NIS2 Umsetzungsgesetz (NIS2UMSUCG)

IT for innovators.

Hans-Martin Kuhn
Cyber Security Consultant
T.I.S.P. TeleTrust Information Security Professional

Email: hans-martin.kuhn@acp.de

IT for innovators.

Agenda

- Wer ist betroffen?
- Geforderte Maßnahmen
- Update NIS2
- ACP-Lösungen

IT for innovators.

NIS2 Prüf-Check

>= 10 Mio. Jahresumsatz und >= 50 Mitarbeiter

Unternehmen	Mitarbeiter		Umsatz		Bilanz
Mittel § 28 Abs. 2 BSIG-E	50-249	oder	< 10 Mio. EUR	und	≥ 10 Mio. EUR
Groß § 28 Abs. 1 BSIG-E	≥ 250	oder	≥ 50 Mio. EUR	und	≥ 43 Mio. EUR

IT for innovators.

NIS2 Prüf-Check

>= 10 Mio. Jahresumsatz <u>oder</u> >= 50 Mitarbeiter

<u>und</u>

IT for innovators.

NIS2 Prüf-Check

>= 10 Mio.
Jahresumsatz oder
>= 50 Mitarbeiter

und

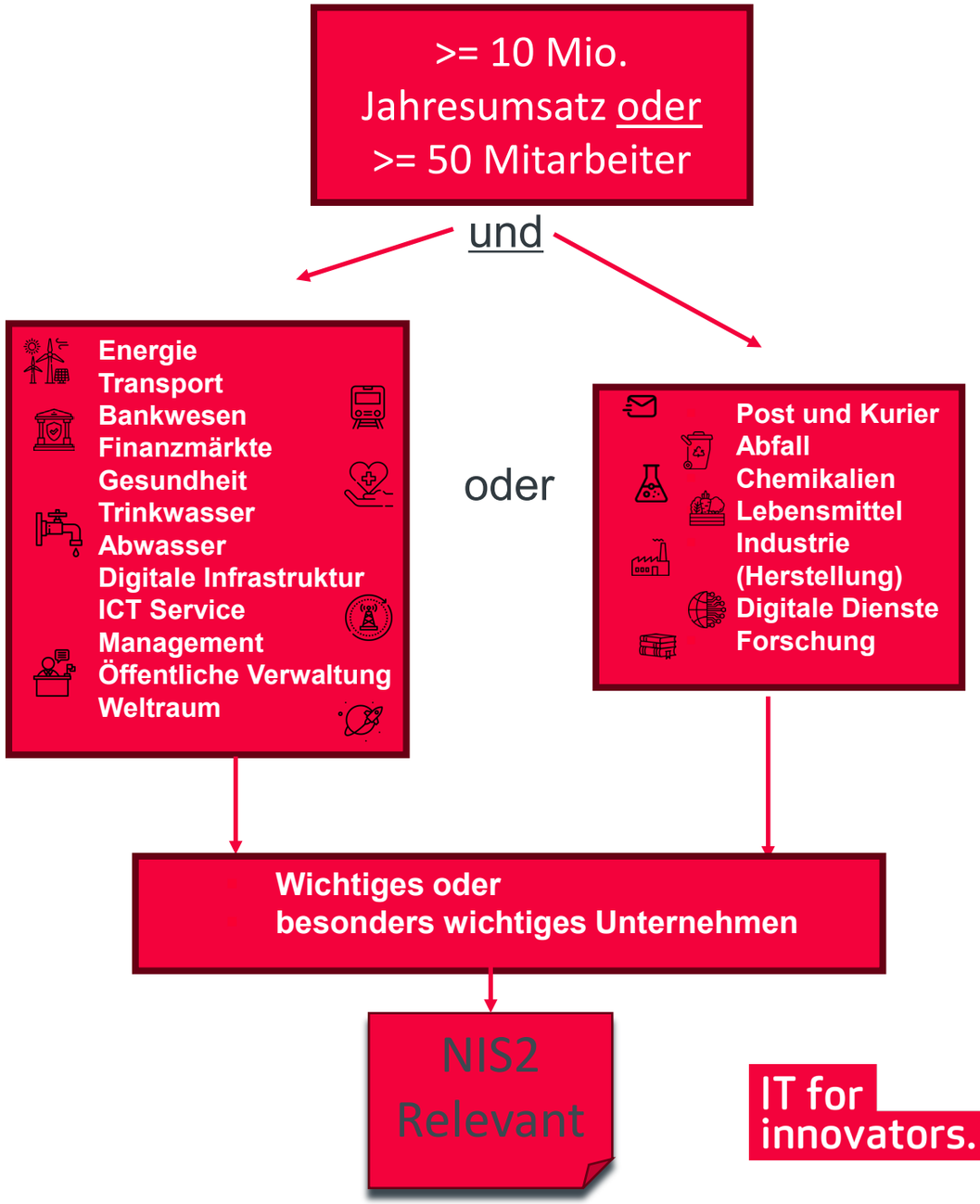
- Energie
- Transport
- Bankwesen
- Finanzmärkte
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- ICT Service Management
- Öffentliche Verwaltung
- Weltraum

oder

- Post und Kurier
- Abfall
- Chemikalien
- Lebensmittel
- Industrie (Herstellung)
- Digitale Dienste
- Forschung

IT for innovators.

