

NIS2 wird in Deutschland jetzt Gesetz!
Es gilt vorbereitet zu sein

Ein praktischer Leitfaden zu den Themen Sensibilisierung, Compliance und Cyber-Resilienz

Lucy Security als Ihr Partner zur Erreichung einer verbesserten
Sensibilisierung als Antwort auf Phishing-Szenarien





Zusammenfassung

NIS2 ist da – und es betrifft fast Alle direkt.

Die NIS2-Richtlinie der EU – in Deutschland umgesetzt als NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) – markiert einen grundlegenden Wandel in der Regulierung der Cybersicherheit in kritischen und wichtigen Sektoren. Die Richtlinie erweitert den Geltungsbereich der betroffenen Unternehmen, verschärft die Fristen für die Meldung von Vorfällen und führt eine verbindliche Rechenschaftspflicht für Führungsteams ein. Am bedeutendsten ist jedoch vielleicht, dass die Bedeutung des sog. “Human Factors” vom Gesetzgeber nicht nur anerkannt, sondern auch in einem Gesetz umgesetzt wird.

Cybersicherheit ist nicht mehr nur ein IT-Problem. Es ist auch Bereich bei dem es um menschliche Verhaltensweisen geht:



Nach NIS2 wird jeder Mitarbeiter Teil der Cyberabwehrstrategie des Unternehmens. Das bedeutet, dass proaktives, kontinuierliches Sicherheitsbewusstsein nicht mehr optional oder eine nachträgliche Checkbox ist – es ist eine gesetzliche Verpflichtung.

Warum dieser Leitfaden?

Dieser Leitfaden soll deutschen Unternehmen helfen, besser zu verstehen:

- Was NIS2 in der Praxis erfordert – insbesondere im Hinblick auf Maßnahmen zum Faktor Mensch.
- Warum „Sensibilisierungstraining“ allein nicht ausreicht.
- Worauf man bei einer Lösung achten sollte um messbare Compliance und echte Resilienz zu erreichen.

Der menschliche Faktor: Von der Nachbetrachtung zur Frontline-Verteidigung

Phishing, Social Engineering und menschliches Versagen sind nach wie vor die Hauptursachen für Datenverstöße in Europa. NIS2 erkennt dies an und verlangt von Unternehmen, dass sie im Rahmen ihres technischen und organisatorischen Risikomanagements **Maßnahmen zur Sensibilisierung und Schulung** umsetzen. Führungskräfte sind ausdrücklich dafür verantwortlich, dass solche Maßnahmen getroffen und umgesetzt werden.

Anders ausgedrückt: **The human risk ist ein Compliance-Problem.**

DIE LUCY SECURITY PLATTFORM und NIS2

Mit seiner langjährigen Erfahrung in der Unterstützung auch deutscher Unternehmen insbesondere gerade in stark regulierten Branchen wie z. B. dem Gesundheitssektor bietet Lucy Security eine der ausgereiftesten Plattformen für Sicherheitsbewusstsein und Phishing-Simulation – prädestiniert für messbare Compliance



Was zeichnet Lucy aus?



Lokalisierung ohne Kompromisse:

Über 130 Sprachen, einschließlich Deutsch mit kundenrelevanten supportzeiten u



On-Premise, Cloud oder Hybrid:

Ihre Daten, Ihre Regeln – vollständig GDPR- und NIS2-konform.



Maßgeschneiderte Sensibilisierungsinhalte:

Anpassbare Module und Simulationen realer Angriffe, die auf Ihre Branche, Kultur und Bedrohungslage zugeschnitten sind.



Integrierte Berichterstellung und KPIs:

Demonstrieren Sie Compliance gegenüber Auditoren – und die Auswirkungen gegenüber der Unternehmensleitung.

Ob Sie ein Betreiber kritischer Infrastrukturen, ein Krankenhaus oder ein mittelständisches Unternehmen sind – mit Lucy können Sie die Sensibilisierungsanforderungen von NIS2 nachhaltig und wirksam umsetzen.“



NIS2 verstehen:

Was ändert sich und warum?

Von NIS1 zu NIS2: Eine stille Revolution in der Cyber-Regulierung

Als die ursprüngliche NIS-Richtlinie (NIS1) 2016 in Kraft trat, unterlagen nur etwa **300 Organisationen** in Deutschland den Cybersicherheitsverpflichtungen. Mit NIS2 steigt diese Zahl auf **über 19.000**.

Diese Ausweitung spiegelt die sich wandelnde Cyber-Bedrohungslandschaft wider – und einen Wandel in der Denkweise der Regulierungsbehörden. Cybersicherheit gilt heute als **geschäftskritische Infrastruktur**, selbst für mittelständische Unternehmen.



Was ist neu unter NIS2?

Schlüsselbereich	NIS1	NIS2
Geltungsbereich	~300 KRITIS-Betreiber	Über 19.000 Unternehmen in 18 Sektoren
Abgedeckte Sektoren	Energie, Verkehr, Gesundheit usw.	Jetzt auch Fertigung, Lebensmittel, Chemie, Post, IKT usw.
Schwellenwert für Unternehmensgröße	Überwiegend große Unternehmen	Umfasst auch mittelständische Unternehmen (250+ Mitarbeiter oder 50 Mio. €+ Umsatz)
Anforderungen an das Bewusstsein	Allgemeine Verpflichtung	Explizite Schulungs- und Sensibilisierungsmaßnahmen erforderlich
Rechenschaftspflicht	Begrenzte Haftung des Vorstands	Führungskräfte sind direkt für die Einhaltung verantwortlich
Geldstrafen	Variable	Bis zu 10 Mio. € oder 2 % des weltweiten Umsatzes (je nachdem, welcher Betrag höher ist)
Zeitplan	Umsetzung	Bis November 2025 werden die Verpflichtungen gesetzlich verbindlich – keine Übergangsfrist

NIS2-Zeitplan



🔴 **Keine Übergangsfrist!** Unternehmen müssen rechtzeitig bereit sein – oder riskieren erhebliche Geldstrafen und Reputationsschäden.

Von statischer Compliance zu risikobasierter Bereitschaft

NIS2 führt einen risikobasierten Ansatz ein. Das bedeutet, dass es keine Übungen mehr gibt, die zwar eine Aktivität zeigen, aber letztlich die Sensibilisierung im Hinblick auf Phishing Szenarien nicht adressieren.. Die Gesetzgebe verlangt, dass Sie:

- Menschliche Schwachstellen identifizieren
- Nutzergruppen im unternehmenskritischen Bereichen priorisieren.
- Gezielte Maßnahmen ergreifen
- Die Wirksamkeit messen und entsprechende Berichte erstellen.

