# Kritische Infrastruktur Wasserversorgung

## Anforderungen an die IT-Sicherheit: Neue und kommende Gesetze in der Wasserversorgung (KRITIS und nicht-KRITIS)

*Dr. -Ing. Sigrid Schwub*

# Aktuelle Bedrohungslage



IT-SICHERHEIT

## Ist Kaspersky wirklich ein Problem?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor de russischen Unternehmen. Doch wie berechtigt es ist, Kaspersky als unsiche bezeichnen, bleibt unklar.

von Eva Wolfangel


17.03.22

## "Cyberangriffe aus Russland eine ernstzunehmende Gefahr"

Der Bundesverband zum Schutz Kritischer Infrastrukturen (BSKI), aber auch Politiker warnen angesichts der politischen Lage in der Ukraine vor Cyber-Attacken. Kanzler Scholz will die Resilienz von kritischen Infrastrukturen stärken.

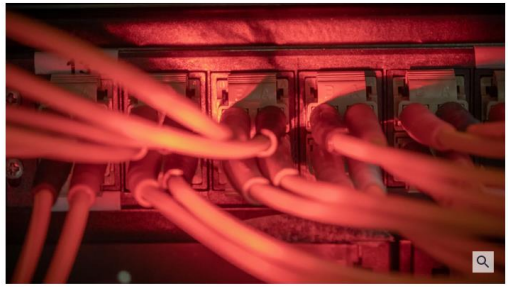
27.02.2022

**Hotline für Unternehmen eingerichtet**

Der BSKI empfiehlt Unternehmen, sich gegen Cyberschäden zu wappnen und entsprechende Vorkehrungen zu treffen. IT-Spezialisten sollten im Angriffsfall verfügbar sein, Notfallpläne sollten überprüft, Sicherheitskopien gemacht werden. Das BSKI-Mitglied NovaStor hat aus diesem Grund eine Hotline geschaltet, unter der sich Unternehmen kostenfrei über Maßnahmen zur Überprüfung ihrer Datensicherung beraten lassen können. Die Hotline ist erreichbar über https://de.novastor.com/#cyberkrise. (sg/dpa)

## Alarmstufe Orange gegen den Blackout

18. Februar 2022, 14:22 Uhr | Lesezeit: 3 min



Jedes mit dem Internet verbundene Gerät ist ein potenzielles Einfallstor für Hacker. Richtig heikel wird es, wenn Unternehmen betroffen sind, die die Versorgung der Bevölkerung mit dem Wichtigsten sicherstellen. (Foto: Picture Alliance/dpa)

**Wenn die Lage in der Ukraine eskaliert, steigt die Wahrscheinlichkeit, dass Hackerangriffe Versorger und Telekommunikation treffen. Die Geheimdienste dürften sich längst in den Computern eingenistet haben.**

Die Farbe ist dunkler geworden. Als Bedrohungsstufe Orange war die Nachricht gekennzeichnet, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn am Montag an Deutschlands essenzielle Unternehmen verschickte. Die obersten Cyberwächter warnten vor Hackerangriffen im Zuge der Ukraine-Krise. Orange bedeutet: "Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs." Zehn Tage zuvor war noch eine Warnung mit der niedrigeren Stufe Gelb an die Betreiber kritischer Infrastruktur herausgegangen. Zu ihnen zählen unter anderem große Gas-, Wasser- und Stromversorger sowie Krankenhäuser.

Überlaufende Klärbecken, verunreinigtes Trink-wasser…

# Stichworte zum Thema IT-Sicherheit



HÜTTL & VIERKORN
BUSINESS- & IT-CONSULTING

RCE

IT-SiG

BSI

DVGW

Grundschutz

Technische Richtlinien/
DVGW Regelwerk

ISO27001

B3S

Wasserhaushaltsgesetz

Kritis-V

NIS

Trinkwasserverordnung

# Anforderungen/Akteure



| Gesetze / Richtlinien | Akteure | Methoden | Umsetzungshilfen / Konkretisierungen |
|---|---|---|---|
| Trinkwasserverordnung | BSI | Grundschutz (BSI) | DVGW Regelwerk/DIN Normen |
| Wasserhaushaltsgesetz | DVGW | ISO27001 | BSI-TR |
| RCE | | CISIS12 | B3S |
| NIS | | | Kritis-V |
| IT-SiG (Artikelgesetz) | | | |

