SIELING
RECHTSANWALTSKANZLEI


Foto: Flemming Holm

Rechtsanwältin Carola Sieling

Fachanwältin für Informationstechnologierecht
Lehrbeauftragte
Datenschutzbeauftragte
IT-Sicherheitsbeauftragte (IT-SiBe/CISO)

kanzlei-sieling.de
technologiewerft.de

Cyberangriff in meiner Organisation - was ist zu tun?

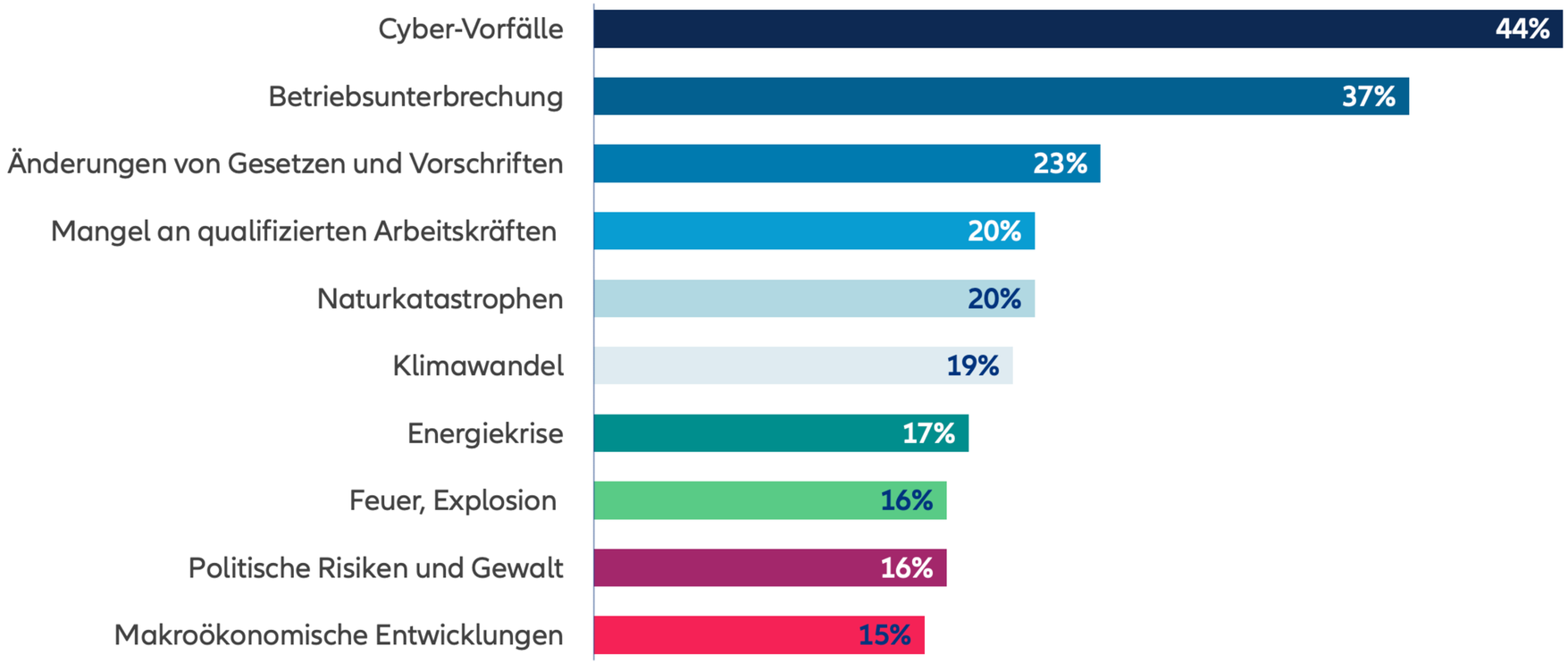
Überblick

- Welche Bedrohungen existieren?
- Abwehr von Cyberangriffen
  - Säule 1: Technik
  - Säule 2: Compliance
  - Säule 3: Management
- Handlungsempfehlungen

Bedrohungslage

Die Top 10 Geschäftsrisiken in Deutschland in 2024

Für weitere Details klicken Sie auf die Balken im Diagramm



Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Umfrageantworten von 3.069 Befragten ausgewählt wurde. Alle Befragten konnten bis zu drei Risiken pro Branche auswählen, weshalb sich die Zahlen nicht auf 100 % summieren. Quelle: Allianz Commercial