Wie Lucy Security dazu passt

Lucy Security **entspricht** bereits **diesen risikobasierten Anforderung von NIS2** – mit leistungsstarken Funktionen, die Unternehmen auch in Deutschland helfen, konform und widerstandsfähig zu bleiben:

- **Risikobewertung und -segmentierung:** Konzentrieren Sie Schulungen auf die wichtigsten Bereiche.
- **Phishing-Simulationen basieren auf realen Bedrohungen:** maßgeschneidert für Abteilungen, Benutzergruppen oder Regionen.
- **Benutzerdefinierte Dashboards und auditfähige Berichte:** Verfolgen Sie KPIs, visualisieren Sie die Abdeckung und weisen Sie die Wirksamkeit nach.

Durch die sofortige Einführung der Lucy-Plattform können Unternehmen **ihre NIS2-Verpflichtungen proaktiv erfüllen** – ohne in letzter Minute hektisch handeln zu müssen.



Wer ist in Deutschland betroffen?

NIS2 bringt Cyber-Regulierung in die Realwirtschaft

Im Gegensatz zu seinem Vorgänger zielt NIS2 nicht nur auf kritische nationale Infrastrukturen ab, sondern erweitert die Aufsicht auf Kernbereiche der Realwirtschaft, darunter Tausende mittelständische und öffentliche Unternehmen in ganz Deutschland.

Nach dem deutschen Umsetzungsgesetz (NIS2UmsuCG) werden regulierte Unternehmen nun in zwei Kategorien eingeteilt:

1. Wesentliche Unternehmen

- Größere Betreiber in Sektoren mit hoher Auswirkung
- In der Regel >250 Mitarbeiter oder 50 Mio. € Umsatz
- Unterliegen vollständiger Compliance und strengster Kontrolle

2. Wichtige Unternehmen

- Mittelständische Unternehmen und öffentliche Dienstleister
- Häufig 50–250 Mitarbeiter oder 10–50 Mio. € Umsatz
- Nach wie vor umfangreiche Verpflichtungen – einschließlich Sensibilisierung, Risikomanagement und Berichterstattung



Welche Branchen sind betroffen?

Sektor	Art des Unternehmens	Schwellenwert (Mitarbeiter/Umsatz)	Beispiele	Geschätzte Anzahl betroffener Organisationen (Deutschland)
Energie (einschließlich Stadtwerke)	Wesentlich	>250 oder 50 Mio. €+	Stadtwerke, Netzbetreiber	1,200+
Transport & Logistik	Wesentlich/wichtig	Größenabhängig	Flughäfen, Fracht, Schiene, Kurierdienste	800+
Gesundheitswesen	Wesentlich/Wichtig	Größenabhängig	Krankenhäuser, Gesundheitstechnologie, Labore	1,000+
IKT und digitale Infrastruktur	Wesentlich	>250 oder 50 Mio. €+	Hosting, DNS, Rechenzentren	300+
Fertigung (Medizin, Chemie)	Wichtig	>50 oder 10 Mio. €+	Pharma, Elektronik, Maschinenbau	3,000+
Food Supply & Retail	Wichtig	>50 oder 10 Mio. €+	Großhändler, Hersteller	2,000+
Finanzmarktinfrastuktur	Wesentlich	Reguliert	Börsen, Zahlungsabwickler	~150
Public Admin & Local Services	Wichtig	>50 oder 10 Mio. €+	Stadtwerke, lokale Versorgungsunternehmen	5,000+

Mittelstand, Stadtwerke und kommunale IT-Anbieter sind fest im Fokus — viele davon zum ersten Mal.

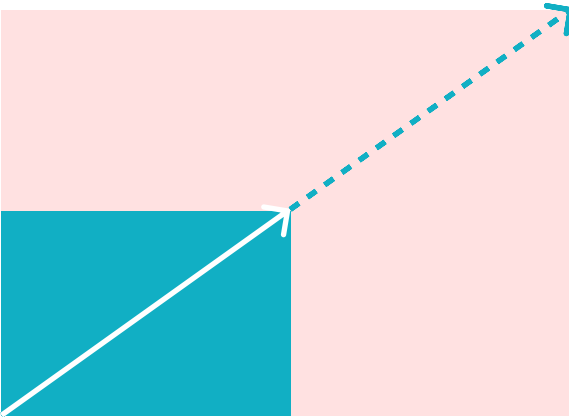
Selbst Organisationen, die traditionell nicht als „kritisch“ angesehen werden, müssen nun mit Awareness Programmen die Sensibilität ihrer Mitarbeiter verbessern und dadurch Bedrohungen minimieren.

Lucy unterstützt Sie – unabhängig von Ihrer Größe

Von 50 bis 50.000 Benutzern – Lucy ist von Grund auf skalierbar.

Ob Sie ein einzelnes Stadtwerk, ein regionales Krankenhaus oder ein nationaler Logistikdienstleister sind – Lucy passt sich Ihrer Größe, Struktur und Bedrohungslage an.

- Modulare Lizenzierung für jede Unternehmensgröße
- Rollenbasierte Schulung und Zielausrichtung
- Zentrale Steuerung, dezentrale Bereitstellung





Menschliches Risiko unter NIS2:

Warum Awareness-Plattformen wichtig sind

Menschliches Verhalten kann man nicht patchen – aber man kann es trainieren

Wenn es um Cyber Security “Vorfälle geht, sprechen die Statistiken eine eindeutige Sprache!:



Über 80 % der Sicherheitsverletzungen sind nach wie vor Folge menschlicher Fehlinterpretationen und Irrtümer.

– Phishing-Klicks, Wiederverwendung von Anmeldedaten, Social Engineering oder versehentliche Datenlecks sind nur einige Beispiele, die zu nennen sind.



Die NIS2-Richtlinie erkennt dies nicht nur an. Sie schreibt vor, dass Unternehmen **menschliche Cyberrisiken** durch Schulungen, Sensibilisierung und messbare Ergebnisse **aktiv managen müssen**.

