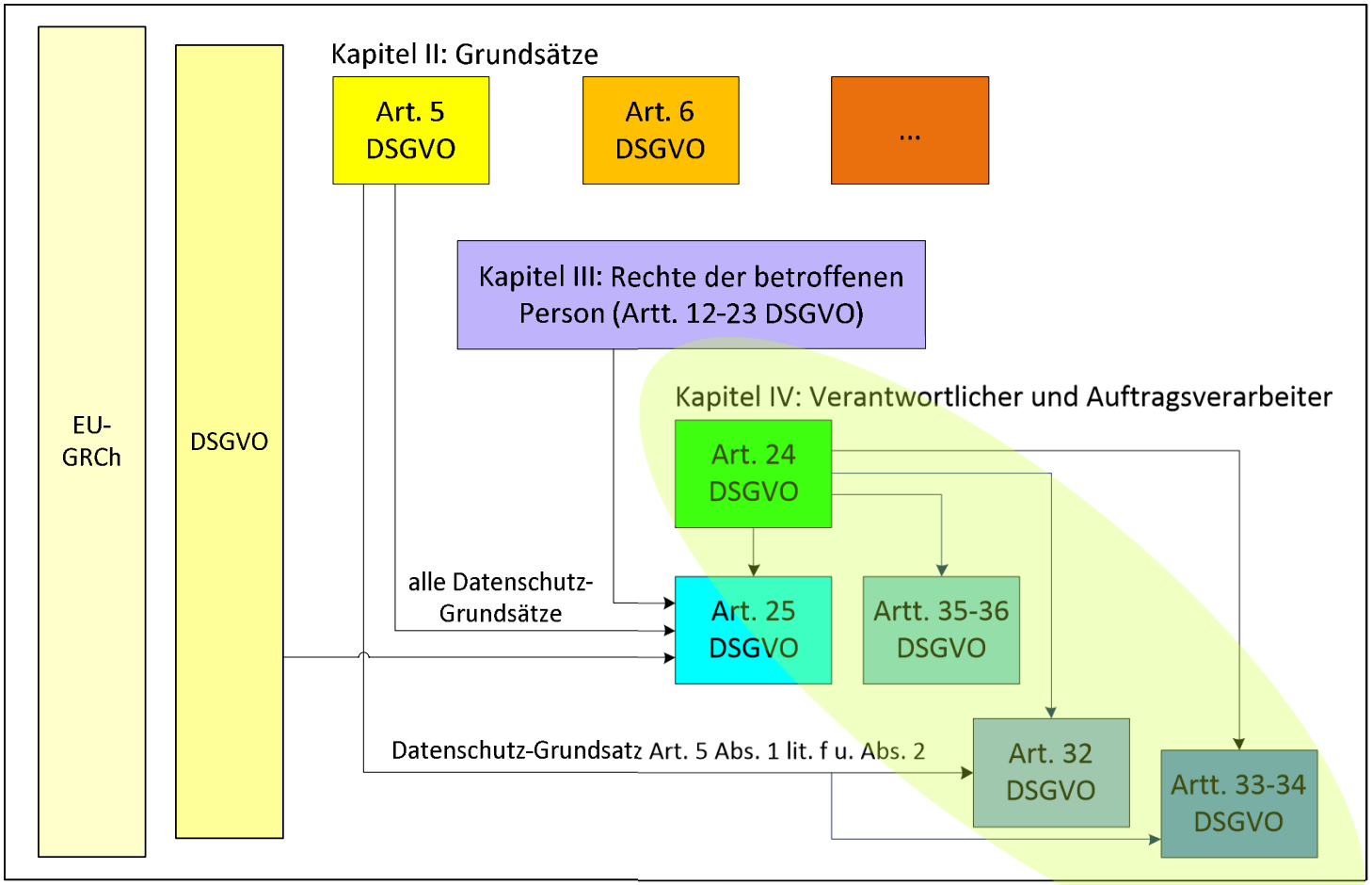
(f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");

Art. 32 DSGVO – Sicherheit

(1) […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
[…]

Überblick

2. Sicherheitspflichten: DSGVO *[mehr als Art. 32]*



2. Sicherheitspflichten: DSGVO

DSGVO: TOMs für (souveräne) Sicherheit:

- Effektiv: wirksam bezüglich beabsichtigter Wirkung; etwaige Nebenwirkungen im Blick

- Nachprüfbar: Möglichkeit aussagekräftiger Prüfungen der zugesicherten Eigenschaften und Wirkungen

- Dauerhaft: jederzeit; auch zukünftig; resilient
- Siehe Artikel 5, 24, 25, 28, 32, 35 DSGVO

2. Sicherheitspflichten: DSGVO

Überblick

Art. 5 DSGVO

(1) Personenbezogene Daten müssen […]
(f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Art. 24 DSGVO

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Art. 25 DSGVO

(1) […] trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z.B. Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Art. 28 DSGVO

(3) […] Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
[…]
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Art. 32 DSGVO

(1) […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
[…]
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
[…]
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Art. 35 DSGVO

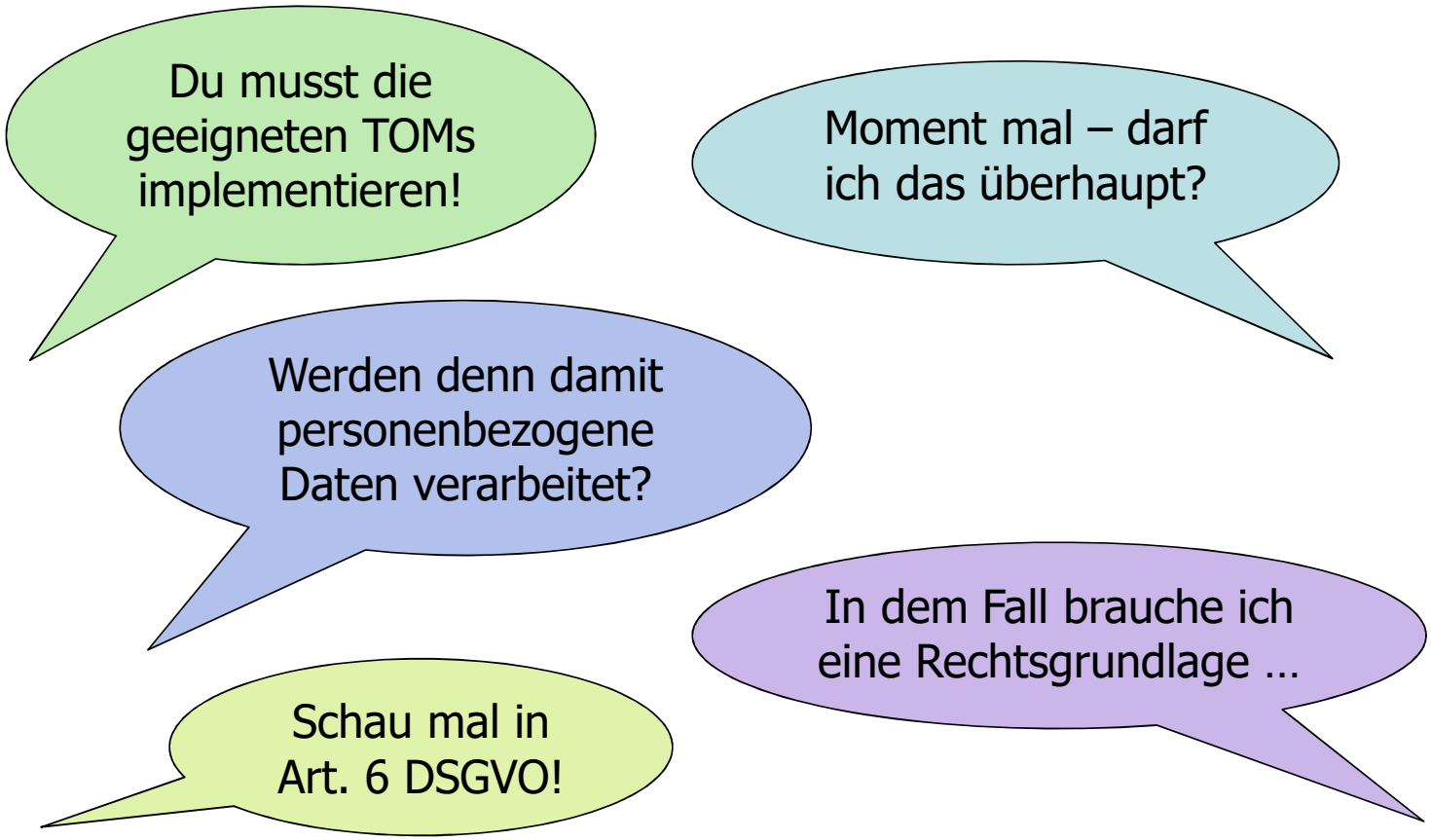
(7) Die Folgenabschätzung enthält zumindest Folgendes:
[…]
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Effektiv: wirksam bezüglich beabsichtigter Wirkung; etwaige Nebenwirkungen im Blick
Nachprüfbar: Möglichkeit aussagekräftiger Prüfungen der zugesicherten Eigenschaften und Wirkungen
Dauerhaft: jederzeit; auch zukünftig; resilient