Quelle: Januar 2024, Allianz Commercial

Bedrohungslage

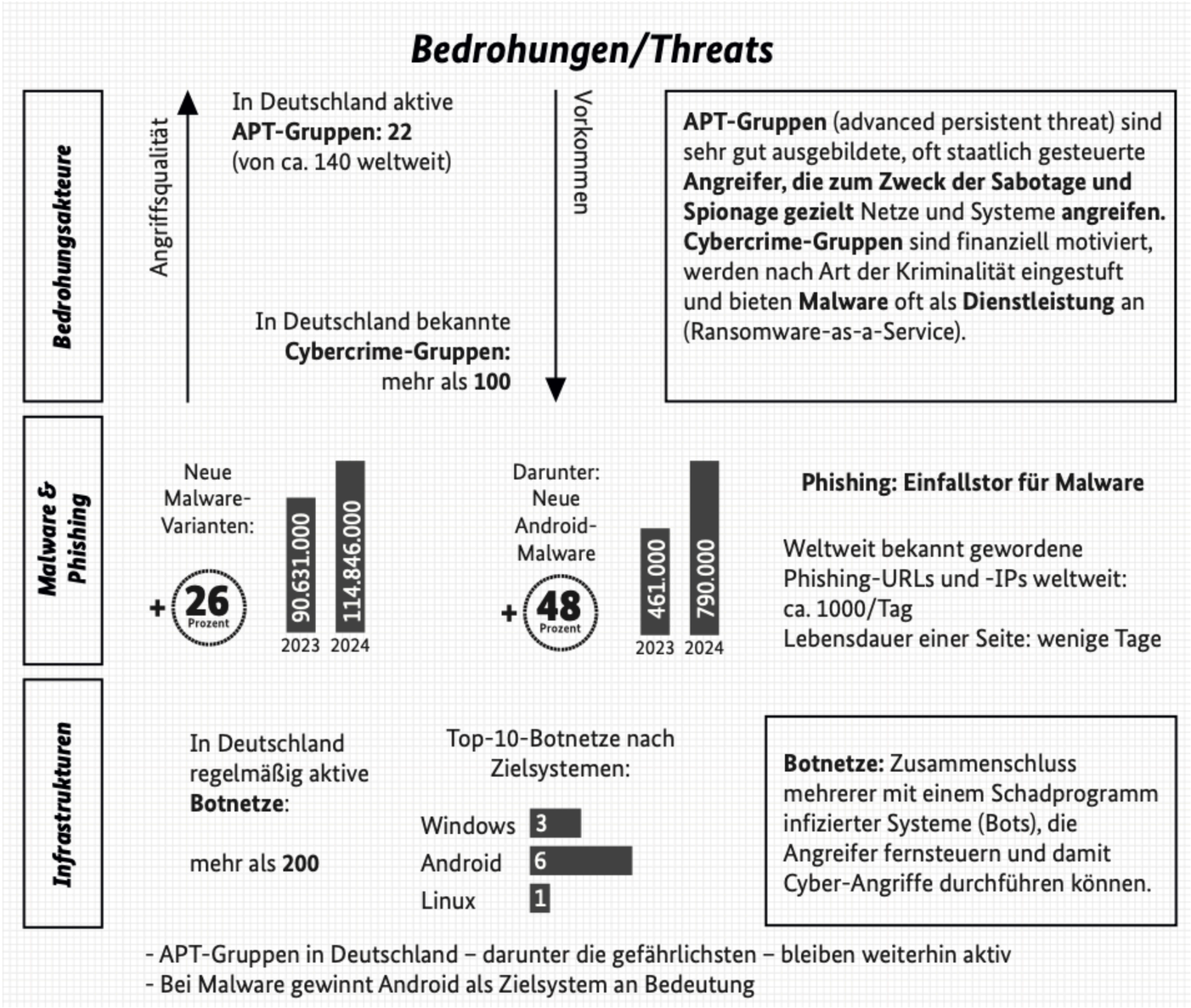
Die Lage der IT-Sicherheit in Deutschland 2024

Datum 12.11.2024

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich einen umfassenden Überblick über die Bedrohungen im Cyberraum. Im Bericht für das Jahr 2024 kommt die Cybersicherheitsbehörde des Bundes zur Einschätzung: Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend.

