



# 11. GELSEN-NET Security Day

Cybersicherheit in NRW – Regulatorische Rahmenbedingungen

Gelsenkirchen, 24. Juni 2024



# Intro



200 Mrd. EUR

171 Mrd. EUR

102 Mrd. EUR

477 Mrd. EUR

2,5 Mio. EUR

25 Bil. USD

17 Bil. USD

4 Bil. USD

6 Bil. USD

200 Mrd. EUR

2,9 Bil. USD

185 Mrd. USD



**200 Mrd. EUR**

Schaden dt. Wirtschaft durch  
Cybercrime

**171 Mrd. EUR**

Sozialer Staat Bundeshaushalt

**102 Mrd. EUR**

Gesamtetat Haushalt NRW

**477 Mrd. EUR**

Gesamtetat Bundeshaushalt

**2,5 Mio. EUR**

Kosten Anhalt-Bitterfeld

**25 Bil. USD**

BIP USA

**17 Bil. USD**

BIP China

**4 Bil. USD**

BIP BRD

**6 Bil. USD**

Schaden Cybercrime

**200 Mrd. EUR**

Kosten Ukrainekrieg für dt.  
Wirtschaft

**2,9 Bil. USD**

Wert Microsoft

**185 Mrd. USD**

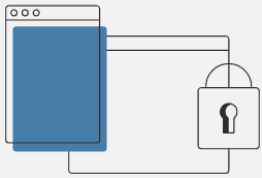
Wert SAP



# Ransomware

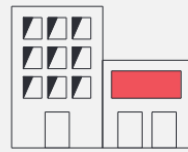
ist weiterhin die größte Bedrohung.

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



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

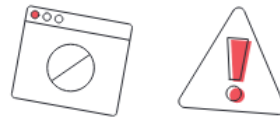
**15** davon richteten sich gegen IT-Dienstleister.



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

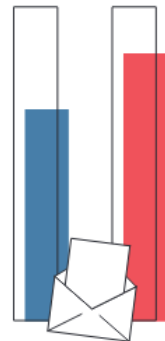
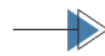


**Eine Viertelmillion** neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



**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.

MIT CVE-BESCHREIBUNG

## GPT-4 kann eigenständig bekannte Sicherheitslücken ausnutzen

Forscher haben festgestellt, dass **GPT-4** allein anhand der zugehörigen Schwachstellenbeschreibungen 13 von 15 **Sicherheitslücken** erfolgreich ausnutzen kann.

