SIELING
RECHTSANWALTSKANZLEI

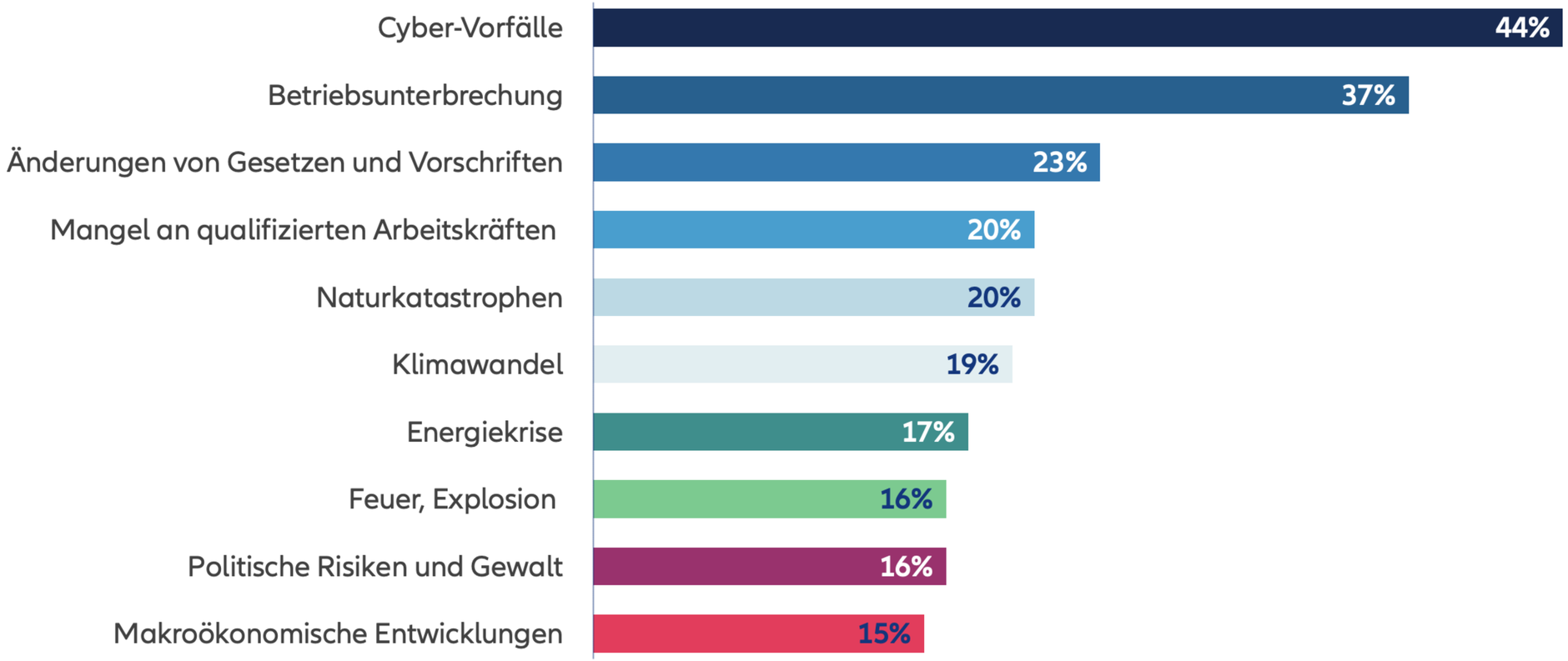
**Rechtsanwältin Anne-Kathrin Titze**

Lehrbeauftragte
Datenschutzbeauftragte
Datenschutzauditorin

# NIS-2 - Was müssen Sie wissen und was ist zu tun?

# Die Top 10 Geschäftsrisiken in Deutschland in 2024

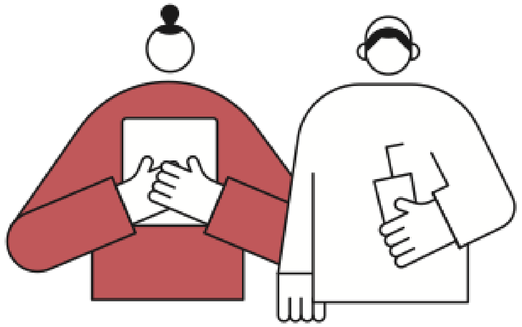
*Für weitere Details klicken Sie auf die Balken im Diagramm*