Quelle: BSI - Bericht zur Lage der IT-Sicherheit 2024

Bedrohungslage



Quelle: BSI - Bericht zur Lage der IT-Sicherheit 2024

Bedrohungslage

Angriffsfläche/Attack Surface

Angriffsfläche

Eine Angriffsfläche besteht aus erreichbaren IT-Systemen wie aktiven IP-Adressen und E-Mail-Adressen. Software auf diesen Systemen kann Schwachstellen aufweisen, die zum Angriff ausgenutzt werden können. Besonders gefährlich: Zero-Day-Verwundbarkeiten, die sofort behoben werden müssen.

Beispiel: Angriffsfläche der Bundesverwaltung:

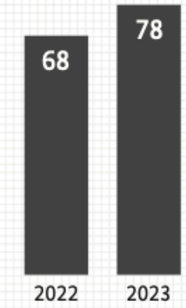
Aus dem Internet erreichbare IP-Adressen: 4500

Aktive E-Mail-Adressen: 639.000

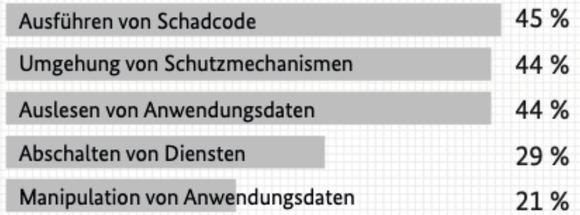
Schwachstellen

Global bekannt gewordene **Schwachstellen** am Tag:

+ 14 Prozent



Global bekannt gewordene **Schwachstellen 2023** nach möglicher **Angriffsart** (Mehrfachnennungen möglich)



Beispiele

Ein System, viele Betroffene: - mind. 37 % der 45.000 Exchange-Server in Deutschland verwundbar[1]
- Zero-Day Schwachstellen bei verschiedenen Ivanti-Produkten ausgenutzt[2]

Android-Geräte in Deutschland

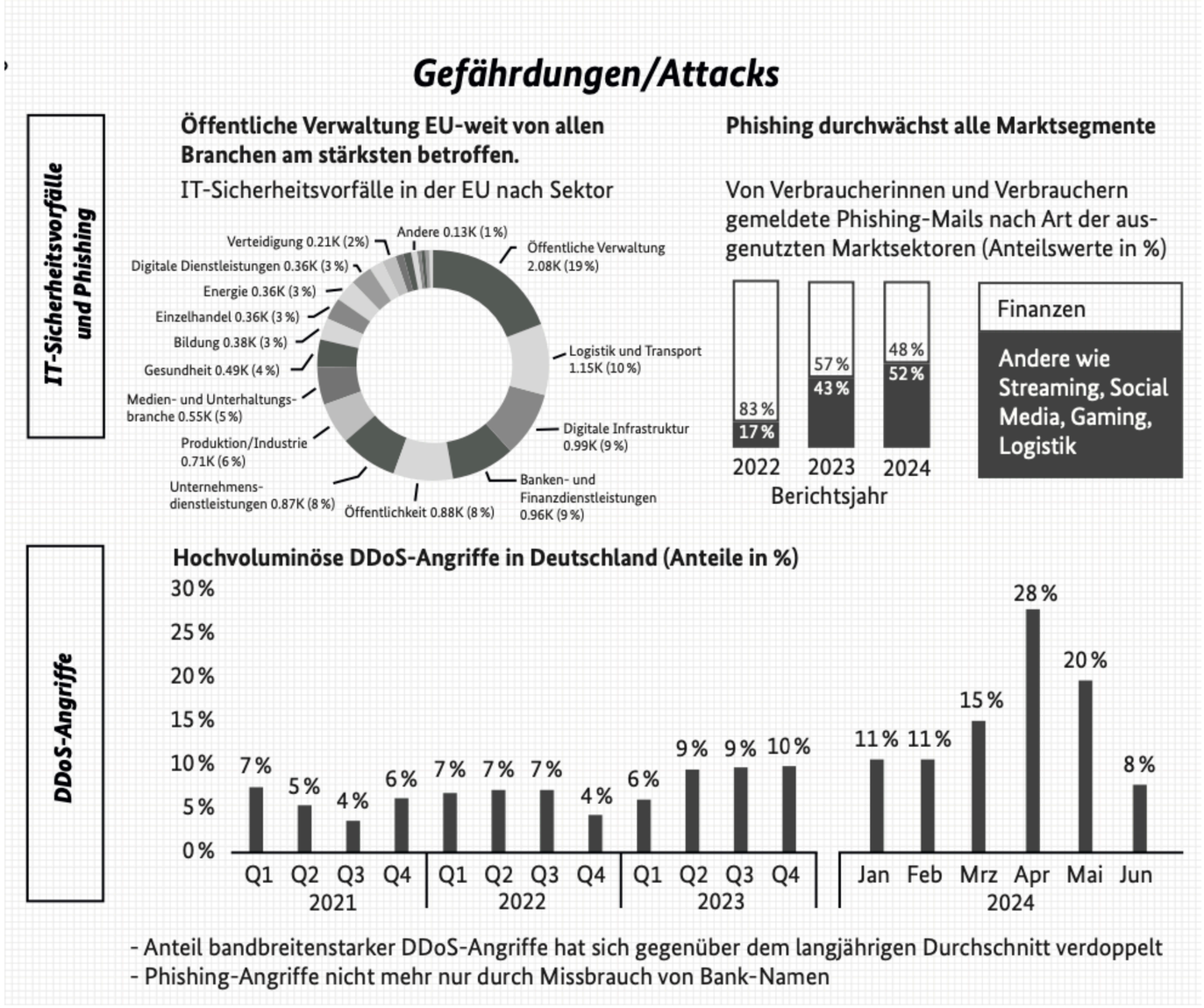
25 Prozent der Geräte erhalten keine Sicherheitsupdates mehr und sind definitiv verwundbar.