Hansen/Probst: Souveräne Sicherheit, Zero Trust und das Datenschutzrecht, DuD 10/2023, 623-628

Überblick

2. Sicherheitspflichten: DSGVO



2. Sicherheitspflichten: DSGVO

- Sicherheit als Rechtspflicht in der DSGVO:
  Was muss, was darf?

- Was darf:
  - Keine Verarbeitung personenbezogener Daten ohne Rechtsgrundlage
  - Das gilt auch für TOMs, die personenbezogene Daten verarbeiten
- Typische Rechtsgrundlagen:
  - Erfüllung einer gesetzlichen Pflicht:
    Art. 6 Abs. 1 Buchst. c DSGVO (i.V.m. … z.B. Art. 32 DSGVO, Regelungen des BSIG-neu)
  - Wahrnehmung einer Aufgabe im öffentlichen Interesse:
    Art. 6 Abs. 1 Buchst. e DSGVO
  - Interessenabwägung:
    Art. 6 Abs. 1 Buchst. f DSGVO
- Erforderlichkeit, Verhältnismäßigkeit, … [„Cybersicherheits-TOM-TOMs"]

Überblick

3. Sicherheitspflichten: NIS2

NIS2: IT-Sicherheit für KRITIS

3. Sicherheitspflichten: NIS2

- Ziel: Sicherung von **N**etz- und **I**nformations**s**ystemen in 18 kritischen Sektoren, grenzüberschreitende Reaktion und Durchsetzung
- NIS2-RL (EU) 2022/2555:
  http://data.europa.eu/eli/dir/2022/2555/2022-12-27
- NIS2-Umsetzungsverordnung (NIS2UmsVO) als delegierter Durchführungsrechtsakt C(2024) 7151 der KOM:
  https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=PI_COM:C(2024)7151
- Umsetzung in DE:
  NIS2-Umsetzungs- und **C**ybersicherheitsstärkungs-**G**esetz (NIS2UmsuCG) verspätet: 02.12.2025 (statt 17.10.2024):
  https://www.recht.bund.de/bgbl/1/2025/301/VO.html

Und die DSGVO? – „Unberührt"! [Art. 2 Abs. 12 und EG 14 NIS2-RL]

Überblick

3. Sicherheitspflichten: NIS2

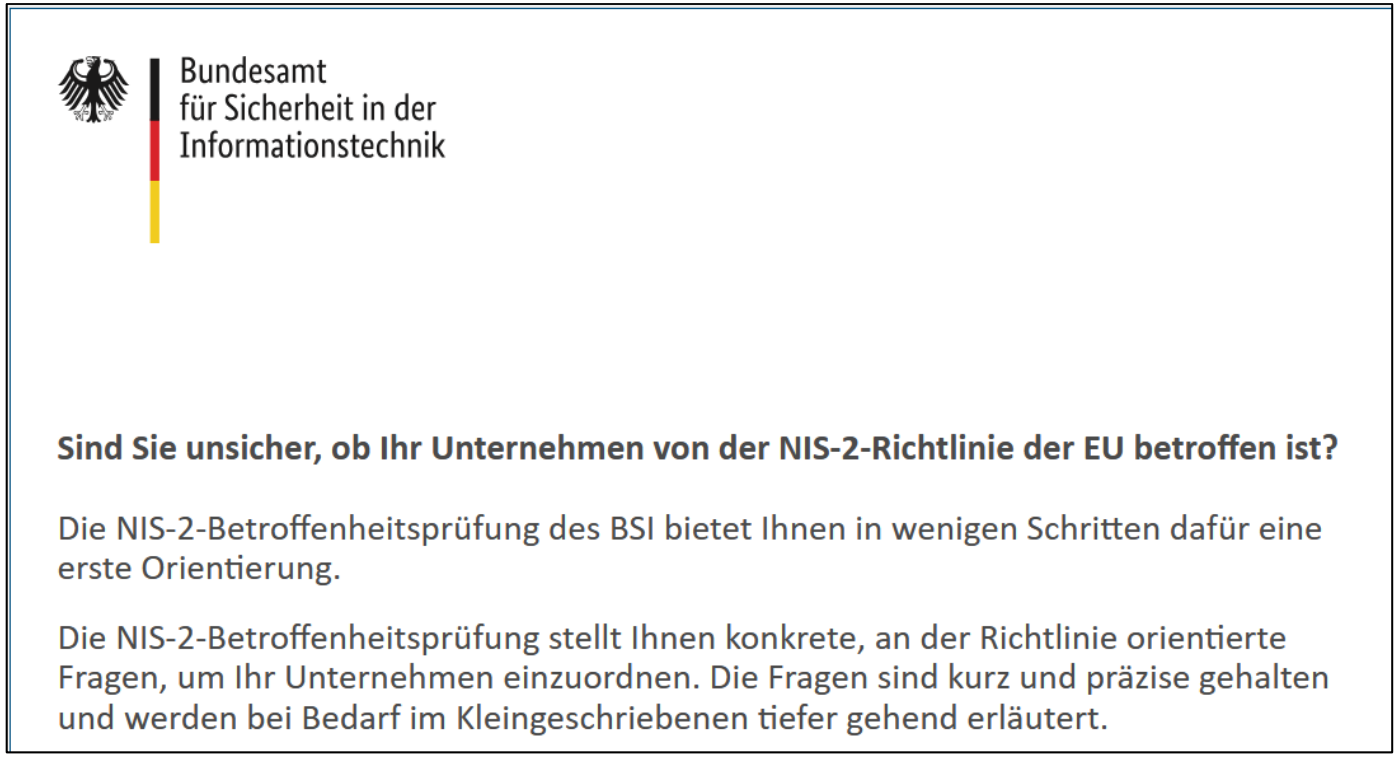
- Für „besonders wichtige" (*essential*) und „wichtige" Einrichtungen (*important entities*) – d.h. im weiteren Sinne Betreiber oder Anbieter von kritischen Infrastrukturen
- Siehe Betroffenheitsprüfung des BSI als zuständige Aufsichtsbehörde
- Sicherheitspflichten:
  - Registrierungspflicht (Meldestelle von BSI und BBK)
  - Risikomanagement
  - Meldepflicht

BBK: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Überblick

3. Sicherheitspflichten: NIS2

Betroffenheitsprüfung



Bundesamt
für Sicherheit in der
Informationstechnik

Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie der EU betroffen ist?

