NIS2 & Programma Informatiebeveiliging

26 maart 2024

Gemeenteraad

Jeroen de Graaf (Strategisch Adviseur, afdeling Staf)

Grootste Cyber risico

De Ransomware-dreiging



Vaker

- Wereldwijde schadekosten voor **ransomware** zullen dit jaar naar verwachting **€ 20 miljard** bedragen, een stijging van **57X** ten opzichte van 5 jaar geleden
- Ransomware is de **snelst groeiende vorm van cybercriminaliteit** en een top cyberdreiging waarmee organisaties worden geconfronteerd.

Gerichter

- Aanvallers gaan minder **"schieten met hagel"** en steeds meer **gericht aanvallen** voor de **grote winsten.**
- Gericht op slachtoffers die een groter **financieel resultaat** kunnen opleveren

Geavanceerder

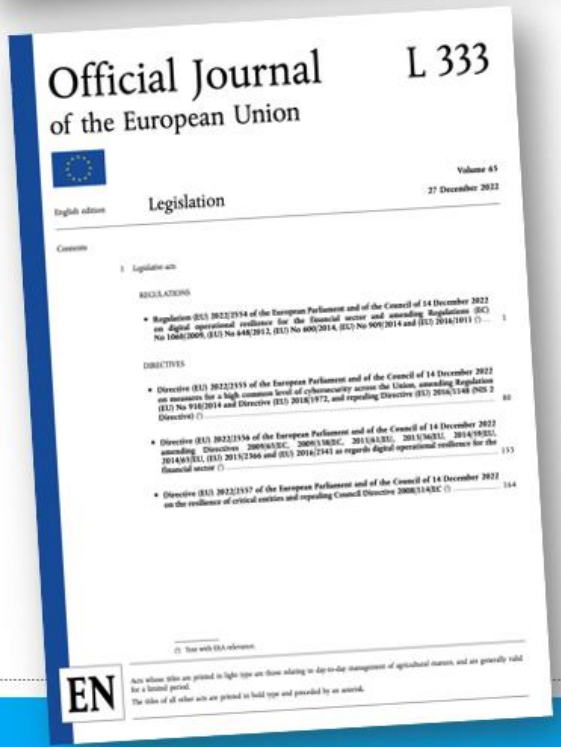
- Aanvallen groeien in verfijning.
- **"Dubbele afpersing"** aanvallen
- Ze nemen **kopieën van gegevens** en dreigen deze openbaar te maken
- Dreigen met het **volledig verwijderen van gegevens**
- Het **cold calling van slachtoffers** die systemen proberen te herstellen

Duurder

- Voor enkele van de meest geavanceerde ransomware-aanvalsgroepen en malwarevarianten wordt gemiddeld meer dan **€ 780,000** per keer betaald;

The NIS2 Directive was officially published in the Official Journal of the EU

Lawels · DECEMBER 27, 2022


Official Journal of the European Union

L 333

Volume 65

27 December 2022

English edition

Legislation

Contents

I Legislative acts

REGULATIONS

• Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (1) 1

DIRECTIVES

• Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (1) 80

• Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (1) 153

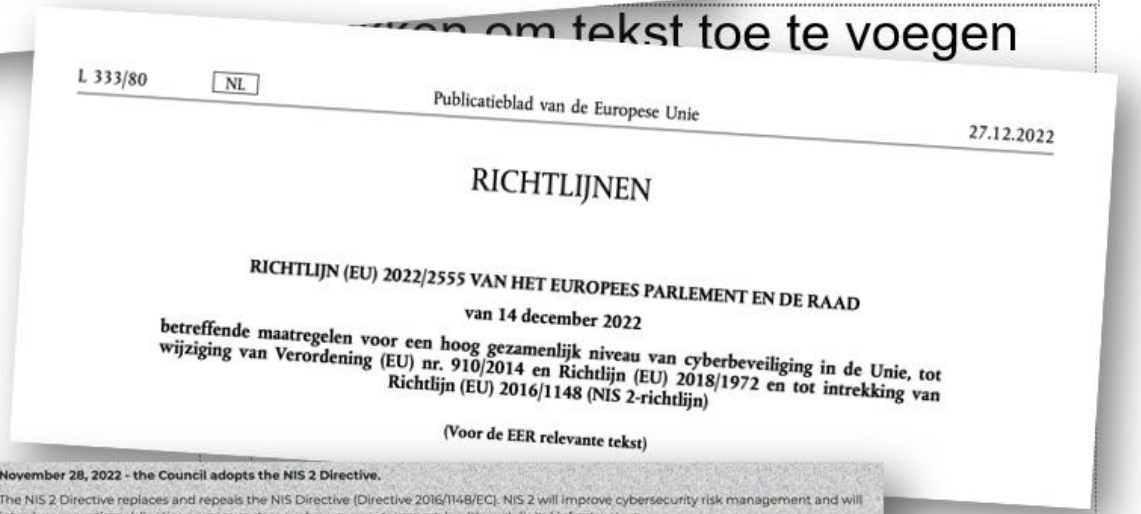
• Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (1) 164

