

NIS 2

Navigieren Sie sicher durch die NIS 2-Welt.



Worum geht es?

EU-Richtlinie zur **N**etzwerk- und **I**nformations**S**icherheit

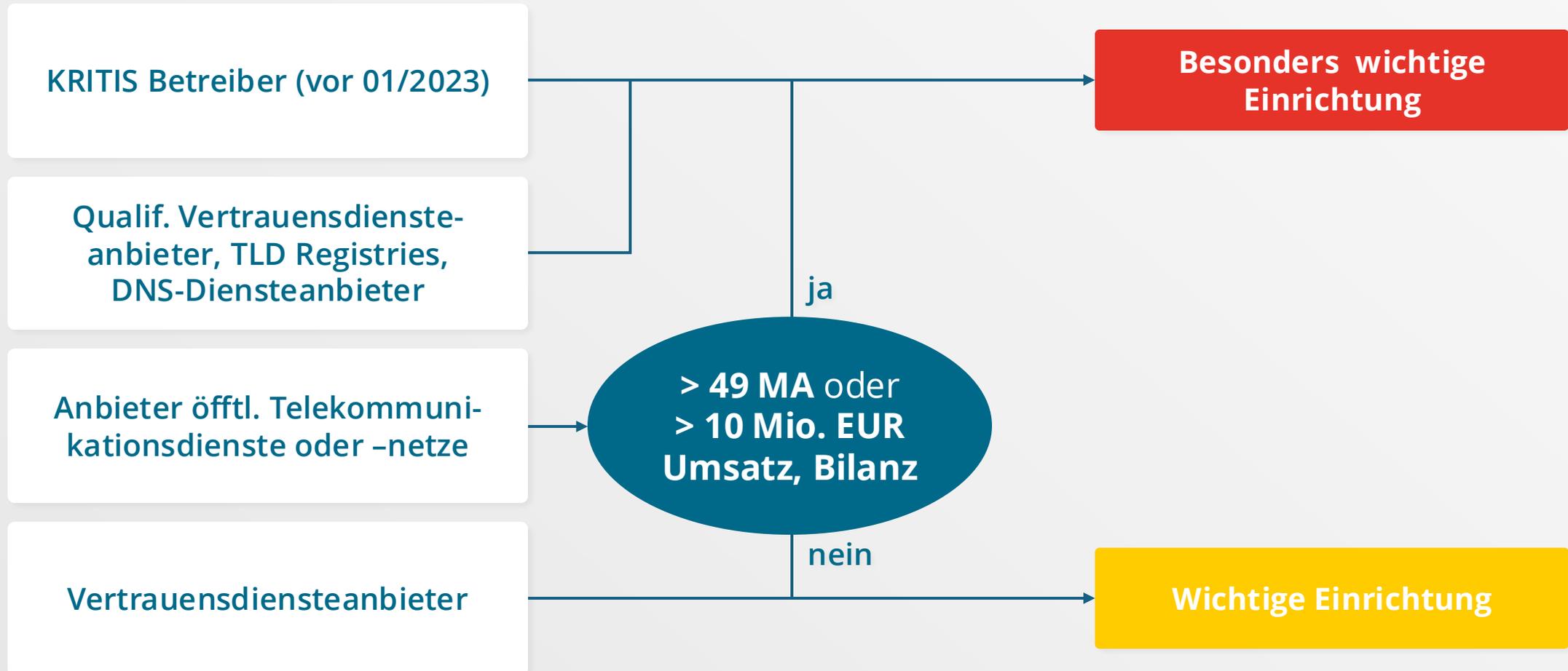


Sicherstellung eines hohen Cybersicherheitsniveaus innerhalb der EU



Optimierung des europäischen Binnenmarktes

Wer ist betroffen?



Wer ist betroffen? (nach Anlage 1)



Energie



Transport & Verkehr



Finanz- und
Versicherungswesen



Gesundheit



Wasser



Weltraum



Informationstechnik &
Telekommunikation

ab 250 MA oder
ab 50 Mio. EUR Umsatz oder
ab 43 Mio. EUR Bilanzsumme

**Besonders wichtige
Einrichtung**

50 bis 249 MA oder
10 bis 50 Mio. EUR Umsatz oder
ab 10 Mio. EUR Bilanzsumme

Wichtige Einrichtung



Wer ist betroffen? (nach Anlage 2)


Transport & Verkehr


Abfallbewirtschaftung


**Produktion, Herstellung
und Handel mit
chemischen Stoffen**


**Anbieter digitaler
Dienste**


**Produktion,
Verarbeitung, Vertrieb
von Lebensmitteln**


Forschung


**Verarbeitendes
Gewerbe/Herstellung
von Waren**

**≥ 50 MA oder
≥ 10 Mio. EUR Umsatz oder
Bilanzsumme**

Wichtige Einrichtung

Identifizierung und Registrierung



**Einrichtungen müssen
sich selbst prüfen/
IDENTIFIZIEREN**



innerhalb von drei Monaten
**beim Bundesamt für Sicherheit
in der Informationstechnik (BSI)
REGISTRIEREN**

**Betreiber kritischer Anlagen
müssen zusätzliche Angaben
machen und jederzeit
erreichbar sein.**



Bundesamt
für Sicherheit in der
Informationstechnik

Was ist zu tun?