Die NIS-2-Betroffenheitsprüfung des BSI bietet Ihnen in wenigen Schritten dafür eine erste Orientierung.

Die NIS-2-Betroffenheitsprüfung stellt Ihnen konkrete, an der Richtlinie orientierte Fragen, um Ihr Unternehmen einzuordnen. Die Fragen sind kurz und präzise gehalten und werden bei Bedarf im Kleingeschriebenen tiefer gehend erläutert.

https://betroffenheitspruefung-nis-2.bsi.de/

Überblick

3. Sicherheitspflichten: NIS2

Bundesamt für Sicherheit in der Informationstechnik

Ist das Unternehmen Betreiber einer kritischen Anlage?

Gemäß § 2 Absatz 10 BSIG sind Kritische Infrastrukturen im Sinne dieses Gesetzes Einrichtungen, Anlagen oder Teile davon, die den Sektoren

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Siedlungsabfallentsorgung

angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSIG (BSI-Kritisverordnung) näher bestimmt.

Prüfen Sie hierzu bitte auch die entsprechenden Schwellenwerte. Prüfen Sie ebenfalls, ob Sie nicht bereits heute durch die geltenden Regelungen des BSIG zu den Betreibern einer kritischen Anlage zählen.

(Details: www.gesetze-im-internet.de/bsi-kritisv/)

○ Ja
◉ Nein

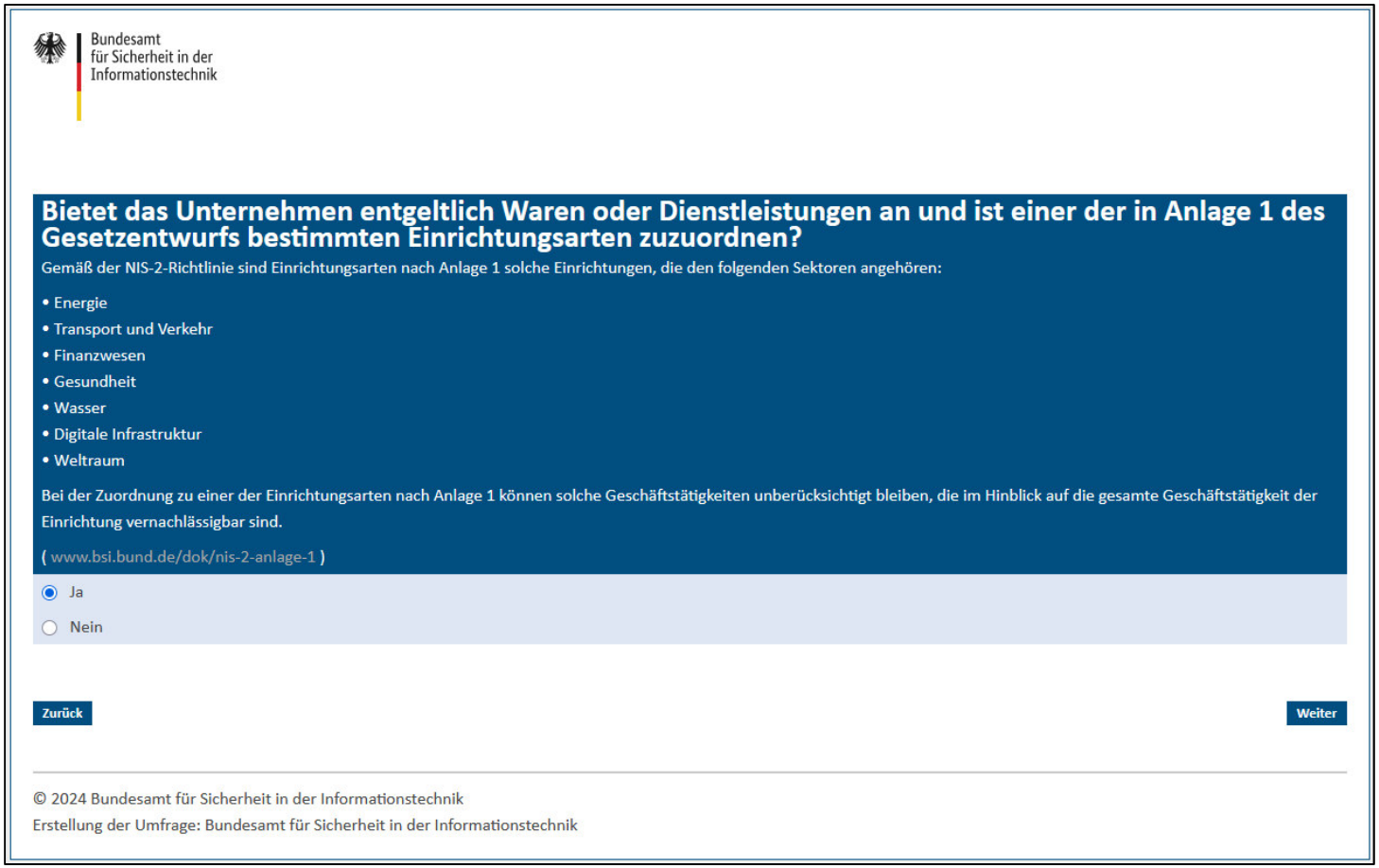
Zurück Weiter

© 2024 Bundesamt für Sicherheit in der Informationstechnik
Erstellung der Umfrage: Bundesamt für Sicherheit in der Informationstechnik

https://betroffenheitspruefung-nis-2.bsi.de/ (Version 2024)

Überblick

3. Sicherheitspflichten: NIS2



Bundesamt für Sicherheit in der Informationstechnik

Bietet das Unternehmen entgeltlich Waren oder Dienstleistungen an und ist einer der in Anlage 1 des Gesetzentwurfs bestimmten Einrichtungsarten zuzuordnen?

Gemäß der NIS-2-Richtlinie sind Einrichtungsarten nach Anlage 1 solche Einrichtungen, die den folgenden Sektoren angehören:

- Energie
- Transport und Verkehr
- Finanzwesen
- Gesundheit
- Wasser
- Digitale Infrastruktur
- Weltraum

Bei der Zuordnung zu einer der Einrichtungsarten nach Anlage 1 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind.