# Anforderungen/Akteure



| Gesetze / Richtlinien | Akteure | Methoden | Umsetzungshilfen / Konkretisierungen |
|---|---|---|---|
| Trinkwasserverordnung | BSI | Grundschutz (BSI) | DVGW Regelwerk/DIN Normen |
| Wasserhaushaltsgesetz | DVGW | ISO27001 | BSI-TR |
| RCE | | CISIS12 | B3S |
| NIS | | | Kritis-V |
| IT-SiG (Artikelgesetz) | | | |

# Gesetzliche Vorgaben



## EU Gesetzgebung

Umsetzung in nationales Recht

## Nationales Recht

**NIS Richtlinie** (Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit)

**IT-SiG** (IT-Sicherheitsgesetz, Artikelgesetz)

**BSIG**, TKG, TMG, AtomG,…

KRITIS-Verordnung (**KRITIS-V**)

# (Gesetzliche) Anforderungen & Haftung



## KRITIS – Änderungen stehen unmittelbar bevor!

Umsetzung in nationales Recht

### NIS Richtlinie

- NIS 1 ist im August 2016 in Kraft getreten
- NIS 2: Okt. 2021: Kompromiss Vorschlag des EU-Parlaments
- 03.12.21: Rat der Europäischen Union hat Entwurf akzeptiert
- Letzte Abstimmung zwischen EU-Rat, EU-Parlament und ITRE (Industrieausschuss) müssen finale Formulierung fixieren
- in Kraft treten wird noch im 1. Halbjahr 2022 erwartet
- NIS 2 muss innerh. Von 18 Monaten nach in Kraft treten in nationales Recht umgesetzt werden (→ IT SiG, KritisV)

### IT-SiG & KritisV

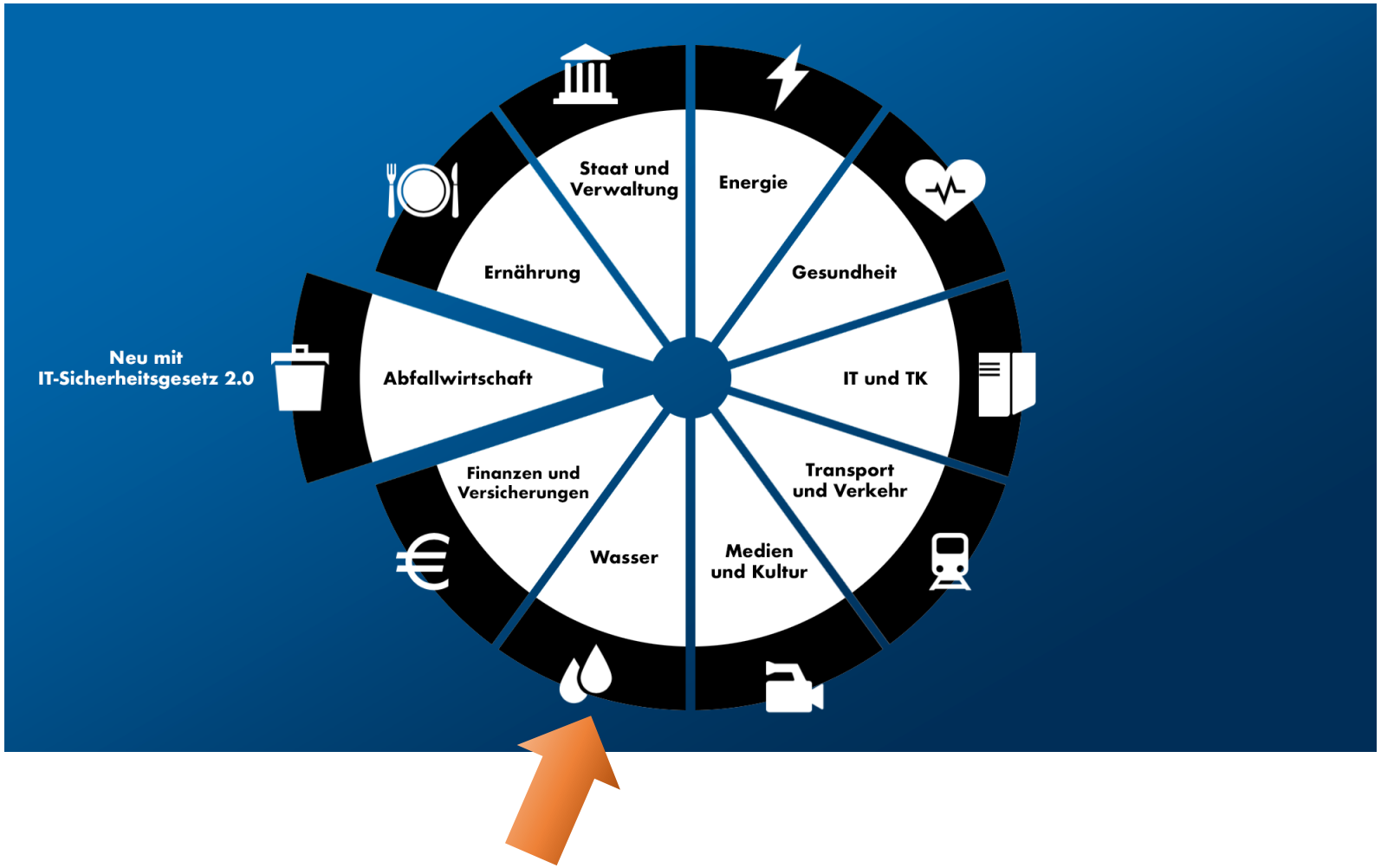
- IT – Sicherheitsgesetz 2.0: In Kraft Treten 18.05.2021
- IT-SiG (Artikelgesetz) ändert das „Gesetz über das Bundesamt in der Informationstechnik“ (BSI-BSIG) sowie weitere (TKG, TMG, EWG)
- Überarbeitung der BSI-Kritis Verordnung (KritisV): Beschluss am 18.08.2021, In Kraft Treten 01.01.2022