Risikomanagementmaßnahmen umsetzen

Maßnahmen sollten ...



**aktuellem Stand
der Technik
entsprechen**



**einschlägige
Normen
berücksichtigen**



**auf gefahren-
übergreifendem
Ansatz beruhen**

Was ist zu tun?

Risikomanagementmaßnahmen umsetzen

NIS2UmsuCG verpflichtet, mindestens folgende Maßnahmen umzusetzen:

**Risikoanalyse- und
Sicherheitskonzepte**

**Konzept zur
Bewältigung von
Sicherheitsvorfällen**

**Backup- und
Krisenmanagement**

**Sicherheit der
Lieferkette**

**Implementierung von
Sicherheitsmaßnahmen**



Risikomanagementmaßnahmen umsetzen

NIS2UmsuCG verpflichtet, mindestens folgende Maßnahmen umzusetzen:

**Bewertung der
Wirksamkeit eigener
Maßnahmen**

**Verfahren und
Schulungen zur
Cyberhygiene**

**Kryptografie und
Verschlüsselung**

**Sicherheit bei Personal
und Anlagen**

**Authentifizierung und
gesicherte Notfall-
kommunikationssysteme**



Betreiber kritischer Anlagen

Betreiber kritischer Anlagen müssen zusätzlich ...

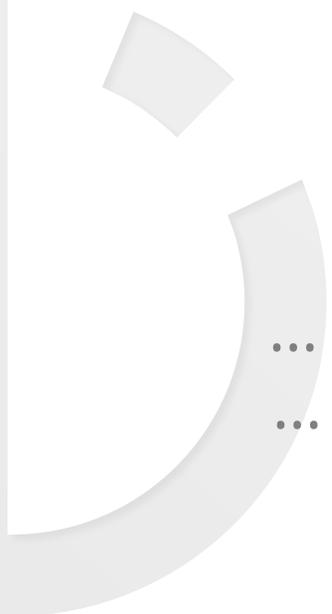


besondere Maßnahmen ergreifen, um IT-Systeme, -Komponenten und -Prozesse zu schützen



Systeme zur Angriffserkennung einsetzen

Geschäftsleitung schulen



GESCHÄFTSLEITUNG

- ... ist **verpflichtet** sich regelmäßig zu **schulen**
- ... ist **verantwortlich** und **persönlich haftbar**

Sicherheitsvorfälle melden

24^h

Erstmeldung erheblicher Sicherheitsvorfall

Verursacht durch **rechtswidrige** oder **böswillige Handlung**?
Grenzüberschreitende Auswirkungen?

72^h

Erstmeldung korrigieren oder bestätigen

erste Bewertung mit Schweregrad, Auswirkungen und ggf. den Kompromittierungsindikatoren

1^M

Abschlussmeldung

Betreiber kritischer Anlagen müssen zusätzlich die Art der betroffenen Anlage und kritischen Dienstleistung melden.

Umsetzung nachweisen

Besonders wichtige Einrichtungen

**stichprobenartige
Prüfungen** durch das BSI

wichtige Einrichtungen

**anlassbezogene
Prüfungen** durch das BSI
*bei gerechtfertigter Annahme, dass
Anforderungen nicht oder nicht
richtig umgesetzt sind*

Betreiber kritischer Anlagen

unterliegen zusätzlichen
Prüfpflichten beim BSI
alle drei Jahre
Sicherheitsaudit

Wer ist verantwortlich?

GESCHÄFTSLEITUNG

... ist **verantwortlich** und **verpflichtet**
Risikomanagementmaßnahmen umzusetzen,
zu überwachen und ist **persönlich haftbar**



... und wenn sich keiner kümmert?



**Verhängung von
Bußgeldern**



**Entzug von
Genehmigungen
vorübergehende
Untersagung
Tätigkeit als
Geschäftsleitung**



**Zusätzlich Folgen
für die Einrichtung**

Und wie geht es nun weiter?

1

**Sind Sie betroffen?
PDV-Quick-Check**

2

**Geschäftsführung
informieren**

3

**zuständige Personen
bestimmen**

4

aktuellen Stand prüfen

5

**Umsetzung
Risikomanagement-
maßnahmen**

6

**Gesetzgebungsprozess
verfolgen**

Weitere Informationsquellen

- VEEAM - PDV NIS 2-Webinar – am 24.09.2024: <https://t1p.de/nis2pdvwebinar>
- Infos des BSI: <https://t1p.de/bsinis2infos>
- OpenKRITIS: <https://t1p.de/openkritisnis2>
- Regierungsentwurf des NIS2UmsuCG: <https://t1p.de/NIS2UmsuCGRegierungsentwurf>
- Teletrust Handreichung Stand der Technik: <https://t1p.de/SdT>
- EU NIS 2 Richtlinie: <https://t1p.de/NIS2EU>



VIELEN DANK!

PDV-Systeme GmbH