(www.bsi.bund.de/dok/nis-2-anlage-1)

(•) Ja
( ) Nein

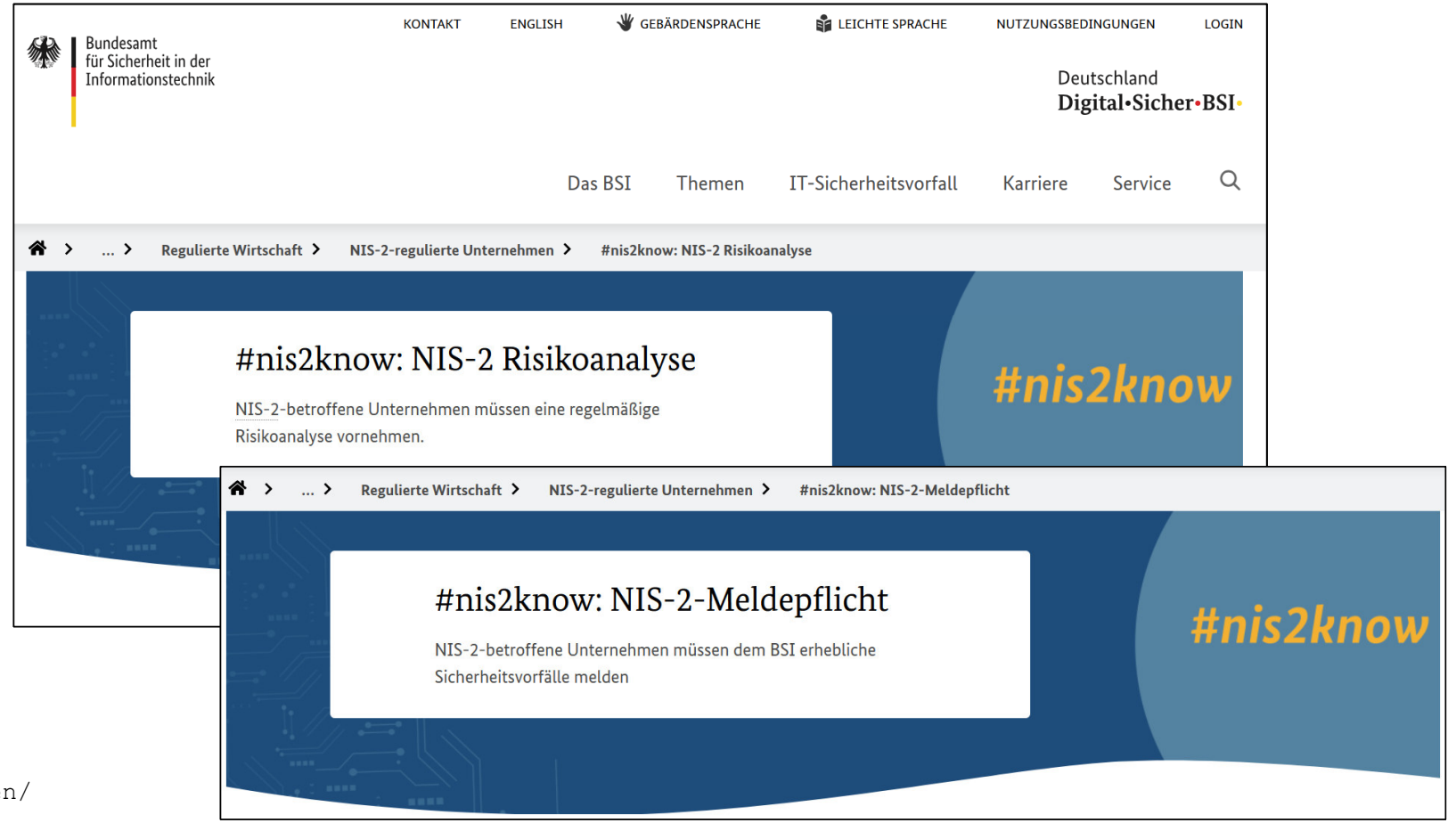
Zurück Weiter

Erstellung der Umfrage: Bundesamt für Sicherheit in der Informationstechnik

https://betroffenheitspruefung-nis-2.bsi.de/ (Version 2024)

Überblick

3. Sicherheitspflichten: NIS2



https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/infopakete_node.html

Überblick

3. Sicherheitspflichten: NIS2 Risikomanagement

- Unternehmen verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen und zu dokumentieren
- Ziel: (a) Störungen der Verfügbarkeit, Integrität und Vertraulichkeit vermeiden und (b) Auswirkungen von Sicherheitsvorfällen möglichst gering halten
- Parameter für Verhältnismäßigkeit: Ausmaß der Risikoexposition, Größe der Einrichtung, Kosten, Eintrittswahrscheinlichkeit, Schwere und Folgen von Sicherheitsvorfällen
- Alle informationstechnischen Systeme, Komponenten und Prozesse, die Unternehmen für die Erbringung ihrer Dienste nutzen, adressieren
- Messlatte: Stand der Technik, einschlägige europäische und internationale Normen, gefahrenübergreifender Ansatz

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/infopakete_node.html

Überblick

3. Sicherheitspflichten: NIS2 Risikomanagement

Risikomanagement-Maßnahmen – mindestens:

- Risikoanalyse
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs (z.B. Backup-Management, Wiederherstellung nach einem Notfall, Krisenmanagement)
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen
- Wirksamkeitsprüfung von Risikomanagementmaßnahmen
- Schulungen und Sensibilisierung zu Cybersicherheit
- Kryptographische Verfahren
- Konzepte für Personalsicherheit (z.B. Zugriffskontrolle)
- Multi-Faktor-Authentifizierung, gesicherte (Notfall-)Kommunikation

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/infopakete_node.html

Überblick

3. Sicherheitspflichten: NIS2 Meldepflicht

Meldung erheblicher Sicherheitsvorfälle an das BSI:

- Beispiel: schwerwiegende Betriebsstörungen der Dienste, die zu finanziellen Verlusten oder Schäden für Dritte führen
- Meldefristen:
  - nach Kenntniserlangung 24 Stunden für die frühe Erstmeldung
  - 72 Stunden für eine Meldung
  - 30 Tage für Abschlussmeldung/Folgemeldung
- Inhalt:
  - Bewertung des Vorfalls inkl. Schweregrad, Auswirkungen und Kompromittierungsindikatoren
  - Kontaktinformationen
- „Das BSI quittiert Meldungen, nimmt ggf. Kontakt auf und verarbeitet Meldungen sanitarisiert in Lageprodukten."

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/infopakete_node.html

Überblick

4. Sicherheitspflichten: CRA

CRA: Sicherheit by Design

Überblick

4. Sicherheitspflichten: CRA

- Cyberresilienz-Verordnung (EU) 2024/2847 (Cyber Resilience Act) als Produktsicherheitsrecht
- Verbesserung der Cybersicherheit für „Produkte mit digitalen Elementen" (≈ vernetzbar mit dem Internet)
- Pflicht des Herstellers zu
  - Cybersicherheit by Design
  - Pflicht zum nachhaltigen Schwachstellenmanagement inkl. Updates
- Für EU-Markt: als Bedingung CRA-Konformität, gekennzeichnet durch CE-Kennzeichen

Icon: Ce Seal Icons by Freepik - Flaticon

4. Sicherheitspflichten: CRA

Erwägungsgrund 78 der DSGVO, Satz 4

(78) […] In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die **Hersteller** der Produkte, Dienste und Anwendungen **ermutigt** werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. […]

Hersteller-Lücke der DSGVO

Bild: Greg Plominski via Pixabay

Überblick

4. Sicherheitspflichten: CRA

Vier Kategorien: aufsteigendes Risiko, zunehmende Pflichten

Standard

- Produkte mit digitalen Elementen, die nicht wichtig und nicht kritisch sind

Wichtig (Klasse I)

- Betriebssysteme
- Browser, Router
- Identitäts- und Passwort-Manager
- Smart-Home-Produkte
- Wearables
- …

Wichtig (Klasse II)

- Hypervisors
- Firewalls, Intrusion Detection
- Manipulationssichere Mikroprozessoren und Mikrocontroller