Diebstahl von Zugangsdaten zu
- Multifaktor-Authentifizierung
- Passwortverwaltung
- Online-Banking
- Firmennetzwerk

- Schwachstellen nehmen seit Jahren kontinuierlich zu
- Vielfältige Angriffstechniken treffen auf einen digitalisierten Alltag – alle können angegriffen werden

Quelle: BSI - Bericht zur Lage der IT-Sicherheit 2024

Bedrohungslage



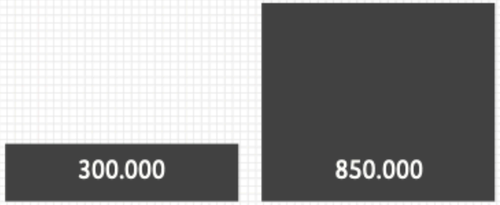
Quelle: BSI - Bericht zur Lage der IT-Sicherheit 2024

Bedrohungslage

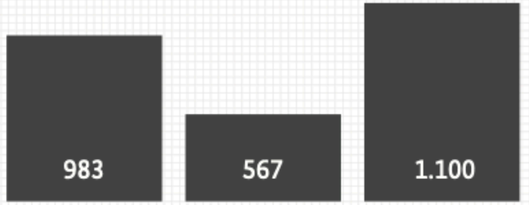
Schadwirkung/Impact

Ransomware

Lösegeld pro Fall
(in US-Dollar, ca. Durchschnitt):



Von Ransomware-Gruppen erbeutete
Lösegelder weltweit (in US-Dollar, Mio.):



KRITIS

Störungen bei KRITIS-Betreibern 490

Beispiele

Ransomware-Angriff auf kommunalen IT-Dienstleister im Oktober 2023

Betroffene Kommunen:	72
Betroffene Arbeitsplätze:	rund 20.000
Betroff. Einwohnerinnen und Einwohner:	rund 1,7 Mio.

Geschätzter Schaden durch Systemausfälle eines **fehlerhaftes Update** in der Software Crowdstrike Falcon:
> 8,5 Mio. Geräte > 5 Milliarden Dollar

VerbraucherInnen

Top-3-Schäden für Verbraucherinnen und Verbraucher bei IT-Sicherheitsvorfällen und Cybercrime (%)

Vertrauensverlust in den Onlinedienst	30
Finanzieller Schaden	26
Zeitlicher Schaden	24

- Exfiltrierte Daten wesentlich mehr wert als verschlüsselte → Fähigkeit zur Prävention muss gestärkt werden
- Schäden im Milliardenbereich, unvorhergesehene Ereignisse, menschliches Versagen → Fähigkeit zur Vorfallsbewältigung muss gestärkt werden