**Bisher: Definition der Einrichtungen, die als Kritische Infrastruktur gelten durch IT-SiG und Kritis-V**

# IT-SiG 2.0: Betroffene Sektoren



IT – Sicherheitsgesetz 2.0: betroffene Sektoren




https://rz10.de/knowhow/it-sicherheitsgesetz-2-0/

# IT SiG 2.0 – Was ist neu?



## Anforderungen des BSIG

- Das IT-Sicherheitsgesetz verpflichtete betroffene Unternehmen, die **IT-Infrastruktur, die für die Erbringung ihrer Dienste notwendig ist, nach dem „Stand der Technik“ abzusichern**. (§ 8a). **Organisatorische und technische Vorkehrungen** sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.“) Eine **regelmäßige Überprüfung** der Maßnahmen im Abstand von jeweils zwei Jahren ist obligatorisch (§8a).

## Neu mit IT-SiG 2.0, seit Mai 2021 in Kraft:

- Das BSI darf **Portscans** an Schnittstellen zu öffentlichen Telekommunikationsnetzen durchführen sowie Honeypots einsetzen (Systeme und Analyse-Maßnahmen für Schadprogramme und Angriffsmethoden). (§7b)
- **KRITIS-Betreiber** müssen **Angriffserkennungssysteme** einsetzen (§8a, 1a).
- Für den Einsatz kritischer Komponenten in kritischen Infrastrukturen muss eine **Garantieerklärung** zur Vertrauenswürdigkeit von Herstellen vorliegen. Diese umfasst unter anderem die gesamte Herstellerkette. (§ 9b)
- Neufassung der **Bußgeldvorschrift** (Strafen bis 2 Mio. EUR).

# BSIG – Bußgeldvorschriften §14



**2 Mio.€**

Anordnungen zur Wiederherstellung oder Gefahrenabwehr zuwiderhandeln

**1 Mio.€**

KRITIS-Maßnahmen nicht umsetzen oder nachweisen

**500 TSD €**

Fehlende Mitwirkung bei Störungsbeseitigung
Fehlende Auskünfte von DSPs
Fehlende Registrierung als KRITIS oder UNBÖFI
Meldungen nicht absetzen bei KRITIS, DSP und UNBÖFI
DSP Maßnahmen nicht umsetzen
Selbsterklärung von UNBÖFI nicht vorlegen
Konformitätsbewertung ohne Genehmigung durchführen
Sicherheitskennzeichen ohne Genehmigung verwenden
Sicherheitsangaben oder Lücken zertifizierter Produkte nicht veröffentlichen

**100 TSD €**

Herstellerinformationen nicht herausgeben
Zugang oder Unterlagen zu KRITIS-Maßnahmen/Registrierung verweigern
Fehlende Erreichbarkeit als KRITIS