Kritisch

- Hardware-Geräte mit Sicherheitsboxen
- Smart-Meter-Gateways
- Fortgeschrittene Security-Geräte
- Chipkarten o.Ä. mit Secure Elements

Icons: Document Icons by Awicon – Flaticon

Überblick

4. Sicherheitspflichten: CRA

Vier Kategorien: aufsteigendes Risiko, zunehmende Pflichten

- Produkte mit digitalen Elementen, die nicht wichtig und nicht kritisch sind

Standard

- Betriebssysteme
- Browser, Router
- Identitäts- und Passwort-Manager
- Smart-Home-Produkte
- Wearables
- …

Wichtig (Klasse I)

…tection

(Klasse II)

- Hardware-Geräte mit Sicherheitsboxen
- Smart-Meter-Gateways
- Fortgeschrittene Security-Geräte
- Chipkarten o.Ä. mit Secure Elements

Kritisch

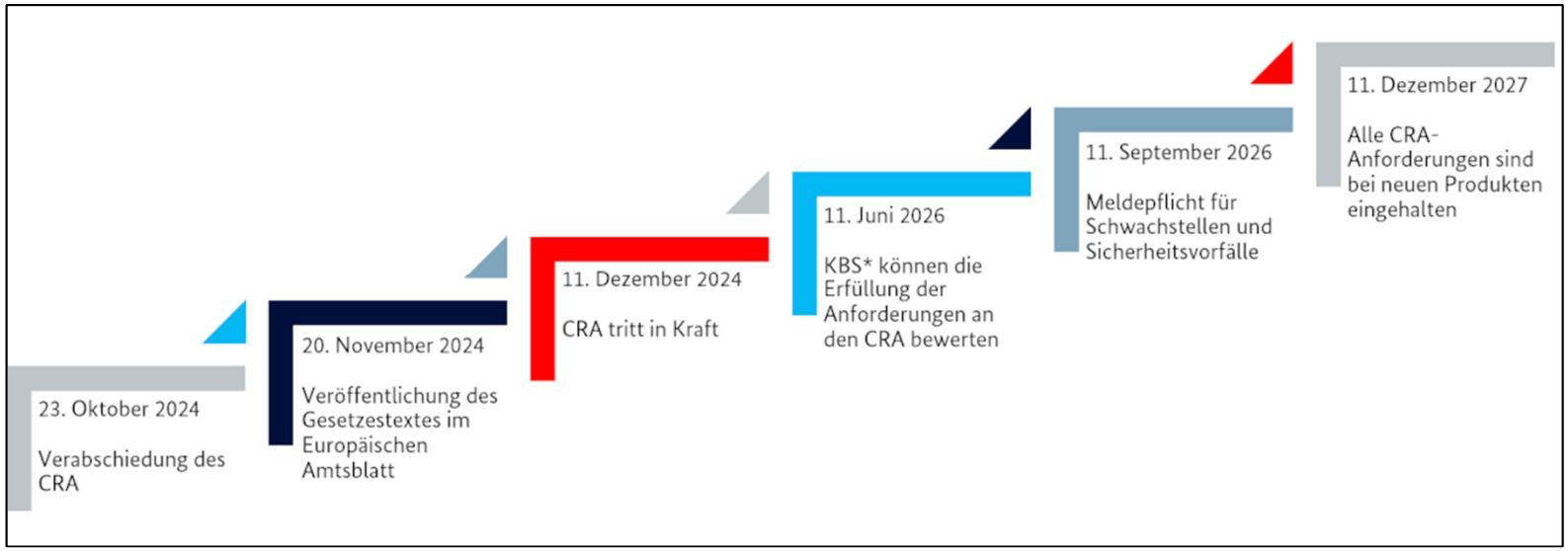
Je größer die Wichtigkeit und Kritikalität der Produkte mit digitalen Elementen, desto anspruchsvoller das Konformitätsbewertungs-verfahren, das durchlaufen werden muss, bevor das Produkt mit einem CE-Kennzeichen versehen und in Verkehr gebracht werden darf.

Icons: Document Icons by Awicon - Flaticon

Überblick

4. Sicherheitspflichten: CRA

Zeitschiene



KBS*: Konformitätsbewertungsstellen

BSI:
https://www.bsi.bund.de/dok/cra

Überblick

4. Sicherheitspflichten: CRA

Anhang I des CRA (Grundlegende Cybersicherheitsanforderungen), Teil 1

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

Überblick

4. Sicherheitspflichten: CRA

Erwägungsgrund 32 des CRA

„[…] Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie die Cybersicherheit im Allgemeinen sind Schlüsselelemente der Verordnung (EU) 2016/679. Durch den Schutz von Verbrauchern und Organisationen vor Cybersicherheitsrisiken sollen die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen auch dazu beitragen, den Schutz personenbezogener Daten und den Schutz der Privatsphäre natürlicher Personen zu verbessern. […]"

Überblick

5. Wie geht‘s zusammen?

Profitiert der Datenschutz – oder wird er zurückgedrängt?

5. Wie geht's zusammen? CRA ↔ DSGVO

Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Art. 24 Abs. 1 DSGVO

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Überblick

5. Wie geht's zusammen?
CRA ↔ DSGVO

CE-Kennzeichen

Info für Nutzende

Technische Dokumentation

SBOM (Software Bill of Materials)

- Basis: Technische Dokumentation des Herstellers
- … über die ganze Lieferkette
- Für Sicherheit wertvoll
- Für Rechenschafts-pflicht des Verantwortlichen wertvoll

Icons: Manual Icons by srip sowie Ce Seal Icons, Document Icons, Product Icons und Source Code Icons by Freepik - Flaticon

Überblick

5. Wie geht‘s zusammen?
CRA ↔ DSGVO

CE-Kennzeichen

Info für Nutzende

Technische Dokumentation

SBOM (Software Bill of Materials)

Art. 31 CRA
Technische Dokumentation

Anhang VII
Inhalt der technischen Dokumentation

u.a. SBOM
(soweit von Bedeutung)

Anhang II
Informationen und Anleitungen für den Nutzer

Icons: Manual Icons by srip sowie Ce Seal Icons, Document Icons, Product Icons und Source Code Icons by Freepik - Flaticon

Überblick

5. Wie geht‘s zusammen?
CRA ↔ DSGVO

CE-Kennzeichen

Anhang I, Teil I Abs. 2 Buchst. e-h CRA

(2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,
[…]
e) … Vertraulichkeit …
f) … Integrität …
g) …
h) … Verfügbarkeit …
[…]

Icons: Manual Icons by srip sowie Ce Seal Icons, Document Icons, Product Icons und Source Code Icons by Freepik - Flaticon

5. Wie geht's zusammen?
CRA ↔ DSGVO

Überblick

1. Motivation
2. Sicherheit und DSGVO
3. Sicherheit und NIS2
4. Sicherheit und CRA

CE-Kennzeichen

Art. 5 Abs. 1 Buchst. c DSGVO

(1) Personenbezogene Daten müssen
[…]
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung")

Anhang I, Teil I Abs. 2 Buchst. g CRA

(2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,
[…]
g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß beschränken („Datenminimierung")

Icon: Ce Seal Icons by Freepik - Flaticon

5. Wie geht‘s zusammen?
NIS2 ↔ DSGVO

Risikomanagement ↔ Datenschutzmanagement

Artikel 32 Absatz 1 DSGVO – Sicherheit der Verarbeitung

(1) […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

[…]

b) die Fähigkeit,
die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

5. Wie geht‘s zusammen?
NIS2 ↔ DSGVO

- Meldepflichten z.B. nach
  - Art. 33 DSGVO: Meldungen der Verletzung des Schutzes personenbezogener Daten
  - § 65 BDSG; §§ in LDSGen
  - § 169 TKG
  - BSIG
  - …
- Nicht vollständig überschneidungsfrei
- Teilweise Unterschiede in Vokabular und Vorgaben (Fristen, Umfang, Umgang mit der Dokumentation …)

Überblick

5. Wie geht's zusammen?
NIS2 ↔ DSGVO

BfDI Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Fachthemen › Basiswissen für die Datenverarbeitung › Digitale Dienste und Messengerdienste › Das Verfahren nach § 169 TKG

Das Verfahren nach § 169 TKG

Durch § 169 TKG werden die TK-Diensteanbieter verpflichtet, die Bundesnetzagentur (BNetzA) und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) sowie unter bestimmten Umständen auch die Betroffenen zu benachrichtigen, wenn der Schutz personenbezogener Daten verletzt worden ist.