in Pocket speichern

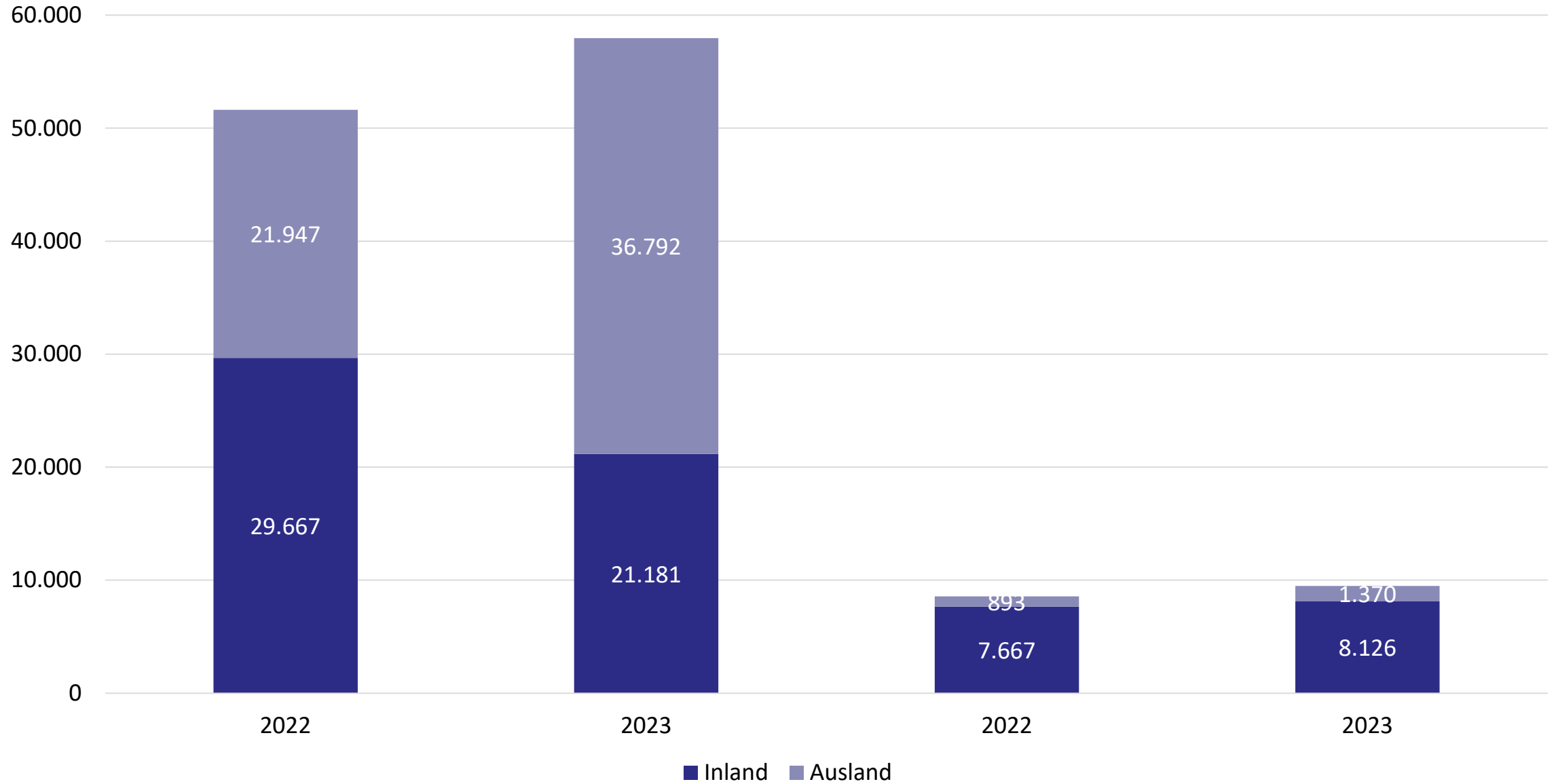
merken



18. April 2024, 12:45 Uhr, Marc Stöckel



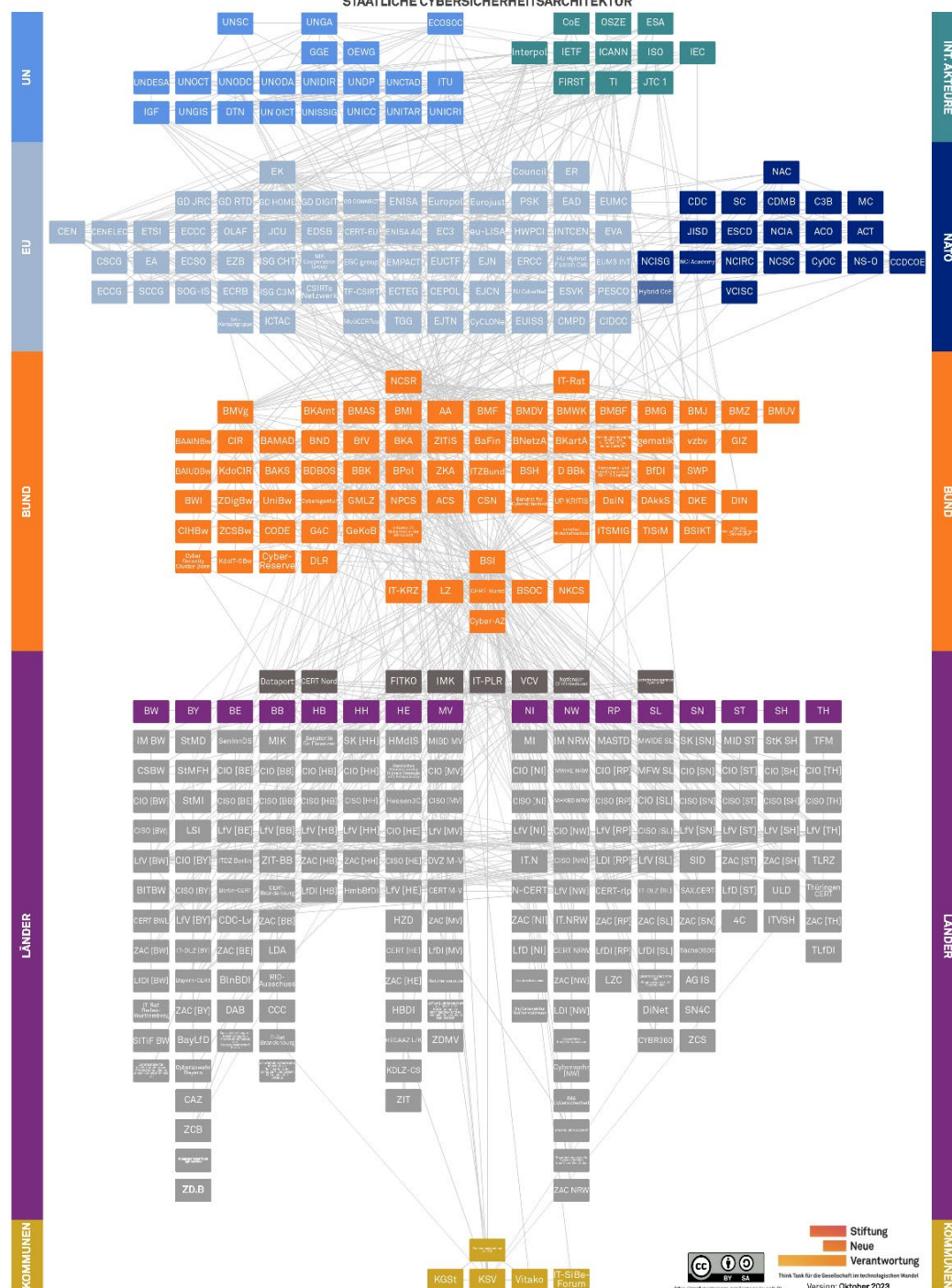
# Fallzahlen Inland / Ausland (PKS)