**20 Mio.€**

als juristische Person/Organ (§30 Abs. 2 OWiG)
Anordnungen zur Wiederherstellung oder Gefahrenabwehr zuwiderhandeln

**10 Mio.€**

als juristische Person/Organ (§30 Abs. 2 OWiG)
KRITIS-Maßnahmen nicht umsetzen oder nachweisen

# BSI-Kritis-V



= Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI Gesetz (BSIG)

*Die Kritis - Verordnung definiert die Schwellenwerte, ab wann ein Betreiber unter die KRITIS Regularien fällt.*

**§ 3 Sektor Wasser**

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Wasser kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die Versorgung der Allgemeinheit mit Trinkwasser (Trinkwasserversorgung);
2. die Beseitigung von Abwasser der Allgemeinheit (Abwasserbeseitigung).

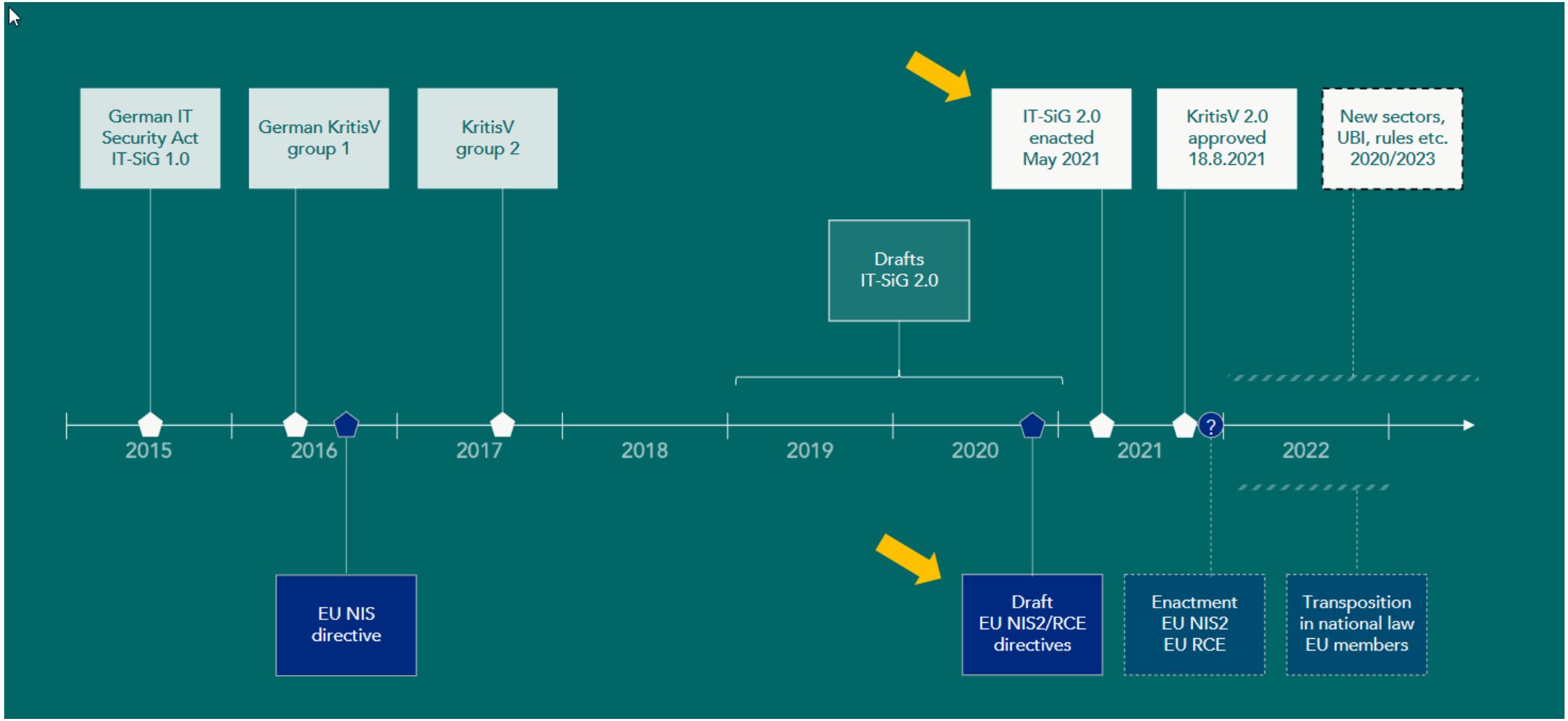
(2) Die Trinkwasserversorgung wird in den Bereichen Gewinnung, Aufbereitung, Verteilung sowie Steuerung und Überwachung von Trinkwasser erbracht.
(3) Die Abwasserbeseitigung wird in den Bereichen Siedlungsentwässerung, Abwasserbehandlung und Gewässereinleitung sowie Steuerung und Überwachung erbracht.
(4) Im Sektor Wasser sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 2 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und die für die Trinkwasserversorgung und Abwasserbeseitigung in den Bereichen erforderlich sind, die in den Absätzen 2 und 3 genannt werden, und
2. den Schwellenwert nach Anhang 2 Teil 3 Spalte D erreichen oder überschreiten.