✓ *Sensibilisierung ist keine einmalige Präsentation. Es handelt sich um ein kontinuierliches Programm, das das Verhalten im Laufe der Zeit verändert.*

Dies ist keine reine Pflichtübung

Gemäß NIS2 erwarten die Regulierungsbehörden von Ihnen Folgendes:

- Identifizieren Sie gefährdete Benutzergruppen
- Rollenspezifische, risikobasierte Schulungen durchführen
- Regelmäßige Simulation von Bedrohungen
- Nachweis der Wirksamkeit Ihrer Programme

Lösungen wie integrierte Tools z.B. bei Microsoft oder statische E-Learning-Folien erfüllen diese Anforderungen nicht. Ihnen fehlen Verhaltensanalysen, Zielgruppenausrichtung, Anpassungsmöglichkeiten und messbare Auswirkungen.

Wie sieht effektive Sensibilisierung aus?

Schlechte Praxis

- Einmalige jährliche Schulung
- Gleiche Schulung für alle Benutzer
- Textlastige Folien oder PDFs
- Keine Phishing-Tests
- Keine Kennzahlen

Konforme, effektive Praxis

- Laufende Kampagnen mit adaptiven Inhalten
- Risikobasierte Segmentierung nach Abteilung oder Rolle
- Interactive, immersive Module mit Praxisbezug
- Regelmäßige Simulationen auf Basis realer Taktiken
- Messbare KPIs: Klickraten, Risikobewertungen, Abdeckungsraten



Lucy Security: Entwickelt für das Managen menschlicher Risiken

Lucy bietet eine **komplette Plattform**, um die Anforderungen der NIS2-Richtlinie zu erfüllen und zu übertreffen – entwickelt für Wirkung, Skalierbarkeit und Verantwortlichkeit.



1. Interaktive Module

Von Phishing-Simulationen über DSGVO bis hin zu KI-Bedrohungen und sicheren Remote-Arbeiten – Lucy bietet ansprechende, spielerische Schulungen, die den Mitarbeitern tatsächlich im Gedächtnis bleiben.



2. Mehrsprachige Reichweite

Über 130 Sprachen. Deutschsprachige Inhalte. Integrierte kulturelle Anpassung.



3. Verhaltensbezogene Erkenntnisse

Verfolgen Sie den Fortschritte, die die Kollegen und Mitarbeiter machen und, das Risikoniveau mit Hilfe von Echtzeit-Dashboards.



4. Benutzerdefinierter Inhaltseditor

Passen Sie Nachrichten, Grafiken und Szenarien an Ihre Branche, Ihre Marke und reale Vorfälle an.

Mit Lucy schulen Sie nicht nur Benutzer – Sie bauen eine **messbare menschliche Firewall** auf, die sowohl Compliance Anforderungen gerecht wird als auch Resilienz unterstützt.



Kern Verpflichtungen gemäß NIS2 und wo Bewusstsein ins Spiel kommt

Compliance ist keine Option – sie ist operativ

Die NIS2-Richtlinie führt eine Reihe harmonisierter **technischer und organisatorischer Maßnahmen (TOMs)** ein, die alle regulierten Unternehmen umsetzen müssen. Dabei handelt es sich nicht um Richtlinien, sondern um gesetzliche Verpflichtungen, die durch Durchsetzungsmaßnahmen, Audits und erhebliche Strafen durchgesetzt werden.

Entscheidend ist, dass neben den traditionellen IT-Sicherheitskontrollen auch **Sensibilisierung und Mitarbeiterschulungen in die TOMs integriert sind**.

Was müssen Unternehmen tun?

NIS2 erfordert ein risikobasiertes Sicherheitsprogramm, das sowohl die technische Infrastruktur als auch das menschliche Verhalten abdeckt. Hier sind die wichtigsten Verpflichtungen:



Umsetzung geeigneter technischer und organisatorischer Maßnahmen (TOMs)

Dazu gehören unter anderem:

- Risikoanalyse und Sicherheitsrichtlinien
- Sichere Zugriffskontrollen und Authentifizierung
- Patch- und Schwachstellenmanagement
- Erkennung und Reaktion auf Vorfälle
- **Mitarbeiterschulungen und Sensibilisierungsprogramme**
- Cyber Hygiene und grundlegende Praktiken
- Risikomanagement in der Lieferkette
- Geschäftskontinuität und Krisenmanagement



Bereitschaft zur Reaktion auf Vorfälle schaffen

- Benachrichtigung der Behörden **innerhalb von 24 Stunden** nach Feststellung eines schwerwiegenden Vorfalls
- Detaillierte Nachverfolgung **innerhalb von 72 Stunden**
- Reichen Sie **innerhalb von 30 Tagen** eine abschließende Nachbetrachtung und Lösung ein



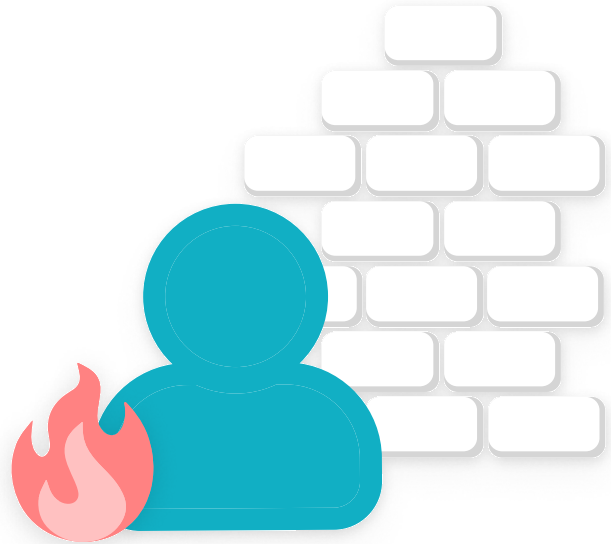
Sicherstellung der Rechenschaftspflicht auf Vorstandsebene

- Die Geschäftsleitung ist für die Umsetzung von TOM verantwortlich
- Sensibilisierungsprogramme müssen nachweisbar, wiederholbar und überprüfbar sein

NIS2-TOM-Anforderungen

- ✓ Risikomanagement
- ✓ Zugriffskontrollen
- ✓ Schwachstellenmanagement
- ✓ **Mitarbeiterschulung und Sensibilisierung**
- ✓ Meldung von Vorfällen
- ✓ Sicherheit der Lieferkette
- ✓ Geschäftskontinuität
- ✓ Krisenreaktion
- ✓ Verschlüsselung und Authentifizierung

● Bereiche, in denen Sensibilisierungsprogramme direkt relevant sind



Wo Lucy für Compliance-Sicherheit sorgt

Lucy Security ist **mehr als nur ein Schulungstool** – es ist ein **bewährtes Hilfsmittel zur NIS2-Compliance**:



1. Auditfähige Aufzeichnungen

Verfolgen Sie Abschlussquoten, Risikobewertungen und den Fortschritt der Benutzer



2. Anpassung an Richtlinien

Anpassbare Inhalte, die Ihren internen TOMs und ISMS entsprechen



3. Integriert in Ihre Prozesse

API- und SCORM-kompatibel



4. Realistische Angriffs Simulationen

Trainieren und testen Sie anhand von Live-Phishing-Techniken

Durch die Einbindung von Lucy in Ihre NIS2-Strategie stellen Sie sicher, dass menschliche Risiken **aktiv gemanagt, nachweislich reduziert und regulatorisch konform** sind.