(1) Text with EEA relevance.

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

EN


L 333/80 NL Publicatieblad van de Europese Unie 27.12.2022

RICHTLIJNEN

RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 14 december 2022

betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)

(Voor de EER relevante tekst)

November 28, 2022 - the Council adopts the NIS 2 Directive.

The NIS 2 Directive replaces and repeals the NIS Directive (Directive 2016/1148/EC). NIS 2 will improve cybersecurity risk management and will introduce reporting obligations across sectors such as energy, transport, health and digital infrastructure.

Next step: The directive will be published in the Official Journal of the European Union in the coming days, and will enter into force on the twentieth day following this publication.

Member states must incorporate the provisions of the NIS 2 Directive into national law in **21 months** from the entry into force of the directive.

Artikel 41

Omzetting

1. Uiterlijk op 17 oktober 2024 gaan de lidstaten over tot de vaststelling en bekendmaking van de noodzakelijke bepalingen om aan deze richtlijn te voldoen. Zij stellen de Commissie daarvan onmiddellijk in kennis.

Zij passen die bepalingen toe met ingang van 18 oktober 2024.

2. Wanneer de lidstaten de in lid 1 bedoelde bepalingen vaststellen, wordt in de bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor de verwijzing worden vastgesteld door de lidstaten.

Tijdlijn

- NIS2 moet vertaald worden in nationale wetgeving
- J&V werkt aan wetsvoorstel
- Consultatieronde voor zomer 2024
- Deadline omzetting EC: 17 oktober 2024
- Nederland gaat deadline niet halen, implementatie geschat 2025

Artikel 20

Governance

1. De lidstaten zorgen ervoor dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreukendoor de entiteiten op dat artikel.

De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.

2. De lidstaten zorgen ervoor dat de leden van de bestuursorganen van essentiële en belangrijke entiteiten een opleiding moeten volgen, en moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

Essentiële en belangrijke entiteiten

t toe te

Voor welke sectoren geldt de NIS2-directive?

NIS1		→	NIS2	
Energie	Transport		Energie	Transport
Bankwezen	Infrastructuur financiële markt		Bankwezen	Infrastructuur financiële markt
Gezondheidszorg	Drinkwater		Gezondheidszorg	Drinkwater
Digitale infrastructuur	Digitale dienstverleners		Digitale infrastructuur	Digitale aanbieders
			Afvalwater	Overheidsdiensten
			Ruimtevaart	Post- en koeriersdiensten
			Afvalstoffen-beheerder	Levensmiddelen
			Chemische stoffen	Wetenschap
			Vervaardiging/ Manufacturing	





C 324/6 NL Publicatieblad van de Europese Unie

— Overheid

— Overheidsinstanties van centrale overheden

— Overheidsinstanties op lokaal niveau

Toezicht vooraf en achteraf

- Arikel 32 essentiële entiteiten: toezicht voor- en achteraf
- Artikel 33 belangrijke entiteiten: toezicht achteraf
- BZK wil mogelijk wel bestuurlijke aansprakelijkheid introduceren

- Kli

Nieuw in de NIS2 is de bestuursverantwoordelijkheid. Niet IT-managers, maar bestuurders zelf spelen een cruciale rol in het toezicht op cyberveiligheid. Doen ze dat niet, dan lopen ze het risico op hoge boetes (tot 10 miljoen euro en 2% van de omzet).



Toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten

1. De lidstaten zorgen ervoor dat de toezichts- of handhavingsmaatregelen die met betrek… vastgestelde verplichtingen aan essentiële entiteiten worden opgelegd, doeltreffend, evenr… rekening houdend met de omstandigheden van elk afzonderlijk geval.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezic… met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten…

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles die worden uitgevoerd door daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie of een bevoegde autoriteit;

c) ad-hocaudits, ook in gevallen waarin dat gerechtvaardigd is op grond van een significant incident of inbreuk op deze richtlijn door de essentiële entiteit;

d) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

e) verzoeken om informatie die nodig is om de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting op grond van artikel 27 om bij de bevoegde autoriteiten informatie in te dienen;

f) verzoeken om toegang tot gegevens, documenten en informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

5. Indien de op grond van lid 4, punten a) tot en met d) en punt f), genomen handhavingsmaatregelen ondoeltreffend zijn, zorgen de lidstaten ervoor dat hun bevoegde autoriteiten de bevoegdheid hebben om een termijn vast te stellen waarbinnen de essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen of aan de eisen van die autoriteiten te voldoen. Indien de gevraagde actie niet binnen de gestelde termijn wordt ondernomen, zorgen de lidstaten ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om:

a) een certificering of vergunning tijdelijk op te schorten of een certificerings- of vergunningsinstantie of een rechterlijke instantie overeenkomstig het nationale recht te verzoeken deze tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de essentiële entiteit verleende diensten of verrichte activiteiten;

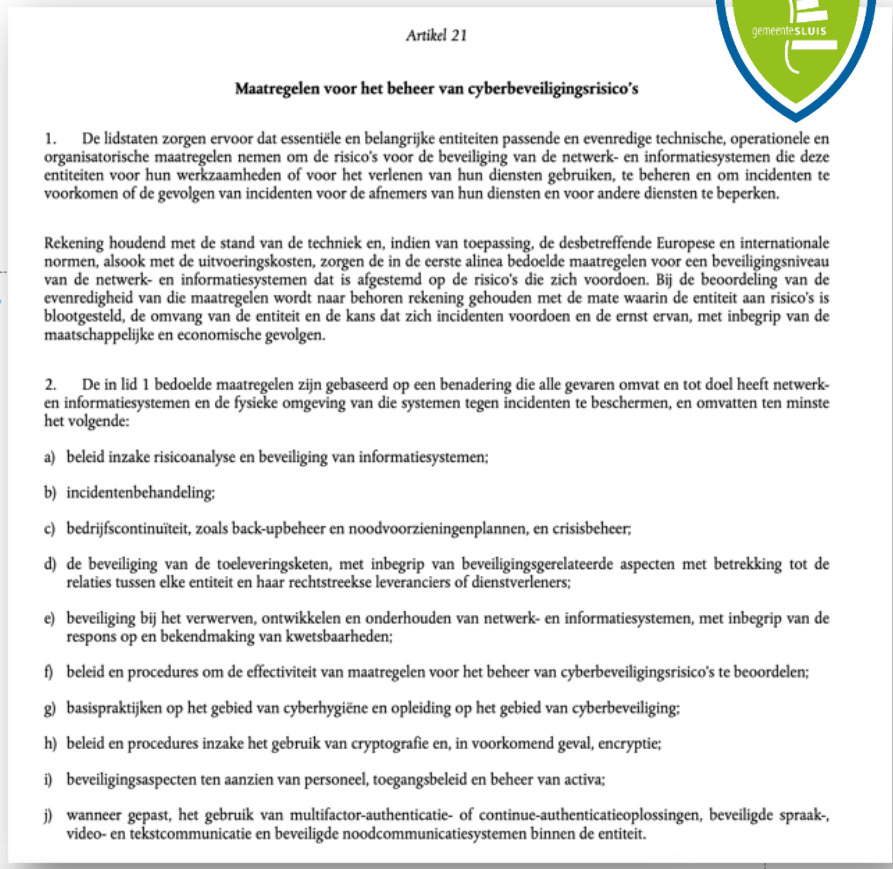
b) verzoeken dat de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

Op grond van dit lid opgelegde tijdelijke opschortingen of verboden worden slechts toegepast totdat de betrokken entiteit de noodzakelijke maatregelen neemt om de tekortkomingen te verhelpen of voldoet aan de vereisten van de bevoegde autoriteit waarvoor dergelijke handhavingsmaatregelen zijn opgelegd. Het opleggen van dergelijke tijdelijke opschortingen of verboden moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het Unierecht en het Handvest, waaronder het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van de verdediging.