# Cybersicherheit in NRW



# STAATLICHE CYBERSICHERSARCHITEKTUR



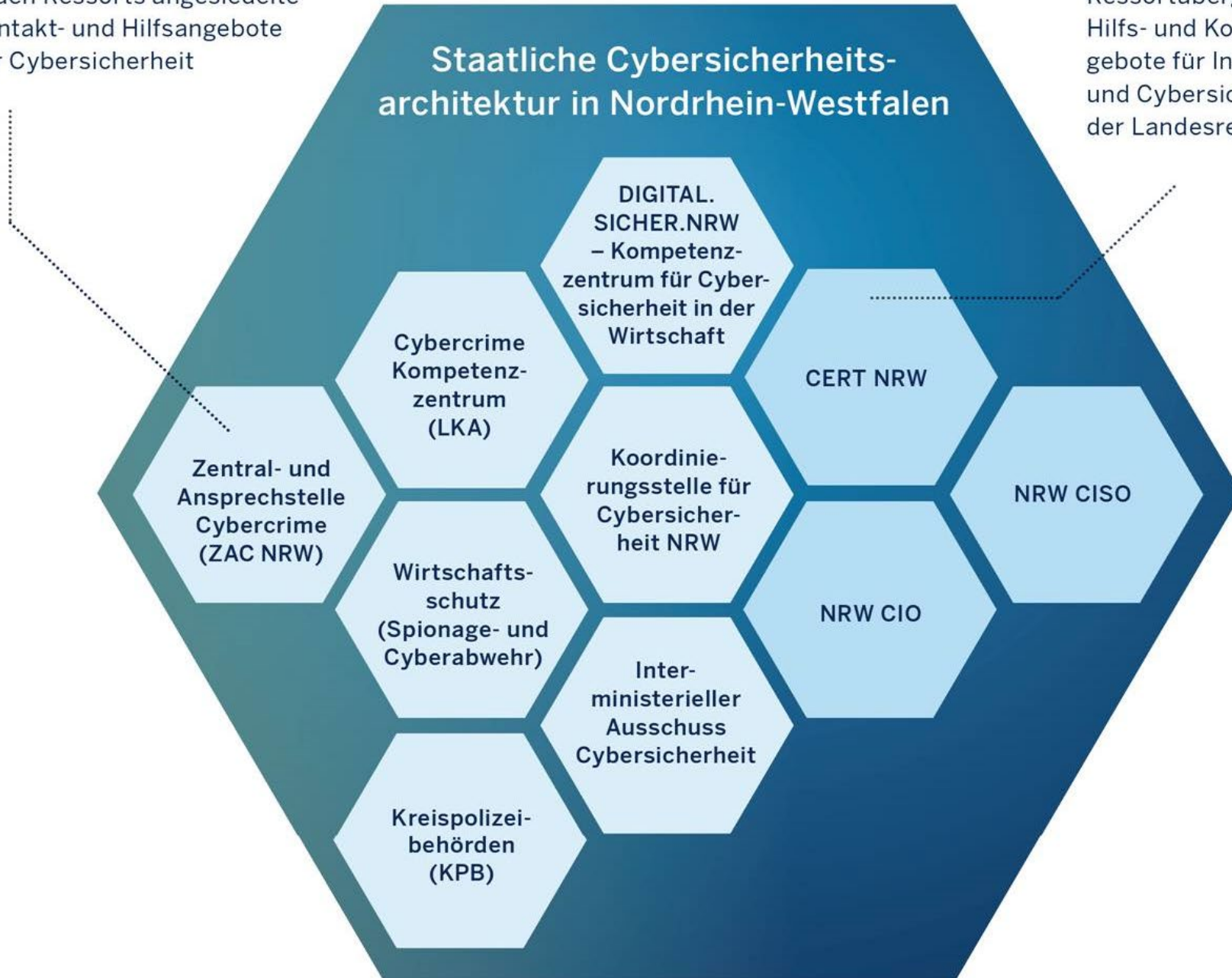


### Kerninstanzen

In den Ressorts angesiedelte Kontakt- und Hilfsangebote zur Cybersicherheit

### Landesverwaltung

Ressortübergreifende Hilfs- und Kontaktangebote für Informations- und Cybersicherheit der Landesregierung



### Wissenschaft und Forschung

Rund 30 Hochschulinstitute  
und außeruniversitäre  
Forschungseinrichtungen  
im Bereich Cybersicherheit

### Kooperationen

Staatliche, teilstaatliche  
sowie private  
Kooperationen im Bereich  
Cybersicherheit

### Wirtschaft

Rund 400 IT-Sicher-  
heitsunternehmen sind  
in Nordrhein-Westfalen  
angesiedelt