NIS2 Prüf-Check



IT for innovators.

NIS2 Prüf-Check

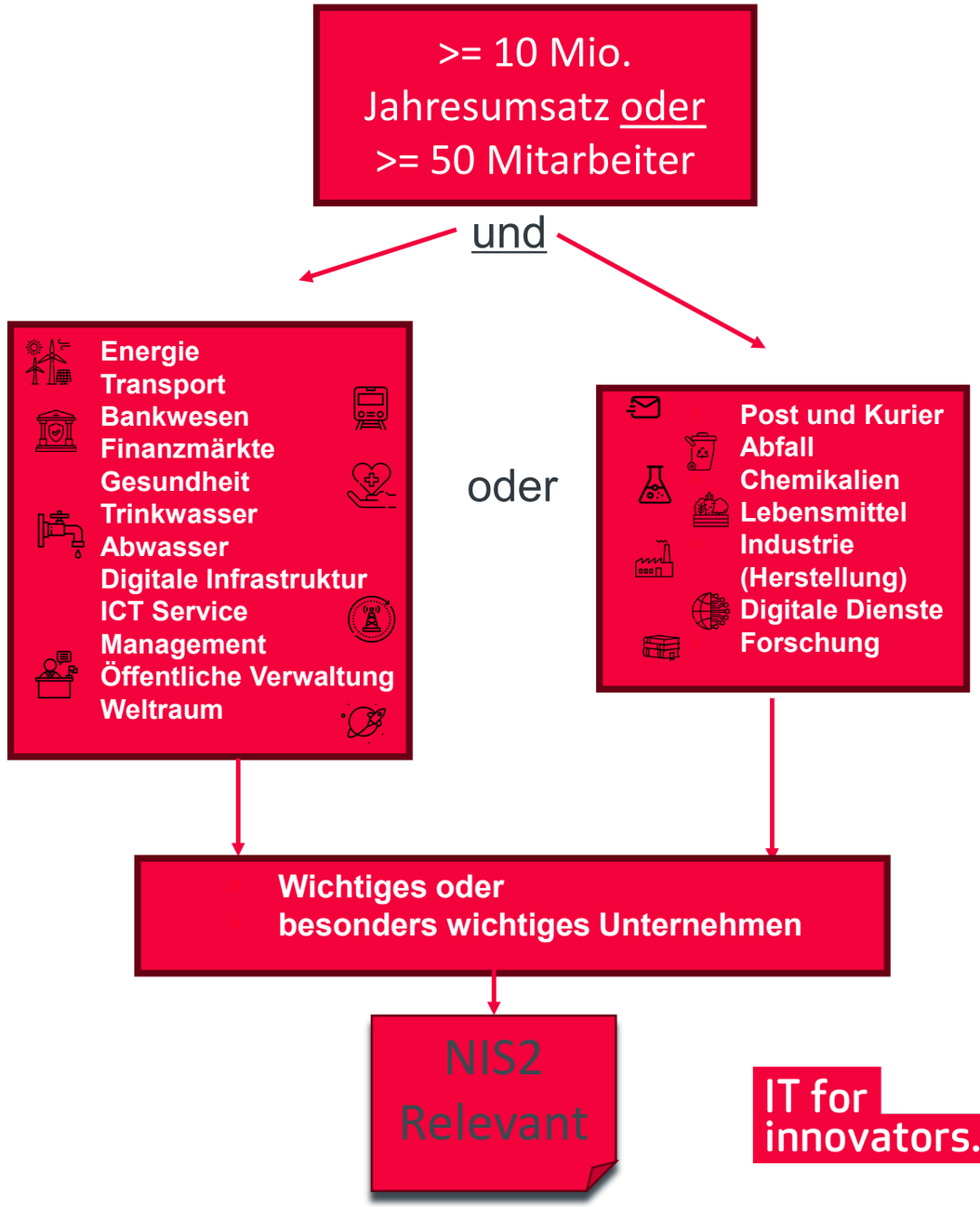
Geforderte Cybersecurity Maßnahmen

Risikomanagement
- Kritische Geschäftsprozesse
- Abhängigkeiten
- Maßnahmen (auch Schulungen der GF)

Informations-Sicherheits-Management
- Organisatorische Maßnahmen: ISMS, BCMS (Notfallplan), Awareness

Technologie
- Maßnahmen nach Stand der Technik: IT, OT, Infrastruktur u. Betrieb

Angriffserkennung: Incident Management, Systeme zur Angriffserkennung (XDR, SIEM, IDS, NDS, etc.)