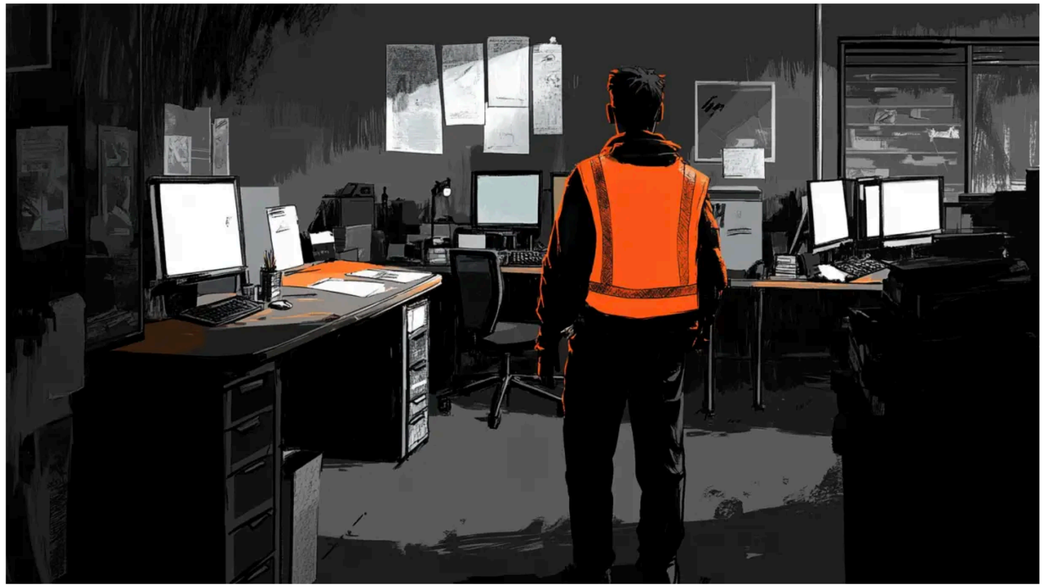
Quelle: BSI - Bericht zur Lage der IT-Sicherheit 2024

Bedrohungslage

Missing Link: Wie ein Unternehmen bei einem Cyberangriff die Kontrolle verlor

Eigentlich fühlt sich der IT-Chef recht sicher. Bis Hacker mitten am Tag in die Firma marschieren – und unbehelligt wieder raus. Die Beute: volle Kontrolle.

368



Auf einen physischen Angriff war das Unternehmen nicht vorbereitet. (Bild: heise online/Midjourney)

03.11.2024, 07:15 Uhr Lesezeit: 11 Min.

Von Anika Reckeweg

Quelle: Heise

Säule 1: Technik

- Back-Up Konzept
- Verschlüsselung
- Netzwerksicherheit
- SIEM etc.

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

Technische und organisatorische Maßnahmen

2023

https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Säule 2: Compliance

- **DSGVO**
- NIS2 / DORA / Kritische Infrastrukturen / CRA
- Geschäftsgeheimnisgesetz
- DIN-ISO - Zertifizierung

Säule 2: Compliance

Art. 32 DSGVO

Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen 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:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

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

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Grundlagen - DSGVO

Was ist eine „Datenpanne“?

Art. 4 Nr. 12 DSGVO: Verletzung des Schutzes personenbezogener Daten

(a) eine Verletzung der Sicherheit,

(b) die, ob unbeabsichtigt oder unrechtmäßig,

(c) zur Vernichtung, zum Verlust oder zur Veränderung oder zur unbefugten Offenlegung von bzw. unbefugten Zugang zu

(d) personenbezogenen Daten führt,

(e) die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Grundlagen

Beispiele für Datenpannen

- Fehlversand von personenbezogenen Daten
- Hackerangriff
- Diebstahl / Verlust von Datenträgern (Rechner, Smartphones, USB-Sticks)
- unbefugtes Weitergeben durch Mitarbeiter – gleichgültig, ob bewusst oder unbewusst
- Offenlegung von Daten (offener Mailverteiler)
- Stromausfall
- Nutzung unzulässiger Kanäle für den Austausch personenbezogener Daten