## Cybersicherheitslandschaft in Nordrhein-Westfalen

Wissenschaft  
und Forschung

Kooperationen

Wirtschaft

Staatliche  
Cybersicherheitsarchitektur

### Kerninstanzen

In den Ressorts angesiedelte  
Hilfs- und Kontaktangebote  
für Cybersicherheit

### Landesverwaltung

Ressortübergreifende  
Hilfs- und Kontaktangebote  
für Informations- und Cyber-  
sicherheit der Landesregierung



Nordrhein-Westfalen verfügt bereits heute über sehr starke Akteure auf dem Gebiet der Cybersicherheit, sei es bei den Sicherheits- und Justizbehörden des Landes, sei es in der Wirtschaft oder der Wissenschaft. Wir wollen unseren Beitrag zur Stärkung dieser Akteure leisten und sie noch besser zu einem starken **Cybernetzwerk für Nordrhein-Westfalen** zusammenführen. Hierzu werden wir die **Koordinierungsstelle Cybersicherheit** der Landesregierung weiterentwickeln und die Cybersicherheitsstrategie des Landes kontinuierlich fortschreiben und weiterentwickeln.

# ZUKUNFTSVERTRAG FÜR NORDRHEIN- WESTFALEN

Koalitionsvereinbarung  
von CDU und GRÜNEN

2022-2027

**CDU** NRW




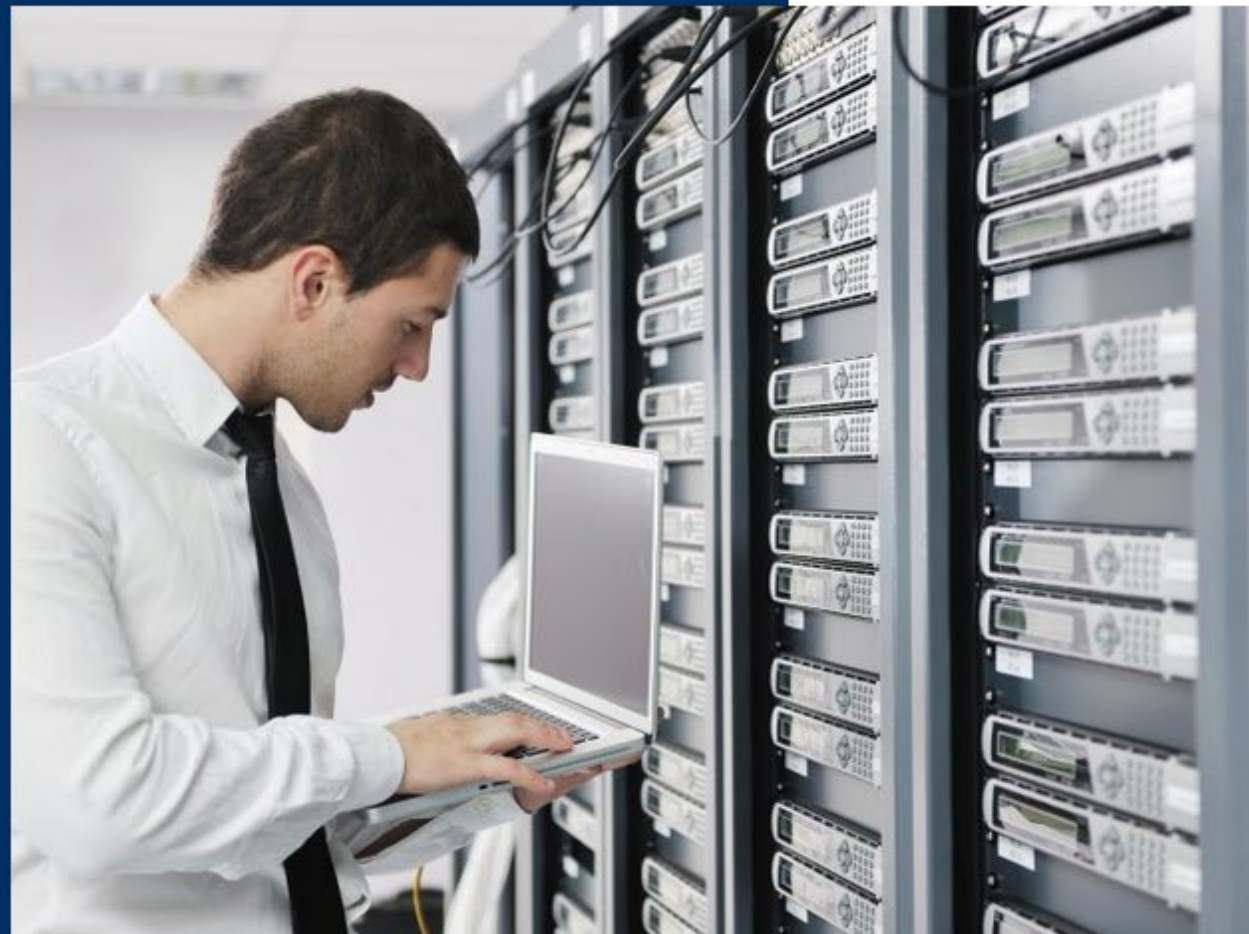


[Startseite](#) | [NRW informieren](#) | [Pressemitteilungen](#) |  
[Cyberkriminalität-Studium für die Polizei](#)

