IAM QUICK SCAN

BROCHURE · NIS2

Wat dekt de IAM Quick Scan van NIS2?

NIS2 verplicht organisaties tot tien beveiligingsmaatregelen (artikel 21 lid 2). Deze brochure laat per maatregel zien of de IAM Quick Scan er vragen over stelt.

Richtlijn (EU) 2022/2555
Art. 21 lid 2, onder a t/m j

OVERZICHT

De tien maatregelen van artikel 21 lid 2

Dit zijn de tien maatregelen uit artikel 21 lid 2 van NIS2. De sterren tonen hoe sterk een maatregel met IAM te maken heeft (drie sterren: kern van IAM). De laatste kolom toont welke vragen uit de IAM Quick Scan erover gaan.

ART.	MAATREGEL	IAM	DEKKING IN DE SCAN
a	Risicoanalyse en beleid voor informatiesystemen	★★☆	Geen directe dekking (A4.1 raakt zijdelings)
b	Incidentafhandeling	★★☆	Gedeeltelijk (A4.8, A5.3)
c	Bedrijfscontinuïteit en crisisbeheer	★★☆	Gedeeltelijk (A4.9)
d	Beveiliging van de toeleveringsketen	★★☆	Gedeeltelijk (A2.3, A3.1, A3.3)
e	Veilige verwerving, ontwikkeling en onderhoud	★☆☆	Geen dekking (voorstel A3.5, nog niet live)
f	Effectiviteit van maatregelen beoordelen	★★☆	Gedeeltelijk (A4.5)
g	Cyberhygiëne en awareness	★☆☆	Geen dekking (voorstel A4.13, nog niet live)
h	Cryptografie en encryptie	★☆☆	Geen dekking, ligt verder van IAM af
i	**HR-beveiliging, toegangsbeleid en assetmanagement**	★★★	**Sterk (A1.1, A1.2, A4.1–A4.4, A5.4)**
j	**Meervoudige authenticatie en continue authenticatie**	★★★	**Sterk (A2.4, A2.5)**

2
maatregelen goed gedekt (i, j): toegang en inloggen

4
maatregelen deels gedekt (b, c, d, f): de scan stelt er enkele vragen over

4
maatregelen niet gedekt (a, e, g, h): de scan stelt er geen vragen over

Bron: Richtlijn (EU) 2022/2555, art. 21 lid 2. Dekking is een indicatieve koppeling van de scanvragen aan de maatregelen, geen juridische toetsing.

SNELLE BLIK PER MAATREGEL

Maatregelen a t/m e

a **Risicoanalyse en beleid** · Geen directe dekking

De scan peilt geen algemene informatiebeveiligingsrisico's. Alleen vraag A4.1 (beleid voor toegang) raakt hier zijdelings aan. Een bredere risicoanalyse hoort in een aparte beoordeling.

b **Incidentafhandeling** · Gedeeltelijk

A4.8 en A5.3 gaan over het signaleren en afhandelen van misbruik van accounts en rechten. De rest van het incidentproces, zoals meldplicht en escalatie, valt buiten de scan.

c **Bedrijfscontinuïteit** · Gedeeltelijk

A4.9 kijkt naar de beschikbaarheid van het IAM-platform en noodtoegang. Back-ups, herstelplannen en crisisbeheer voor de rest van de organisatie worden niet gevraagd.

d **Toeleveringsketen** · Gedeeltelijk

A2.3, A3.1 en A3.3 raken externe partijen: leveranciers en koppelingen met applicaties die toegang nodig hebben. Contractafspraken en leveranciersbeoordeling zelf zijn geen onderdeel.

e **Veilige verwerving en ontwikkeling** · Geen dekking

De scan vraagt niet of nieuwe applicaties veilig worden aangeschaft en gebouwd, bijvoorbeeld of IAM-eisen vooraf worden meegenomen. Voorstel: vraag A3.5 toevoegen. Die staat nog niet in de plugin.

Let op: de koppeling aan vraagnummers is een indicatie. Ze zegt of de scan er iets over vraagt, niet of uw organisatie voldoet.

SNELLE BLIK PER MAATREGEL

Maatregelen f t/m j

f **Effectiviteit beoordelen** · Gedeeltelijk

A4.5 vraagt naar periodieke controle van rechten (hercertificering). Dat is een deel van het geheel; audits en metingen van andere maatregelen vallen erbuiten.

g **Cyberhygiëne en awareness** · Geen dekking

De scan vraagt niet of medewerkers worden getraind in veilig omgaan met wachtwoorden en accounts. Voorstel: vraag A4.13 toevoegen. Die staat nog niet in de plugin.

h **Cryptografie en encryptie** · Geen dekking

Dit onderwerp ligt verder van IAM af. Alleen indirect speelt het mee, bijvoorbeeld bij het opslaan van geheimen. Het hoort in een aparte beoordeling.

i **HR-beveiliging, toegangsbeleid en assetmanagement** · Sterk

Het kernterrein van IAM. A1.1, A1.2, A4.1 t/m A4.4 en A5.4 gaan over in-, door- en uitstroom van medewerkers, toegangsbeleid, rollen en het inzicht in welke systemen en gegevens er zijn.

j **Meervoudige en continue authenticatie** · Sterk

A2.4 en A2.5 vragen direct naar MFA en sterke authenticatie. Dit is een van de weinige maatregelen in NIS2 die letterlijk over IAM gaat.

Wat betekent dit voor u?

1 De IAM Quick Scan dekt vooral de maatregelen over toegang en inloggen: toegangsbeleid en HR-beveiliging (i) en meervoudige authenticatie (j).

2 Vier maatregelen (b, c, d, f) komen deels aan bod: de scan stelt er een paar vragen over, maar dekt het onderwerp niet volledig. Gebruik de uitkomst als startpunt voor een gesprek, niet als eindoordeel.

3 Vier maatregelen (a, e, g, h) komen niet aan bod: risicoanalyse, veilige ontwikkeling, awareness en cryptografie. Daarvoor is een aparte beoordeling nodig. Voor e en g stellen we twee extra scanvragen voor (A3.5 en A4.13).

Indicatie, geen audit. Deze brochure koppelt de scanvragen aan artikel 21 lid 2 van Richtlijn (EU) 2022/2555 en is geen juridisch advies of nalevingsverklaring. Bespreek de uitkomsten altijd met een implementatieconsultant.

Bron: EUR-Lex, CELEX 32022L2555 (NIS2-richtlijn).