**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**

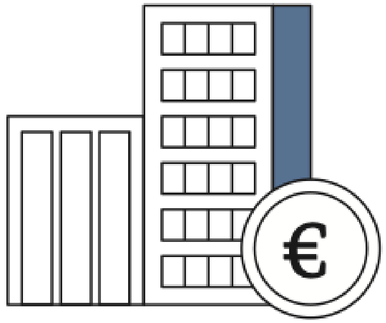
## Top 3-Bedrohungen je Zielgruppe:

### Gesellschaft



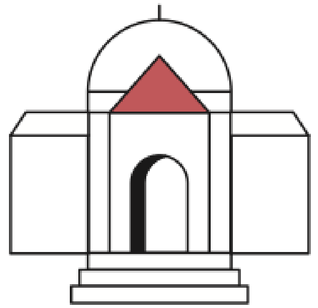
***Identitätsdiebstahl***
Sextortion
Phishing

### Wirtschaft




***Ransomware***
Abhängigkeit innerhalb der IT-Supply-Chain
Schwachstellen, offene oder falsch konfigurierte Online-Server

### Staat und Verwaltung

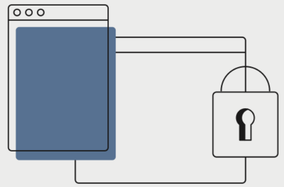


***Ransomware***
APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

# Ransomware

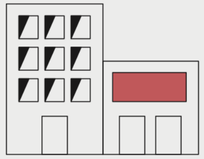
**ist weiterhin die größte Bedrohung.**

**2** **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



**68** erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

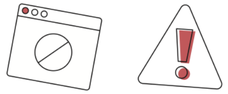
**15** davon richteten sich gegen **IT-Dienstleister**.



Mehr als **2.000** **Schwachstellen** in Software-Produkten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

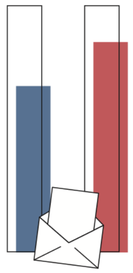
## Eine Viertelmillion

neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



**66%**

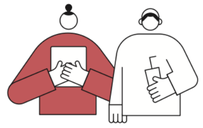
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
**34%** Erpressungsmails,
**32%** Betrugsmails

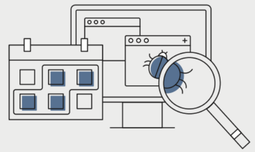


**84%**

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

### Top 3-Bedrohungen je Zielgruppe:

| Gesellschaft | Wirtschaft | Staat und Verwaltung |
|---|---|---|
|  |  |  |
| ***Identitätsdiebstahl*** | ***Ransomware*** | ***Ransomware*** |
| Sextortion | Abhängigkeit innerhalb der IT-Supply-Chain | APT |
| Phishing | Schwachstellen, offene oder falsch konfigurierte Online-Server | Schwachstellen, offene oder falsch konfigurierte Online-Server |



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

**370** **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220
2022

5.100
2021

**7.120**

Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland
**Digital•Sicher•BSI•**

**IT-Sicherheitsgesetz:**

Das IT-Sicherheitsgesetz (IT-SiG 2.0) legt gesetzliche Anforderungen an KRITIS Betreiber und Unternehmen mit besonderen öffentlichen Interesse fest.

Beim BSI registriert: Derzeit 800 Unternehmen mit ca. 1600 Anlagen sowie ca. 3000 Unternehmen mit besonderen öffentlichen Interesse (UBI)

**EU-Richtlinie NIS 2 - Network-and-Information-Security-Richtlinie 2.0:**

NIS2 betrifft alle mittleren und großen Unternehmen, die auf dem Binnenmarkt der Europäischen Union tätig sind.

