

# NIS2-Richtlinie (EU) 2022/2555

verpflichtet kritische Einrichtungen  
zu höheren Sicherheitsstandards.

Die NIS2-Richtlinie ist der verbindliche europäische Rahmen zur Stärkung der Cybersicherheit. Sie reagiert auf die zunehmende Abhängigkeit von digitalen Infrastrukturen und setzt einheitliche Sicherheitsstandards für besonders relevante Einrichtungen fest.

## Relevante Bereiche

Viele gesellschaftliche und wirtschaftliche Kernbereiche sind heute von IT- und Netzwerksystemen abhängig. Um Ausfälle und Sicherheitsrisiken in diesen sensiblen Umfeldern zu reduzieren, definiert die NIS2-Richtlinie zwei Stufen betroffener Strukturen.

### Besonders wichtige Einrichtungen

- Energie
- Verkehr
- Banken und Finanzmarkt
- Gesundheitswesen
- Trinkwasserversorgung
- Digitale Infrastruktur

### Wichtige Einrichtungen

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemische Industrie
- Lebensmittelproduktion
- Verarbeitendes Gewerbe
- Digitale Dienste

Ausfälle oder Angriffe in diesen Bereichen können erhebliche Auswirkungen auf Versorgungssicherheit, Wirtschaft und öffentliche Ordnung haben.

## Anforderungen der NIS2

Betroffen sind vor allem mittlere und größere Einrichtungen in kritischen Sektoren (häufig ab ca. **50 Mitarbeitenden oder 10 Mio. EURO Jahresumsatz**). Gefordert werden technische und organisatorische Maßnahmen zur Sicherstellung sicherer Systeme, u. a.:

- **Systeme müssen geschützt werden**  
z. B. Netzwerke, Steuerungen, Computer
- **Störungen und Angriffe müssen gemeldet werden**  
Damit schnell reagiert und Schäden begrenzt werden können
- **Es muss Notfallpläne geben**  
Damit der Betrieb nach Störungen oder Angriffen schnell weiterlaufen kann
- **Technische Strukturen müssen dokumentiert sein**  
Damit Systeme nachvollziehbar, prüfbar und sicher betreibbar bleiben
- **Mitarbeitende sollen informiert und geschult sein**  
Damit Fehler, Sicherheitslücken und Risiken vermieden werden

Für die physische Netzwerkinfrastruktur bedeutet das insbesondere:

- **Dokumentation aller Leitungswege und Anschlusspunkte**
- **Eindeutige Kennzeichnung von Kabeln und Ports**
- **Aktuelle Netzpläne**

## Beitrag von NetPeppers

**Mess- und Prüfgeräte für Kupfer- und Glasfaserinfrastrukturen von NetPeppers unterstützen die Umsetzung der NIS2-Anforderungen, indem sie die physische Sicherheit, Zuverlässigkeit und Resilienz von Netz- und Informationssystemen erhöhen. Präzise Mess- und Prüfverfahren spielen dabei eine zentrale Rolle bei der Absicherung passiver und aktiver IT- und Telekommunikationsverkabelungen.**

Der Einsatz von Kupferzertifizierern, OTDR-Systemen, Dämpfungsmessgeräten, Spleißtechnik und weiteren Prüfmethoden ermöglicht eine zuverlässige Überprüfung der Infrastruktur und liefert belastbare Dokumentationen für Audits sowie behördliche Anforderungen. So entsteht die Grundlage für ein resilient aufgebautes und nachweislich sicheres Netzwerk gemäß NIS2.

Wir unterstützen Sie bei der Umsetzung der Richtlinie mit passenden Mess- und Prüflösungen.

## Cyber Security Tester

Der CyberScope® ist ein tragbares Netzwerk- und Cybersecurity-Analysegerät, das IT- und OT-Netzwerke sichtbar macht, überprüft und analysiert – ohne den laufenden Betrieb zu stören.

Er dient als technisches Prüf- und Kontrollinstrument, um den tatsächlichen Sicherheitszustand des Netzwerks objektiv zu bewerten.



## NIS2-Anforderung und Beitrag des CyberScope® von NetAlly

### Kenntnis aller relevanten IT-/OT-Assets im Netzwerk

- Automatische Erkennung und Inventarisierung aller verbundenen Geräte, inkl. IP, MAC, Hersteller und Kommunikation

### Identifikation und Bewertung von Cyber-Risiken

- Analyse der Netzwerkkonfiguration, Erkennung unsicherer Protokolle, Ports und Kommunikationspfade

### Präventive technische Schutzmaßnahmen

- Aufdeckung von Fehlkonfigurationen, veralteten Diensten und unsicheren Netzwerkparametern

### Erkennung von Sicherheitsvorfällen und Anomalien

- Analyse von Netzwerkverkehr und Protokollen zur Identifikation ungewöhnlicher oder unerwarteter Aktivitäten

### Schutz vor unbefugtem Zugriff

- Identifiziert unbekannte oder nicht genehmigte Geräte im Netzwerk

### Früherkennung von Sicherheitsereignissen

- Unterstützung bei der schnellen Lokalisierung von Auffälligkeiten und potenziellen Angriffen

### Nachweise für Audits und Behörden

- Erstellung technischer Mess- und Analyseergebnisse als Audit- und Compliance-Nachweis

### Sicherer, stabiler Betrieb kritischer Netze

- Regelmäßige Prüfungen ohne Eingriff in den laufenden Betrieb

Art. Nr.: **CYBERSCOPE-CE-X2** (wired & wireless)