… **22 Mio. m³** gewonnene/aufbereitete/verteile/überwachte Wassermenge pro Jahr
…**500.000 angeschlossene Einwohner** für Kanalisation/Kläranlage/überwachte Einwohner

# NIS 2.0 – die Timeline






Quelle: www.openkritis.de

# NIS 2 – Stand 03/2022

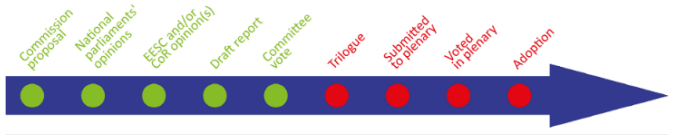


## NIS 2: wer ist betroffen?

- Definiert Wesentliche Einrichtungen (Energie, Verkehr, Bankenwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Pharmazeutik, **Trinkwasserversorgung, Abwasserwirtschaft,** digitale Infrastrukturen (u.a. Anbieter von Rechenzentrumsdiensten) öffentliche Verwaltung, Weltraum, sowie wichtige Einrichtungen.

- Die bisherigen EU NIS und ECI (European Critical Infrastructures) Direktiven werden 2021 durch NIS2 und EU RCE abgelöst. Beide Direktiven müssen noch in der EU verabschiedet und dann in nationales Recht überführt werden. Dazu sind die Trilog-Verhandlungen zwischen EU-Parlament, EU-Kommission und EU-Rat im Gange. Bis Ende Juni 2022 wird die Abstimmung im Parlament erwartet.

| **Proposal for a directive on measures for a high common level of cybersecurity across the Union** | | |
|---|---|---|
| *Committee responsible:* | Industry, Research and Energy (ITRE) | COM(2020) 823<br>16.12.2021 |
| *Rapporteur:* | Bart Groothuis (Renew, the Netherlands) | 2020/0359(COD) |
| *Shadow rapporteurs:* | Eva Maydell (EPP, Bulgaria)<br>Eva Kaili (S&D, Greece)<br>Rasmus Andresen (Greens/EFA, Germany)<br>Thierry Mariani (ID, France)<br>Evžen Tošenovský (ECR, Czechia)<br>Marisa Matias (The Left, Portugal) | Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision') |
| *Next steps expected:* | Trilogue negotiations | |



# NIS 2.0 – Anwendungsbereich



- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

*Artikel 2*

***Anwendungsbereich***

(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[28] angesehen werden.

(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn

d) sich eine mögliche Störung des von der Einrichtung erbrachten Dienstes auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

Der Anwendungsbereich wird nicht mehr durch nationale Verordnungen (KRITIS-V) und länderspezifischen Schwellenwerte bestimmt, sondern direkt in der europäischen Richtlinie → kein/kaum nationaler Spielraum mehr!

# NIS 2.0 – Anwendungsbereich-Sektoren



*ANHANG I*

*WESENTLICHE EINRICHTUNGEN:*

*SEKTOREN, TEILSEKTOREN UND ARTEN VON EINRICHTUNGEN*

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| 6. Trinkwasser | | Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie 98/83/EG des Rates[23], jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch nur ein Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist, die nicht als wesentliche oder wichtige Dienste eingestuft werden |
| 7. Abwasser | | Unternehmen, die kommunales, häusliches oder industrielles Abwasser im Sinne des Artikels 2 Nummern 1 bis 3 der Richtlinie 91/271/EWG des Rates[24] sammeln, entsorgen oder behandeln. |

