

Entwicklung, Mitigation und Versicherung von Cyber- Risiken

Förderkreis für die Versicherungslehre

7. November 2023

Dipl.-Kffr. Jutta Berger-Knickmeier
Head of Underwriting
Commercial Insurance

Alexander Siering, LL.M.
Underwriter Cyber Risks
Commercial Insurance

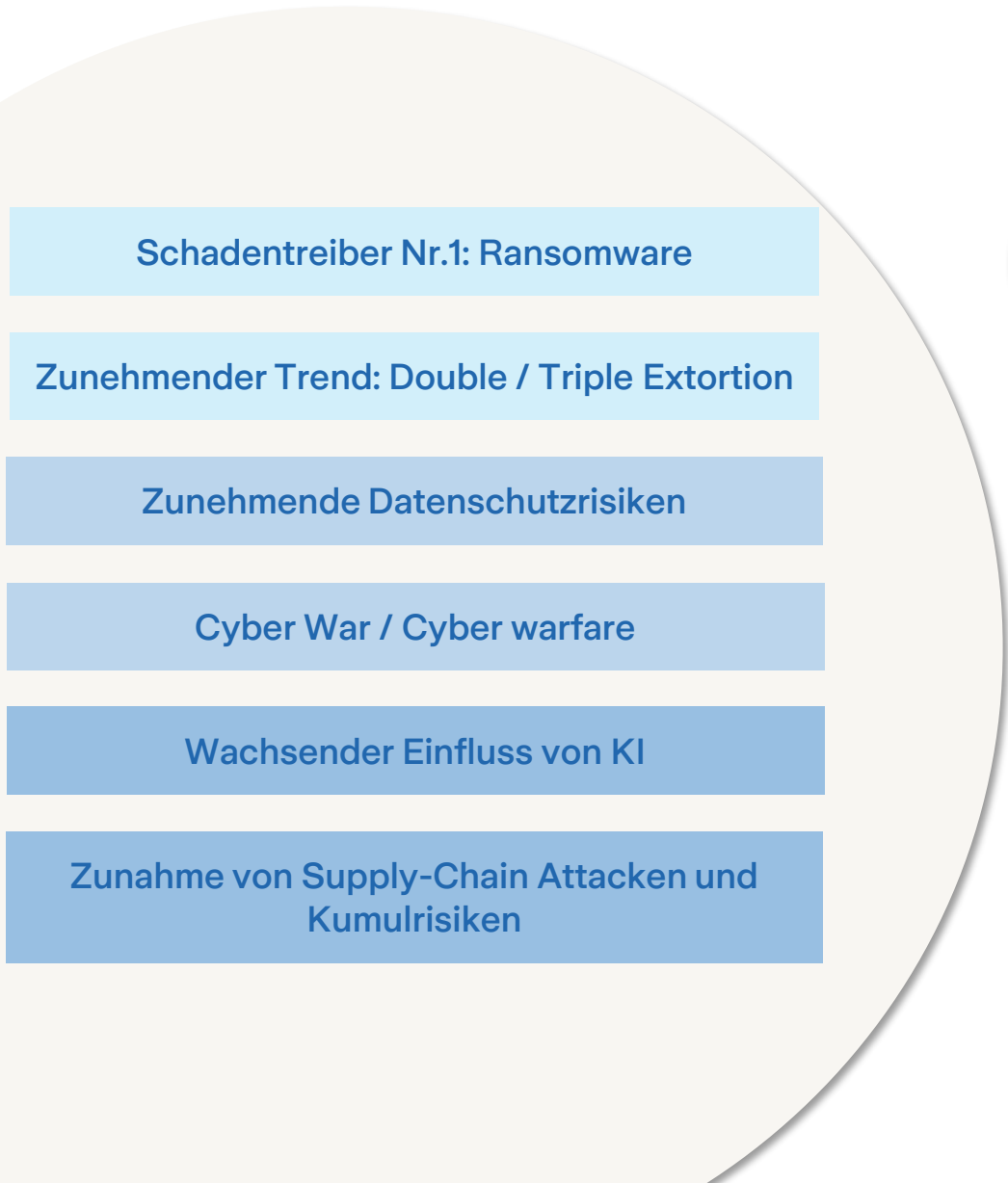


Risikolage



Cyber 2023 – Aktuelle Risikosituation und Schadenbeispiele

Status Quo



tagesschau

Sorge um Deutschlands IT-Sicherheit

Die Ukraine hat erneut einen gezielten Cyber-Angriff gegen die Energieversorgung des Landes abwehren können. Der Vorfall führt dennoch zu wachsender Sorge um die kritische Infrastruktur auch in Deutschland.