IT for innovators.

NIS2 Prüf-Check

Geforderte Cybersecurity Maßnahmen

Risikomanagement
- Kritische Geschäftsprozesse
- Abhängigkeiten
- Maßnahmen (auch Schulungen der GF)

Informations-Sicherheits-Management
- Organisatorische Maßnahmen: ISMS, BCMS (Notfallplan), Awareness

Technologie
- Maßnahmen nach Stand der Technik: IT, OT, Infrastruktur u. Betrieb

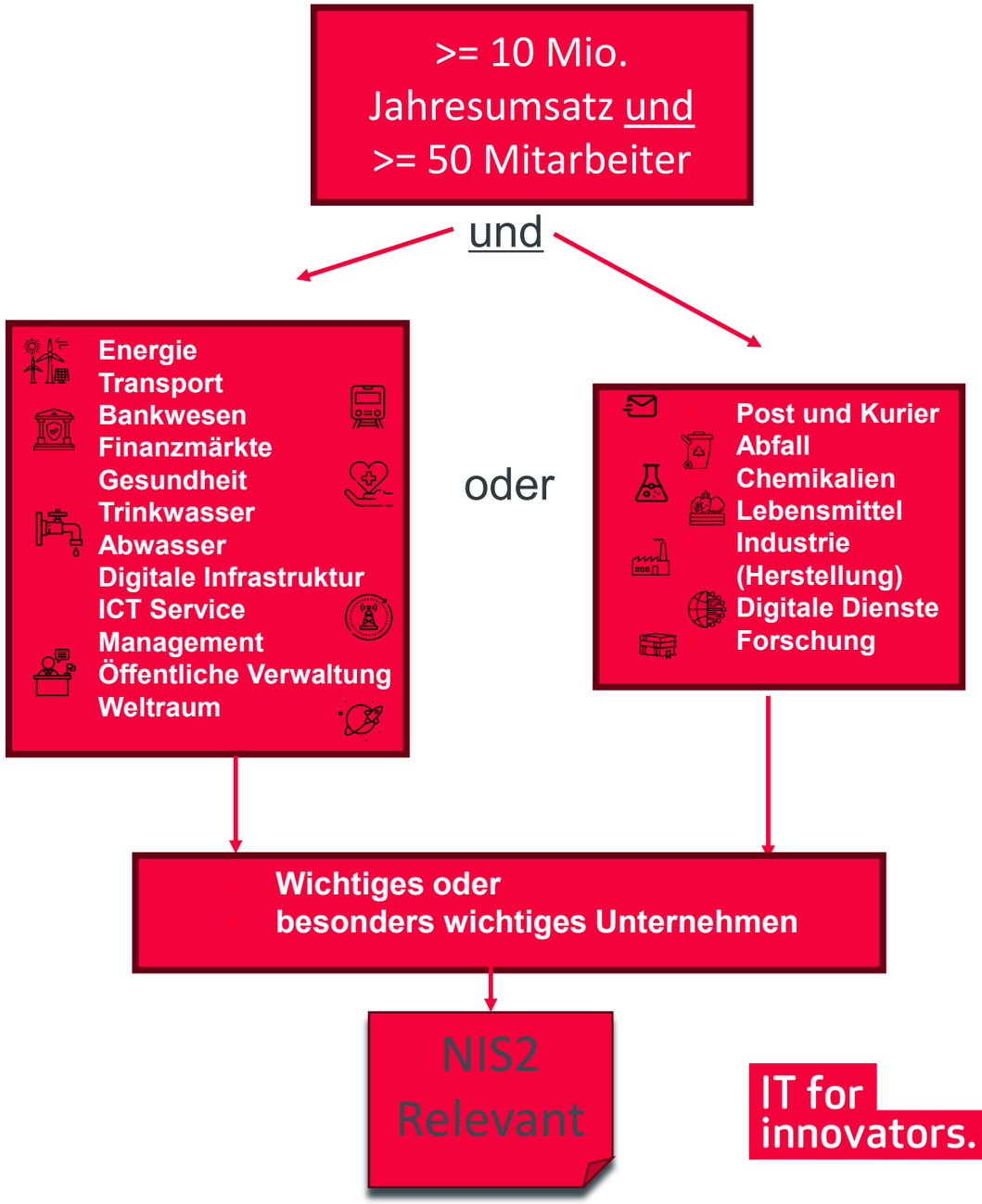
Angriffserkennung: Incident Management, Systeme zur Angriffserkennung (XDR, SIEM, IDS, NDS, etc.)