Der Sektor Wasser mit Trinkwasserversorgung und Abwasserbehandlung gilt als „Wesentliche Einrichtung“ („essential entitiy“)

# NIS 2.0 – Anwendungsbereich-KMU Def.



- Neu ist, dass die Schwellenwerte nun direkt in der NIS Richtlinie definiert werden, nicht mehr durch Nationales Recht (bisher: KritisV). Neuer Anwendungsbereich (Artikel 2 (1): NIS 2 Richtlinie gilt **für ALLE öffentliche und private Einrichtungen, die als wesentlich oder wichtig klassifiziert** wurden. Ausgenommen sind nur kleine oder Kleinstunternehmen gemäß der KMU Definition 2003/361/EG der Kommission (d.h. nur Unternehmen mit <50 MA UND Jahresumsatz oder Jahresbilanz < 10 Mio. Euro sind ausgenommen)

- ABl. L 124 vom 20.5.2003, Satz (13): *„…erweist es sich als notwendig zu bestätigen, dass ein Unternehmen, dessen Unternehmensanteile oder Stimmrechte zu **25 % oder mehr von einer staatlichen Stelle oder Körperschaft des öffentlichen Rechts** kontrolliert werden, **kein KMU** ist.“*

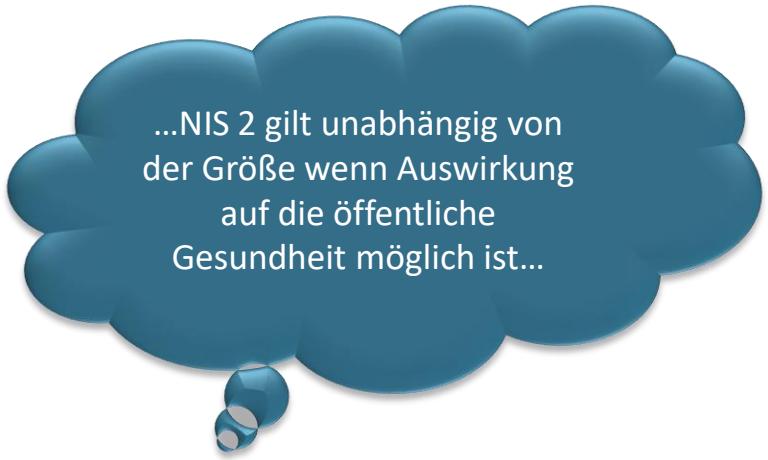
***→ ALLE kommunalen Einrichtungen sind gem. NIS 2 Entwurf unabhängig von ihrer Größe KRITISCHE Infrastruktur***

# NIS 2.0 – Anwendungsbereich-KMU Def.



**Vorschlag ITRE (Ausschuss des Parlaments)**

1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of ***Article 2(2) and (3) of the Annex to*** Commission Recommendation 2003/361/EC[28]. ***By way of derogation from Article 3(4) of the Annex to Recommendation 2003/361/EC, entities with a stake of 25% by a public body shall be considered to be SMEs.***




*„Da Frankreich aktuell die Ratspräsidentschaft innehat und sich den Abschluss des Dossiers auf die Fahnen geschrieben hat, könnten französische Ratsvertreter im Trilog nochmals nachlegen.“*

https://www.heise.de/news/Deutsche-Wirtschaft-fordert-Schutz-der-Verschluesselung-und-sichere-Behoerden-6333954.html

**Bestimmung der Partner- und Verbundunternehmen bei öffentlichen Einrichtungen?**

Entlehnung aus „Dezemberbeihilfen“:

„Demnach ist auch bei öffentlichen Unternehmen zu prüfen, inwiefern ein wirtschaftlicher Verbund mit anderen Unternehmen vorliegt, wobei insbesondere das Bestehen von Kontrollbeteiligungen relevant ist. Bei einem kommunalen Unternehmen dürfte der maßgebliche Verbund zum Beispiel in der Regel auf Ebene der Kommune enden, da diese eine eigene öffentlich-rechtliche Gebietskörperschaft mit Selbstverwaltungsrecht ist.“

# NIS 2.0 – Was steht im Entwurf?



Was müssen kritische Infrastrukturen erfüllen?

**Cyber Security**

Betreiber in der EU müssen mindestens folgende Cyber Security Maßnahmen umgesetzen, um die IT und Netzwerke ihrer kritischen Dienstleistungen zu schützen: Art. 17 Art. 18

1. **Policies**: Richtlinien für Risiken und Informationssicherheit
2. **Incident Management**: Prävention, Detektion und Bewältigung von Cyber Incidents
3. **Kontinuität**: BCM und Krisenmanagement
4. **Supply Chain**: Sicherheit in der Lieferkette — bis zur sicheren Entwicklung bei Zulieferern
5. **Test und Audit**: Methoden zur Messung der Effektivität von Informationssicherheit
6. **Kryptographie**: Angemessener Einsatz von Verschlüsselung

→ Erfüllung des BSIG, welches nochmals zur Umsetzung der NIS2 Richtlinie überarbeitet werden muss!

# NIS 2.0 – Sicherheit in der Lieferkette



*Artikel 5*

***Nationale Cybersicherheitsstrategie***

(2) Im Rahmen der nationalen Cybersicherheitsstrategie nehmen die Mitgliedstaaten insbesondere die folgenden Konzepte an:

a) ein Konzept für die Cybersicherheit in der Lieferkette für IKT-Produkte und -Dienste, die von wesentlichen und wichtigen Einrichtungen für die Erbringung ihrer Dienste genutzt werden;

b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;

→ Bereits jetzt bei Neuanschaffungen geeignete Hersteller wählen

# NIS 2.0 – Kontrollen & Nachweise



*Artikel 29*

**Aufsicht und Durchsetzung in Bezug auf wesentliche Einrichtungen**

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wesentliche Einrichtungen befugt sind, in Bezug auf diese Einrichtungen folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich Stichprobenkontrollen;

b) regelmäßige Prüfungen;

c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;

d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien;

e) Anforderung von Informationen, die für die Bewertung der von der Einrichtung ergriffenen Cybersicherheitsmaßnahmen erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Meldepflicht gegenüber der ENISA nach Artikel 25 Absätze 1 und 2;

f) Anforderung des Zugangs zu Daten, Dokumenten oder sonstigen Informationen, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind;

g) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

Weitreichende Kontrollbefugnisse des BSI, auch ohne „Verdacht“ / „Anlass“

# NIS 2.0 – Haftung



*Artikel 29*

**Aufsicht und Durchsetzung in Bezug auf wesentliche Einrichtungen**

(6) Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung die in dieser Richtlinie festgelegten Verpflichtungen erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung der in dieser Richtlinie festgelegten Verpflichtungen haftbar gemacht werden können.

Auch persönliche Haftung für verantwortliche (natürliche) Personen!
Bußgelder s. BSIG

# Exkurs - Haftung im Schadensfall



Um einer (persönlichen) Haftung sowie Schadensersatzpflicht zu entgehen, müssen **ALLE** Unternehmen

1. den Stand der Technik erfüllen
2. ein Risikomanagement haben
3. eine ordnungsgemäße Dokumentation darüber vorweisen können

Auch für Kommunen gilt: **Jeder Leiter einer Verwaltung**, egal ob Bürgermeister oder Gemeinschaftsvorsitzender, sowie jeder Geschäftsführer eines Unternehmens ist für die Einhaltung der Vorschriften der gesellschaftlichen Sorgfaltspflicht sowie der gesetzlichen Regelungen (IT SiG, KritisV) **verantwortlich**.
Sind die IT-Mängel schuldhaft zu vertreten, d.h. hätten die Mängel bei gebotener Sorgfalt erkannt werden können, so **haftet der kommunale Betrieb** für dadurch entstandene Schäden. (Amtshaftung: Haftung der juristischen Person des öffentlichen Rechts nach § 839 BGB i.V.m. Art. 34 GG für rechtswidriges schuldhaftes Handeln)

**Auch öffentlich-rechtliche Verbände haften für Umweltschäden** (15.12.2020):
Der Europäische Gerichtshof (EuGH) hat entschieden, dass juristische Personen des öffentlichen Rechts – wie z. B. kommunale Wasserverbände – für Umweltschäden haften können, auch wenn sie aufgrund gesetzlicher Aufgabenübertragung im öffentlichen Interesse tätig werden. Grundlage hierfür ist das Umweltschadensgesetz und die ihm zugrunde liegende EU-Umwelthaftungsrichtlinie.