Frankfurter Allgemeine

Hacker und Spione kosten Unternehmen 203 Milliarden Euro

G DATA Bedrohungsreport

Angriffe im Sekundentakt: Rund 100 Malware-Varianten pro Minute

Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet

NZZ-Redaktion
11.05.2023, 19.15 Uhr

Risk Management

Siemens and UCLA say data compromised in MOVEit data breach

June 27, 2023

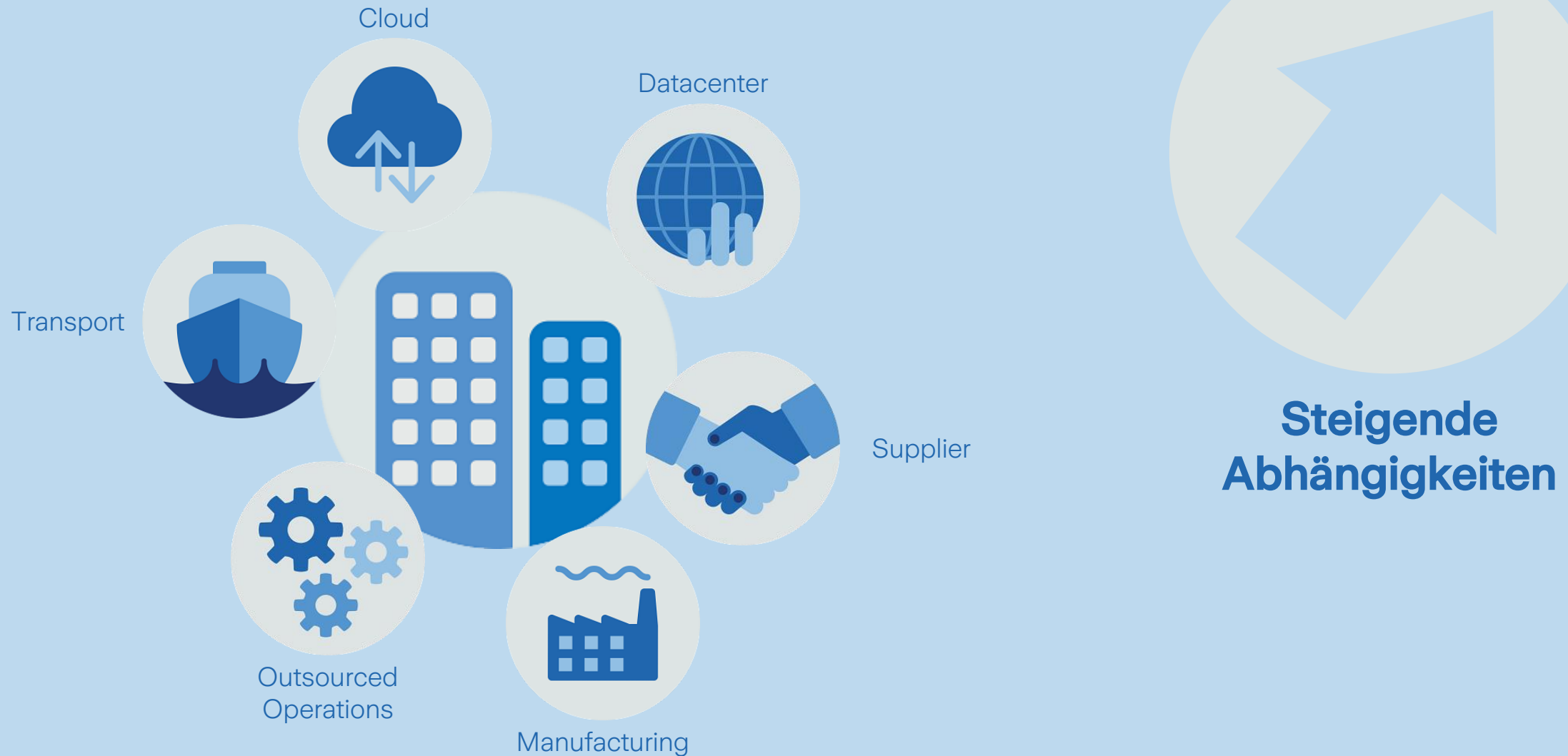


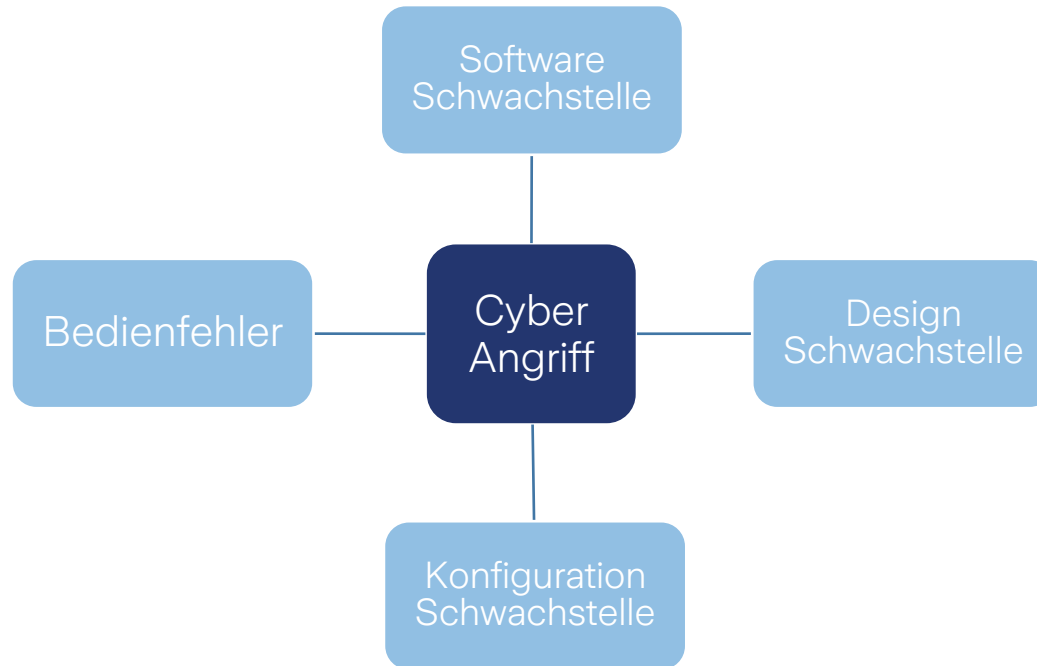
Handelsblatt

<https://www.handelsblatt.com> > ... > Banken

Cyberangriff legt Internetseite der Bafin lahm

04.09.2023 — Nach einer **Attacke** auf die Server ist der Internetauftritt der Behörde nur eingeschränkt erreichbar ... **Cyberangriff** legt Internetseite der **Bafin** ...

