Voorlegger vergadering Raad van Bestuur UWV

	Vergadering Raad van bestuur			
Datum	4 april 2023			
Agendapunt	Agendapunt	4	Nummer	23 – 114
Onderwerp	Vrijgave budget voor uitvoering van het Next Level Security 2 (NLS-2) programma			
Directeur	CIO			
Opsteller	5.1 lid 2 sub e	5.1 lid 2 sub e		
Portefeuillehouder RvB	Nathalie van Berkel			

Onderwerp heeft instemming van	
Directeur	**Toelichting**
Portfoliobureau Centraal	PB adviseert akkoord te gaan met de budgetvrijgave van €3.148k tot en met december 2023 en € 939K t/m mei 2024. Dit omvang 2023 is hiermee €513k hoger dan de portfolio-opstelling, hiervoor wordt aanspraak gemaakt op de reserves. PB constateert dat bij de realisatie van het deeltrajecten Back-up & Recovery testinzet van de divisies nodig is. PB kan niet vaststellen in hoeverre, deze in de regel schaarse capaciteit, is vrijgespeeld bij de divisies. In FCC worden geen betrokken divisies benoemd. PB adviseert hierover sluitende afspraken te maken en deze door de divisies vast te laten zetten in FCC. PB adviseert om voor de maatregelen die in het kader van NLS 1 en 2 worden geïmplementeerd een plan op te stellen op basis waarvan het bereikte niveau van digitale weerbaarheid aantoonbaar structureel op het gewenste niveau blijft. Het project heeft een totale kosteninschatting van €4,9 miljoen. Daarmee wordt dit project gedeeld met SZW in het kader van Grote ICT Projecten.

Door Raad van bestuur te nemen besluiten

1. Het goedkeuren van het vervolgen van de uitvoering van het bijgevoegde programmaplan en vrijgave van € 4.087K voor de uitvoering van activiteiten van 1 maart 2023 tot en met mei 2024 (€ 3.148K in 2023 en € 939K in 2024). In 2023 is voor de maanden januari en februari reeds € 365K vrijgegeven door middel van kapstokvrijgave.
2. Kennis te nemen van het plan en begroting 2023 en 2024.

Samenvatting onderwerp en reden bespreking

In toenemende mate communiceert het UWV digitaal met burgers, bedrijven en (overheids-) partners. Dit resulteert in een efficiënte en klantgerichte overheid en introduceert ook risico's op betrouwbaarheid en continuïteit in de informatievoorziening. Door mondiale ontwikkelingen op het gebied van cybercriminaliteit bestaat een verhoogd risico voor UWV om hiervan slachtoffer te worden en gevoelige informatie te verliezen. Ook is er sprake van een verhoogd risico op het gebied van continuïteit van de bedrijfsvoering van UWV als gevolg van cybercriminaliteit.

Om de risico's die voortkomen uit dreiging op het gebied van cybercriminaliteit te mitigeren is in 2020 aangevangen met het vergroten van de volwassenheid van UWV op het gebied van digitale weerbaarheid. Een aantal verbeteringen is inmiddels gerealiseerd, onder andere door middel van het eerste Next Level Securityprogramma. Omdat niet alle maatregelen binnen het volledige cybersecurityspectrum zijn opgepakt is de volwassenheid op het gebied van digitale weerbaarheid momenteel niet groot genoeg. Daarom is het noodzakelijk de digitale weerbaarheid van UWV verder te vergroten.

De noodzaak tot verbetering van de cybersecurity is expliciet benoemd in het UWV Informatie Plan 2023-2027. Vanuit het besef dat het noodzakelijk is om digitale weerbaarheid te zien als onderdeel van de

basishygiëne van de gehele organisatie, is een vervolg gedefinieerd op het programma Next Level Security: Next Level Security 2 (verder NLS-2).

Het doel van het programma NLS-2 is het aantoonbaar verhogen van de digitale weerbaarheid van UWV en het verankeren van cybersecurity.

De doelstelling van het programma NLS-2 wordt bereikt door het inrichten van maatregelen om cyberincidenten zoveel mogelijk te voorkomen, tijdig te detecteren, schade als gevolg van cyberincidenten te beperken door middel van adequate reactie en voorbereid te zijn op het uitvoeren van activiteiten ten behoeve van het herstel naar aanleiding van cyberincidenten. Hiervoor wordt de cybersecurity voor UWV voor mensen, processen en technologie verbeterd en wordt daarmee de volwassenheid op het gebied van digitale weerbaarheid vergroot. De organisatie wordt daarmee in staat gesteld om de steeds toenemende risico's op het gebied van cybersecurity te mitigeren. Naast het uitvoeren van een aantal projecten ten behoeve van het vergroten van de digitale weerbaarheid wordt het volwassenheidsniveau van UWV op het gebied van cybersecurity voor het volledige domein van cybersecurity door middel van een assessment vastgesteld (op basis van CMMI), waarna wordt bepaald wat er is benodigd om het niveau van volwassenheid verder te verhogen in een vervolg op het programma.