De in dit lid bedoelde handhavingsmaatregelen zijn niet van toepassing op onder deze richtlijn vallende overheidsinstanties.

Zorgplicht

- Bestuurder verantwoordelijk voor beheer risico's
- Minimale informatiebeveiligingsmaatregelen op basis van internationale normen (ISO27001 en ISO27002)
- Risicogebaseerd



Artikel 21

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in de eerste alinea bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

2. De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

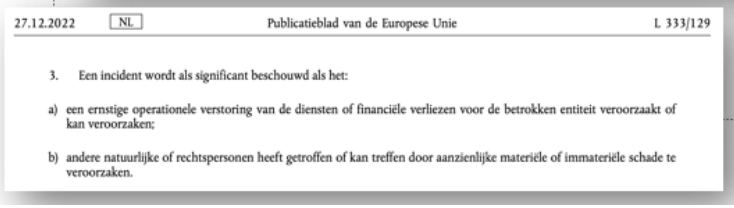
f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.



27.12.2022 NL Publicatieblad van de Europese Unie L 333/129

3. Een incident wordt als significant beschouwd als het:

a) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken;

b) andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Meldplicht

- 3 fasen meldplicht

- Eerste melding binnen 24 uur na kennis neming van incident
- Update van eerste melding binnen 72 uur met inbegrip van ernst, gevolgen en indicatoren voor aantasting
- Eindrapportage na 1 maand

Artikel 23

Rapportageverplichtingen

4. De lidstaten zorgen ervoor dat de betrokken entiteiten, voor de in lid 1 bedoelde melding, bij het CSIRT of, indien van toepassing, de bevoegde autoriteit:

a) onverwijld en in elk geval binnen 24 uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing geven, waarin, indien van toepassing, wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben;

b) onverwijld en in elk geval binnen 72 uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding indienen met, indien van toepassing, een update van de in punt a) bedoelde informatie, een initiële beoordeling van het significante incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting;

c) op verzoek van het CSIRT of, indien van toepassing, de bevoegde autoriteit, een tussentijds verslag indienen over relevante updates van de situatie;

d) uiterlijk één maand na de indiening van het in punt b) bedoelde incidentmelding, een eindverslag indienen waarin het volgende is opgenomen:

i) een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan;

ii) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;

iii) toegepaste en lopende risicobeperkende maatregelen;

iv) in voorkomend geval, de grensoverschrijdende gevolgen van het incident;



Titel II. De inrichting en samenstelling van het gemeentebestuur

Hoofdstuk I. Algemene bepaling

Artikel 6

In elke gemeente is een raad, een college en een burgemeester.

- Beheersmaatregelen goedkeuren
- Toezien op naleving
- Volgen van een training
- Aanbieden soortgelijke training
- Verantwoordelijkheid nemen



Zorg voor voldoende budgettering voor digitale veiligheid en NIS2-implementatie

Oefen actieve controle en kaderstelling uit, met aandacht voor budgetallocatie en collegeverantwoording.

Verwerf grondig inzicht in NIS2 en de gevolgen voor de gemeenschap. Bevorder bewustwording rondom informatiebeveiliging in gemeente.

Ontwikkel en handhaaf duidelijke digitale veiligheidskaders in lijn met NIS2.

Stel kritische vragen over data- en privacybeheer en betrek de CISO voor expertise.

Wat is……

Opzet bestaan

- Richt zich op de vraag of het **ontwerp** van de maatregelen de risico's kunnen beheersen en daadwerkelijk **bestaan**.
- De auditor beoordeelt of de **beschrijving** van de maatregelen en de manier waarop ze zijn opgezet, voldoende zijn om het risico te beheersen.
- De auditor beoordeelt of de interne controlemaatregelen die zijn ontworpen om een bepaald risico te beheersen, daadwerkelijk **aanwezig zijn** en of ze adequaat zijn ontworpen om het risico te beheersen.

en Werking

- Richt zich op de vraag of de maatregelen ook daadwerkelijk **effectief** zijn en in de praktijken worden **nageleefd**.
- De auditor onderzoekt of de maatregelen ook daadwerkelijk **werken zoals bedoeld**. De auditor onderzoekt of de maatregelen effectief zijn in het beheersen van het risico en of ze worden nageleefd door de medewerkers.