Quelle: ©stockpics - stock.adobe.com

Die Meldepflicht nach § 169 TKG unterscheidet sich von der Meldepflicht nach Art. 33 DSGVO, die dann anwendbar ist, wenn das auf den gemeldeten Verstoß anwendbare Recht die DSGVO ist. Weitere Informationen zur Meldepflicht nach Art. 33 DSGVO können dem Artikel „Meldung von Datenschutzverstößen" entnommen werden. Meldungen nach Art. 33 DSGVO können dem BfDI über ein Online-Formular übermittelt werden.

Fachthemen › Telekommunikation › Unternehmenspflichten › Datenschutz

Seit dem 25. Mai 2018 ist in diesem Zusammenhang auch die Datenschutz-Grundverordnung (DSGVO) zu beachten, die eigene Meldepflichten gegenüber der für den Datenschutz zuständigen Aufsichtsbehörde vorsieht (Art. 33 DSGVO). Soweit Unternehmen personenbezogene Daten für die geschäftsmäßige Erbringung von Telekommunikationsdiensten verarbeiten, liegt die Zuständigkeit für Meldungen nach Art. 33 DSGVO ausschließlich bei dem BfDI. Bei Meldungen von Datenschutzverletzungen ist deshalb zu differenzieren, ob es sich um Meldungen nach § 169 TKG handelt, die gegenüber der Bundesnetzagentur und dem BfDI zu melden sind, oder um solche nach Art. 33 DSGVO, die nur dem BfDI zu melden sind.

Die Meldepflicht nach Art. 33 DSGVO ist dann anwendbar, wenn das auf den gemeldeten Verstoß anwendbare Recht die DSGVO ist. Dies ist der Fall bei allgemeinen personenbezogenen Daten natürlicher Personen, insbeson
Umsetzung der ePrivacy-Richtlinie (2
Datenschutzregelungen enthält (vgl. A
Lebenssachverhalt neben der DSGVO
Datenschutzregelungen des TKG verle
werden.

Bundesamt für Sicherheit in der Informationstechnik

Melde- und Informationsportal

Login **Registrierung** **Meldung abgeben** Meldestellenübersicht

Übersicht und Erläuterung der Meldestellen

- Meldestelle Allianz für Cybersicherheit
- Meldestelle Bund (§ 4 BSIG)
- Meldestelle Cyber-Sicherheitsnetzwerk
- Meldestelle KRITIS
  - IT-Sicherheitsgesetz, BSI-Gesetz und BSI-Kritisverordnung
  - Kontaktstelle benennen
  - Meldepflicht
  - Registrierung
  - Registrierung für Behörden / Aufsichtsbehörden/ Zentrale Kontaktstellen der Länder
  - Änderungen an den Registrierungsdaten an das BSI übermitteln
- Meldestelle Luftsicherheit
- Meldestelle Schwachstellen und Sicherheitslücken

Screenshots: BNetzA, BfDI, BSI, …

5. Wie geht's zusammen?
NIS2 ↔ DSGVO

- Meldungen für Sicherheit UND Datenschutz möglich?

  Brandenburg/Ritter: Entbürokratisierung im Datenschutz – Wie die Erfüllung der Meldepflichten nach DSGVO und NIS 2-RL vereinfacht werden könnte, in: EuDIR 4/2025

- Ohnehin Vereinheitlichungsbestrebungen zur Entbürokratisierung
  - Formulare?
  - Portal(e)?
  - Informationen?
  - Abwicklung?
  - Sonderrolle Auftragsverarbeiter

Überblick

5. Wie geht‘s zusammen?

"essential and important entities"

Erw.gr. 121 Sätze 1-2 NIS-2-RL

(121) Die Verarbeitung personenbezogener Daten durch wesentliche und wichtige Einrichtungen in dem zur Gewährleistung der Sicherheit von Netz- und Informationssystemen erforderlichen und verhältnismäßigen Umfang könnte auf der Grundlage als rechtmäßig angesehen werden, dass diese Verarbeitung einer rechtlichen Verpflichtung entspricht, der der Verantwortliche gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 unterliegt.
Die Verarbeitung personenbezogener Daten könnte auch für berechtigte Interessen erforderlich sein, die von wesentlichen und wichtigen Einrichtungen sowie von Anbietern von Sicherheitstechnologien und -diensten, die im Namen dieser Einrichtungen handeln, gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 wahrgenommen werden, auch wenn eine solche Verarbeitung für Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder die freiwillige Mitteilung relevanter Informationen gemäß dieser Richtlinie erforderlich ist.
[…]

Überblick

5. Wie geht‘s zusammen?

Erw.gr. 121 Satz 4 NIS-2-RL

(121) […]

Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden, zentralen Anlaufstellen und CSIRTs könnte eine rechtliche Verpflichtung darstellen oder als für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich angesehen werden, die dem jeweiligen Verantwortlichen gemäß Artikel 6 Absatz 1 Buchstabe c oder e und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 übertragen wurde, oder zur Verfolgung eines berechtigten Interesses der wesentlichen und wichtigen Einrichtungen gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung.

[…]

Überblick

5. Wie geht‘s zusammen?

Erw.gr. 121 Satz 5 NIS-2-RL

(121) […]

Darüber hinaus könnten im nationalen Recht Vorschriften festgelegt werden, die es den zuständigen Behörden, zentralen Anlaufstellen und CSIRTs ermöglichen, besondere Kategorien personenbezogener Daten gemäß Artikel 9 der Verordnung (EU) 2016/679 zu verarbeiten, soweit dies zur Gewährleistung der Sicherheit der Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen erforderlich und verhältnismäßig ist, insbesondere indem geeignete und besondere Maßnahmen zum Schutz der Grundrechte und Interessen natürlicher Personen vorgesehen werden, einschließlich technischer Beschränkungen für die Weiterverwendung solcher Daten und die Anwendung modernster Sicherheits- und Datenschutzvorkehrungen wie Pseudonymisierung oder Verschlüsselung, wenn die Anonymisierung den verfolgten Zweck erheblich beeinträchtigen könnte.

5. Wie geht‘s zusammen?
NIS2 ↔ DSGVO

"essential and important entities"

§ 30 BSIG-neu – Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen […] zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informations-technischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. […] Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungs-kosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. […] ist […] zu dokumentieren […]

Überblick

5. Wie geht's zusammen?

Prüffragen:

- Bin ich Adressat der Regelungen im Cybersicherheitsrecht? Inwieweit?
- Was verändert sich bei den eingesetzten Produkten (CRA) und Dienstleistern (NIS2)? Ggf. nachfragen! Technische Dokumentation?
- Hat dies Auswirkungen auf die eigene Verarbeitung personenbezogener Daten? Neue Risikoeinschätzung! DSFA?

