NIS-2-Factsheet

www.link11.com

LINK11

1. WAS VERLANGT NIS-2?

Die NIS-2-Richtlinie verpflichtet betroffene Organisationen, risikobasierte technische und organisatorische Maßnahmen zur Absicherung ihrer Netz- und Informationssysteme umzusetzen. Zu den Mindestanforderungen zählen insbesondere:

- Risikoanalyse und IT-Sicherheitskonzepte
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs (Business Continuity), Wiederherstellung und Krisenmanagement
- Sicherheit der Lieferkette und eingesetzter Dienstleister
- Bewertung der Wirksamkeit von Sicherheitsmaßnahmen

Das Ziel besteht darin, ein nachweisbares, dem Stand der Technik entsprechendes Sicherheitsniveau mit Fokus auf Verfügbarkeit, Resilienz und kontrollierte Prozesse zu erreichen.

2. ROLLE VON DDOS-SCHUTZ UNTER NIS-2

DDoS-Schutz ist kein isolierter Compliance-Baustein, sondern Teil der technischen Maßnahmen.

Sicherstellung der Verfügbarkeit kritischer Dienste	Begrenzung der Auswirkungen von Sicherheitsvorfällen.	Unterstützung von Business-Continuity- und Krisenprozessen.

Das Ziel besteht darin, ein nachweisbares, dem Stand der Technik entsprechendes Sicherheitsniveau mit Fokus auf Verfügbarkeit, Resilienz und kontrollierte Prozesse zu erreichen.

3. ZIELBILD & SCOPE

Typische geschützte Assets sind:

- Internet-Anbindungen und Netzwerkschnittstellen
- Web-Anwendungen und Portale
- APIs
- DNS-Dienste

Optional:

- VPN-Zugänge
- Branchenspezifische Schnittstellen (z. B. OT-Gateways)

Schutzebenen:

- Netzwerkebene (Layer 3/4): volumetrische Angriffe, Protokoll-Floods, Reflection/Amplification
- Applikationsebene (Layer 7): HTTP-Floods, Slow-Rate-Angriffe, applikationsspezifische DoS-Angriffe
- Multi-Vektor-Angriffe: Kombination mehrerer Angriffstypen gleichzeitig

Grundsätzlich kann DDoS-Schutz, abhängig vom Einsatz-Szenario, in unterschiedlichen Betriebsmodellen umgesetzt werden:

- Always-on oder On-Demand
- Cloud-basiertes Scrubbing, In-Line- oder Hybrid-Architekturen
- Georedundante Plattform mit verteilten Standorten (z. B. Anycast, Multi-PoP) zur Erhöhung der Resilienz
- Redundanz- und Failover-Konzepte zur Absicherung gegen Ausfälle von Standorten, Leitungen oder Komponenten

Ziel ist eine minimale Beeinflussung der Latenz im Normalbetrieb und eine schnelle, automatisierte Gegenmaßnahme im Angriffsfall.

UNTERSTÜTZUNG ZENTRALER NIS-2-ANFORDERUNGEN DURCH LINK11

Risikomanagement & technische Maßnahmen

NIS-2 fordert dokumentierte, risikobasierte Sicherheitsmaßnahmen.

→ Link11 reduziert Verfügbarkeitsrisiken für kritische Dienste durch spezialisierte DDoS-Schutzmechanismen und deren Einbindung in bestehende ISMS- und Risikomanagement-Prozesse.

Incident Handling & Reporting

NIS-2 verlangt definierte Prozesse zur Erkennung, Behandlung und Meldung von Sicherheitsvorfällen.

→ Link11 stellt Monitoring, Alarmierung, Protokollierung und Reporting bereit, um DDoS-Incidents nachvollziehbar zu erkennen, zu behandeln und zu dokumentieren. Diese Informationen können in interne Melde- und Eskalationsprozesse integriert werden.

Business Continuity & Krisenmanagement

NIS-2 fordert Maßnahmen zur Aufrechterhaltung des Betriebs und zur Wiederherstellung nach Vorfällen.

→ DDoS-Mitigation mit automatischer Abwehr, Redundanz und skalierbarer Kapazität unterstützt die Verfügbarkeitsziele sowie die operativen BCM-Konzepte der Organisation.

Monitoring & Wirksamkeitsnachweis

NIS-2 verlangt die regelmäßige Bewertung der Wirksamkeit von Sicherheitsmaßnahmen.

→ Link11 ermöglicht transparente Auswertungen über Dashboards, KPIs, Logs und Reports, die sich als Nachweis gegenüber internen Prüfern, Auditoren und Aufsichtsstellen nutzen lassen.

Lieferkette & Dienstleistersteuerung

Die Richtlinie adressiert die Sicherheit der Lieferkette explizit.

→ Link11 wird als kontrollierter Sicherheitsdienstleister mit klaren vertraglichen Regelungen, Rollenmodellen und definierten Schnittstellen zu Betrieb und Incident Management in die eigene Governance eingebunden.

Integration in bestehende Sicherheits- und Betriebsprozesse
Der Link11 Schutz bietet APIs und Sicherheitsausgaben, die unter anderem zur Unterstützung der Integration in die folgenden Systeme und Prozesse verwendet werden können:

- SIEM- und Monitoring-Systeme (Events, Logs, Alarme)
- SOC- und Incident-Response-Prozesse (Runbooks, Eskalationen)
- Ticket- und Workflow-Systeme
- SMS-, BCM- und Audit-Prozesse zur Nachweisführung

Ziel ist eine konsistente Einbettung in bestehende Governance-, Risiko- und Compliance-Strukturen.

Governance, Rollen & Verantwortlichkeiten
Für einen NIS-2-konformen Betrieb sind klare Zuständigkeiten erforderlich:

- **Kunde:** Definition der Schutzobjekte, Risikobewertung, Einbindung in BCM/ISMS, Entscheidungs- und Meldeprozesse
- **Link11:** Betrieb der DDoS-Schutzkomponenten, Monitoring, Mitigation, technische Reports, definierte Eskalationswege.

Diese Aufgabenverteilung kann beispielsweise in einem RACI-Modell (Responsible, Accountable, Consulted, Informed) dokumentiert werden. Dies unterstützt die Transparenz gegenüber Management, Revision und Aufsicht.

Der DDoS-Schutz von Link11 ist ein zentraler technischer Baustein zur Umsetzung wesentlicher NIS-2-Anforderungen. Er deckt Bereiche wie Risikomanagement, Incident Handling, Resilienz, Governance und die Steuerung von Sicherheitsdienstleistern in der Lieferkette ab. Zwar ersetzt er keine organisatorischen oder prozessualen Pflichten, jedoch stärkt er gezielt die Verfügbarkeit kritischer Dienste. Gleichzeitig unterstützt er Unternehmen dabei, Wirksamkeit, Nachweise und Dokumentationspflichten verlässlich zu erfüllen.

Gemeinsam setzen wir Ihre Schutzziele effizient und nachweisbar um. Als ihr Partner integrieren wir DDoS-Schutz und Web Security nahtlos in Ihre IT-Sicherheit.

LINK11

+49 69 5800492677
sales@link11.com
www.link11.com

NIS-2 gemeinsam meistern:
Stärken wir Ihre Resilienz.