Programma Informatiebeveiliging

Hoe gaan we alles realiseren?

Van risico analyse naar prioriteitstelling.

Van prioriteitstelling via projecten naar implementatie.

Dreigingsanalyse gemeente Sluis 2023

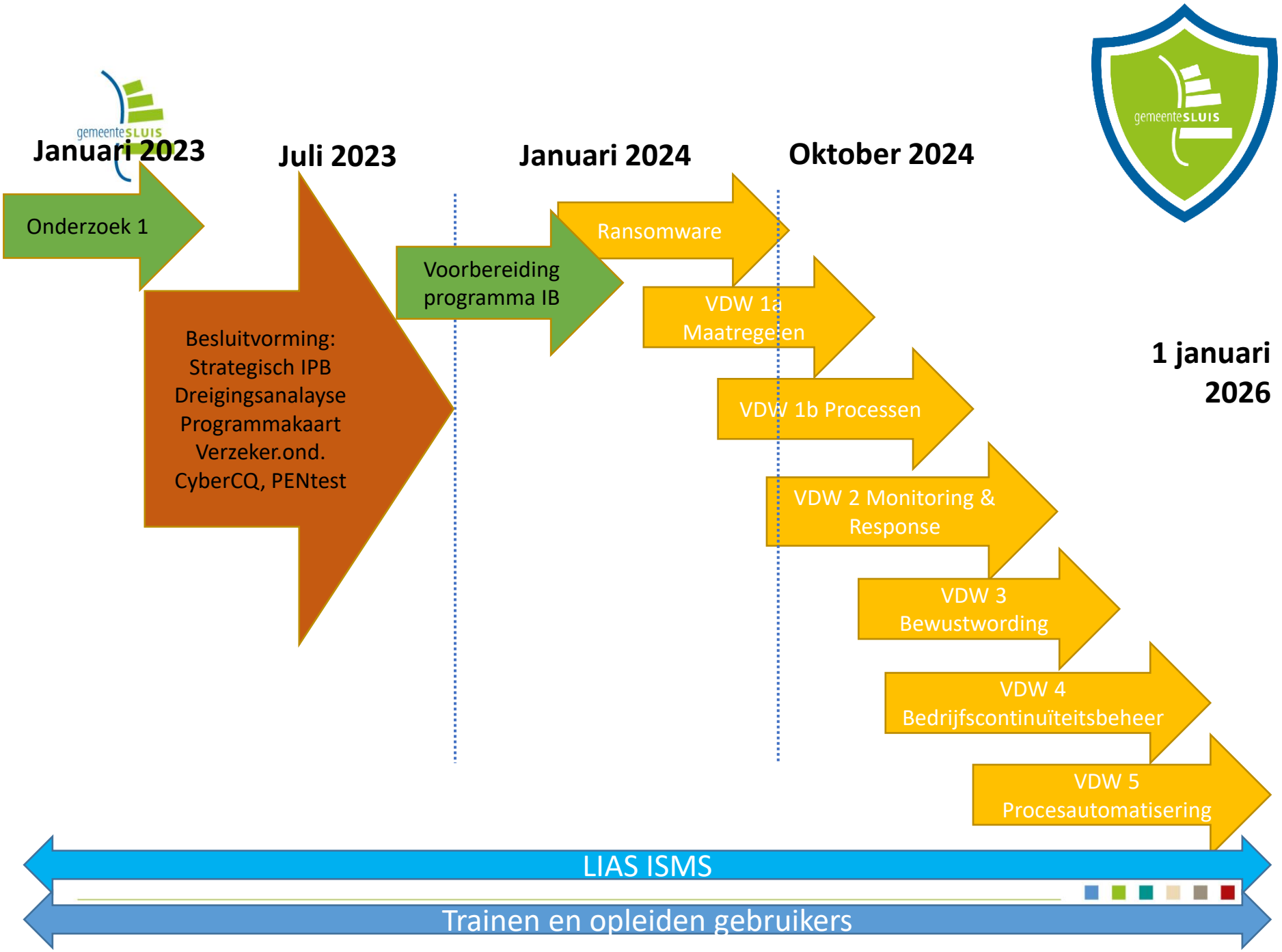
Dreiging	Kwetsbaarheid	Gebeurtenis	Gevolg
Ransomware	• Software niet up to date • Onvoldoende kennis & ib-bewustzijn bij medewerkers • BIO beheersmaatregelen niet op niveau	• Applicatie niet beschikbaar • Leverancier niet beschikbaar • Verlies data	• Uitkeringen niet betalen • Uitval systemen • Misbruik persoonsgegevens
Kwetsbare software	• Software niet up to date • Verouderde/complexe technologie	• Applicatie niet beschikbaar • Leverancier niet beschikbaar • Verlies data	• Uitkeringen niet betalen • Uitval systemen • Misbruik persoonsgegevens
Uitval (cloud leverancier)	• Kritieke rol leverancier • Geen uitwijk	• Applicatie niet beschikbaar • Leverancier niet beschikbaar	Uitkeringen niet betalen Uitval systemen
Eigen medewerkers	• Onvoldoende kennis • Onvoldoende bewustzijn • Te veel rechten in software	• Applicatie niet beschikbaar • Verlies data	Uitkeringen niet betalen Uitval systemen Misbruik persoonsgegevens
Spionage	• Geen zicht op kwetsbare medewerkers • Te veel rechten in software	• Verlies data	Misbruik persoonsgegevens
Uitval nutsvoorzieningen	• Geen uitwijk • Geen alternatieve bron	• Applicatie niet beschikbaar • Leverancier niet beschikbaar	• Uitkeringen niet betalen • Uitval systemen