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist

Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck" an.

8	Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen

- Immer (auch wenn sich nichts verändert): Überprüfung der eigenen TOMs! Erforderlichkeit/Verhältnismäßigkeit? Stimmt die Rechtsgrundlage noch?

Überblick

Exkurs DSGVO ⇆ Sicherheit

Exkurs: Is the cure worse than the disease?

- Was, wenn eine Sicherheitsmaßnahme selbst ein (Datenschutz-)Risiko darstellt?
- Bei Verarbeitung personenbezogener Daten: DSGVO (+BDSG/LDSG usw.)
- Z.B. Protokollierung, Beschäftigtenüberwachung, Einsatz von Biometrie, Virenscan

Bild: Sabrina Belle via Pixabay

Überblick

Beispiel: Virenscan

Bundesamt für Sicherheit in der Informationstechnik

OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.4: Schutz vor Schadprogrammen

Cloud-Dienste zur Verbesserung der Detektionsleistung der Virenschutzprogramme SOLLTEN genutzt werden. Falls Cloud-Funktionen solcher Produkte verwendet werden, MUSS sichergestellt werden, dass dies nicht im Widerspruch zum Daten- oder Geheimschutz steht. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung die Möglichkeit bieten, auch komprimierte Daten nach Schadprogrammen zu durchsuchen.

OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen (B)

Das Virenschutzprogramm MUSS für seine Einsatzumgebung geeignet konfiguriert werden. Die Erkennungsleistung SOLLTE dabei im Vordergrund stehen, sofern nicht Datenschutz- oder Leistungsgründe im jeweiligen Einzelfall dagegen sprechen. Wenn sicherheitsrelevante Funktionen des Virenschutzprogramms nicht genutzt werden, SOLLTE dies begründet und dokumentiert werden. Bei Schutzprogrammen, die speziell für die Desktop-Virtualisierung optimiert sind, SOLLTE nachvollziehbar dokumentiert sein, ob auf bestimmte Detektionsverfahren zugunsten der Leistung verzichtet wird. Es MUSS sichergestellt werden, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_1_4_Schutz_vor_Schadprogrammen_Edition_2022.pdf

Überblick

Beispiel: Virenscan

ars TECHNICA

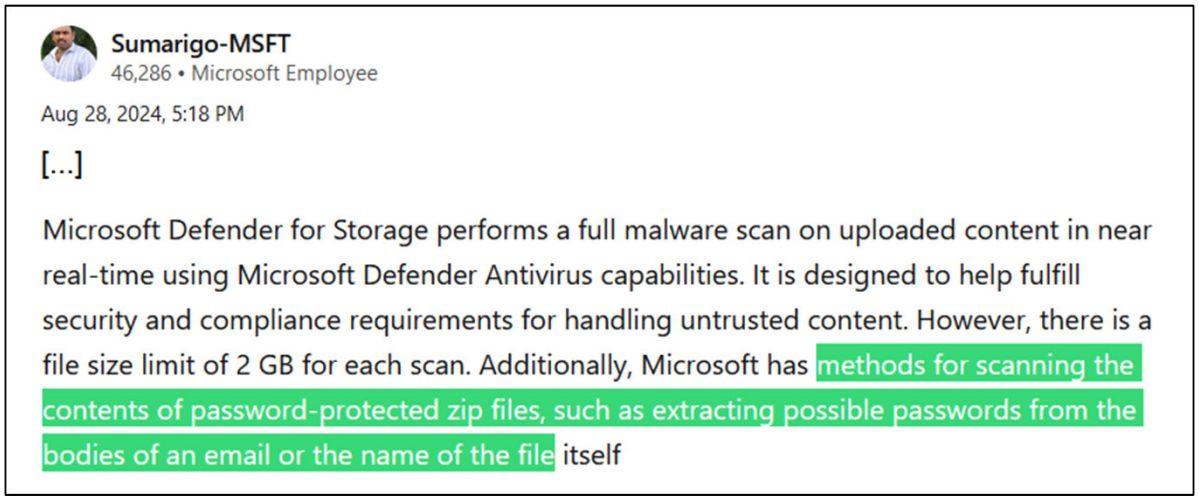
PRYING EYES —

Microsoft is scanning the inside of password-protected zip files for malware

If you think a password prevents scanning in the cloud, think again.

DAN GOODIN - 5/16/2023, 2:15 AM

https://arstechnica.com/information-technology/2023/05/microsoft-is-scanning-the-inside-of-password-protected-zip-files-for-malware/



Sumarigo-MSFT
46,286 • Microsoft Employee

Aug 28, 2024, 5:18 PM

[...]

Microsoft Defender for Storage performs a full malware scan on uploaded content in near real-time using Microsoft Defender Antivirus capabilities. It is designed to help fulfill security and compliance requirements for handling untrusted content. However, there is a file size limit of 2 GB for each scan. Additionally, Microsoft has methods for scanning the contents of password-protected zip files, such as extracting possible passwords from the bodies of an email or the name of the file itself

https://learn.microsoft.com/en-us/answers/questions/2007466/are-costs-incurred-when-attempting-to-scan-passwor

Überblick

Beispiel: Virenscan

ars TECHNICA

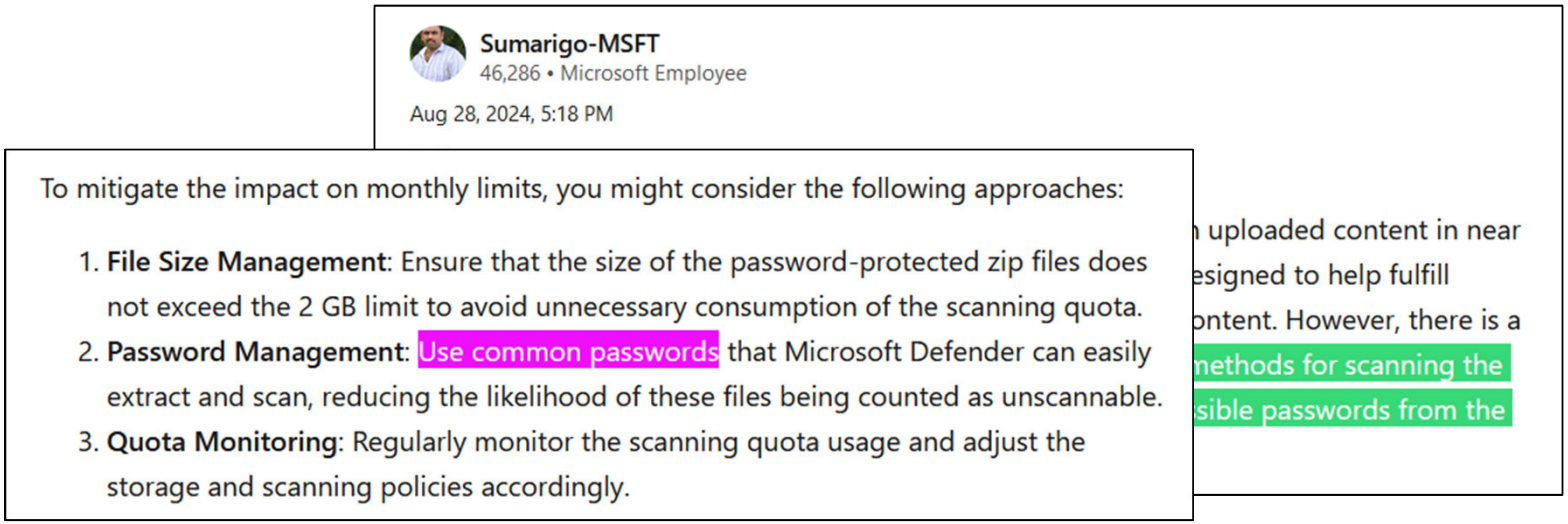
PRYING EYES —

Microsoft is scanning the inside of password-protected zip files for malware

If you think a password prevents scanning in the cloud, think again.