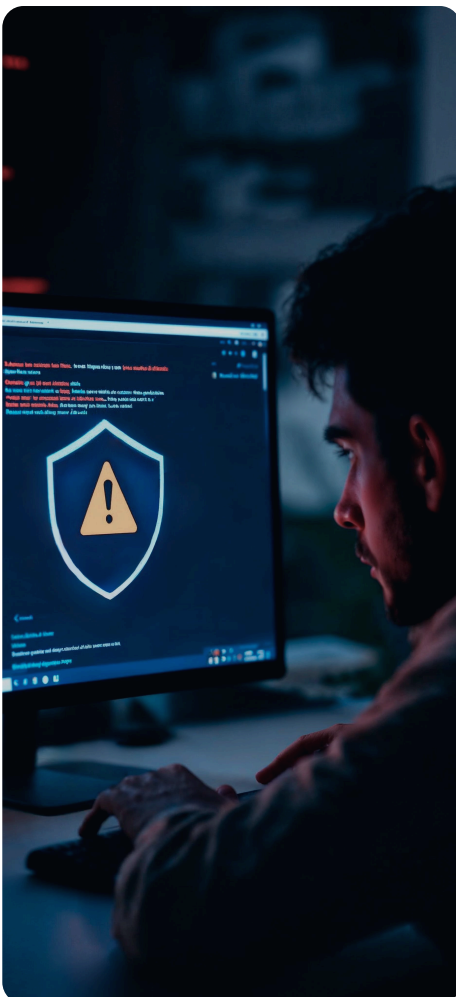
So erstellen Sie ein wirksames Sensibilisierungsprogramm

Von jährlichen Schulungen zu kontinuierlichen Awareness Security Programmen.

Bewusstseinsveranstaltungen, bei denen man nur ein Kästchen ankreuzt, sensibilisieren nicht und ändern demzufolge auch kein Verhalten. Die Regulierungsbehörden wissen das, die CISOs wissen das – und jetzt, unter NIS2, **reichen eine solche Herangehensweise nicht mehr aus.**

Um menschliche Cyberrisiken effektiv zu reduzieren (und die Compliance zu gewährleisten), müssen Unternehmen **strukturierte, wiederholbare und anpassungsfähige Sensibilisierungsprogramme** entwickeln, die sich mit realen Bedrohungen und realen Benutzern befassen.

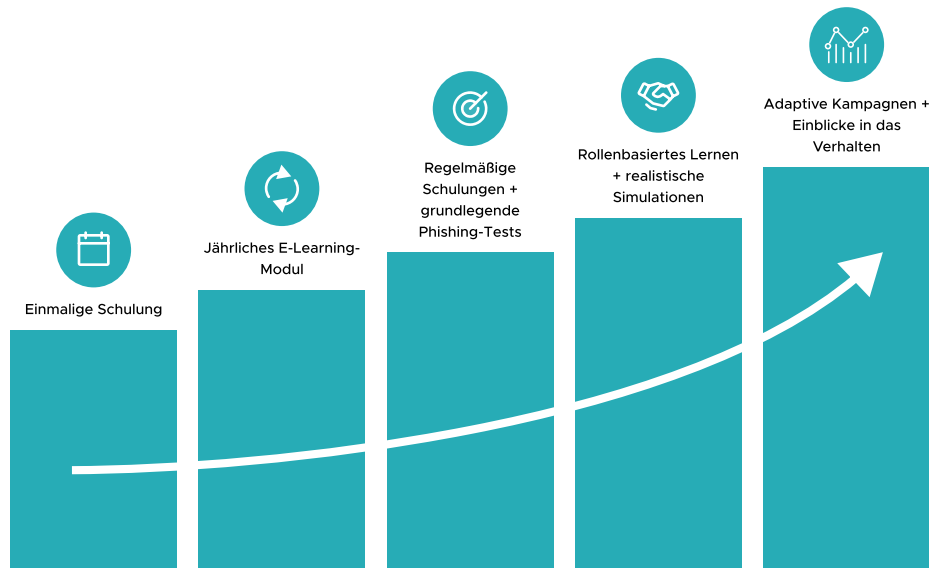
 **Wiederholung, Rollenrelevanz und realitätsnahe Simulationen** sind der Standard, kein nice to have.



Wie sieht ein effektives Sensibilisierungsprogramm aus?

Um NIS2 zu erfüllen und Risiken wirklich zu reduzieren, sollte Ihr Sensibilisierungsprogramm Folgendes umfassen:

- ✓ **Maßgeschneiderte Inhalte**
Verschiedene Abteilungen sind mit unterschiedlichen Bedrohungen konfrontiert – Ihr HR-Team benötigt andere Schulungen als Ihr DevOps-Team. Maßgeschneiderte Botschaften verbessern die Relevanz und die Beibehaltung von Wissen.
- ✓ **Laufende Kampagnen**
Einmalige Schulungen verlieren schnell an Wirkung. Programme sollten das ganze Jahr über laufen, Auffrischungen beinhalten und ein kumulatives Verständnis aufbauen.
- ✓ **Phishing-Simulationen**
Generische Test-E-Mails spiegeln keine realen Bedrohungen wider. Simulationen, die auf echten Phishing-Angriffen basieren, lehren Benutzer, tatsächliche Risiken zu erkennen und zu melden.
- ✓ **Rollenbasierte Lernpfade**
Führungskräfte, Controlling, IT-Administratoren – jeder benötigt zielgerichtete Inhalte. Einfache Lösungen sind können das nicht adressieren.
- ✓ **Positive Verstärkung**
Gamification, Nudges und Feedbackschleifen fördern sicheres Verhalten ohne Schuldzuweisungen oder Ermüdungserscheinungen.