Stutten van analyse



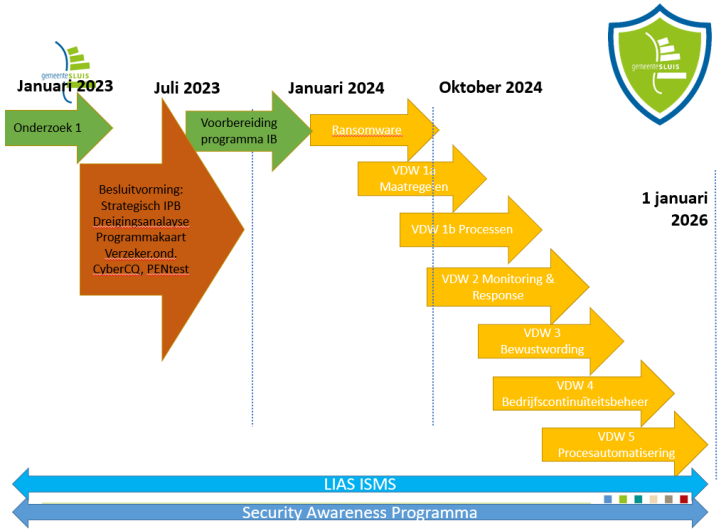
Dreigingsanalyse Sluis

Cyber risico evaluatie AON	PEN-test CyberCloud	VDW programma IBD


Januari 2023
Juli 2023
Januari 2024
Oktober 2024
1 januari 2026
Onderzoek 1
Besluitvorming:
Strategisch IPB
Dreigingsanalyse
Programmakaart
Verzeker.ond.
CyberCQ, PENtest
Voorbereiding programma IB
Ransomware
VDW 1a Maatregelen
VDW 1b Processen
VDW 2 Monitoring & Response
VDW 3 Bewustwording
VDW 4 Bedrijfscontinuïteitsbeheer
VDW 5 Procesautomatisering
LIAS ISMS
Trainen en opleiden gebruikers

Aanpak

- 1.Bepalen as/is (uitvoeren nulmeting op de opzet, bestaan en werking)
- 2. NIS 2/ BIO Wat moet er nog gebeuren om tot werkingsniveau te komen opstellen werkpakket
- 3. Bouw & ontwerp van het product
- 4. Business Transition
- 5. Evaluatie en Afronding project



Next steps en vragen

- ✓ Programmaplan inclusief budgettering (Mei)
- ✓ Besluitvorming College & Raad (Juni)
- ✓ Uitvoering projecten (Juni→)