Het verhogen van de digitale weerbaarheid van UWV is een verantwoordelijkheid van de gehele organisatie. Om veilig te kunnen blijven werken en klanten op het juiste niveau van dienst te zijn, moet iedereen zich bewust zijn van de risico's en van de wijze waarop deze risico's gemitigeerd worden, van bestuurder tot eindgebruiker. Cybersecurity ontstaat niet alleen door het nemen van technische maatregelen. De door middel van de door het programma NLS-2 te realiseren maatregelen beperken zich niet tot het ICT-domein en hebben zodoende impact op de gehele organisatie.

Het NLS-2 programma wordt in nauwe samenwerking met de CISO Office uitgevoerd. Maatregelen worden vanuit strategisch en tactisch perspectief bepaald, vanuit de stelselverantwoordelijkheid van de CISO Office voor Informatiebeveiliging en Privacybescherming (IB&P). Hierdoor worden de verbeteractiviteiten door het NLS-2 programma beheersbaar en in samenhang gerealiseerd.

Wij vragen de Raad van bestuur om goedkeuring voor het vervolgen van de uitvoering van het bijgevoegde programmaplan en vrijgave van € 4.087K voor de uitvoering van activiteiten van 1 januari 2023 tot en met mei 2024 (€ 3.148K in 2023 en € 939K in 2024). In 2023 is voor de maanden januari en februari reeds € 365K vrijgegeven door middel van kapstokvrijgave.

Gevolgen voor mensen

Digitale weerbaarheid (en cybersecurity) is een UWV-breed aandachtsgebied. Bij de uitvoering van het programma NLS-2 zijn de divisies en stafafdelingen van geheel UWV actief betrokken. Alleen op die manier vindt de gewenste verhoging van het volwassenheidsniveau van de operationele securitybasis (inclusief infrastructurele aanpassingen) van geheel UWV succesvol plaats.

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

Het programma NLS-2 levert een bijdrage aan de organisatiedoelstelling van UWV waarin steeds hogere eisen worden gesteld aan cybersecurity. Het programma NLS-2 is inherent verbonden aan de realisatie van het UIP en rand voorwaardelijk voor de naleving van externe standaarden en wet- en regelgeving.

Door het realiseren van de programmadoelstelling van het programma NLS-2 wordt de digitale weerbaarheid van UWV verhoogd en wordt cybersecurity verankerd in de bedrijfsvoering. Het inrichten van afdoende maatregelen, vanuit een zero-trust benadering, helpt bij het voorkomen en/of tijdig detecteren van incidenten en stelt UWV in staat om schade te beperken. De resultaten van het programma NLS-2 dragen bij aan het leveren van moderne en betrouwbare ICT-oplossingen en het leveren van een solide fundament voor de dienstverlening en informatievoorziening van geheel UWV.

Voor de maakbaarheid van het programma NLS-2 is prioriteit op het gebied van cybersecurity binnen de bredere veranderagenda van UWV randvoorwaardelijk en wordt een belangrijke rol van de divisies gevraagd. Gezien de aanwezige aandacht binnen UWV op het gebied van IB&P en het groeiende besef binnen de organisatie en daarbuiten (zoals bij leveranciers) dat maatregelen op het gebied van cybersecurity noodzakelijk zijn, wordt aan deze randvoorwaarde voldaan. Daarnaast wordt de maakbaarheid van het programma vergroot doordat IB&P expliciet aandacht heeft in het UIP. Verder is ook door middel van de invoering van de BIO de aandacht voor het onderwerp prominent aanwezig.

De maakbaarheid van de resultaten van het programma is afhankelijk van externe (ICT-) leveranciers. De prioriteit bij deze leveranciers voor de realisatie van maatregelen op het gebied van cybersecurity, en het opnemen daarvan in nieuwe en/of aangepaste dienstverlening, moet actief worden bestuurd, rekening houdend met andere ontwikkelingen, programma's en projecten.

Binnen de organisatie is het kennisniveau op het gebied van cybersecurity relatief laag. Ook is de capaciteit binnen de organisatie op het gebied van cybersecurity niet breed beschikbaar. Het kennisniveau en beschikbare capaciteit vragen op een aantal gebieden samenwerking met externe organisaties en/of extern in te huren capaciteit. In de binnen het programma NLS-2 uit te voeren projecten wordt met betrekking tot het verankeren van veranderingen in de organisatie hiermee rekening gehouden. Kennisoverdracht aan de lijnorganisatie is expliciet opgenomen in de activiteiten van de verschillende projecten binnen het programma NLS-2.

Strategische aspecten van het besluit

Binnen het UWV Informatieplan is een aantal (strategische) doelstellingen gedefinieerd. Het programma NLS-2 geeft hieraan in belangrijke mate invulling:

Versterken ICT-fundament

- Het programma NLS-2 draagt bij aan een goed werkende, betrouwbare en beschikbare ICT, als essentiële randvoorwaarde voor de dienstverlening aan cliënten, bedrijven en partners en voor de ondersteuning van de medewerkers om deze dienstverlening te kunnen verrichten.