Stufe Beschreibung	Häufige Schwachstelle
1. Einmalige Schulung	Keine Beibehaltung, keine Verhaltensänderung
2. Jährliches E-Learning-Modul	Innerhalb weniger Wochen vergessen
3. Regelmäßige Schulungen + grundlegende Phishing-Tests	Allgemein, begrenzte Messung
4. Rollenbasiertes Lernen + realistische Simulationen	Maßgeschneidert, beginnt das Verhalten zu beeinflussen
5. Adaptive Kampagnen + Einblicke in das Verhalten	Messbare Veränderung und Risikominderung

🎯 Ziel: Erreichen von Level 5, um die NIS2-Anforderungen zu erfüllen.

Wie Lucy echte Wirkung ermöglicht



Tools zur Simulation realer Angriffe

Importieren, bereinigen und wiederverwenden Sie tatsächliche Phishing-Versuche, die Ihre Benutzer erhalten haben – so wird das Training zu 100 % relevant.



Kampagnen-Generator und Inhaltseditor

Erstellen Sie benutzerdefinierte Workflows, ändern Sie Nachrichten und passen Sie den Ton an Ihre Unternehmenskultur und Bedrohungslage an.



Lokalisierte, zielgerichtete Schulungen

Über 130 Sprachen. Intelligente Segmentierung. Unterstützung für abteilungs- und regionspezifische Rollouts.

Mit Lucy bieten Sie nicht nur Schulungen an – Sie **verändern Verhaltensweisen und reduzieren reale Risiken**, mit vollständiger Kontrolle und vollständiger Transparenz.



Messung der Wirksamkeit und Nachweis der Compliance

Was man nicht messen kann, kann man auch nicht nachweisen – oder verbessern

NIS2 fragt nicht nur: „Schulen Sie Ihre Mitarbeiter?“

Es fragt: „Können Sie nachweisen, dass Ihr Sensibilisierungsprogramm funktioniert?“

Bei der Compliance geht es nicht mehr um Richtlinien auf dem Papier – es geht um den Nachweis der Umsetzung und der Wirkung. Aufsichtsbehörden und Prüfer erwarten messbare Ergebnisse:

Wer hat die Schulung erhalten? Wann? Wie oft? Was war das Ergebnis?

Um diese Anforderungen zu erfüllen, muss Ihre Sensibilisierungslösung **klare Kennzahlen, Einblicke in das Verhalten und Berichtstools** bieten – nicht nur Inhalte.

Was sollten Sie messen?



1. Teilnahmekennzahlen

- Abschlussquoten nach Abteilung, Region oder Risikogruppe
- Prozentualer Anteil der im Rahmen von NIS2 geschulten Mitarbeiter
- Schulungshäufigkeit und Auffrischungszyklen



2. Ergebnisse der Phishing-Simulation

- Klickraten nach Benutzergruppen
- Meldesraten und Reaktionszeiten
- Risikobewertung basierend auf wiederholtem Verhalten



3. Verhaltensindikatoren im Zeitverlauf

- Verbesserung der Benutzer Entscheidungen unter simuliertem Druck
- Rückgang risikoreichen Verhaltens
- Auseinandersetzung mit Sensibilisierungsinhalten



4. Audit-fähige Dokumentation

- Zeitbasierte Schulungsprotokolle
- Kampagnenverlauf
- Nachweis von Verbesserungen und Korrekturmaßnahmen

Wichtige Leistungsindikatoren

Phishing-Meldungsrate:

72%

Klick-Risiko-Score:

<12% im Vergleich zum Vorquartal

Zeitraumen für die Durchführung einer Schulungs:

5.4 Tage

Abdeckung: 98%

der Zielgruppe geschult

Wie Lucy Ihnen hilft, immer einen Schritt voraus zu sein



Integrierte Berichts-Engine

Erstellen Sie detaillierte, exportierbare Berichte für interne Überprüfungen, Audits und Aufsichtsbehörden – nach Benutzergruppe, Datumsbereich, Inhaltstyp und mehr.



Verhaltensanalyse

Lucy verfolgt Risiko Trends unabhängig Abteilungen und Personen und hilft Ihnen damit, Ihre Bemühungen auf die Bereiche zu konzentrieren, in denen das menschliche Risiko am höchsten ist.



KPI-gesteuerte Sensibilisierungsprogramme

Nutzen Sie die Daten von Lucy, um Kampagnen kontinuierlich zu optimieren und Fortschritte zu demonstrieren – nicht nur Aktivitäten.

Lucy macht Bewusstseinsbildung zu einer **Compliance-fähigen, Erkenntnis orientierten Disziplin** – und verschafft Ihnen so Kontrolle, Klarheit und Sicherheit vor jedem Audit.



Leitfaden für Käufer: Worauf Sie bei einer Lösung achten sollten

Nicht alle Sensibilisierung Tools sind NIS2-kompatibel

Gemäß NIS2 muss Ihr Awareness Security Konzept weit mehr umfassen als generische E-Learning Übungen oder gelegentliche Phishing-Tests.. Sie muss die Einhaltung von Vorschriften unterstützen, Verhaltensänderungen fördern und an die Kommunikationsstruktur Ihres Unternehmens angepasst werden können – unabhängig davon, ob Sie ein Stadtwerk mit 50 Mitarbeitern oder ein Unternehmen mit 5.000 Mitarbeitern sind.

Verwenden Sie diese Checkliste, um Ihre Optionen zu bewerten.