Pflichten

Grundsätzliche Registrierung

Strenge Meldepflichten
- 24 h bei erheblichem Sicherheitsvorfall
- 72 h aktualisierte Meldung mit Bewertung bei erheblichem Sicherheitsvorfall
- Nach einem Monat Abschlussbericht

… regelmäßige Updates bei längeren Vorfällen



IT for innovators.

NIS2 Prüf-Check

Geforderte Cybersecurity Maßnahmen

Risikomanagement
- Kritische Geschäftsprozesse
- Abhängigkeiten
- Maßnahmen (auch Schulungen der GF)

Informations-Sicherheits-Management
- Organisatorische Maßnahmen: ISMS, BCMS (Notfallplan), Awareness

Technologie
- Maßnahmen nach Stand der Technik: IT, OT, Infrastruktur u. Betrieb

Angriffserkennung: Incident Management, Systeme zur Angriffserkennung (XDR, SIEM, IDS, NDS, etc.)

Pflichten

Grundsätzliche Registrierung

Strenge Meldepflichten
- 24 h bei erheblichem Sicherheitsvorfall
- 72 h aktualisierte Meldung mit Bewertung bei erheblichem Sicherheitsvorfall
- Nach einem Monat Abschlussbericht

… regelmäßige Updates bei längeren Vorfällen

Verschärfte Sanktionen

>= 10 Mio. Jahresumsatz oder >= 50 Mitarbeiter

und

Energie
Transport
Bankwesen
Finanzmärkte
Gesundheit
Trinkwasser
Abwasser
Digitale Infrastruktur
ICT Service Management
Öffentliche Verwaltung
Weltraum

oder

Post und Kurier
Abfall
Chemikalien
Lebensmittel
Industrie (Herstellung)
Digitale Dienste
Forschung

Wichtiges oder besonders wichtiges Unternehmen

NIS2 Relevant

IT for innovators.

NIS2 Prüf-Check

Geforderte Cybersecurity Maßnahmen

Risikomanagement
- Kritische Geschäftsprozesse
- Abhängigkeiten
- Maßnahmen (auch Schulungen der GF)

Informations-Sicherheits-Management
- Organisatorische Maßnahmen: ISMS, BCMS (Notfallplan), Awareness

Technologie
- Maßnahmen nach Stand der Technik: IT, OT, Infrastruktur u. Betrieb

Angriffserkennung: Incident Management, Systeme zur Angriffserkennung (XDR, SIEM, IDS, NDS, etc.)

Pflichten

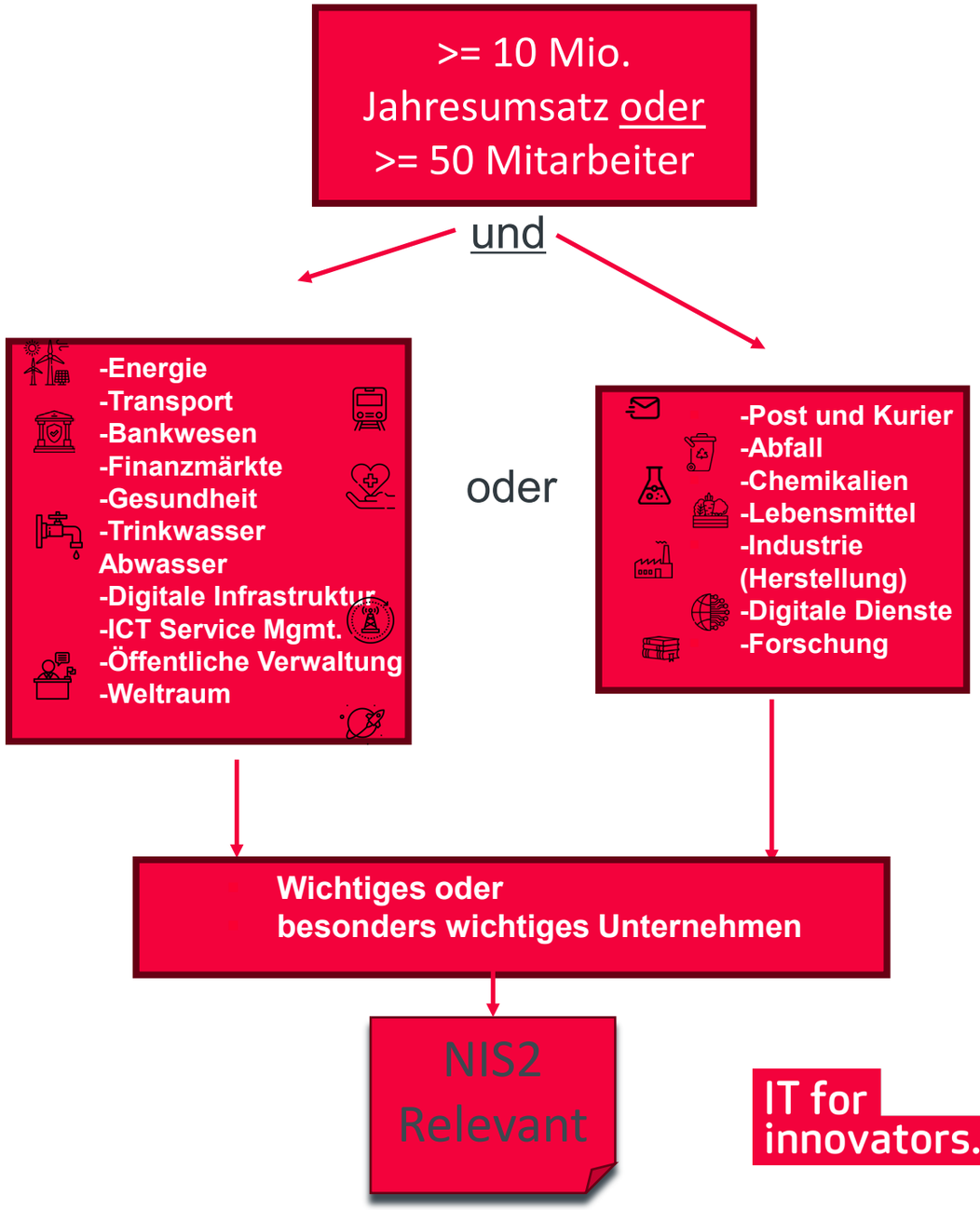
Grundsätzliche Registrierung

Strenge Meldepflichten
- 24 h bei erheblichem Sicherheitsvorfall
- 72 h aktualisierte Meldung mit Bewertung bei erheblichem Sicherheitsvorfall
- Nach einem Monat Abschlussbericht

… regelmäßige Updates bei längeren Vorfällen

Verschärfte Sanktionen

Unternehmen	Mitarbeiter		Umsatz		Bilanz
Mittel	50-249	und	≥10 Mio. EUR	und	≥10 Mio. EUR
Groß	≥ 250	und	≥ 50 Mio. EUR	und	≥ 43 Mio. EUR



IT for innovators.

Technische und organisatorische Maßnahme Mindestanforderungen,§ 30 IV BSIG-E

Maßnahmen	Lösung - Umsetzungsempfehlung
1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	ISMS, Risikobewertung ISO 27005
2. Bewältigung von **Sicherheitsvorfällen**	XDR/EDR, MDR, IPS, SIEM, Incident Response, Automatisierung
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	Notfallplan, Backup Strategie, Recovery Strategie
4. Sicherheit der **Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	Sicherheitsrichtlinie für/mit Dienstleistern, Monitoring (Fernzugriffe etc.)
5. Sicherheitsmaßnahmen bei **Erwerb**, **Entwicklung** und **Wartung** von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich **Management und Offenlegung von Schwachstellen**	Richtlinien und Prozesse bei Einkauf und Entwicklung, Zertifikate, CVE-Check

IT for innovators.

Technische und organisatorische Maßnahme Mindestanforderungen,§ 30 IV BSIG-E

Maßnahmen	Lösung - Umsetzungsempfehlung
6. Konzepte und Verfahren zur Bewertung der **Wirksamkeit** von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Analog Punkt 1, ISMS, Risikobewertung ISO 27005, KPI (Verinice)
7.grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen** im Bereich der Cybersicherheit	Transparenz u. Visibilität schaffen, bspw. Inventarisierung, Assetmanagement, Patchmanagement, CVE-Check. Logmanagement, PAM, PIM. Ransomware Quick-Check Awareness-Schulungs-Konzept
8.Konzepte und Verfahren für den Einsatz von **Kryptografie** und **Verschlüsselung**	Richtlinien erstellen (BSI-Konzept), Festplattenverschlüsselung, Kommunikationsverschlüsselung…
9.Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle** und **Management von Anlagen**	Richtlinien, PIM, MFA, Secure Access, ZTNA, Awareness-Schulungen
10.Verwendung von Lösungen zur Multi-Faktor-**Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte **Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte **Notfall-kommunikationssysteme** innerhalb der Einrichtung.	Multi-Faktor Authentifizierung, E-Mail-Verschlüsselung, ZTNA, Secure Access Verschlüsselung Sprachströme (Telefonie verschlüsselt), Kunden-PK verschlüsselt, Notfallplan…

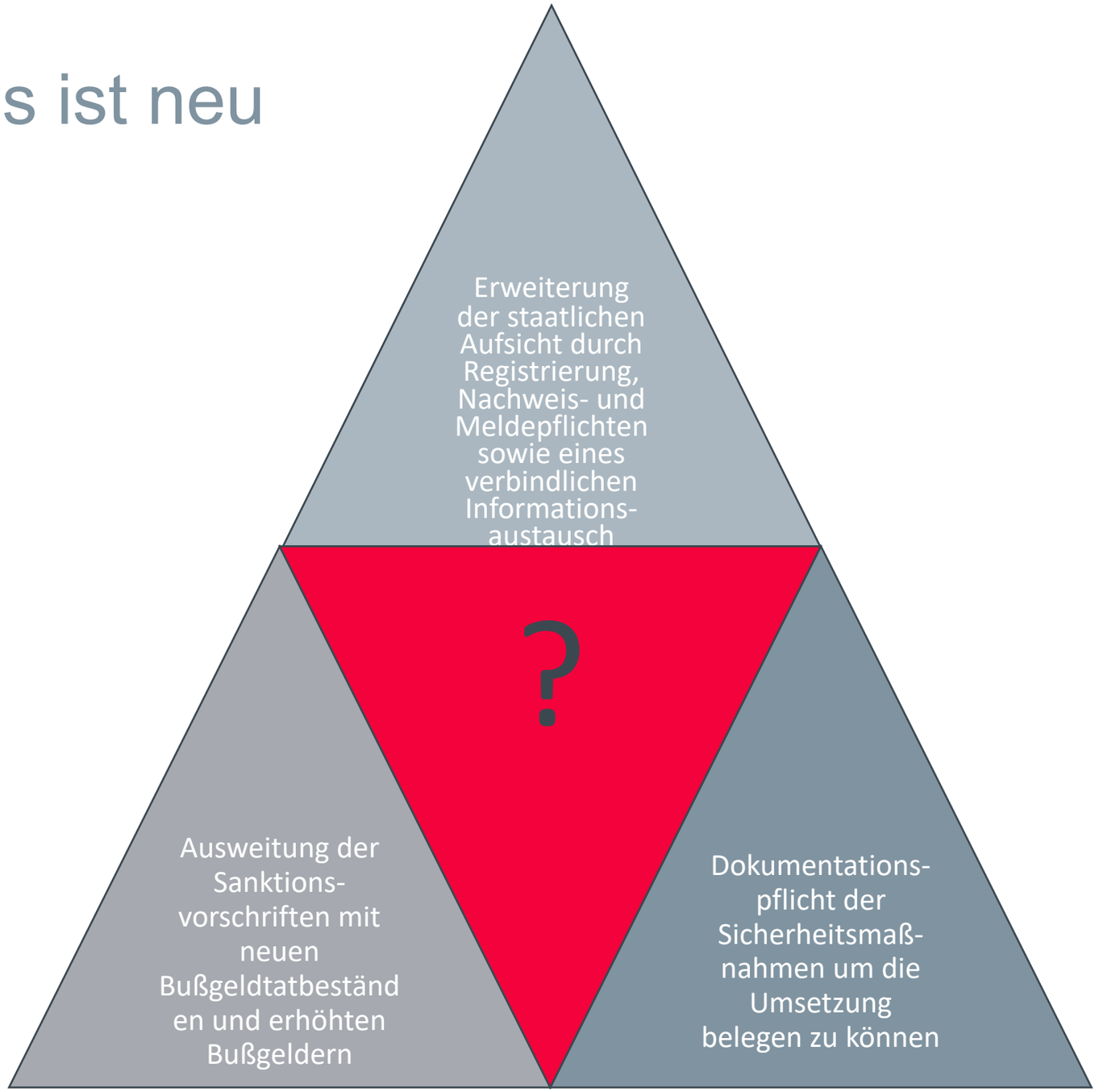
IT for innovators.

NIS2 Neuerungen - Diskussionspapier des Bundesministeriums des Innern und für Heimat für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

27.12.2022: Veröffentlichung der europäischen NIS2-Richtline im EU-Amtsblatt
16.01.2023: Inkrafttreten der europäischen NIS2-Richtline
April + Juli 2023: erster + zweiter deutscher Referentenentwurf NIS2
27.09.2023: dritter deutscher Entwurf (Diskussionspapier zum Dialog mit der Wirtschaft/ Verbändeabstimmung) NIS2
(April 2024: weiterer Referentenentwurf/Diskussionspapier?)
Ca. März 2024: Verkündung NIS2UmsuCG (IT-Sicherheitsgesetz 3.0); das deutsche NIS2-Umsetzungsgesetz
Spätestens 17.10.2024: Umwandlung der europäischen NIS2-Richtlinie in deutsches Recht abgeschlossen
18.10.2024: NIS2UmsuCG (deutsches NIS2-Umsetzungsgesetz) in Kraft, Unternehmen müssen sich an die Vorschriften halten

IT for innovators.