Verbeteren informatiebeveiliging & privacy

- De maatregelen en werkzaamheden die worden uitgevoerd binnen het programma NLS-2 (organisatorisch, technisch, procesmatig) dragen bij aan het voorkomen of tijdig detecteren van incidenten, het beperken van schade en het efficiënt en effectief kunnen herstellen in geval van incidenten. Inclusief grip op sturing op de leverancierskeketen.
- De toenemende digitalisering en aangescherpte wetgeving stellen steeds hogere eisen aan IB&P. Om aan deze eisen te kunnen voldoen is een strategische IB&P-veranderagenda opgesteld die als leidraad geldt voor de uit te voeren trajecten in de komende jaren. De resultaten van het programma NLS-2 dragen bij aan het leveren van moderne en betrouwbare ICT-oplossingen en het leveren van een solide fundament voor de dienstverlening en informatievoorziening van geheel UWV.

Verhogen digitale weerbaarheid

- Op het gebied van cybersecurity worden steeds hogere eisen gesteld. Hierbij streeft UWV naar een volwassenheidsniveau, zowel in mens, proces en techniek, dat recht doet aan het dreigingslandschap waarmee UWV te maken heeft. Het wereldwijd toenemende dreigingsbeeld dwingt UWV om de operationele securitybasis te versterken en door te groeien naar een hoger volwassenheidsniveau. Dit vindt plaats door middel van het programma NLS-2.
- Digitale weerbaarheid (en cybersecurity) is een UWV-breed aandachtsgebied. Bij de uitvoering van het programma NLS-2 zijn de divisies en stafafdelingen van geheel UWV actief betrokken. Alleen op die manier vindt de gewenste verhoging van het volwassenheidsniveau van de operationele securitybasis (inclusief infrastructurele aanpassingen) van geheel UWV succesvol plaats. Het NLS-2 programma is geen (security) compliance programma; hiervoor vindt binnen UWV de implementatie plaats van de Baseline Informatiebeveiliging Overheid (BIO). Het NLS-2 programma leidt daarentegen wel tot verbeteringen die bijdragen aan het voldoen aan de BIO.

Bedrijfsvoering (personeel/financieel)

Programmakosten

Uitvoering van het programma NLS-2 vindt plaats van 1 mei 2022 tot en met 31 mei 2024. De kosten hebben betrekking op de uitvoering van de activiteiten en projecten in scope van het programma NLS-2. Hierbij is sprake van de aanschaf en implementatie van software ter ondersteuning van de resultaten.

- De kosten van de uitvoering van het programma NLS-2 bedragen voor de periode van 1 januari 2023 tot en met 31 mei 2024 een bedrag van € 4.452K (waarvan € 3.513K in 2023 en € 939K in 2024).
- In 2023 is voor de maanden januari en februari van de hiervoor genoemde bedragen reeds € 365K vrijgegeven door middel van kapstokvrijgave.
- In de periode mei 2022 tot en met december 2022 is een bedrag van € 452K gerealiseerd.
- De totale kosten voor uitvoering van het programma NLS-2 bedragen € 4.903K.

Structurele meerkosten

Als gevolg van het programma ontstaan structurele meerkosten als gevolg van de implementatie van nieuwe standaardsoftware en de ontwikkeling van nieuwe processen. Voor de implementatie van deze nieuwe standaardsoftware en het eerste jaar exploitatiekosten is in het programmaplan vanaf 2024 een jaarlijks bedrag van € 500K begroot voor licentiekosten en beheerkosten.

Personeel

Er wordt voorzien dat de beheerlast van securityfuncties door het uitvoeren van het programma NLS-2 groter wordt, zowel op operationeel niveau (zoals bij het USOC) als op tactisch en strategisch niveau (CISO

Office). De omvang van deze toename wordt gedurende de uitvoering van het programma duidelijk, waarna wordt vastgesteld of er extra formatie noodzakelijk is. In voorkomende gevallen wordt de impact gedurende de uitvoering van het programma NLS-2 en de projecten binnen het programma verkend in gesprekken met de OC/OR, waarna verdere uitwerking wordt voorgelegd aan de stuurgroep.

Duurzaamheid

N.v.t.

Vervolgtraject besluitvorming

Na een akkoord van de Raad van Bestuur wordt de uitvoering van het programma vervolgd op de wijze zoals dit is verwoord in het bijgevoegde programmaplan.

Communicatie

Communicatie over het besluit van de Raad van Bestuur vindt vanuit het programma NLS-2 plaats binnen de organisatie. Er vindt geen externe communicatie plaats (met uitzondering van de communicatie die is benodigd aan betrokken externe leveranciers).

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.

Het programmaplan voor het programma NLS-2 bevat bedrijf kritische informatie met betrekking tot de securityfuncties binnen UWV. Deze informatie kan voor (kwaadwillende) buitenstaanders mogelijk aanleiding zijn om kwetsbaarheden in deze securityfuncties te zoeken en de bedrijfsvoering van UWV te verstoren.