Voorlegger vergadering Raad van Bestuur UWV

	Vergadering Raad van Bestuur		
Datum	7 februari 2023		
Agendapunt	Agendapunt 15	Nummer	23 – 042
Onderwerp	3e IB&P tertaalrapportage CISO 2022		
Directeur	Directeur C-ICT		
Opsteller	5.1 lid 2 sub e en 5.1 lid 2 sub e		
Portefeuillehouder RvB	Nathalie van Berkel		
	Onderwerp heeft instemming van		
Directeur	**Toelichting**		

Door Raad van bestuur te nemen besluiten

Kennis te nemen van de 3e IB&P tertaalrapportage CISO 2022

Aanleiding

Met deze voorlegger informeert CISO-Office de RvB over de IB&P-tertaalrapportage CISO. In deze rapportage zijn de hoogtepunten weergegeven van de werkzaamheden van afgelopen tertaal. Hiermee informeert CISO-Office UWV over de voortgang die heeft plaatsgevonden op relevante onderwerpen van Informatiebeveiliging en privacybescherming (IB&P). De selectie van onderwerpen is samengesteld op basis van de mate van impact op UWV en bijdrage aan de UWV-brede doelstellingen.

Eerder werd de RvB over ontwikkelingen betreffende IB&P (inclusief het onderwerp risicomanagement) geïnformeerd via de FG tertaalrapportage. Vanwege de overdracht van de stelselverantwoordelijkheid van Informatiebeveiliging en Privacy (IB&P) van Bestuurszaken naar de CIO, brengt de CIO via het CISO-Office een eigen rapportage uit. De FG tertaalrapportage en CISO-Office tertaalrapportage zijn tegelijkertijd geagendeerd.

De tertaalrapportage wordt nu aangeleverd in de vorm van een samenvatting in een voorlegger. De informatiebehoefte is op dit moment groter dan wat deze tertaalrapportage biedt. In het komende tertaal zal er daarom informatie opgehaald worden over de verwachtingen en behoeften met betrekking tot IB&P-stuurinformatie. Met deze input zal de tertaalrapportage een nieuwe vorm krijgen.

Ontwikkelingen

De belangrijkste ontwikkelingen zijn:

- BIO Implementatie en In Control Verklaring
- IB&P Strategische Agenda
- UWV-brede IB&P incidenten
- E-learning
- Adviesaanvraag: herijking IB&P Governance

Hieronder worden deze onderwerpen toegelicht.

BIO Implementatie en In Control Verklaring

UWV moet en wil voldoen aan de relevante wet- en regelgeving op het gebied van informatiebeveiliging en privacy (IB&P). Voor IB&P is de Baseline Informatie Beveiliging (BIO) de belangrijkste baseline. De BIO-implementatie binnen UWV is in volle gang – waarbij het streven is om uiterlijk per 1-1-2026 BIO-compliant te zijn in opzet, bestaan en werking. UWV staat hier voor een uitdaging wat betreft de bestaande capaciteit (zowel centraal als decentraal) en de benodigde capaciteit om deze doelstelling te realiseren. Er zijn binnen de organisatie wel vacatures opengesteld om de benodigde capaciteit te verkrijgen, maar de uitdaging zit vooral in het vervullen van die vacatures met mensen met de juiste kennis en kunde. Dat betekent dat er zowel centraal als decentraal keuzes gemaakt worden.

Alle bedrijfsonderdelen hebben uiterlijk december een deel-ICV opgeleverd aan het BIO-Regieteam. Uit de opgeleverde deel-ICV's zijn de nodige verbeterplannen gekomen waar een vervolg aan gegeven dient te worden.

De deel-ICV's die aangeleverd werden verschillen onderling erg in kwaliteit en kwantiteit waardoor het opstellen van de geconsolideerde ICV moeizaam verliep. Een belangrijk aandachtspunt is het vastleggen van de bewijslast, deze was vaak in onvoldoende mate aanwezig. De tweedelijnscontrole op de BIO-implementatiewerkzaamheden heeft voor het eerst plaatsgevonden, maar ook dit proces kan nog verbeterd worden.

De geconsolideerde ICV is opgesteld en opgeleverd ter ondertekening. Hier zijn ook voor het ICV-proces zelf verbeterpunten uit gekomen, zoals het ondersteunen van de bedrijfsonderdelen in (het coördineren van) het opzetten van generieke controls die relevant zijn voor alle bedrijfsonderdelen en een eenduidige manier van aanleveren.

Daarnaast is er via de voorlegger aan de RvB van 10 januari 2023 voorgesteld om het verplicht stellen van eenduidige wijze van verantwoording. Aan de algemeen directeuren wordt gevraagd om een Baseline Informatiebeveiliging Overheid (BIO) roadmap op te stellen in lijn met de door de RvB uitgesproken ambitie om in 2026 volledig compliant te zijn aan de BIO.