Grundlagen

Meldepflicht an Aufsichtsbehörde gem. Art. 33 DSGVO, EG: 85-88

Wer? Verantwortliche Stelle

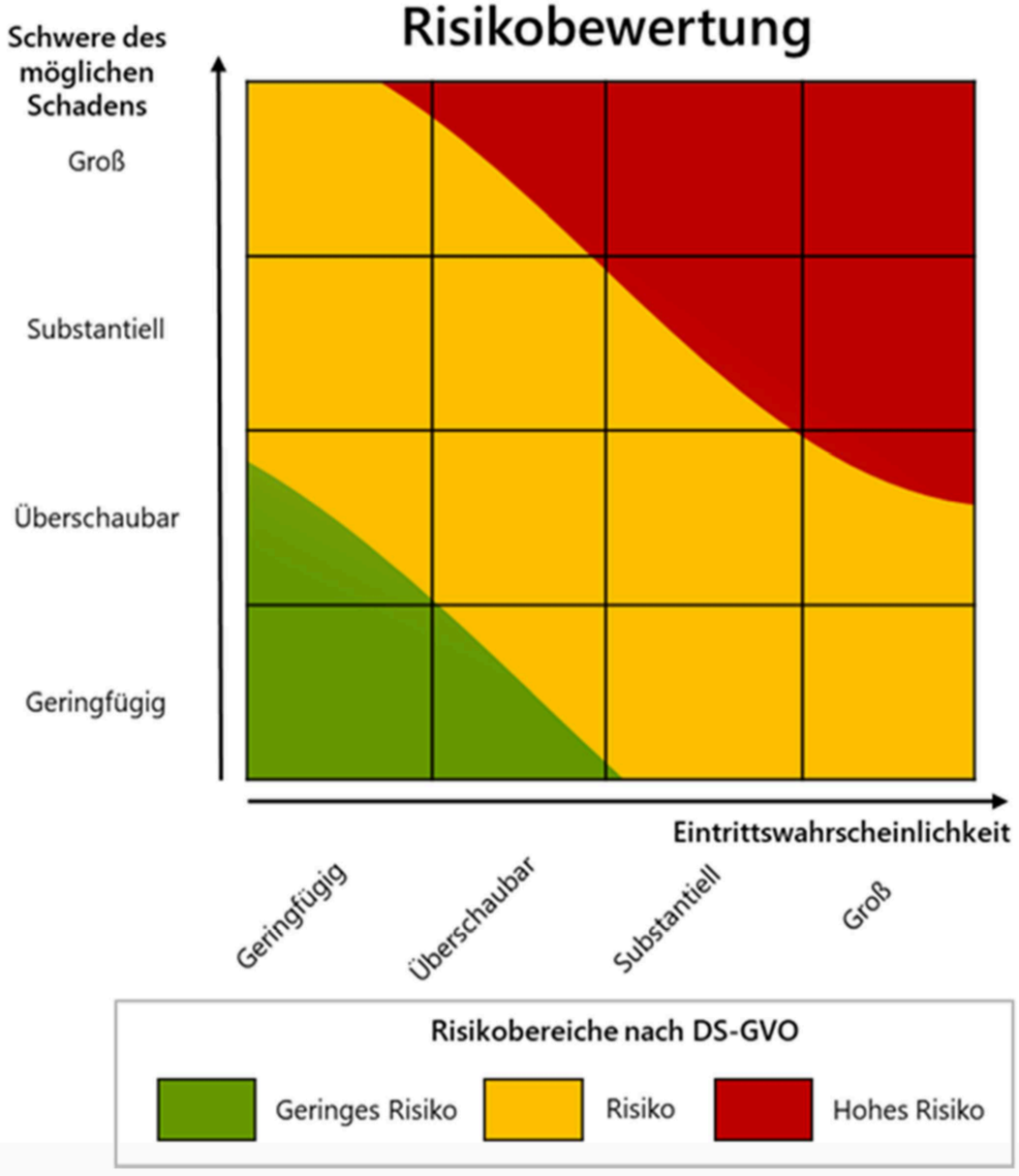
Wann? nicht, wenn voraussichtlich nicht zu einem Risiko für Rechte und Freiheiten natürlicher Personen führt

DSGVO unterscheidet: „geringes Risiko“, „Risiko“, „hohes Risiko“

Zur Risikobeurteilung sind möglichst die beschriebenen Phasen zu durchlaufen:

1. Risikoidentifikation
2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden
3. Zuordnung zu Risikoabstufungen

Grundlagen



Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.

Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.

Quelle: Kurzpapier des DSK

Grundlagen

Meldepflicht an Aufsichtsbehörde: Art. 33 DSGVO

Aufzählung möglicher Risiken: ErwG 75

- Materielle Schäden, Immaterielle Schäden, Physische Schäden, schließlich alle negativen Folgen

- …, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt

- unverzüglich, möglichst innerhalb von 72 Stunden nach Bekanntwerden

- Inhalt

Grundlagen

Dokumentationspflicht

Art. 33 Absatz 5 DSGVO

„Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.“

Grundlagen

Auftragsverarbeitung

Nach Artikel 28 Absatz 3 Buchstabe f DSGVO muss ein Auftragsverarbeitungsvertrag vorsehen, dass der Auftragsverarbeiter

„unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt“

Nach Artikel 33 Absatz 2 DSGVO hat der eingesetzte Auftragsverarbeiter eine ihm bekannt gewordene Verletzung des Schutzes der personenbezogenen Daten, die er im Auftrag des Verantwortlichen verarbeitetet, „unverzüglich“ an den Verantwortlichen zu melden.