# Cyberkriminalität-Studium für die Polizei

Innenminister Reul: Cyber-Cops sind unsere  
Antwort auf die Kriminalitätsverschiebung in  
den digitalen Raum

 28. April 2022








[Startseite](#) | [NRW informieren](#) | [Pressemitteilungen](#) |  
[Cybercrime-Kriminalinspektionen gehen an den Start](#)

# Mehr Polizei im Netz: Cybercrime- Kriminalinspektionen gehen an den Start

Innenminister Herbert Reul: Auch im World Wide Web gehen wir auf Verbrecherjagd

 22. Februar 2024



# Regulatorische Rahmenbedingungen



## **Aktiengesetz** **§ 91 Organisation. Buchführung**

- (1) Der Vorstand hat dafür zu sorgen, daß die erforderlichen Handelsbücher geführt werden.
- (2) Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.
- (3) Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten.

## **Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)** **§ 43 Haftung der Geschäftsführer**

- (1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.
- (2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.

## **Gesetz über die Haftung für fehlerhafte Produkte** **(Produkthaftungsgesetz - ProdHaftG)** **§ 1 Haftung**

- (1) Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Im Falle der Sachbeschädigung gilt dies nur, wenn eine andere Sache als das fehlerhafte Produkt beschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist.

## **Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477)** **§ 75c IT-Sicherheit in Krankenhäusern**

- (1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.
- (2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

## **Bürgerliches Gesetzbuch (BGB)** **§ 823 Schadensersatzpflicht**

- (1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.
- (2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.





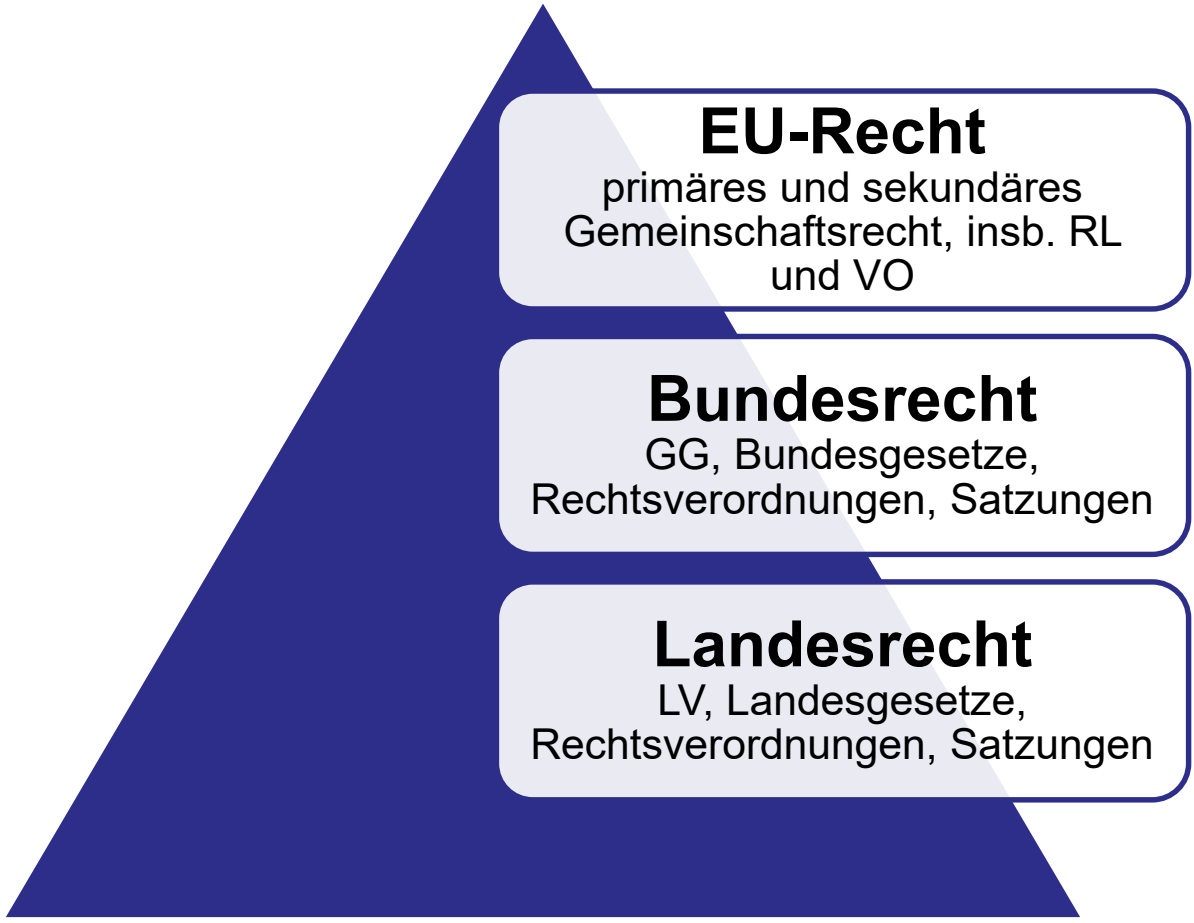


13. September 2017, State of the Union Address, former President Jean-Claude Juncker:

*"In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks."*







NIS 2016	<b>NIS2</b> 2022	CER 2022
DORA 2022	CRA 2019	AIA 2024
DSA 2024	DMA 2024	EHDS 2024 ?
ECA 2023	Data Act 2024	DGA 2022