IB&P Strategische Agenda

Bij het schrijven van deze tertaalrapportage was de IB&P Strategische Agenda nog niet opgesteld. Deze zal in het komende tertaal opgesteld worden. Wanneer deze gereed is, zal deze geagendeerd worden bij de Raad van Bestuur.

UWV-brede IB&P incidenten

In het afgelopen tertaal hebben zich de volgende security-incidenten met hoge impact voorgedaan:

Aanhoudende Phishing-campagnes

UWV is in de maanden oktober en december getroffen door verschillende Phishing-campagnes. Deze campagnes zijn gericht op meerdere overheidsinstanties waaronder Rijkswaterstaat en de Nationale Politie.

De werkwijze van de criminelen achter deze campagnes is om via mail de ontvanger binnen de organisatie te verleiden om kwaadaardige software te installeren. Het doel hierachter is het installeren en verspreiden van o.a. ransomware door toegang tot de computer van de ontvanger te krijgen en vandaaruit verder over de ICT-infrastructuur te verspreiden. Door een goede samenwerking tussen het Security Operations Center van UWV, de partners binnen de Rijks-ISAC (NCSC) en de leverancier KPN, kon snel en adequaat maatregelen worden genomen om verspreiding van de phishing-campagne (en daarmee malware-verspreiding) tegen te gaan. Ook bestaande preventieve maatregelen zijn effectief gebleken om bijvoorbeeld malafide bestandsextensies te blokkeren. Het resultaat op basis van de beschikbare analyse is gebleken dat de UWV-omgeving hierdoor niet gecompromitteerd is.

Het Nationaal Cyber Security Center (NCSC) is een onderzoek gestart naar deze aanhoudende Phishing-campagnes om de grootte van de verspreiding, attributie naar actoren en oorsprong van mailconversaties in beeld te brengen. UWV heeft aan dit onderzoek een bijdrage geleverd. Publicatie van de bevindingen wordt medio januari 2023 verwacht.

5.1 lid 2 sub i

E-learning

Het traject Next Level Security 2 is in het leven geroepen om de structurele verhoging van de digitale weerbaarheid van UWV te realiseren en cybersecurity te verankeren. In het deelproject Cyber Safe Behaviour wordt er gewerkt aan een UWV-breed awareness-programma. Door middel van het basis awareness-programma zal er structureel gewerkt worden aan de verhoging van bewustwording van de medewerkers en het op de juiste manier handelen als er een vermoeden van cybercriminaliteit bestaat. Dit bestaat uit meerdere elementen zoals een IB&P Kennisbank, Security awareness tooling en een e-learning. In het afgelopen tertaal is de keuze voor een leverancier gemaakt. In het komende tertaal vindt implementatie plaats. In Q2 dit jaar kan de e-learning dan in gebruik worden genomen.

Adviesaanvraag: Herijking IB&P Governance

In 2020 liep het project Herijking IB&P Governance. Het doel was de governance van IB&P wijzigen omwille van een betere sturing op IB&P en een hoger volwassenheidsniveau. Dit leidde ertoe dat de CIO stelselverantwoordelijke is voor IB&P. Om deze stelselverantwoordelijkheid te realiseren, is een adviesaanvraag ingediend die nu is vastgesteld, inclusief Business Continuity Management. Tegelijkertijd zijn werkzaamheden uitgevoerd om de veranderingen in de IB&P-governance te effectueren, door zowel het CISO-Office als de kwartiermakerorganisatie (KMO-organisatie). De uitvoerende plannen zullen via de Thematafel gedeeld worden, waarna deze verder uitgewerkt kunnen worden. In het komende tertaal zal de KMO worden afgebouwd. Alle werkzaamheden worden dan overgedragen aan CISO-Office.

Gevolgen voor mensen

N.v.t.

Kansen en risico’s voor (de opdracht van) UWV

N.v.t.

Strategische aspecten van het besluit

N.v.t.

Bedrijfsvoeringsaspecten

N.v.t.

Duurzaamheid

N.v.t.

Vervolgtraject besluitvorming

N.v.t.

Communicatie

Communicatie vindt plaats via reguliere kanalen.

Openbaarheid

Deze documenten kunnen openbaar gemaakt worden (onderbouw ook de keuzes voor opties 2, 3 en 4):
1 ☐ Ja, in hun geheel.
2 ☒ Deels, markeer in de documenten wat niet openbaar gemaakt kan worden.
3 ☐ Nee, de bijbehorende bijlage(n) niet.
4 ☐ Nee, helemaal niet.

Ad 2. Gezien de gevoeligheid van de informatie van het onderwerp UWV-brede IB&P incidenten wordt deze informatie niet openbaar gemaakt.