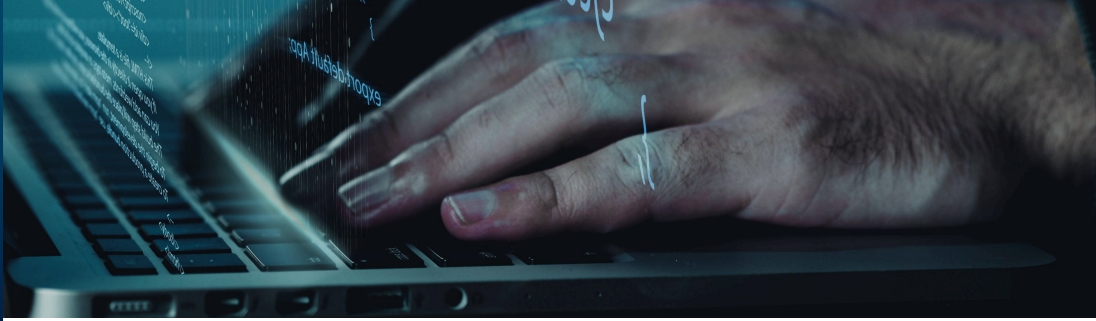
Checkliste für Käufer von Sensibilisierungsplattformen für NIS2

Auswahlkriterien	Was Sie beachten sollten
1. Anpassbarkeit	Können Sie Schulungsinhalte, Vorlagen und Szenarien an Ihre Richtlinien, Ihr Branding und Ihre Bedrohungslage anpassen?
2. Deutsche Sprache und kultureller Kontext	Ist die Plattform vollständig für Deutschland lokalisiert – nicht nur übersetzt, sondern auch an Ihr regulatorisches und kulturelles Umfeld angepasst?
3. Prüfpfad und Berichterstellung	Bietet die Lösung zeit gestempelte Aufzeichnungen, Abschlussdaten, Risikokennzahlen und revisionsfähige Exporte?
4. Phishing-Simulationsfunktionen	Können Sie reale Angriffe simulieren, darunter E-Mail-, QR-Code-, SMS- und dateibasierte Bedrohungen – mit realistischen Ergebnissen und Analysen?
5. Integration mit anderen Systemen	Kann die Plattform mit Ihren bestehenden HR-, LMS-, AD/LDAP- oder SIEM-Systemen verbunden werden, um eine nahtlose Benutzer Synchronisierung und Berichterstellung zu ermöglichen?
6. Skalierbarkeit und Flexibilität	Ist die Plattform für KMUs und Unternehmen gleichermaßen geeignet, mit flexiblen Lizenzierungs-, Bereitstellungsoptionen und Kampagnensteuerung?
7. Nachgewiesene Ergebnisse	Gibt es echte Fallstudien, Referenzen oder Erfahrungsberichte, die messbare Auswirkungen in Unternehmen wie Ihrem zeigen?

Lucy erfüllt die Anforderungen – dank ihres Designs

Kriterien	Lucy-Sicherheit
Anpassbarkeit	 Vollständiger Content-Editor + Phishing-Szenario-Generator
Unterstützung der deutschen Sprache und Kultur	 Deutsche Benutzeroberfläche, Support und Inhalte
Prüfpfad und Berichterstellung	 Integrierte Dashboards + exportierbare Audit-Protokolle
Phishing-Simulations Funktionen	 Import realer Angriffe + Multi-Channel-Tests
Integration mit Systemen	 AD, SCORM, API, SIEM und HR-Synchronisierung bereit
Flexibilität für KMU bis hin zu Großunternehmen	 Modulare, skalierbare Lizenzierung für 50 bis 50.000 Benutzer
Bewährte Ergebnisse	 Wird von deutschen Energie-, Gesundheits- und Regierungsorganisationen verwendet

 Lucy wurde von Anfang an für Organisationen entwickelt, die ihr Sicherheitsbewusstsein unter Beweis stellen müssen – und nicht nur darüber reden.



Bereitstellungsmodelle, Daten Residenz und Support

Ihre Daten, Ihre Regeln – ohne Kompromisse

NIS2 legt den Schwerpunkt auf operative Resilienz und Sicherheit in der Lieferkette, was bedeutet, dass Käufer über die Funktionalität hinausblicken und prüfen müssen, wie und wo Sicherheitslösungen eingesetzt werden.

- ✓ Wo werden die Daten gespeichert?
- ✓ Wer hat Zugriff darauf?
- ✓ Können wir in einem regulierten Umfeld die Kontrolle behalten?

Dies sind nicht nur IT-Fragen – es sind Fragen auf Vorstandsebene gemäß den Rechenschaftsregeln von NIS2.

Bereitstellungsmodelle sind wichtig

Wählen Sie eine Plattform, die zu Ihrer Sicherheitsarchitektur passt – nicht umgekehrt.

Modell	Vorteile	Ideal für
Vor Ort	Volle Datenkontrolle, keine externen Speicher, lokale Backups	Stark regulierte Organisationen, KRITIS, öffentlicher Sektor
Private Cloud	Isolierte Umgebung, hohe Verfügbarkeit, mehr Kontrolle als bei einer Shared Cloud	Mittelständische Unternehmen mit hybriden IT-Umgebungen
SaaS (Public Cloud)	Schnelle Bereitstellung, minimaler IT-Aufwand	KMU mit begrenzten Infrastruktur Ressourcen

 **Lucy unterstützt alle drei Modelle** – so können Sie sowohl Ihre technischen als auch Ihre rechtlichen Anforderungen sicher erfüllen.

Datenhoheit und -souveränität

Lucy gewährleistet Datenhoheit gemäß den Anforderungen der EU und auch Deutschlands:



In Deutschland gehostete Optionen verfügbar



Alle Daten verbleiben gemäß den Grundsätzen der DSGVO und NIS2 innerhalb der EU



Vom Kunden kontrollierte E-Mail-Domains und Aufbewahrung von Phishing-Daten

Sie kontrollieren die Daten, die Zustellung und die Sichtbarkeit – jederzeit.

Support, der Ihre Sprache spricht

Cyber-Bewusstsein ist keine Plug-and-Play-Angelegenheit. Sie benötigen zeitnahen Support, der Ihren betrieblichen, regulatorischen und sprachlichen Kontext versteht. Lucy hat ein:



Deutschsprachiges
Support-Team



eine auf NIS2-
Anforderungen
zugeschnittene
Implementierungsberatung



Coaching für
Schulungskampagnen und
Best Practices



Vollständige
Dokumentation und
Onboarding-Tools

Warum dies für NIS2 wichtig ist

- ✓ Datenhosting und Zugriffskontrolle sind Teil des **Risikomanagements in der Lieferkette** im Rahmen von TOMs
- ✓ Regulierungsbehörden können Unterlagen zum **Datenfluss, zur Datenverarbeitung und zu Zugriffsberechtigungen** anfordern
- ✓ Vendor Lock-in oder Speicherung außerhalb der EU könnten **Compliance-Warnsignale** auslösen

Lucy wurde von Anfang an für die europäischen Vorschriften entwickelt. Wir helfen Ihnen, rechtlichen, technischen und betrieblichen Anforderungen ohne Kompromisse gerecht zu werden.