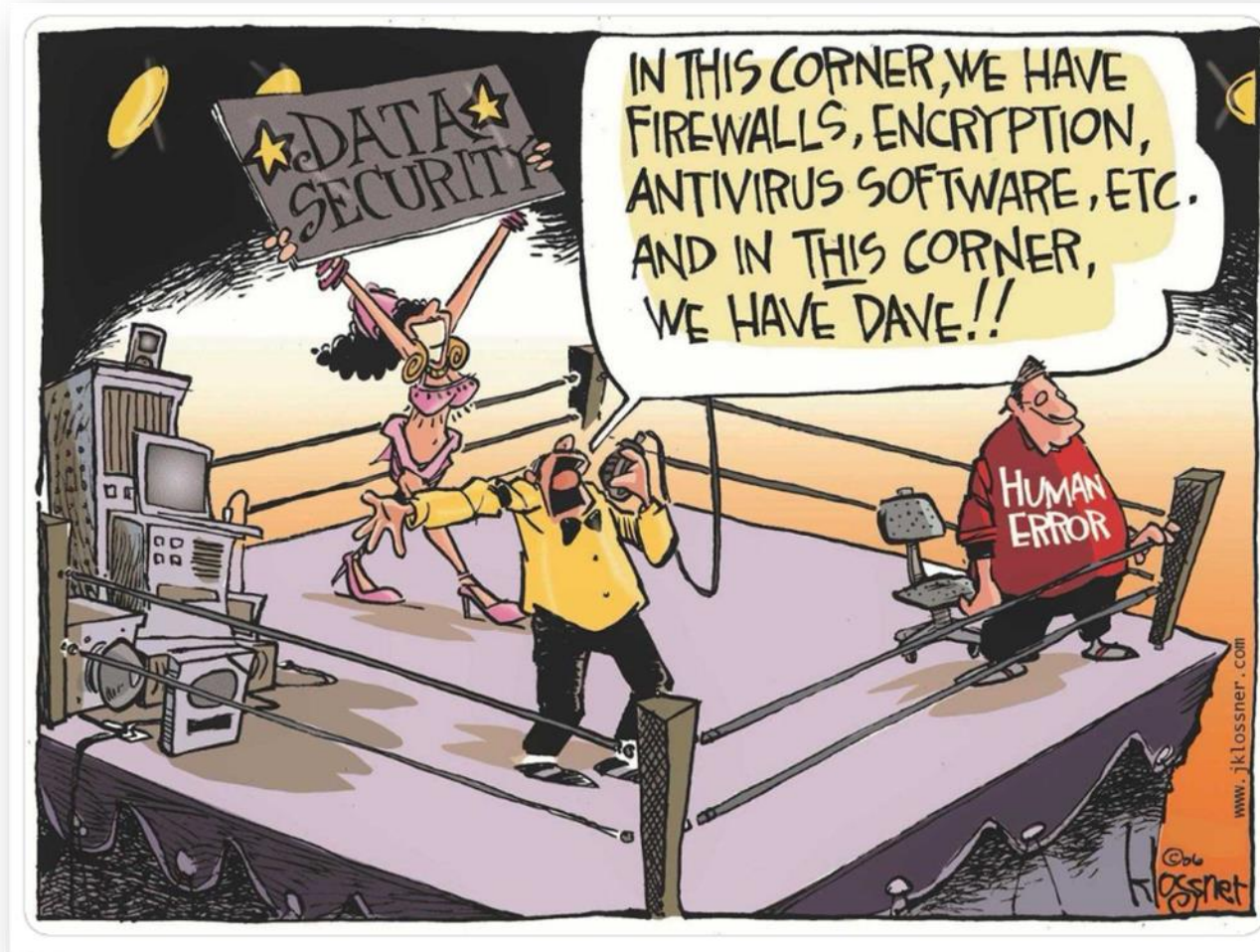




„Alle diese Arten von Schwächen lassen sich bei der heutigen Komplexität der Informationsverarbeitung prinzipiell nicht vollständig vermeiden.“ (BSI)

Entwicklungen...

“Was bleibt konstant?”



Quelle: [Human error Dave \(devhumor.com\)](http://devhumor.com)

Darknet

Praxisbeispiele



NIS 2

Werden wir alle zur kritischen Infrastruktur?



NIS2

Implikationen für Unternehmen in Deutschland

heise online [heise +](#) [Jetzt 1 Monat für 0 € testen](#) [Anmelden](#)

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal

TOPTHEMEN:
KÜNSTLICHE INTELLIGENZ ENERGIE E-HEALTH WINDOWS LINUX & OPEN SOURCE PODCASTS

heise online > Security > Cybersecurity > Wie NIS2UmsuCG und KRITIS-DachG Deutschlands Cybersicherheit verändern werden

Wie NIS2UmsuCG und KRITIS-DachG Deutschlands Cybersicherheit verändern werden

Mit neuen Gesetzen wird das bisherige Recht der IT-Sicherheit nicht nur an die Bedrohungen angepasst, sondern erheblich erweitert. Manager müssen z...