Ca. 30.000 Unternehmen betroffen

BMI: geschätzte Kosten für Privatwirtschaft 1,5 Milliarden EUR jährlich

**2020 -** EU-Kommission legt neue **Cyberstrategie** für das Jahrzehnt vor.


Pillars and key action areas of the European Security Union Strategy

CRA

NIS2

DORA

ePrivacy

CER

# NIS-2

- Richtlinie ist seit Januar 2023 wirksam
- Umsetzungsfrist läuft am **17.10.2024** aus
  - bisher wurden mehrere Entwürfe des NIS2UmsuCG öffentlich, zuletzt der Referentenentwurf vom 7.5.2024
  - Regierungsentwurf wurde verabschiedet (24.07.2024)
  - Noch nicht verkündet

# (CER-Richtlinie)
# Richtlinie (EU) 2022/2557

Am 16.01.2023 sind zwei EU-Richtlinien für besseren Schutz kritischer Infrastrukturen in Kraft getreten.

## EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience / CER-Richtlinie)

Die **CER-Richtlinie** verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschläge oder Sabotage zu stärken.

- Zusammen mit NIS-2 verabschiedet
- Ziel: (physische) Resilienz von „Kritischen Infrastrukturen“ innerhalb der Europäischen Union

# „Digital Operational Resilience Act“ („DORA“)
# VO (EU) 2022/2554

- Adressat: Finanzbranche
- am 16. Januar 2023 in Kraft getreten und wird am 17. Januar 2025 wirksam.
- Ziel: Vereinheitlichung und Verschärfung von Cybersicherheit-Standards zu Zwecken der digitalen Betriebsstabilität

# NIS-2

- Unternehmen in **18 Sektoren**
- Unternehmen **> 50 Mitarbeitern** und über **10 Mio. EUR** Jahresumsatz bzw. Bilanzsumme
- Sonderfälle: größenunabhängig

# NIS-2

Zur Berechnung der Schwellenwerte sind die Zahlen und Daten **etwaiger Partnerunternehmen** und/oder **verbundener Unternehmen** zu berücksichtigen. Eine Ausnahme gilt nur dann, wenn Ihre Einrichtung eine selbständige Einrichtung ist (Siehe EW 16 NIS2-Richtlinie).

# NIS-2

- erhebliche **Änderungen**!
- Unterscheidung zwischen **„wesentlich“** und **„wichtig“**
- **Öffentliche** und **private** Einrichtungen
  - die ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben (und)
  - die in den Anhängen I (**„hohe Kritikalität“**) und II (**„sonstige kritische Sektoren“**) der Richtlinie konkretisiert werden

# NIS-2

**mittleres Unternehmen: 50-249 Beschäftigte, 10-50 Mio. Euro Umsatz, < 43 Mio. Euro Bilanz**

**großes Unternehmen: >250 Beschäftigte, > 50 Mio. Euro Umsatz, > 43 Mio. Euro Bilanz**

| wesentliche Einrichtung | wichtige Einrichtung |
|---|---|
| großes Unternehmen in Sektor gem. Anhang I | mittleres Unternehmen in Sektor gem. Anhang I oder II |
| bestimmte Sonderfälle | bestimmte Sonderfälle |

# Überblick über die regulierten Sektoren gem.  Anhang I der NIS-2

- Energie
- Verkehr
- Bankwesen
- Finanzmarktstrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur (z.B.  Anbieter von Cloud-Computing-Dienstleistungen oder Rechenzentrumsleistungen)
- Verwaltung von IKT-Diensten (B2B)
- Öffentliche Verwaltung
- Weltraum

## Überblick über die regulierten Sektoren gem.  Anhang II der NIS-2

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/ Herstellung von Waren (z.B. Maschinenbau)
- Anbieter digitaler Dienste (z.B.  Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Sozialen Netzwerken)
- Forschung

# NIS2 - Umfangreiche Anforderungen an IT-Sicherheit und an das Management

- Risikomanagement
- Policies
- Continuity Management
- Incident Management
- Authentifizierung
- Notfallkommunikation
- Lieferkette
- Schulung
- Verschlüsselung
- Erweiterte Pflichten für Leitungsorgane