Zusätzliche Informationen: 🍀 **Benötigen Sie Hilfe? Lassen Sie einen vertrauenswürdigen Partner die Verwaltung für Sie übernehmen**
Kleineres Team? Begrenzte IT-Kapazitäten? Kein Problem.

Die Einhaltung der NIS2-Vorschriften kann überwältigend sein – insbesondere für **kleinere Organisationen wie Stadtwerke, mittelständische Hersteller oder lokale Behörden** ohne eigenes Cybersicherheitspersonal. Aus diesem Grund arbeitet Lucy Security mit einem Netzwerk **zertifizierter Managed Service Provider (MSPs)** in ganz Deutschland zusammen, die Folgendes leisten können:



Ihr Sensibilisierungsprogramm **einrichten**
und konfigurieren



Die Compliance verfolgen und **Berichte**
erstellen



Laufende Schulungen und **Phishing-**
Simulationen durchführen



Support in der Landessprache und **Planung**
von **Maßnahmen bei Vorfällen anbieten**

Mit einem von Lucy zertifizierten Partner profitieren Sie von der gesamten Leistungsfähigkeit unserer Plattform – ohne den damit verbundenen Betriebsaufwand.

- ✓ Schnelle Einarbeitung
- ✓ Kompetente Konfiguration
- ✓ Lokaler, deutschsprachiger Support
- ✓ Volle Transparenz, null Stress

Sie behalten die Kontrolle. Ihr Partner kümmert sich um die Komplexität.

✉️ Fragen Sie uns nach einem empfohlenen MSP in Ihrer Region



Abschließende Empfehlungen und nächste Schritte

Bei NIS2 geht es nicht nur um Technologie – es geht um Menschen

Bis Oktober 2025 werden Tausende deutscher Unternehmen – von lokalen Stadtwerken bis hin zu mittelständischen Herstellern – neuen gesetzlichen Verpflichtungen gemäß NIS2 unterliegen. Viele unterschätzen noch immer den Umfang, die Dringlichkeit und den Fokus auf den Faktor Mensch in dieser Richtlinie.

NIS2 verlagert die Cybersicherheit von der IT auf das gesamte Unternehmen. Das bedeutet, dass Ihr Sensibilisierungsprogramm nicht länger eine Nebensache sein darf – es muss strukturiert, wiederholbar, risikobasiert und nachweislich wirksam sein.

Abschließende Empfehlungen

- ✓ **Fangen Sie frühzeitig an – warten Sie nicht bis zum Stichtag.**

Der Aufbau eines NIS2-konformen Sensibilisierungsprogramms braucht Zeit. Beginnen Sie jetzt, um überstürzte, oberflächliche Ansätze zu vermeiden.

- ✓ **Verlassen Sie sich nicht auf integrierte oder generische Tools.**

Einfache Präsentationen oder einheitliche E-Learning-Programme erfüllen nicht die NIS2-Standards für Wirksamkeit und Überprüfbarkeit.

- ✓ **Wählen Sie eine Plattform, die von Grund auf NIS2-fähig ist.**

Lokalisierung, Flexibilität, Audit-Berichte und realitätsnahe Simulationen sind unerlässlich.

- ✓ **Dokumentieren Sie alles.**

Von Benutzerschulungen bis hin zu Phishing-Ergebnissen – Ihre Fähigkeit, Ihre Bemühungen und Verbesserungen nachzuweisen, ist genauso wichtig wie Ihre technische Ausstattung.

- ✓ **Holen Sie sich bei Bedarf Unterstützung von Experten.**

Die Zusammenarbeit mit einem vertrauenswürdigen Lucy MSP kann Ihnen helfen, Ihre Verpflichtungen ohne zusätzlichen Aufwand zu erfüllen.

Nächste Schritte mit Lucy Security

Lucy Security genießt das Vertrauen von Unternehmen in ganz Deutschland und bietet:

- ✓ **NIS2-konforme Sensibilisierungs- und Simulation Kampagnen**
- ✓ **Vollständige Prüfpfade, Risikokennzahlen und Benutzerverfolgung**
- ✓ **Bereitstellungsoptionen, die Ihren IT- und Compliance-Anforderungen entsprechen**
- ✓ **Deutschsprachiger Support und lokalisierte Inhalte**
- ✓ **Skalierbare Lizenzen für 50 bis 50.000 Benutzer**

Ganz gleich, ob Sie in der Energiebranche, im Gesundheitswesen, im Finanzwesen oder im öffentlichen Dienst tätig sind – mit Lucy können Sie menschliche Risiken in menschliche Resilienz umwandeln – und dies auch nachweisen.

 **Lassen Sie uns darüber sprechen:** Buchen Sie eine kostenlose Beratung mit unserem NIS2-Readiness-Team

 **Fordern Sie eine Demo an:** Sehen Sie die Lucy-Plattform in Aktion

 **Finden Sie einen Managed Partner:** Für die reibungslose Durchführung von Sensibilisierungsprogrammen

NIS2 ist obligatorisch. Die Vorbereitung darauf ist optional – bis sie es nicht mehr ist.

Lucy hilft Ihnen dabei, Compliance in Vertrauen zu verwandeln.

Extras:

- **Anhang:** Beispiel für einen Test- und Schulungskalender – Bitten Sie einen SE um Erstellung
- **Checkliste:** „Ist Ihr Unternehmen bereit für NIS2?“
- **Glossary:** NIS2 key terms for execs and project teams

Checkliste:

Ist Ihr Unternehmen bereit für NIS2?

Diese kurze Checkliste soll Ihnen helfen, Ihren aktuellen Stand der Vorbereitung im Hinblick auf NIS2 zu bewerten – insbesondere auf Verpflichtungen den “human factor” betreffend..