Süddeutsche Zeitung

SZ Plus | Ukraine | Oktoberfest | Politik | Wirtschaft | Meinung | Panorama | Sport | München | Kultur

> Computer & Digital

NIS2-Richtlinie: Ein neuer Weg zur Stärkung der Cyber Security in Europa

Montag, 17. Juli 2023 11:41

Gleiss Lutz

AKTUELLES KOMPETENZ EXPERTEN KARRIERE SOZIJÄT INTERNATIONAL
MANDATE & KANZLEI NEWS KNOW-HOW VERANSTALTUNGEN

Startseite > Aktuelles > Know-how > Entwurf eines Umsetzungsgesetzes für NIS2 – Umfassende Erweiterung von Cybersicherheitspflichten und direkte Haftung der Geschäftsleitung

DIGITAL ECONOMY

ENTWURF EINES UMSETZUNGSGESETZES FÜR NIS2 – UMFASSENDE ERWEITERUNG VON CYBERSICHERHEITSPFLICHTEN UND DIREKTE HAFTUNG DER GESCHÄFTSLEITUNG

VERSICHERUNGSMONITOR

Aktuelles Kommentare Leute Analysen Cartoon / Quiz Stellenmarkt 18 Ever

STARTSEITE > ABO > CYBER: NIS 2 WIRD DIE NEUE DSGVO


Cyber: NIS 2 wird die neue DSGVO

VON NINA NÖTHLING AM 26. OKTOBER 2023

ARTIKEL DRUCKE

Die neuen EU-Cybersicherheitsvorgaben für Unternehmen, NIS 2, haben weitreichende Konsequenzen für Cyber- und vor allem D&O-Versicherer. Das sagte Rechtsanwalt Paul Malek bei einem Webinar der Kanzlei Clyde & Co. Die Auswirkungen seien ähnlich umfangreich wie bei der Einführung der Datenschutz-Grundverordnung (DSGVO) 2018. Die NIS2-Vorgaben können Fluch und Segen zugleich sein. Der deutsche Entwurf zur Umsetzung der Richtlinie hat es in sich. Besonders für D&O-Versicherer könnte er viele und teure Gerichtsverfahren mit sich bringen.


Begriffsbestimmungen (§28 NIS2UmsuCG)



Kritische Anlagen


- Energie
- Transport/Verkehr
- Finanz-
/Versicherungswesen
- Gesundheitswesen
- Wasser/Abwasser
- Ernährung
- Information- und
Telekommunikation
- Weltraum
- Siedlungsabfälle

→ Schwellenwerte gem.
RechtsVO entscheidend



Bes. wichtige Einrichtung

- Betreiber **kritischer Anlagen**
- Unternehmen gem. **Anlage 1**
und **>KMU**
- Bestimmte IT-Services
- Telekommunikationsdienste



Wichtige Einrichtung

- Unternehmen gem. **Anlage 1**
und **2** und **KMU**:
 - Produktion chemischer
Stoffe
 - Produktion von
Lebensmitteln
 - Verarbeitendes Gewerbe
 - etc.

Pflichtenkatalog (Auszug)

- Meldepflichten bei Sicherheitsvorfällen, vgl. § 32 NIS2UmsuCG:
- Registrierungspflicht, vgl. § 33 NIS2UmsuCG
- Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter, vgl. § 38 NIS2UmsuCG
- Risikomanagementmaßnahmen, § 30 Abs. 1 NIS2UmsuCG



Für **Besonders wichtige Einrichtungen** und **wichtige Einrichtungen** gilt:

Technische und organisatorische Maßnahmen sollen den **Stand der Technik** einhalten und auf einen gefahrübergreifenden Ansatz beruhen sowie **Mindestvoraussetzungen** erfüllen (§ 30 Abs. 2 NIS2UmsuCG):

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von Sicherheitsvorfällen
3. Back Up Management/Wiederherstellung im Notfall
4. Sicherheit in der Lieferkette
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahme in der Cybersicherheit
7. Schulungen
8. Kryptografie/Verschlüsselung
9. Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung

→ Für Betreiber **kritischer Anlagen** gelten gem. §31 NIS2UmsuCG gesonderte Anforderungen (vgl. auch §8a Abs. 1a BSIG)



§ 60 Abs. 2 Nr. 2 NIS2UmsuCG:

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 30 Absatz 1 (...) eine dort genannte Maßnahme **nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig** ergreift.

Bußgelder:

- **Wichtige Einrichtung** (§ 60 Abs. 6 NIS2UmsuCG):
Verstoß gegen Risikomanagementmaßnahmen Geldbuße bis zu 7 Millionen Euro oder mit einem Höchstbetrag von mindestens 1,4 % des weltweiten Umsatzes.
- **Besonders wichtige Einrichtungen** (§ 60 Abs. 7 NIS2UmsuCG):
Verstoß gegen Risikomanagementmaßnahmen Geldbuße bis zu 10 Millionen Euro oder mit einem Höchstbetrag von mindestens 2 % des weltweiten Umsatzes.

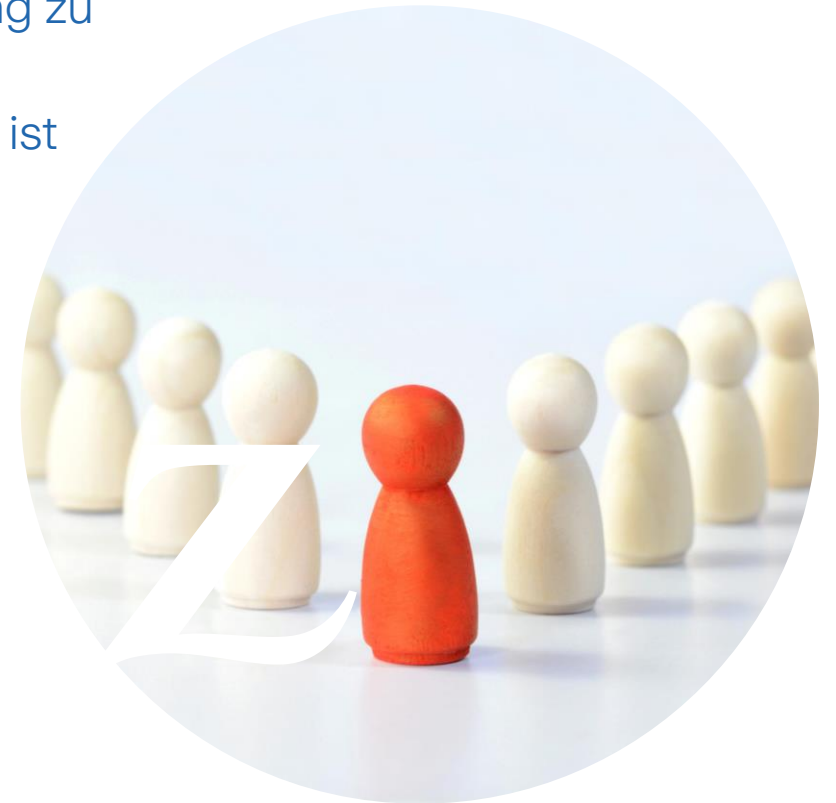


§ 38 NIS2UmsuCG:

Abs. 1: Geschäftsleiter **besonders wichtiger** Einrichtungen und **wichtiger Einrichtungen** sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen **Risikomanagementmaßnahmen** (...) zu billigen und ihre Umsetzung zu überwachen.

Die Beauftragung **eines Dritten** zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.

Abs. 2: Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Die Amtshaftung bleibt unberührt.



§ 38 NIS2UmsuCG:

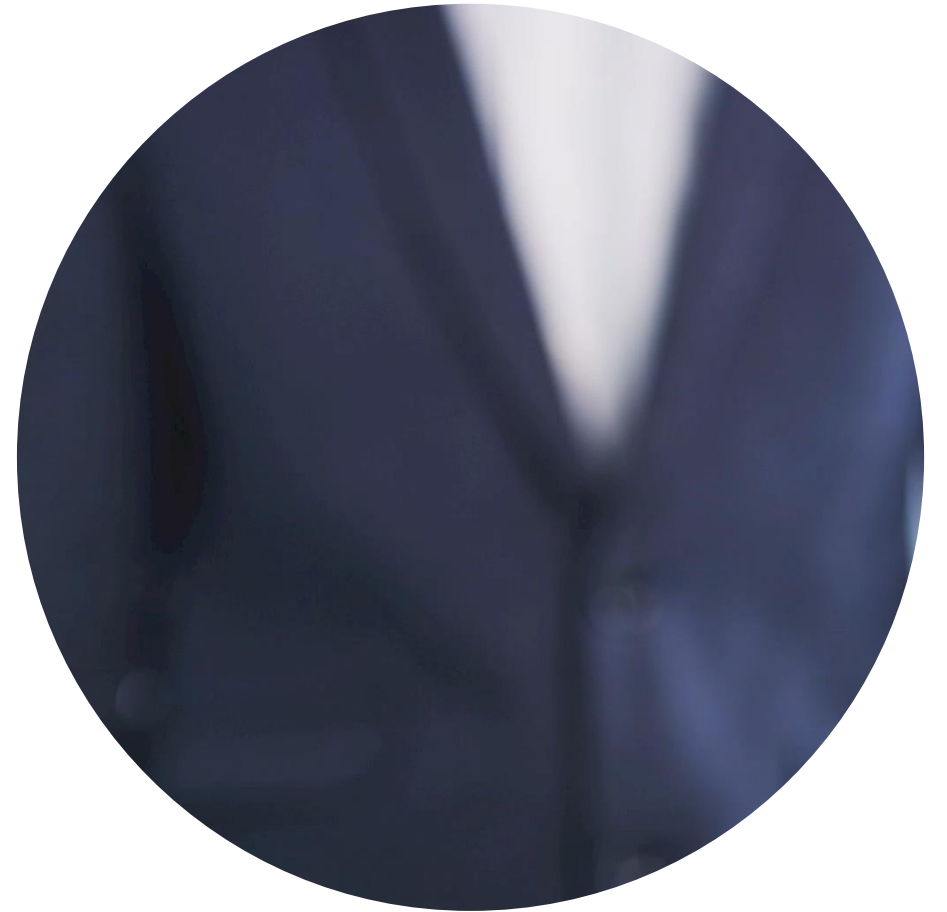
Abs. 1: Geschäftsleiter **besonders wichtiger** Einrichtungen und **wichtiger Einrichtungen** sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen **Risikomanagementmaßnahmen** (...) zu billigen und ihre Umsetzung zu überwachen.

Die Beauftragten
nicht

Abs. 2
der Ein
unber

527		(2) Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Die Amtshaftung bleibt unberührt.	Umsetzung Art. 20 Abs. 1 Uabs.1 aE. NIS-2. Die NIS-2 gibt eine reine Binnenhaftung im Verhältnis Einrichtung-Geschäftsleiter vor. Vom Schadensbegriff sind sowohl Regressansprüche als auch Bußgeldforderungen umfasst. Umsetzung von Art. 20 Abs. 1 Uabs. 2. Die Vorschriften über die Amtshaftung gehen der Haftungsregel in Satz 1 vor, eine Ausweitung der bestehenden
-----	--	--	--

Versicherung von Cyber- Risiken und Grenzen der Versicherbarkeit



Worin liegt der Nutzen einer Cyber-Versicherung?



Professionelle Hilfe
im Krisenfall



Schnelle
Betriebsfortführung



Präventive Unterstützung
durch den Versicherer



Phishing-
Simulation

Awareness-
Trainings



Reduzierung des
finanziellen Risikos



Unterstützung durch
IT-Experten



24/7/365
Notfallhotline



u.v.m.