Art. Nr.: **CYBERSCOPE-AIR-E-X2** (wireless)

Art. Nr.: **CYBERSCOPE-XRF** (wired only)

## NetPeppers GmbH

Carl-Benz-Str. 5 · 82266 Inning

Tel.: +49-89-219097300

E-Mail: mail@netpeppers.com

[www.netpeppers.com](http://www.netpeppers.com)

Weitere Informationen und die Produkte erhältlich bei Ihrem Fachhändler:

## Messgeräte | Spleißgerät

### DÄMPFUNGS- UND LEISTUNGSMESSGERÄTE FÜR GLASFASER

Optische Dämpfungsmessgeräte (OLTS, Light Source & Power Meter) messen die tatsächliche Einfügedämpfung eines LWL-Links – ein zwingender Bestandteil jeder Abnahme.



## Beitrag zur NIS2-Erfüllung

### Qualitätssicherung von kritischen LWL-Ressourcen

- Sicherstellung, dass die Glasfaserverbindungen die für kritische Systeme erforderliche Performance bieten.
- Abnahmemessungen verhindern Netzinstabilität in der Betriebsphase.

### Erkennung von Manipulationen

- Plötzliche Dämpfungsveränderungen können auf Fasersplits, Abzweige oder physische Angriffe hinweisen – eine wichtige Maßnahme zur Detektion physischer Bedrohungen gemäß NIS2.

### Langzeitdokumentation

- OLTS-Protokolle sind Bestandteil des technischen Sicherheitsnachweises im Rahmen der NIS2-Compliance.

Art. Nr.: **NP-FIBER-SPI1MMKIT** | **NP-FIBER-SPI1QUADKIT**  
**NP-FIBER-SPI1SMKIT**

### SPLEIßGERÄTE (FUSION SPLICER)

Spleißgeräte sorgen für dauerhaft stabile und verlustarme Verbindungen innerhalb der Glasfaserinfrastruktur.



CFS200

CFS100

### Aufbau robuster, hochverfügbarer Netzinfrastrukturen

- Qualitativ hochwertige Spleiße reduzieren das Ausfallrisiko im Backbone und in Zugangsnetzen
- Besonders in kritischen Bereichen (Industrienetze, KRITIS-Versorger, Campusnetze) sind zuverlässige Spleiße für Netzredundanz und Notfallkommunikation ein essentielles Fundament

### Vermeidung technischer Schwachstellen

- Schlechte Spleißqualität kann zu Störungen führen, die als Sicherheitsrisiko gelten.

### Nachweisbare Installation gemäß Standard

- Die protokollierten Spleißdaten unterstützen die Compliance-Dokumentation im Kontext der NIS2-Anforderungen.

Art. Nr.: **NP-CFS200** | **NP-CFS100**



## Messgeräte

### OTDR-GERÄTE

(OPTICAL TIME DOMAIN REFLECTOMETER)

OTDRs dienen der detaillierten Analyse von Glasfaserstrecken. Sie ermöglichen es, strukturelle und dämpfungs-basierte Fehler in der LWL-Infrastruktur zu erkennen.



## Beitrag zur NIS2-Erfüllung

### Risikomanagement und Schwachstellenanalyse

- OTDR-Messungen decken Faserbrüche, Biegeradien-Überschreitungen, mangelhafte Steckverbinder sowie verdeckte Manipulationen an der Strecke auf.
- Regelmäßige OTDR-Tests dienen als präventive Wartung und reduzieren das Risiko ungeplanter Ausfälle in kritischen Netzen.

### Sicherstellung der Netzresilienz

- Durch lückenlose Ereignisprotokolle und Messkurven wird die strukturelle Integrität der Glasfaser physisch abgesichert.
- Betreiber können abweichende Dämpfungswerte frühzeitig erkennen und Gegenmaßnahmen einleiten.

### Nachweisführung gegenüber Behörden und Auditoren

- Validierte OTDR-Messberichte bestätigen den ordnungsgemäßen Zustand der Backbone- und Access-Infrastruktur.
- Dies unterstützt Melde- und Dokumentationspflichten gemäß NIS2.

Art. Nr.: NP-FIBER1000

### KUPFERZERTIFIZIERER

(CAT-, POE- UND LINK-ZERTIFIZIERUNG)

Kupferzertifizierer prüfen Twisted-Pair-Netzwerke gemäß ISO/IEC- und TIA-Standards. In sicherheitskritischen Bereichen (z. B. Krankenhäuser, Energieversorger, Rechenzentren) ist zuverlässige Kupferverkabelung für IoT (Internet der Dinge) – und OT-Systeme (Operational Technology, digitale Steuerungssysteme) zentral.



### Zertifizierung kritischer Infrastruktur

- Kupferzertifizierer stellen sicher, dass alle Netzwerkverbindungen normgerecht sind und die spezifizierte Bandbreite zuverlässig liefern.
- PoE-Tests gewährleisten stabile Stromversorgung für Kameras, Zutrittskontrollsysteme und Sensorik – alles sicherheitsrelevante NIS2-Themen.

### Minimierung physischer Ausfallrisiken

- Frühzeitige Erkennung von NEXT-Störungen, Schirmungsfehlern oder Aderbruch reduziert das Risiko kritischer Ausfälle.

### Audit- und Nachweispflichten

- Zertifizierungsprotokolle dienen als technische Nachweise, die Betriebsfähigkeit und Compliance dokumentieren.

Art. Nr.: AEM-TestPRO-100NET