DAN GOODIN - 5/16/2023, 2:15 AM

https://arstechnica.com/information-technology/2023/05/microsoft-is-scanning-the-inside-of-password-protected-zip-files-for-malware/



Sumarigo-MSFT
46,286 • Microsoft Employee
Aug 28, 2024, 5:18 PM

To mitigate the impact on monthly limits, you might consider the following approaches:

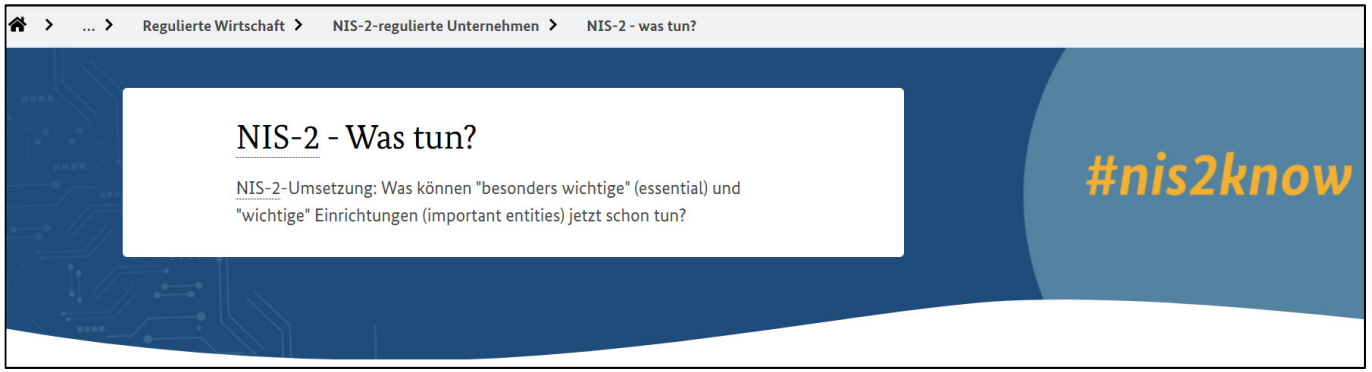
1. **File Size Management**: Ensure that the size of the password-protected zip files does not exceed the 2 GB limit to avoid unnecessary consumption of the scanning quota.
2. **Password Management**: Use common passwords that Microsoft Defender can easily extract and scan, reducing the likelihood of these files being counted as unscannable.
3. **Quota Monitoring**: Regularly monitor the scanning quota usage and adjust the storage and scanning policies accordingly.

uploaded content in near
esigned to help fulfill
ontent. However, there is a
methods for scanning the
sible passwords from the

https://learn.microsoft.com/en-us/answers/questions/2007466/are-costs-incurred-when-attempting-to-scan-passwor

Überblick

5. Wie geht's zusammen? (BSI zu NIS2)



1. Benennen Sie zuständige Personen
2. Übernehmen Sie als Leitung die Verantwortung
3. Machen Sie eine (erste) Bestandsaufnahme Ihrer Sicherheit
4. Verbessern Sie Ihre Informationssicherheit kontinuierlich
5. Bereiten Sie sich auf die Meldepflicht und den Empfang von Warnungen und Lageberichten vor

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun_node.html

6. Fazit und Ausblick

- Gute Nachricht: ähnliche Definitionen von Sicherheit
- Verpflichtung nach
  - DSGVO:
    - Trifft den Verantwortlichen sowie den Auftragsverarbeiter
    - Bezug: Verarbeitung personenbezogener Daten
  - NIS2:
    - Trifft den Betreiber und den Anbieter
    - Bezug: Kritische Infrastrukturen (Systeme / Dienstleistungen)
  - CRA:
    - Trifft Hersteller und Händler/Einführer
    - Bezug: Produkte mit digitalen Elementen (ggf. wichtig oder kritisch)

Überblick

6. Fazit und Ausblick

- Datenschutz braucht Sicherheit
- NIS2: Sicherheit für KRITIS++
- CRA: Sicherheit by Design
- Profitiert der Datenschutz – oder wird er zurückgedrängt?
  - Toppt Sicherheit alles?
  - Welche Rolle spielen die Datenschutz-beauftragten der Organisation?
  - Feld für Zertifizierung? Modular?

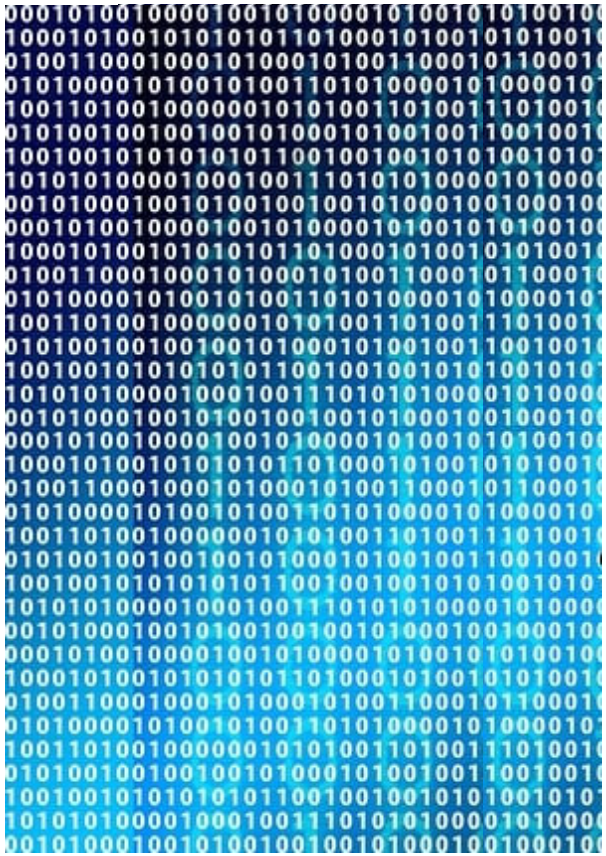


Bild: kalhh via Pixabay

Überblick

6. Fazit und Ausblick

- Gegenläufige Vorgaben oder Interpretationen nicht ausgeschlossen
  - *„unberührt"* reicht nicht
  - Best-Practice von Aufsichtsbehörden (DSGVO, NIS2, CRA, KI-VO, …) nötig
- Gesamtschau der Digitalrechtsakte (technische Dokumentation, Herstellerverantwortung, Haftung) → ganzheitlich Risikobeherrschung effektiv, nachweisbar und dauerhaft
- Mehr Digitale Souveränität nötig

Bild: kalhh via Pixabay

Überblick

6. Material

- AG KRITIS: https://ag.kritis.info/
- BSI: Betroffenheitsprüfung NIS-2, https://betroffenheitspruefung-nis-2.bsi.de/
- BSI: NIS-2 – Was tun?, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun_node.html
- DSK: Kriterien für Souveräne Clouds, 2023, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf