Die 10 Maßnahmen, die Sie wirklich brauchen

Willkommen zurück. Dies ist die Einheit, in der aus „NIS2 einhalten" kein Schlagwort mehr ist, sondern eine Liste von zehn konkreten Dingen wird. In den nächsten fünfzig Minuten übersetzen wir jede dieser Maßnahmen aus der Rechtssprache heraus, sehen zu, wie ein Krankenhaus einige davon tatsächlich anwendet, und dann — der wichtigste Teil — markieren Sie, wo Ihre eigene Organisation bei jeder einzelnen steht.

NIS2 Ready — Cybersicherheits-Compliance für die öffentliche Verwaltung und kritische Infrastrukturen

Einheit 3 von 6 · Übung · ~50 Minuten · baut auf den Einheiten 1–2 auf, funktioniert aber auch für sich allein

Das Klinikum Ostheide weiß nicht, wo es anfangen soll

Lernen wir die Beispielorganisation dieser Einheit kennen, bevor wir uns die Liste ansehen.

Das **Klinikum Ostheide** ist ein regionaler Krankenhausverbund — mehrere Standorte, Patientenaktensysteme, Medizingeräte auf den Stationen und die Gebäudetechnik, die einen Operationssaal am Laufen hält. Unter NIS2 ist es eine in den Anwendungsbereich fallende Einrichtung des Gesundheitssektors. Es hat nichts mit den Nordholm-Organisationen aus früheren Einheiten zu tun; Sie müssen diese nicht kennengelernt haben.

Der Interims-IT-Leiter hat gerade eine Aufgabe übertragen bekommen, die einfach klingt und es nicht ist: „Machen Sie uns fit für unsere erste NIS2-Compliance-Prüfung.„ Die Richtlinie sagt, die Organisation müsse *geeignete und verhältnismäßige* Risikomanagementmaßnahmen ergreifen — zehn Kategorien davon. Auf dem Papier sind das vier Worte. In der Praxis fühlt sich „zehn Maßnahmen, risikoangemessen“ abstrakt an, bis jemand es auf *dieses* Krankenhaus mit *diesen* Systemen übersetzt.

> „Zehn Maßnahmen, risikoangemessen" — wo fängt man da überhaupt an?
>
> Dem Interims-IT-Leiter fehlt kein Wissen. Ihm fehlt eine *Übersetzung*: von einem Rechtskatalog zu „was heißt das eigentlich konkret, was ich hier, am Montag, in diesem Gebäude tun muss?"

Diese Übersetzung ist diese ganze Einheit. Und hier ist das Erste, was klargestellt werden muss, denn es ist das mit Abstand häufigste Missverständnis dieser zehn Maßnahmen.

Das ist nicht nur ein Problem der IT-Abteilung

Wenn Menschen „zehn Cybersicherheitsmaßnahmen" hören, denken sie an Firewalls und Server und denken: *Das ist Sache der IT, nicht meine.* Einige der zehn sind tatsächlich technisch. Aber mehrere sind eindeutig organisatorisch — wer darf was tun, wer wird geschult, was passiert, wenn ein Lieferant ausfällt. Diese werden nicht in einem Serverraum gelöst.

> Behalten Sie das für die gesamte Einheit im Hinterkopf
>
> Von den zehn Maßnahmen sind rund die Hälfte **organisatorisch oder personenbezogen**, nicht technisch: Governance, Schulung, Zugriffsrichtlinien, Lieferantenmanagement, Betriebskontinuität. Wenn Sie nicht in der IT arbeiten, betrifft Sie diese Liste trotzdem — und das durchgearbeitete Beispiel weiter unten wird immer wieder kennzeichnen, welche Maßnahmen die gesamte Organisation betreffen und nicht nur die IT.

Was Art. 21 tatsächlich verlangt

Vor der Liste selbst noch ein einordnender Satz — denn er verändert, wie Sie alle zehn lesen.

NIS2 händigt Ihnen **keine** Einkaufsliste von Produkten aus, die Sie kaufen sollen. Es nennt kein einziges Werkzeug, keine Marke, kein Zertifikat. Es verlangt Maßnahmen, die *geeignet und verhältnismäßig* zu Ihrem tatsächlichen Risiko sind — bemessen daran, wie groß Sie sind, wie exponiert Sie sind und wie schwerwiegend ein Vorfall wäre.

Dieses Wort — verhältnismäßig — leistet viel Arbeit, und das ist eine gute Nachricht.

„Geeignet und verhältnismäßig" — die Rechtsformulierung, einmalig

Das ist **Art. 21 Abs. 1**. Es bedeutet, dass ein kleines kommunales Amt und ein großer Krankenhausverbund beide *dieselbe* Maßnahme mit sehr unterschiedlicher Umsetzung erfüllen können. Niemand erwartet von einer Behörde mit 40 Personen, dass sie ein 24/7-Security-Operations-Center betreibt. Die Pflicht skaliert mit Ihnen. *(Wir kommen gegen Ende dieser Einheit darauf zurück, wie das aussieht.)*

Die zehn Maßnahmen, in einfacher Sprache

Hier sind sie — alle zehn, aus Art. 21 Abs. 2, Buchstaben (a) bis (j). Für jede: zuerst die alltägliche Bedeutung, dann der formale Name in Klammern, damit Sie ihn später wiedererkennen. Lesen Sie die Spalte „Was das für Sie bedeutet" von oben nach unten; die Begriffe in Klammern stehen zur Referenz da, nicht zum Auswendiglernen.

#	**Was das für Sie bedeutet (einfache Sprache)**	**Formale Kategorie (Art. 21 Abs. 2)**	**Überwiegend…**
1	Wissen, was schiefgehen könnte, und die Regeln zum sicheren Betrieb der Systeme festhalten	Risikoanalyse & Sicherheit für Informationssysteme (a)	Organisatorisch
2	Einen Plan haben für den Fall, *wenn* etwas schiefgeht — nicht nur *falls*	Bewältigung von Sicherheitsvorfällen (b)	Beides
3	Nach einer Störung weiterlaufen (und wiederherstellen) können — Backups, Notfallwiederherstellung	Aufrechterhaltung des Betriebs & Krisenmanagement (c)	Beides
4	Sicherstellen, dass die Lieferanten und Dienste, von denen Sie abhängen, nicht Ihr Schwachpunkt sind	Sicherheit der Lieferkette (d)	Organisatorisch
5	Systeme sicher erwerben und entwickeln und Schwachstellen begegnen, wenn sie auftauchen	Sicherheit bei Erwerb, Entwicklung & Wartung (e)	Technisch
6	Prüfen, dass Ihre Maßnahmen tatsächlich wirken — nicht einfach annehmen, dass sie es tun	Bewertung der Wirksamkeit der Maßnahmen (f)	Organisatorisch
7	Menschen grundlegende Cyberhygiene vermitteln und sie schulen	Cyberhygiene & Schulungen (g)	Personen

8	Verschlüsselung dort einsetzen, wo es sinnvoll ist, mit klaren Regeln dafür	Kryptografie & Verschlüsselung (h)	Technisch
9	Steuern, wer worauf Zugriff hat — Personalsicherheit, Zugriffsrechte, die eigenen Anlagen kennen	Personalsicherheit, Zugriffskontrolle & Anlagenmanagement (i)	Beides
10	Anmeldungen fälschungssicher machen und einen Kommunikationskanal erhalten, der einen Notfall übersteht	Multi-Faktor-Authentifizierung & gesicherte Notfallkommunikation (j)	Technisch

Beachten Sie die letzte Spalte. Zählen Sie die Maßnahmen, die nicht rein technisch sind — Risikoregeln, Lieferantenmanagement, Wirksamkeitsprüfungen, Schulung, Zugriffsrichtlinien. Das ist der Großteil der Liste. Genau deshalb scheitert „an die IT übergeben und vergessen" bei einer Compliance-Prüfung.

> ### Der Ein-Satz-Test, ob eine Maßnahme „Ihre" ist
>
> Fragen Sie: *Könnte dies wegen einer Entscheidung, einer Gewohnheit oder einer Lücke in der Verantwortung scheitern — statt wegen fehlender Technik?* Wenn ja, ist es zumindest teilweise eine organisatorische Maßnahme, und sie braucht eine verantwortliche Person außerhalb der IT.

Ein schneller Eindruck davon, wo Sie stehen

Vor dem durchgearbeiteten Beispiel ein interaktiver Dreißig-Sekunden-Exkurs — und ein erster Vorgeschmack auf etwas, das Sie in Einheit 6 richtig machen werden. Denken Sie nicht zu viel nach: Wie viele der zehn Maßnahmen sind wirklich **vorhanden**, wie viele nur **teilweise** (begonnen oder ungetestet), und der Rest fällt dann in **fehlt**. Bewegen Sie die beiden Schieberegler und beobachten Sie, wie Ihr Bild Gestalt annimmt.

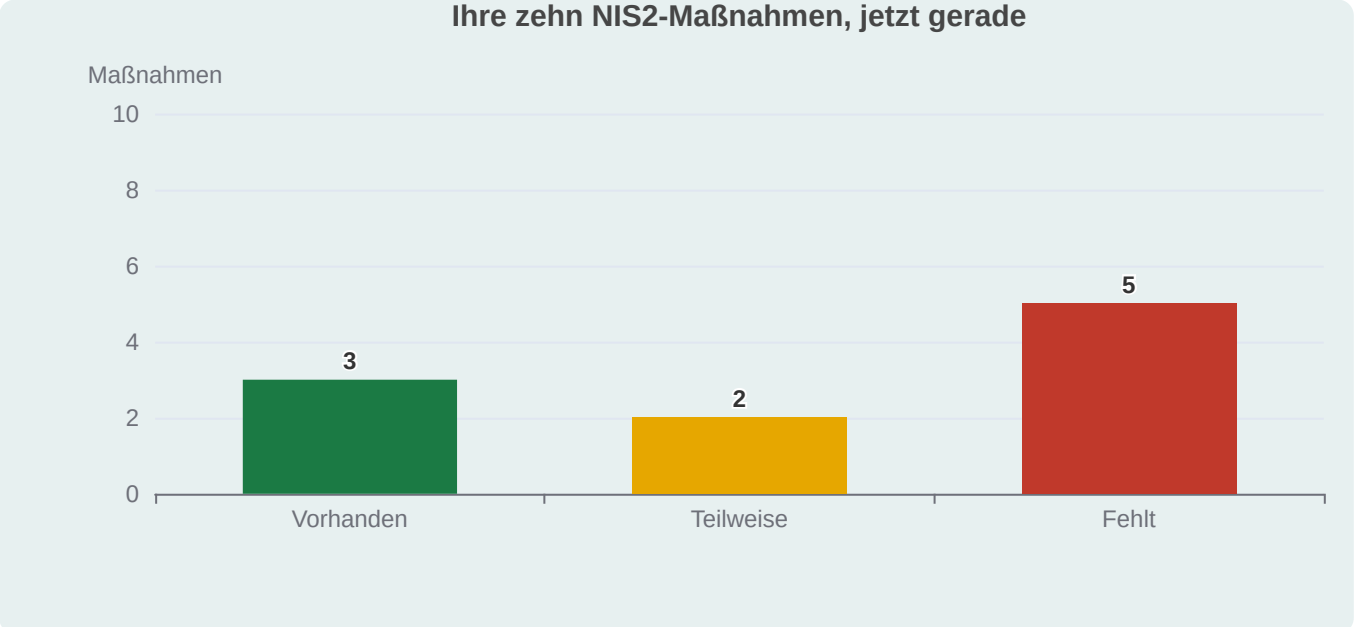
> ### 👉 Diese Übung ist interaktiv — ziehen Sie an den Schiebereglern
>
> Die beiden Schieberegler unten sind live. Während Sie sie bewegen, berechnet und färbt sich das Balkendiagramm darunter sofort neu, und „fehlt" füllt den Rest für Sie auf. Probieren Sie es aus — hier wird nichts gespeichert oder bewertet.

Maßnahmen, die wirklich **vorhanden** sind (funktionierend, und Sie könnten Nachweise vorlegen):

3 vorhanden

Maßnahmen, die nur **teilweise** vorhanden sind (begonnen, unvollständig oder ungetestet):

2 teilweise



Welche Gestalt dieses Diagramm gerade angenommen hat — eine Wand aus Rot, ein gesunder Block aus Grün oder etwas dazwischen — es ist eine Momentaufnahme, keine Note. Es geht nicht um die genauen Zahlen; es geht darum, dass „konform / nicht konform" immer eine falsche Wahl war. Bereitschaft ist ein Spektrum, und Sie können heute sehen, wo darauf Sie sich befinden.

> Sehen Sie sich an, was hier gerade passiert ist
>
> Zwei Schieberegler, ein Live-Balkendiagramm, das sich neu färbt und neu berechnet, während Sie ziehen, „fehlt", das den Rest automatisch auffüllt — und **all das ist etwa ein Dutzend Zeilen einfacher Text in diesem Dokument**. Keine App, kein Server, kein Plugin, kein separates Werkzeug. Doppelklicken Sie in LiaScript auf das Diagramm, um den Code dahinter zu sehen. In Einheit 6 wächst dieselbe Idee zu Ihrem vollständigen **NIS2-Readiness-Score** heran.