# NIS2 - Aufsichtsbehörden und Strafen

- Registrierungs- und Meldepflichten
- Strikte Überwachung und Aufsicht durch Behörden (national und EU)
- Strafen (Mindestniveau) nach Maximalprinzip
  - 10 Mio. EUR oder 2% globaler Umsatz (Essential)
  - 7 Mio. EUR oder 1,4% globaler Umsatz (Important)

# NIS2- UmsetzungsG (Stand: Juli 2024)

- Aufsicht: BSI
- Adressat
  - Besonders wichtige Einrichtungen (wesentliche Einrichtungen und Betreiber kritischer Anlagen (ex-KRITIS)
  - Wichtige Einrichtungen

# NIS2- UmsetzungsG (Stand: Juli 2024)

- Governance
  - Geschäftsleiter müssen Risikomanagementmaßnahmen billigen und überwachen
  - Geschäftsleiter haften für Schaden bei Pflichtverletzung
  - Pflicht-Schulungen

# NIS2 - Checkliste

- Eigene Betroffenheit klären
- Betroffenheit von Kunden und Lieferanten klären (Lieferkettensicherheit ist laut NIS-2 zu gewährleisten)
- Registrierungs- und Meldepflichten beachten
- Erforderliche und geeignete Maßnahmen (TOOM = technische, operative, organisatorische Maßnahmen) ergreifen
- Umsetzungsgesetze in den Mitgliedsstaaten beachten

## ISO-Standards und andere Richtlinien:

Internationale Standards wie ISO 27001 (Informationssicherheitsmanagement) und ISO 22301 (Business Continuity Management) bieten bewährte Verfahren und Leitlinien zur Gewährleistung der Informationssicherheit im Rechnungswesen. Unternehmen sollten diese Standards als Rahmenwerk nutzen und sie an ihre spezifischen Anforderungen anpassen.

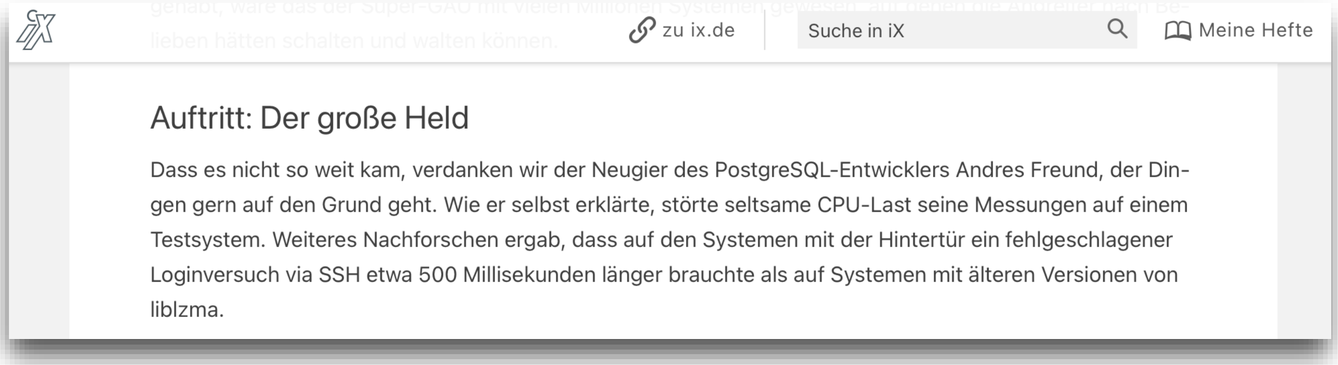
# Und nicht vergessen:
# Nerds retten die Welt!

Nach Entdeckung des xz-Hacks

## »Wir haben wirklich Glück gehabt«

Der Microsoft-Entwickler Andres Freund hat eine IT-Sicherheitskatastrophe verhindert. Selbst CEO Satya Nadella gratulierte ihm. Eine US-Behörde fordert derweil Konsequenzen.

06.04.2024, 09.08 Uhr



# Vielen Dank!

Rechtsanwältin Anne-Kathrin Titze

Lehrbeauftragte

Datenschutzbeauftragte

Datenschutzauditorin
kanzlei-sieling.de
technologiewerft.de