NIS-2-Factsheet

www.link11.com

LINK11

1. WELKE EISEN STELT DE NIS2 RICHTLIJN?

De NIS2 richtlijn verplicht betrokken organisaties om risicogebaseerde technische en organisatorische maatregelen te implementeren ter beveiliging van hun netwerk- en informatiesystemen. De minimale vereisten omvatten met name:

- Risicoanalyse en IT-beveiligingsconcepten;
- Beheer van security incidenten
- Continuïteit van de bedrijfsvoering (business continuity), herstel en crisismanagement;
- Beveiliging van de supply chain en service providers;
- Periodieke evaluatie van de effectiviteit van beveiligingsmaatregelen.

Het doel is om een aantoonbaar, state-of-the-art security niveau te bereiken met focus op beschikbaarheid, weerbaarheid en gecontroleerde processen.

2. ROL VAN DDOS-BESCHERMING ONDER NIS2

DdoS bescherming is geen op zichzelf staand compliance component, maar maakt deel uit van de technische maatregelen:

Waarborgen van de beschikbaarheid van kritieke diensten	Beperken van de impact van security incidenten	Ondersteunen van bedrijfscontinuïteit en crisisprocessen

DDoS weerbaarheid is een essentieel onderdeel van het vereiste security niveau, vooral voor internet toegankelijke diensten (bijvoorbeeld webapplicaties, API's, DNS en netwerkverbindingen).

3. DOELSTELLING & SCOPE

Typisch beschermde assets zijn:

- Internetverbindingen en netwerkinterfaces;
- Webapplicaties en portals;
- API's;
- DNS services.

Optioneel:

- VPN toegang;
- Sector-specifieke interfaces (bijvoorbeeld OT-gateways).

Beschermingsniveaus:

- Netwerklaag (laag 3/4): volumetrische aanvallen, protocol floods, reflectie-en amplificatieaanvallen;
- Applicatielaag (laag 7): HTTP floods, slow-rate aanvallen, applicatiespecifieke DoS aanvallen;
- Multi-vector aanvallen: combinatie van meerdere aanvalstypen tegelijk.

Afhankelijk van het implementatiescenario kan DDoS bescherming doorgaans in verschillende operationele modellen worden gerealiseerd:

- Always-on of on-demand;
- Cloud-gebaseerde scrubbing, in-line of hybride architecturen;
- Geo-redundante platforms met gedistribueerde locaties (bijvoorbeeld Anycast, Multi-PoP) ter verhoging van de weerbaarheid;
- Redundantie- en failover concepten ter bescherming tegen uitval van locaties, verbindingen of componenten.

Het doel is om de impact op latency tijdens normale bedrijfsvoering te minimaliseren en bij een aanval snelle, geautomatiseerde tegenmaatregelen te bieden.

ONDERSTEUNING VAN CENTRALE NIS2 VEREISTEN DOOR LINK11

Risk management & technische maatregelen

NIS2 vereist gedocumenteerde, risicogebaseerde security maatregelen.

→ Link11 verlaagt beschikbaarheidsrisico's voor kritieke diensten via gespecialiseerde DDoS-beschermingsmechanismen en integratie in bestaande ISMS- en risk management processen

Incidentafhandeling & rapportage

NIS2 vereist gedefinieerde processen voor het detecteren, afhandelen en rapporteren van security incidenten.

→ Link11 biedt monitoring, alarmering, logging en rapportage om DDoS-incidenten detecteerbaar, beheersbaar en traceerbaar te maken. Deze informatie kan worden geïntegreerd in interne rapportage- en escalatieprocessen.

Business Continuity & crisismanagement

NIS2 vereist maatregelen om de bedrijfsvoering te waarborgen en incidenten te herstellen.

→ DDoS-mitigatie met automatische bescherming, redundantie en schaalbare capaciteit ondersteunt de beschikbaarheidsdoelstellingen van de organisatie en de concepten van business continuity management (BCM).

Monitoring & bewijs van effectiviteit

NIS2 vereist periodieke evaluatie van de effectiviteit van security maatregelen.

→ Link11 maakt transparante evaluaties mogelijk via dashboards, KPI's, logs en rapportages, die als bewijs kunnen dienen voor interne auditors, externe auditors en toezichthoudende instanties

Supply chain- en serviceprovidermanagement

De richtlijn adresseert expliciet de security van de supply chain.

→ Link11 wordt geïntegreerd in de eigen governance als gecontroleerde security-dienstverlener met duidelijke contractuele afspraken, rolmodellen en gedefinieerde interfaces richting operations en incident management.

Integratie in bestaande security- en operationele processen
De bescherming van Link11 biedt API's en security outputs die onder andere integratie ondersteunen in:

- SIEM- en monitoringsystemen (events, logs, alarmen);
- SOC- en incident response processen (runbooks, escalaties);
- Ticket- en workflowsystemen;
- ISMS-, BCM- en auditprocessen voor bewijsbeheer.

Het doel is een consistente integratie in bestaande governance-, risk- en compliance structuren.

Governance, rollen & verantwoordelijkheden
Voor een NIS2-conforme werking zijn duidelijke verantwoordelijkheden vereist:

- **Klant:** definitie van te beschermen assets, risk assessment, integratie in BCM/ISMS, besluitvormings- en rapportageprocessen
- **Link11:** Exploitatie van DDoS-beschermingscomponenten, monitoring, mitigatie, technische rapportage, gedefinieerde escalatiepaden.

Deze taakverdeling kan bijvoorbeeld worden vastgelegd in een RACI-model (Responsible, Accountable, Consulted, Informed). Dit ondersteunt transparantie richting management, audit en toezicht.

De DDoS bescherming van Link11 is een belangrijk technisch component voor de implementatie van essentiële NIS2-vereisten. Het dekt gebieden zoals risk management, incidentafhandeling, weerbaarheid, governance en het beheer van security service providers binnen de supply chain. Hoewel het geen organisatorische of procedurele verplichtingen vervangt, versterkt het gericht de beschikbaarheid van kritieke diensten. Tegelijkertijd helpt het bedrijven om verplichtingen rond effectiviteit, verificatie en documentatie betrouwbaar na te komen.

Samen realiseren we uw beveiligingsdoelen efficiënt en aantoonbaar. Als uw partner integreren we DDoS-bescherming en webbeveiliging naadloos in uw IT-beveiliging.

LINK11

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

Samen NIS-2 beheersen:
Laten we je weerbaarheid versterken