# NIS2-Richtlinie (EU 2022/2555) / NIS2UmsCG



Die NIS2-Richtlinie ist eine EU-weite Gesetzgebung zur Netzwerk- und Informationssicherheit und legt Cybersecurity-Mindeststandards in der EU fest.

Bis Oktober 2024 müssen alle EU-Mitgliedsstaaten die NIS2-Richtlinie in nationale und regionale Gesetzgebung überführen.

In Deutschland erfolgt Umsetzung durch das NIS2UmsuCG.

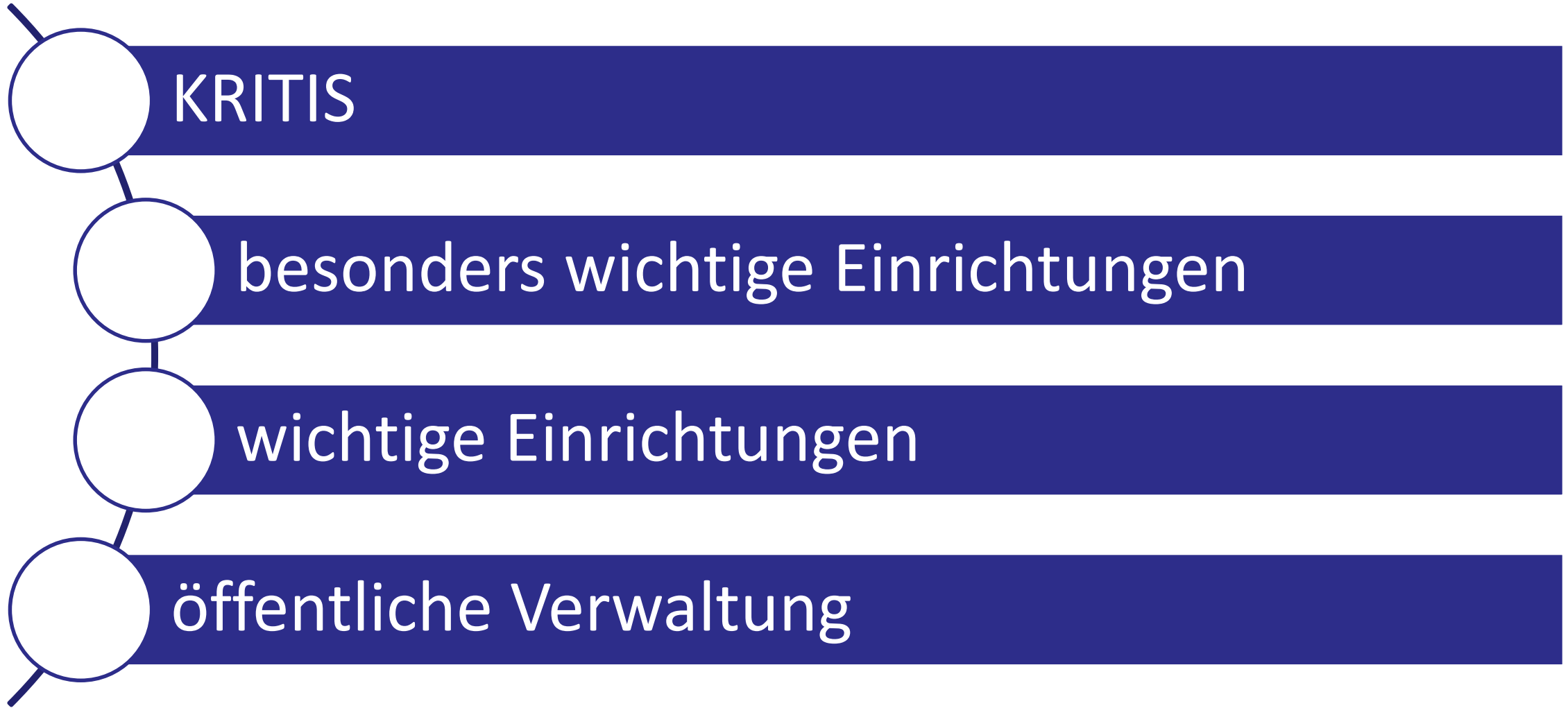
Länderbeteiligung nach § 47 Abs. 1 GGO Bund abgeschlossen, 4. Referentenentwurf angekündigt. Abschluss (nach BMI): Juli 2024