Was ist neu



IT for innovators.

Meldepflichten, § 32 BSIG-E und noch offene Punkte

Stufe 1: frühe Erstmeldung	• 24 h: Vorfall wegen erheblichem Sicherheitsvorfall Grenzüberschreitende Auswirkungen?
Stufe 2: bestätigende Erstmeldung	• 72 h: Bestätigung der Informationen, erste Bewertung: Schweregrad? Auswirkungen? Kompromittierungs-indikatoren?
Stufe 3: Zwischenmeldung	• Statusaktualisierung auf Ersuchen des BSI
Stufe 4: Abschlussmeldung	• 1 Monat: ausführliche Beschreibung, Art und Ursache, Abhilfemaßnahmen, grenzüberschreitende Auswirkungen

§ 32 BSIG-E Abs. 2: ggf. Fortschrittsbericht anstatt Abschlussbericht, wenn Vorfall noch andauert

IT for innovators.

Einige Änderungen vom 2. Referentenentwurf zum Diskussionspapier…

IT for innovators.

persönliche Haftung der Geschäftsleitung

§ 38

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen Risiko-managementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.

(2) Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Satz 1 gilt nicht für Geschäftsleiter besonders wichtiger Einrichtungen des Teilsektors Zentralregierung des Sektors öffentliche Verwaltung.

(3) Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 2 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(4) Die Geschäftsleiter von besonders wichtigen Einrichtungen und wichtigen Einrichtungen müssen und deren Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken so-wie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

§ 38

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen Risiko-managementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

(2) Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 1 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.

(3) Die Geschäftsleiter von besonders wichtigen Einrichtungen und wichtigen Einrichtungen müssen und deren Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken so-wie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

IT for innovators.

Haftung der Geschäftsleitung

§ 64 Abs. 10 BSIG-E

Sofern besonders wichtige Einrichtungen den Anordnungen des BSI trotz Fristsetzung nicht nachkommen, kann das BSI die jeweils zuständige Aufsichtsbehörde des Bundes auffordern

1. *die Genehmigung für einen Teil oder alle Dienste oder Tätigkeiten dieser Einrichtung vorübergehend auszusetzen*

2. ***den natürlichen Personen**, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben in der besonders wichtigen Einrichtung zuständig sind, die Wahrnehmung der **Leitungsaufgaben vorübergehend untersagen**.*

IT for innovators.

Zu § 34 Referentenentwurf §39 Diskussionspapier

Die 2-jährige Prüfungen für **besonders wichtige Einrichtungen** *(Referentenentwurf § 34)* und Betreiber kritischer Anlagen, sind im vorliegenden Diskussionsentwurf Prüfungen nur noch **alle drei Jahre** und **nur** für **Betreiber kritischer Anlagen** vorgesehen, *(Diskussionspapier §39).*

Wichtige und besonders wichtige Einrichtungen müssen wie gehabt Maßnahmen umsetzen, aber regulär keine Nachweise darüber erbringen. Das BSI kann **einzelne Einrichtungen** jedoch zu Nachweisen und auch Prüfungen verpflichten, und die Einhaltung der NIS2-Vorgaben auch selbst überprüfen, §64, §65.

Zu § 30 (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)

Alt: Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 berücksichtigt die Einrichtung **oder der Betreiber** die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse. Einrichtungen müssen bei der Erwägung geeigneter Maßnahmen nach Satz 1 die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durch-geführten koordinierten Risikobewertungen kritischer Lieferketten berücksichtigen.

Neu: Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 sind durch die Einrichtung die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse zu berücksichtigen. Einrichtungen müssen bei der Erwägung geeigneter Maßnahmen nach Satz 1 die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten berücksichtigen.

IT for innovators.

§ 30 dient der Umsetzung von Artikel 21 der NIS-2-Richtlinie. Für Einrichtungen der Bundesverwaltung wird § 30 durch § 44 umgesetzt.

Stand Verwaltungs- und Bildungseinrichtungen?

Der IT-Planungsrat hat als **zentrales politisches Steuerungsgremium** "für eine effiziente und sichere digitale Verwaltung" mit dem Beschluss 2023/39 Anfang November die Länder und den Bund gebeten, den Anwendungsbereich der NIS2-Richtlinie just "**nicht** auf Einrichtungen der **öffentlichen Verwaltung** auf lokaler Ebene **sowie Bildungseinrichtungen** zu erstrecken".