Durchgearbeitetes Beispiel: Das Klinikum Ostheide wendet vier der zehn an

Hören wir auf aufzulisten und fangen wir an anzuwenden. Hier sind vier der zehn Maßnahmen, durchgearbeitet an der tatsächlichen Umgebung des Klinikums Ostheide — sie zeigen die *Überlegung*, nicht nur das Abhaken eines Kästchens. Lesen Sie alle vier: Beachten Sie, wie dieselbe Richtlinie vier völlig unterschiedliche Arten von Arbeit hervorbringt — ein Backup testen, bewusst *nicht* übersichern, eine Vertragsklausel formulieren und Menschen schulen.

Maßnahme 3 — Aufrechterhaltung des Betriebs: das Patientenakten-Backup

Das Klinikum Ostheide führt elektronische Patientenakten. Wenn diese Akten an einem Freitagabend durch Ransomware verschlüsselt werden, können die Stationen am Samstagmorgen noch funktionieren?

Maßnahme 10 — MFA für Anmeldungen des klinischen Personals

Klinisches Personal meldet sich an sensiblen Systemen an, oft an gemeinsam genutzten Arbeitsplätzen, oft in Eile.

- **Geeignete Umsetzung:** regelmäßige, *getestete* Backups, offline oder isoliert aufbewahrt, plus ein Wiederherstellungsverfahren, dem ein gestresstes Nachtschicht-Team tatsächlich folgen könnte.
- **Warum „getestet„ wichtig ist:* *ein Backup, das noch nie jemand wiederhergestellt hat, ist eine Hoffnung, kein Plan. Das ist* Aufrechterhaltung* des Betriebs, nicht „ein Backup irgendwo“.

- **Geeignete Umsetzung:** Multi-Faktor-Authentifizierung an klinischen Systemen — ein zweiter Faktor über das Passwort hinaus, so gewählt, dass er die Notfallversorgung nicht verlangsamt.
- **Das Spannungsfeld der Verhältnismäßigkeit:** Sicherheit, die eine Ärztin mitten in der Reanimation blockiert, ist die *falsche* Sicherheit. Hier bedeutet „geeignet" ausdrücklich schnell — die Maßnahme und die Patientensicherheit werden gemeinsam entworfen.

Maßnahme 4 — Sicherheit der Lieferkette: der Geräte-Lieferant

Ein modernes Krankenhaus lebt von externer Ausrüstung — Bildgebungssystemen, Überwachungsgeräten, deren Fernwartungszugängen.

- **Geeignete Umsetzung:** wissen, welche Lieferanten in Ihre Systeme hineingreifen können, und sie im *Vertrag* auf Sicherheitserwartungen verpflichten — ihr schwaches Passwort wird zu Ihrem Sicherheitsvorfall.
- **Warum es organisatorisch ist:** gelöst im Einkauf und in Verträgen, nicht durch eine Firewall-Regel. Oft *sieht* niemand in der IT den Fernzugangskanal des Lieferanten überhaupt, bis er das Einfallstor ist.

Maßnahme 7 — Cyberhygiene & Schulung: alle

Die Person, die auf die überzeugende Phishing-E-Mail klickt, ist meist nicht in der IT.

- **Geeignete Umsetzung:** grundlegende, wiederkehrende Schulung für *alle* Mitarbeitenden — verdächtige Nachrichten erkennen, schnell melden, Passwörter nicht wiederverwenden — plus die Schulung der Leitung, die NIS2 verlangt (Einheit 5).
- **Der Kernpunkt:** diese Maßnahme enthält überhaupt keinen Server. Sie ist der klarste Beweis dafür, dass NIS2-Compliance eine organisationsweite Aufgabe ist.

Vier Maßnahmen, vier sehr unterschiedliche Gestalten — eine über das Testen von Backups, eine über das *Nicht*-Übersichern, eine über Verträge, eine über Menschen. Diese Vielfalt ist die eigentliche Lehre: „zehn Maßnahmen" sind nicht zehn IT-Aufgaben.

> **Verhältnismäßigkeit in einem Satz**
>
> Ein großer Krankenhausverbund testet Backups über viele Standorte hinweg und prüft Dutzende von Lieferanten; ein kommunales Amt mit 40 Personen testet vielleicht ein Backup und verwaltet drei Lieferanten. **Dieselben Maßnahmen, bemessen auf die Organisation** — so wirkt Art. 21 wie beabsichtigt.

Ordnen Sie nun die zehn Ihrem eigenen Bereich zu

Hier ist die Übung, um die herum diese Einheit aufgebaut ist. Markieren Sie für jede der zehn Maßnahmen, wo Ihre Organisation — oder der Teil, für den Sie verantwortlich sind — heute tatsächlich steht. Seien Sie ehrlich: eine Wand aus „fehlt" ist ein *nützliches* Ergebnis, kein Scheitern. Es ist eine To-do-Liste, die Sie vor fünf Minuten noch nicht hatten.