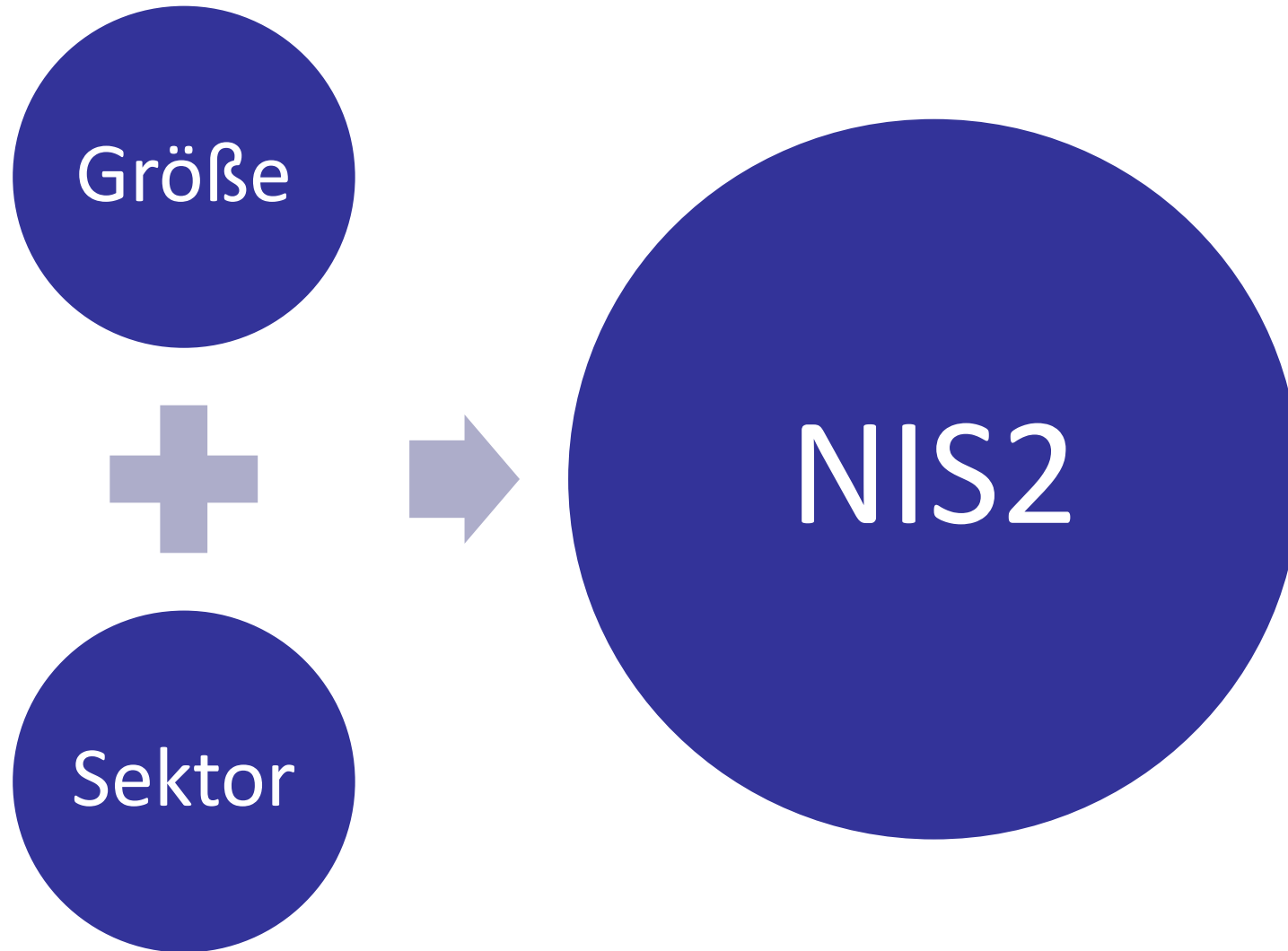


Versorgungsrelevanz

Wertschöpfung







## Mittlere Unternehmen

- 50 – 249 MA  
und Umsatz < 50 Mio.  
EUR oder Bilanz < 43  
Mio. EUR
- < 50 Mitarbeiter  
und Umsatz 10 - 50 Mio.  
EUR und Bilanz 10 – 43  
Mio. EUR

## Große Unternehmen

- > 249 MA
- Umsatz > 50 Mio. EUR  
und Bilanz > 43 Mio. EUR

## Von Unternehmensgröße unabhängig

- KRITIS
- besondere Auswirkungen
- qualifizierte  
Vertrauensdienste
- TLD-Registries
- DNS-Dienste



# KRITIS

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

# NIS2

Energie  
Wasser und Abwasser  
Gesundheit  
Transport und Verkehr  
Finanzen und Versicherungen  
Informationstechnik und  
Telekommunikation  
Digitale Dienste u. Infrastruktur  
Weltraum  
Lebensmittel  
Entsorgung, Abfallbewirtschaftung  
Verarbeitendes Gewerbe  
Chemie – Prod., Herstellung, Handel  
Forschung  
Post- und Kurierdienste