Präventionsangebot
Cyber Awareness in
Kooperation mit Perseus

und

Cyber Services von
Zurich Resilience Solutions

Die Vorteile unseres Online-Portals für Cybersicherheit



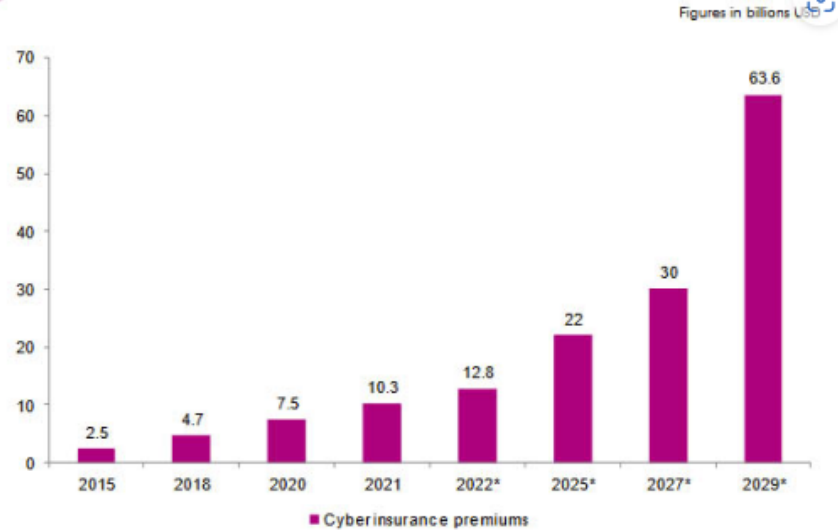
Flexible Online-Trainings für Cybersicherheit und Datenschutz

Einfach, verständlich und kompakt: Unsere Online-Trainings vermitteln grundlegendes Wissen zu Cybersicherheit, Datenschutz sowie Phishing und schärfen das Bewusstsein für Gefahren aus dem Netz, konkrete Handlungsempfehlungen inklusive.

[Zu unseren Online-Trainings](#)

- + **Cybersicherheit**
- + **Datenschutz**
- + **Phishing**

Cyber premiums evolution: 2015-2029



* Estimates

Sources : Munich Re, Fortune Business Insights and Research & Markets

Ca. 14,5 Mrd. ww Prämienvolumen Ende 2023 bei einer durchschnittlichen Wachstumsrate von 25%.

Darüber liegendes Wachstum in Deutschland für die Jahre 2020 bis 2023 (schätzungsweise).



Commercial Risk

26.07.2023

Insurance & Risk Management News

Global cyber market improving for buyers but more capacity needed

Captives

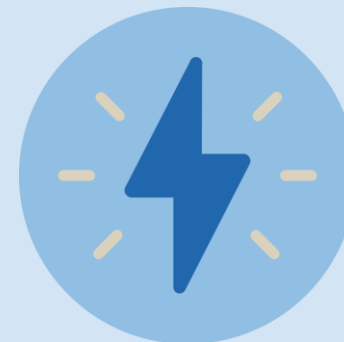




Gestiegene Schadenzahlen
und neue Risiken



Feinjustierung von Fragebögen und
Bedingungswerken



Gestiegene Anforderung an
Kunden und deren Cyber Security

z.B. Patch-Management,
Notfallplan, Backup-
Prozess



Stärkere Betrachtung
von Kumulrisiken



Prämien und Kapazitäten derzeit in
Stabilisierung

Weiterhin
spannender
Markt, der
gemeinsamen
Austausch
fordert

“Wo führt das hin?”



Sorgfältige Betrachtung der nationalen und internationalen Entwicklungen und der steigenden Cyber-Gefahren



Analyse der systemischen Risiken und weltweit möglichen Kumulszenarien



Zunehmender Fokus auf weiterer Unterstützung der Kunden bei der Verbesserung der Cyber-Security

Aktuelle rechtliche Entwicklungen:

Deckungseinwände eines Cyberversicherers (LG Tübingen 4 O 193/21)

Immaterielle Schäden und Pflichtverletzungen nach DSGVO (EuGH C-300/21)

Fragen & Diskussion

Vielen Dank für Ihre
Aufmerksamkeit!