Grundlagen

Meldepflicht aus Art. 34 DSGVO

- Meldung zusätzlich an Betroffenen, wenn ein hohes Risiko besteht.
- Ausnahmen: Art. 34 Abs. 3 DSGVO

Grundlagen

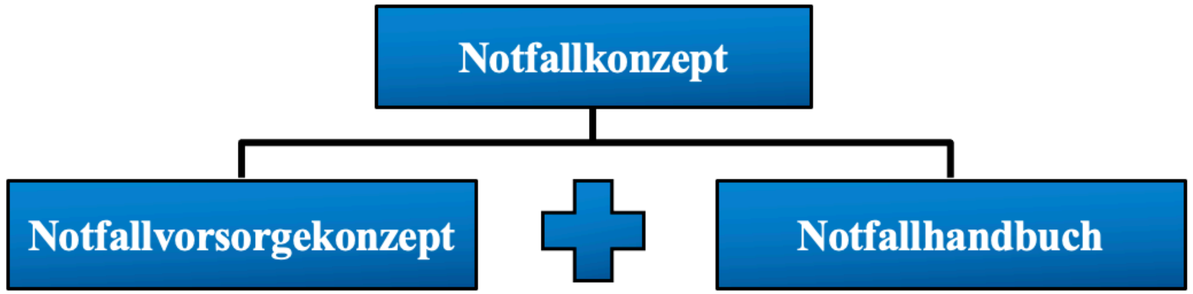
Sanktionen bei Verletzungen der Meldepflicht

- Bußgelder gem. Art. 83 Abs. 4 a DSGVO
- Maßnahmen gem. Art. 58 DSGVO
- Schadenersatzanspruch gem. Art. 83 DSGVO

Säule 3: Management

- Wie können Cyberangriffe abgewehrt werden?
- Welche Prozesse sind bei einem Cyberangriff / Datenpanne wichtig?
- Wie sollten Mitarbeitende/ Geschäftsleitung / IT / DSB reagieren?
- Wie sehen die Prozesse aus?
  - Incident Response Prozess und Notfallplan, BCM, Risikomanagement Business-Impact Analyse, Back-Up
  - **VORAB** Durchspielen von gängigen Angriffsmethoden
  - **VORAB** Meldewege / Prozesse / Richtlinien intern schaffen
  - **VORAB** und r**egelmäßig** Schulungen durchführen

Säule 3: Management



- Das **Notfallvorsorgekonzept** beschäftigt sich mit den Aspekten, die präventiv umzusetzen sind, um Notfälle zu verhindern und/oder Schäden zu begrenzen zu können.
- Es wird ergänzt durch das **Notfallhandbuch**, das u.a. Handlungsanweisungen und Kontaktinformationen für Notfälle beinhaltet.

Quelle: BSI Notfallvorsorgekonzept

UMFRAGE

Zu unregelmäßig

Angebot an Cybersicherheitsschulungen und -trainings im Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

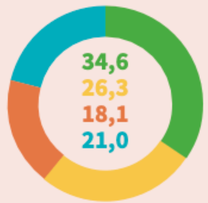
Bietet Ihr Unternehmen für alle Mitarbeiterinnen und Mitarbeiter (Online-)Schulungen / Veranstaltungen / Trainings rund um das Thema Cybersicherheit an?

ja, regelmäßig | ja, aber eher unregelmäßig | nein, nur für ausgewählte Abteilungen | Nein, ich habe noch nie von so einem Angebot in unserem Unternehmen gehört.

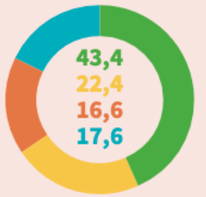
insgesamt

nach Unternehmensgröße

100 bis 249 Mitarbeiterinnen und Mitarbeiter



250 bis 999 Mitarbeiterinnen und Mitarbeiter



1000 und mehr Mitarbeiterinnen und Mitarbeiter

Quelle: https://b1.de/cybersicherheit_2024

Handlungsempfehlungen

- **Meldung des Angriffs unverzüglich entsprechend der vorgegebenen Meldekette (Erstkontakt)**

Hier ist unbedingt auf Schnelligkeit und unverzüglich zu achten. Schnelles Handeln ist Grundlage dafür, dass weitere Schaden vermieden werden kann.