# Was muss ich tun?



Aktuelle politische Lage

NIS2 / IT-SiG Anforderungen

Sicherung der öffentlichen Wasserversorgung / Gesundheit

Reduktion des Haftungsrisikos

1. Ein Risikomanagement einführen und eine ordnungsgemäße Dokumentation darüber vorweisen können, d.h. ein **ISMS einführen**
2. Den **Stand der Technik** erfüllen
3. Ein Cybersicherheitskonzept erstellen und erfüllen

➡ Zu erledigen bis NIS2-In-Kraft-Treten + 18 Monate, d.h. ~ **Mitte-Ende 2024**

# ISMS



Einführung eines Informations-Sicherheits-Management-Systems (ISMS), z.B. :

- ISO 27001
- CISIS12
- BSI-Grundschutz

→ Regelung der Ablauforganisation
→ Kontinuierliche Verbesserung der IT-Sicherheit (PDCA-Zyklus)
→ Systematische Kontrolle und Nachverfolgung von Maßnahmen

Durch ein ISMS verfügt man über die geforderten Organisationsstrukturen und Nachweisdokumente
Ein ISMS beinhaltet auch ein Risikomanagementsystem, inkl. Notfallplanung usw. (Stichwort BCM = Business Continuity Management)

# ISMS – Beispiel ISO 27001



## Beispiel ISO/IEC 27001: international führende Norm für Informationssicherheits-Managementsysteme

Sie bietet Organisationen aller Größen klare Leitlinien für die Planung, Umsetzung, Überwachung und Verbesserung ihrer Informationssicherheit. Die Anforderungen sind generell anwendbar und gelten für private sowie öffentliche Unternehmen oder gemeinnützige Institutionen.

***Hinweis: Aktuell gibt es noch Fördergelder für die Einführung eines Managementsystems***

- *Zuschuss für: kommunale Gebietskörperschaften und deren Zusammenschlüssen sowie die von ihnen in öffentlich-rechtlicher Form geführten Unternehmen und Einrichtungen mit Sitz in Bayern.*
- *Zuschuss von 50% für Beratung, Schulung, Zertifizierung*
- *Gilt noch bis 31.12.2022*

# Stand der Technik – B3S Wasser und Grundschutz



## Was bedeutet „Stand der Technik“??

### BSI Grundschutz

- Wurde 2021 als überarbeitetes Kompendium herausgegeben
- Der Grundschutz gliedert sich in sog. Bausteine (thematische Aufteilung)
- Jeder Baustein besteht aus Unterpunkten
- Berücksichtigt sowohl **technische** als auch **organisatorische** Anforderungen, d.h. ist ähnlich einem Managementsystem nach ISO 27001
- Der Grundschutz differenziert die Maßnahmen nach dem Schutzbedarf (normaler bzw. erhöhter Schutzbedarf)

### B3S Wasser (Branchenstandard Wasser)

- Der Stand der Technik kann von Betreibern oder Verbänden in B3S (Branchenstandards)erfasst …werden.
- Aktueller B3S Wasser: Gibt vor, was als Stand der Technik erfüllt werden muss wenn der Betreiber unter die KritisV fällt, aber auch was erfüllt werden muss, wenn der Betreiber Unterhalb der Schwellenwerte der KritisV liegt. (Derzeitiger Schwellenwert: 22 Mio $m^3$ Wasser)
- Der B3S Wasser referenziert bei der Definition des „Stand der Technik“ auf den BSI Grundschutz. Er gibt an, welche Unterpunkte von welchem Baustein erfüllt werden müssen.

# Möglichkeiten zur Unterstützung



## Grundschutz-Check = IST Analyse

- Überprüfung des organisatorischen und technischen IST Zustandes
- Bericht mit Schwachstellenanalyse
- Gap-Analyse zu B3S (Grundschutz) und/oder ISO27001

## ISMS

- Unterstützung bei der Einführung eines ISMS oder einer Vorstufe
- Stellen eines externen ISB (Informations-Sicherheits-Beauftragten) zur Aufrechterhaltung des ISMS

## Technische Umsetzung

- Erstellung und Umsetzung eines Soll-Konzepts
- Laufende Begleitung möglich

# Kontaktdaten



HÜTTL & VIERKORN
BUSINESS- & IT-CONSULTING

**Hüttl & Vierkorn Wirtschaftsberatungs GmbH & Co.KG**
Weinbergstraße 30
91710 Gunzenhausen

09831 / 68394-0
schwub@huettl-vierkorn.de