Governance und Verantwortung

- Wir haben ermittelt, ob wir gemäß NIS2UmsuCG als wesentliche oder wichtige Einrichtung gelten.
- Unsere Führungskräfte sind sich ihrer Verantwortlichkeiten gemäß NIS2 bewusst
- Cybersicherheit wird auf Vorstandsebene mit definierten Rollen und Verantwortlichkeiten behandelt



Technische und organisatorische Maßnahmen (TOMs)

- Wir haben TOMs dokumentiert, die auf einem risikobasierten Ansatz beruhen.
- Zugriffskontrolle, Authentifizierung und Pläne für die Reaktion auf Vorfälle sind vorhanden.
- Cyberrisiken in der Lieferkette werden bewertet und angegangen



Risiko und Bewusstsein (Human Factor)

- Wir führen ein strukturiertes, fortlaufendes Sensibilisierungstraining durch (keine einmaligen Schulungen).
- Die Schulungsinhalte sind auf die jeweilige Rolle, Abteilung und das Risikoniveau zugeschnitten
- Es werden regelmäßig Phishing-Simulationen mit realistischen, lokalisierten Szenarien durchgeführt
- Wir messen Klickraten, Meldeverhalten und Verbesserungen im Zeitverlauf



Berichterstattung und Compliance

- Die Ergebnisse der Schulungen und Simulationen werden nachverfolgt und sind auditfähig.
- Wir verfügen über einen 24/72/30-Stunden-Workflow für die Meldung von Vorfällen
- Wir können unsere Sensibilisierungsmaßnahmen gegenüber externen Aufsichtsbehörden oder Prüfern nachweisen



Plattform und Support

- Unsere Awareness Security Plattform unterstützt mehr als 100 Sprachen
- Unsere Lösung bietet detaillierte Metriken, Risiko-Dashboards und exportierbare Protokolle
- Wir verfügen über interne Kapazitäten – oder einen vertrauenswürdigen Managed Partner –, um unsere Programme effektiv durchzuführen.



Glossar

Glossar: NIS2–Schlüsselbegriffe für Führungskräfte und Projektteams

NIS2 (Richtlinie (EU) 2022/2555)

Die überarbeitete Richtlinie der EU zur Sicherheit von Netz- und Informationssystemen. Sie legt strengere Cybersicherheitsverpflichtungen für ein breiteres Spektrum öffentlicher und privater Organisationen in kritischen und wichtigen Sektoren fest.

NIS2UmsuCG

(NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

Deutsches Gesetz zur Umsetzung von NIS2. Es legt fest, wie die Richtlinie auf deutsche Organisationen anzuwenden ist, einschließlich Schwellenwerten, Branchenlisten, Durchsetzung und Sanktionen.

Wesentliche Einrichtungen (EE)

Organisationen mit einer kritischen Rolle in Gesellschaft und Wirtschaft – häufig große Infrastrukturanbieter –, die den höchsten Verpflichtungen der NIS2 unterliegen.

Wichtige Unternehmen (IE)

Mittelständische Unternehmen und Dienstleister in wichtigen Branchen (z. B. Fertigung, Logistik, Lebensmittel, IT), die weiterhin einer erheblichen behördlichen Aufsicht unterliegen.

TOMs (technische und organisatorische Maßnahmen)

Eine Reihe von Maßnahmen, die Unternehmen ergreifen müssen, um ihre IT-Systeme und -Prozesse zu sichern – darunter Sensibilisierungsschulungen, Zugriffskontrolle, Reaktion auf Vorfälle und Risikobewertungen.

24/72/30-Regel

Der Zeitplan für die Meldung von Vorfällen gemäß NIS2:

- Erste Meldung innerhalb von **24 Stunden**
- Detaillierte Aktualisierung innerhalb von **72 Stunden**
- Abschlussbericht innerhalb von **30 Tagen**

Sensibilisierungsprogramm

Eine strukturierte, kontinuierliche Initiative zur Schulung der Mitarbeiter über Cybersicherheitsbedrohungen, sicheres Verhalten und Reaktionsprotokolle. Ein wichtiger TOM gemäß NIS2.

Phishing-Simulation

Ein gefälschter, aber realistischer Cyberangriff, der an Mitarbeiter gesendet wird, um ihr Bewusstsein zu testen und zu verbessern. Wird häufig verwendet, um Schwachstellen zu messen und Mitarbeiter in sicherem Verhalten zu schulen.

Risikobasierter Ansatz

NIS2 verlangt von Organisationen, dass sie Cybersicherheit (einschließlich Schulungen) auf der Grundlage der spezifischen Risiken, denen sie ausgesetzt sind, priorisieren – nach Abteilung, Rolle oder Gefährdungsgrad.

Prüfpfad

Ein dokumentiertes Protokoll über Maßnahmen, abgeschlossene Schulungen, Vorfälle und Reaktionen – entscheidend für den Nachweis der Compliance bei behördlichen Überprüfungen.

Cyberisiko in der Lieferkette

Das Risiko, das durch Drittanbieter und Dienstleister entsteht. NIS2 verlangt von Unternehmen, diese Risiken proaktiv zu bewerten und zu managen.

Verantwortlichkeit

NIS2 macht Führungskräfte persönlich für die Einhaltung der Vorschriften verantwortlich. Die Unternehmensleitung muss sicherstellen, dass Sensibilisierungsprogramme, TOMs und Maßnahmen zur Reaktion auf Vorfälle vorhanden und wirksam sind.



Referenzen und weiterführende Literatur

1. NIS2-Richtlinie (amtlicher EU-Text)

Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>

2. Deutscher Umsetzungsentwurf: NIS2UmsuCG

Bundesministerium des Innern und für Heimat (BMI) – Gesetzesentwurf (auf Deutsch)
<https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2.html>

3. ENISA – Agentur der Europäischen Union für Cybersicherheit

NIS2-Compliance-Leitfaden, sektorspezifische Berichte und Best Practices
<https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive/nis2-directive>

4. Bundesamt für Sicherheit in der Informationstechnik (BSI)

Deutsche Cybersicherheitsbehörde – technische Leitlinien und branchenspezifische Informationen
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitsanforderungen/NIS2/nis2_node.html

5. NIS2 Scope Tool (ENISA)

Ein hilfreiches Tool, um festzustellen, ob Ihre Organisation unter die NIS2-Richtlinie fällt
<https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive/scope-tool>

6. Bundesnetzagentur – Definitionen kritischer Infrastrukturen (Deutschland)

Sektorspezifische Kriterien und Schwellenwerte, die für die Einstufung als wesentliche/wichtige Einrichtung gemäß NIS2 relevant sind
https://www.bnetza.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/KRITIS/kritis-node.html

7. ENISA-Berichte zur Bedrohungslage

Jährlicher Überblick über sich entwickelnde Cyber-Bedrohungen und -Trends, einschließlich Phishing und Risiken durch den Faktor Mensch
<https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>

8. NIS2-FAQ der Europäischen Kommission

Einfach verständliche Fragen und Antworten zur Umsetzung und zum Geltungsbereich von NIS2
<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>



LUCY
AWARENESS