IT for innovators.

Stand der Gesetzgebung NIS2

Während bei der Umsetzung des gleichzeitig anstehenden KRITIS-Dachgesetzes neben der Ressortabstimmung bereits die Länder- und Verbändeanhörungen für den zweiten Referentenentwurf abgeschlossen sind, **gibt es beim NIS2UmsuCG kaum Fortschritte**. Ein erster **Referentenentwurf kursierte inoffiziell** bereits im Sommer 2023, das federführende **Bundesministerium des Innern und für Heimat veröffentlichte jedoch keine offizielle Version.** Um wenigstens etwas Transparenz zu schaffen, lud man im Herbst Verbände und Organisationen der Zivilgesellschaft ein, ein Diskussionspapier zu wirtschaftsrelevanten Aspekten des NIS2UmsuCG zu kommentieren (siehe ix.de/z316). **Über die Ursachen der Verzögerung lässt sich nur spekulieren.** Möglich ist, dass die Ressortabstimmung auf erheblichen Widerstand einzelner Bundesministerien gestoßen ist. Im weiteren Verlauf wäre dann eine **Anhörung der Länder sowie der Verbände und der Zivilgesellschaft der nächste Schritt** – ob und wann es dazu kommen wird, ist derzeit unklar. Der Zeitplan, den Gesetzentwurf durchs Kabinett und das anschließende parlamentarische Verfahren zu bringen, ist mittlerweile äußerst eng – **und eine Fristüberschreitung des Startdatums 18. Oktober 2024 nicht mehr unwahrscheinlich.**

Quelle:IX-2024-03-NIS2.pdf

IT for innovators.

Wie können wir unterstützen

Was Sie tun können

- Betroffenheit klären
- Registrieren
- Ressourcen einplanen

IT for innovators.

Security Interview

Essential Controls 10/162 | NIST CSF Reference Function 10/162 | Sensor or Baseline 10/162

« »

- Inventarisierung und Kontrolle von Unternehmens-Assets 5/5
- Inventarisierung und Kontrolle von Software-Assets 5/6
  - ✓ 6. Existiert ein aktuelles, regelmäßig gepflegtes Inventarverzeich…
  - ✓ 7. Wird die im Unternehmen eingesetzte Software aktuell noch u…
  - ✓ 8. Wird nicht autorisierte Software regelmäßig entfernt?
  - ✓ 9. Werden Software Inventarisierungstools eingesetzt?
  - ⊘ 10. Findet ein regelmäßiger Abgleich mit gelisteter und autorisier…
  - ~~11. Wird die Verwendung von nicht autorisierten Software-Kompon…~~
  - 12. Werden Kontrollen (signaturbasiert) durchgeführt um die Autori…
- Datenschutz 0/14
- Sichere Konfiguration von Unternehmensressourcen und Soft… 0/12
- Benutzerkonten-Management 0/6
- Verwaltung der Zugriffskontrolle 0/8
- Kontinuierliches Schwachstellen-Management 0/7
- Audit Log Management 0/12

Werden Kontrollen (signaturbasiert) durchgeführt um die Autorisierung sicherzustellen bzw. werden nicht autorisierte Skripte geblockt?

▾ Details

Priorität	1 (Standard)
NIST CSF Referenz Funktion	Protect
CIS Implementation Groups	3
Sensor/Baseline	Application Control System

Erfüllungsgrad:

Vollständig | In großen Teilen | In einigen Teilen | Kaum oder gar nich

Nicht anwendbar

- ACP_HZB-1 Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme - Antwortbogen
- ACP_HZB-2 Bewältigung von Sicherheitsvorfällen - Antwortbogen
- ACP_HZB-3 Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Kri
- ACP_HZB-4 Sicherheit der Lieferkette - Antwortbogen
- ACP_HZB-5 (App-Anw) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssysten
- ACP_HZB-5 (Indistruelle IT) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssys
- ACP_HZB-5 (IT-Systme) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssyster
- ACP_HZB-5 (Netze und Kommunikation) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Inf
- ACP_HZB-6 Konzepte und Verfahren zur Bewertung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- ACP_HZB-7 grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit - Antw
- ACP_HZB-8 Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung - Antwortboger
- ACP_HZB-9 Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen - Antwortbog
- ACP_HZB-10 MFA, Authentifizierung Sprach, Video, Textkommunikation u Notfallkommunikationssysteme - Antwortboge

IT for innovators.

Fragen?

Vielen Dank für Ihre Aufmerksamkeit.

IT for innovators.