Nutzen Sie die drei Spalten: **vorhanden** (funktionierend, und Sie könnten Nachweise vorlegen), **teilweise** (begonnen, unvollständig oder ungetestet), **fehlt** (noch nicht wirklich vorhanden).

vorhanden	teilweise	fehlt	
◯	◯	◯	1 — Risikoregeln & Sicherheitsrichtlinien schriftlich festgehalten
◯	◯	◯	2 — Ein Plan zur Bewältigung von Vorfällen, wenn sie eintreten
◯	◯	◯	3 — Getestete Backups & ein Wiederherstellungs-/Kontinuitätsplan
◯	◯	◯	4 — Lieferanten-/Lieferkettensicherheit in Verträgen
◯	◯	◯	5 — Sicherer Systemerwerb & Umgang mit Schwachstellen
◯	◯	◯	6 — Prüfung, ob die Maßnahmen tatsächlich wirken
◯	◯	◯	7 — Cyberhygiene-Grundlagen & Mitarbeiterschulung
◯	◯	◯	8 — Verschlüsselung eingesetzt, wo sie sinnvoll ist
◯	◯	◯	9 — Zugriffskontrolle, Personalsicherheit & Anlageninventar
◯	◯	◯	10 — Multi-Faktor-Anmeldungen & Notfallkommunikation

Nun die zwei Anschlussfragen, die aus dem Raster Handeln machen.

Wählen Sie **eine** Maßnahme, die Sie mit „fehlt„ oder „teilweise“ markiert haben. Was ist der einzelne kleinste nächste Schritt, der sie voranbringen würde — und wer wäre dafür verantwortlich?

Texteingabe ...

Welche der zehn hat Sie überrascht, weil sie eher *organisatorisch* als technisch ist — etwas, von dem Sie zuvor angenommen hätten, es sei „ein Problem der IT"?

Texteingabe ...

> **Nicht bewertet, nirgends abgelegt**
>
> Dieses Arbeitsblatt ist eine private Selbstdiagnose. Nichts hier wird über Ihren eigenen Browser hinaus bewertet oder gespeichert — es dient dazu, Ihnen eine Ausgangskarte zu geben, kein Zeugnis.

Zusammenfassung & Selbsttest

Drei kurze Fragen, nicht bewertet — ein Bauchgefühl-Check, wie die zehn Maßnahmen tatsächlich wirken.

1. Was bedeutet „geeignet und verhältnismäßig" für die Maßnahmen nach Art. 21?

- ◯ Jede Organisation muss alle zehn nach demselben technischen Standard umsetzen
- ◯ Die Maßnahmen skalieren mit Größe, Exponiertheit und Risiko Ihrer Organisation
- ◯ Kleine Organisationen sind von den Maßnahmen vollständig befreit

2. Welche dieser Aufgaben ist *nicht* in erster Linie Sache der IT-Abteilung?

- ◯ Multi-Faktor-Authentifizierung bei System-Anmeldungen
- ◯ Verschlüsselung sensibler Daten
- ◯ Sicherheit der Lieferkette in Lieferantenverträgen

3. Richtig oder falsch: Das richtige Sicherheitsprodukt zu kaufen, reicht aus, um Art. 21 zu erfüllen.

- ◯ Richtig
- ◯ Falsch

Bevor Sie gehen: eine kurze Reflexion

Blicken Sie zurück auf Ihr Selbstbewertungs-Raster. Wenn nächsten Monat eine Compliance-Prüfung stattfände, welche einzelne Maßnahme würden Sie am wenigsten gerne genau unter die Lupe genommen sehen — und was hindert Sie daran, sie zuerst zu beheben?

Texteingabe ...

Als Nächstes

Einheit 4 — Bewältigung und Meldung von Sicherheitsvorfällen. Wir bleiben beim Klinikum Ostheide — aber diesmal ist der Vorfall echt, keine Übung. Wenn der Montagmorgen-Moment *kein* Fehlalarm ist, stellt Ihnen NIS2 eine Uhr: 24 Stunden, 72 Stunden, ein Monat. Einheit 4 zeigt genau, was wann fällig ist.

Quellen:

1. Richtlinie (EU) 2022/2555 (NIS2), Art. 21 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit, inkl. Buchstaben a–j) — `data/cybersichert.pdf`
2. Richtlinie (EU) 2022/2555 (NIS2), Art. 20 (Governance — Billigung/Überwachung durch das Leitungsorgan, in Einheit 5 vertieft) — `data/cybersichert.pdf`
3. Kursagenda — `journal.md` → `## Agenda`