Wie kann das sichergestellt werden?

- Regelmäßige Schulung
- BSI IT-Notfallkarte

Handlungsempfehlungen

- **Meldepflichtigkeit intern und extern prüfen**
  - Vorgesetzte / Geschäftsleitung / Datenschutzbeauftragter
  - Versicherung, soweit vorhanden
  - Datenschutzrechtliche Aufsichtsbehörde (Art. 33 DSGVO)
  - Betroffene (Art. 34 DSGVO)
  - BSI (§ 8b Absatz 4 BSIG betrifft Betreiber Kritischer Infrastrukturen)
  - Bundesnetzagentur: gemäß § 168 TKG (Art. 73 KI-VO)

Handlungsempfehlungen

- **Sofortige Eindämmung / erste Maßnahmen treffen**

Beispielsweise betroffenen Systeme vom Internet oder vom Internet Netzwerk trennen, um weiteren Zugriff zu verhindern und die Verbreitung von Schadsoftware zu stoppen.

Unbedingt auf Anweisung innerhalb der Meldekette warten.

Dauerhaft im Prozess, je nach Kenntnislage, sollten Maßnahmen zur Schadensbegrenzung ergriffen werden,

- Maßnahmen zu Wiederherstellung der Daten
- zur Verhinderung des Datenmissbrauchs

Handlungsempfehlungen

- **Untersuchung / Hinzuziehung von Cybersecurity-Spezialisten**

Es ist es ratsam, vorab eine Zusammenarbeit mit Cybersecurity-Spezialisten sicherzustellen, damit im Ernstfall auch ein Partner, der im besten Falle die Infrastruktur kennt, unterstützen kann und **erreichbar** ist.

Ermitteln Sie die Ursache, den Umfang, den Ablauf; angriffsspezialisierte Teams wie Computer-Emergency-Response-Teams (CERT) oder Computer-Security-Incident-Response-Teams (CSIRT) können dabei helfen.

Handlungsempfehlungen

- Strafanzeige erstatten

Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen

Im Falle eines Cybercrime-Vorfalles ist ein entschlossenes und schnelles Handeln erforderlich!

Die Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft stehen Ihnen als Unternehmen dabei als kompetenter und vertrauensvoller Partner zur Verfügung, sowohl für Informationen zur Vermeidung von Cybercrime-Angriffen als auch im Falle von Cybercrime-Straftaten gegen Ihr Unternehmen!

Bitte beachten Sie, dass die nachfolgenden Kontaktdaten NUR für Wirtschaftsunternehmen gelten. Privatpersonen wenden sich bitte an die Onlinewachen der Polizeien der Länder →.

Handlungsempfehlungen

- **Passen Sie das Schutzniveau ihrer Systeme an**

Stellen Sie sicher, dass ihr System auf einen sicheren Stand zurückgesetzt (Wiederanlauf-,Wiederherstellungspläne) und entsprechend abgesichert wird, um zukünftige, insbesondere ähnliche Angriffe zu verhindern.

Handlungsempfehlungen

- **Dokumentation des Vorfalls und der Maßnahmen**

Stellen Sie dauerhaft sicher, dass ein Cyberangriff von Anfang bis Ende ordentlich dokumentiert wird, ständig aktualisiert wird und etwaigen Compliance-Anforderungen entspricht.

Infos

- Bewertung des Risikos: Kurzpapier des DSK

- zur Meldepflicht mit anschaulichen Praxisbeispielen: Leitlinien des Europäischen Datenschutzausschusses:
  https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/03/Leitlinien-für-die-Meldung-von-Verletzungen-des-Schutzes-personenbezogener-Daten-.pdf

  https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

- Handreichung der Aufsichtsbehörde in Hamburg

- Informationen zu häufigen Ursachen von Datenschutzverletzungem (u.a. Cyberangriffen) und Abwehrmaßnahmen stellt die Aufsichtsbehörde in Sachsen-Anhalt bereit

Infos

- Das BSI bietet wertvolle Informationen
  - Zum Umgang mit Cyberangriffen
  - Zur Erstellung von Notfallplänen
  - Und Listen von IT-Sicherheitsdienstleistern

Dankeschön!

Foto: Flemming Holm

Rechtsanwältin Carola Sieling

XING www.xing.com/profiles/Carola_Sieling
LinkedIn www.linkedin.com/in/carolasieling/
Mastodon legal.social/@CarolaSieling