## besonders wichtige Einrichtungen

### große Unternehmen

- Energie
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheitswesen
- Trinkwasser Abwasser
- IT und TK
- Verwaltung IKT-Dienste
- Weltraum

### mittlere Unternehmen

- Anbieter öffentlicher TK-Netze

## wichtige Einrichtungen

### mittlere Unternehmen

- Energie
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheitswesen
- Trinkwasser, Abwasser
- IT und TK
- Verwaltung IKT-Dienste
- Weltraum

### große und mittlere Unternehmen

- Logistik
- Siedlungsabfallentsorgung
- Produktion
- Chemie
- verarbeitendes Gewerbe
- digitale Dienste



**Versorgungsrelevanz**

5.500 Unternehmen

**Wertschöpfung**

29.000 / 6.500 Unternehmen



---

Regulatorische  
Vorgaben

Risikomanagementmaßnahmen

---

Meldung erheblicher Sicherheitsvorfälle

---

Registrierung

---

Nachweispflichten

---

Aufsicht,  
Sanktion,  
Haftung

Aufsicht

---

Bußgelder

---

Haftung der Leitungsorgane

---

persönliche Haftung, nicht übertragbar

---

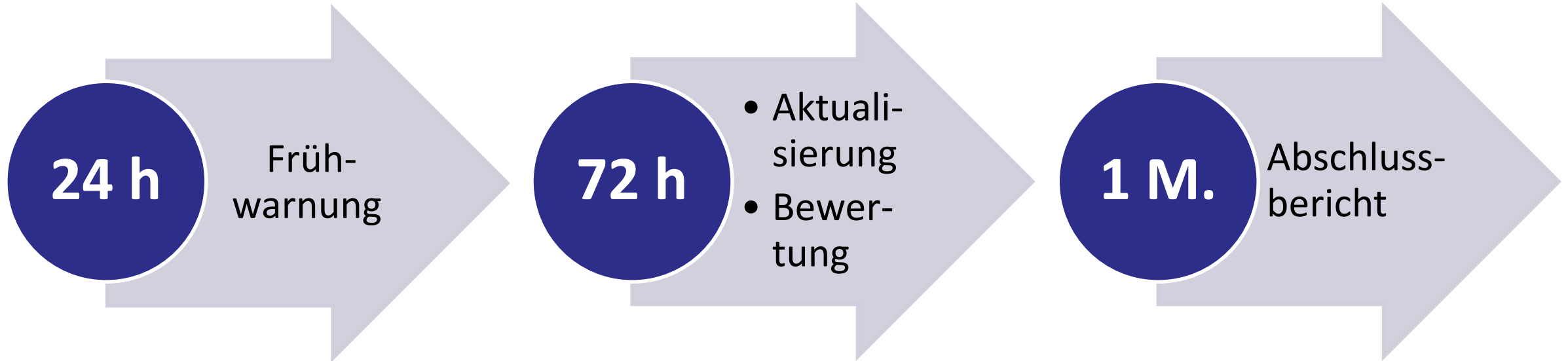


## Risikomanagementmaßnahmen (Auszug)

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Schulungen Cybersicherheit und Cyberhygiene
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)



# Meldepflichten



## Registrierung

- eigenverantwortliche Identifikation und Registrierung
- KRITIS-Anlagen: 1. Werktag nach Identifikation
- b.w. und w. Unternehmen innerhalb von 4 Monaten
- BSI-Registrierung möglich
- im Zweifel: Registrierung vornehmen

## Nachweispflichten

- besonders wichtige Einrichtungen betroffen
- Audits, Prüfungen oder Zertifizierung
- Betreiber kritischer Anlagen: Systeme zur Angriffserkennung



# Aufsicht

Aufsichtsbehörde: BSI

b.w.: ex-ante und ex-post-Aufsicht

Durchsetzungsmaßnahmen

# Sanktion

bis zu 10 Mio. EUR oder  
2% des weltweiten  
Konzernumsatzes

vgl.: DSGVO

# Haftung

Leitungsorgane

Genehmigung und  
Überwachung der  
Umsetzung

keine Übertragung =  
pers. Haftung



# CER-RL (EU 2022/2557) / KRITIS-Dachgesetz





Verpflichtet die Mitgliedstaaten, kritische Einrichtungen zu identifizieren und deren physische Widerstandsfähigkeit gegenüber Bedrohungen wie Naturgefahren, Terroranschläge oder Sabotage zu stärken.

Es werden Mindeststandards für **Betreiber Kritischer Infrastrukturen** festgelegt.

Ein zentrales Meldesystem für Störungen soll das bestehende Meldewesen im Cybersicherheitsbereich ergänzen.

Kritische Betreiber müssen (wahrscheinlich) bis spätestens 2026 durch Staaten identifiziert werden, die Betreiber wiederum müssen bis spätestens 2027 Maßnahmen umsetzen.



# Fazit und Ausblick





**Koordinierungsstelle-Cybersicherheit-NRW@im.nrw.de**

