VOORSTEL aan Dagelijks Bestuur

Datum	07 september 2023
Nummer	
Opsteller	Maarten Vrolijk
Onderwerp	Advies Uitvoeringsplan Informatiebeveiliging 2024-2025
Samenvatting	Cybersecurity is onderdeel van het dagelijks beheer van de ICT-infrastructuur en het hebben van een veilige werkplek. Het rekenkameronderzoek uit 2022 en de te verwachten nieuwe wetgeving uit Europa (NIS2.0) maakt dat er aanvullende maatregelen op het terrein van cybersecurity nodig zijn. Op verzoek heeft Bureau Noordbeek een analyse uitgevoerd en de benodigde maatregelen benoemd. Alle benodigde maatregelen zijn opgenomen in het Uitvoeringsplan Informatiebeveiliging 2024–2025: Dit plan beoogt derhalve de cybersecurity bij de deelnemers en afnemer te vergroten en te borgen. Eea is in gezamenlijkheid met alle deelnemers (Ciso's en Informatiemanagers) opgesteld. De kosten hiervan bedragen € 121.000 in 2024 en structureel -maar enigszins aflopend- € 308.000 vanaf 2025.
Voorstel	Instemmen met het Uitvoeringsplan Informatiebeveiliging 2024-2025 en deze ter vaststelling aanbieden aan het AB van 13 december 2023.
Interne toetsing	O Juridische gevolgen X Financiële gevolgen O Personele gevolgen O Item voor de PVT
Toelichting	Zie bijgevoegde memo Advies uitvoeringsplan informatiebeveiliging 2024 – 2025'.

M.A. Vrolijk
Directeur a.i. SSC DeSom

BESLUIT van het Dagelijks Bestuur

Datum	07 september 2023
Nummer	
Voorstel	Instemmen met het Uitvoeringsplan Informatiebeveiliging 2024-2025 en deze ter vaststelling aanbieden aan het AB van 13 december 2023.
Besluit	Conform voorstel.

Namens het Dagelijks Bestuur van de GR SSC DeSom, d.d. 09 oktober 2023

de voorzitter,

J. Franx

de directeur a.i.,

M.A. Vrolijk

Memo

Aan : Algemeen Bestuur
Van : SSC DeSom
Datum : 11 september 2023

Betreft : Advies uitvoeringsplan informatiebeveiliging 2024 - 2025

Managementsamenvatting

Cybersecurity maakt een niet meer weg te denken deel uit van het dagelijks beheer van de ICT-infrastructuur en het hebben van een 'veilige' werkplek. SSC DeSom en onze deelnemers zien deze ontwikkelingen alleen maar toenemen en onderkennen de noodzaak tot het nemen van maatregelen om de veiligheid te vergroten en verder te borgen. Gelet op de snelle ontwikkelingen, maar bovenal de omvang en de continuïteit van dreigingen is een uitvoeringsplan niet alleen wenselijk maar ook noodzakelijk. Onze belangenvereniging, De VNG, heeft via nieuwsbrieven gemeenten al vaker gewezen op mogelijke gevaren en de noodzaak tot het nemen van maatregelen op het gebied van Cybersecurity.

Daarnaast zien we nieuwe wetgeving uit Europa op ons afkomen. De Baseline Informatiebeveiliging Overheid (BIO), jarenlang en nog steeds de leidraad en het normenkader voor processen en te nemen maatregelen binnen informatiebeveiliging, wordt op termijn ondersteund door nieuwe Europese wetgeving NIS2.0 ook wel Network and Information Systems genoemd wordt in 2024 in de Tweede Kamer ter besluitvorming gebracht en zal daarna in werking treden. De NIS2.0 gaat verder dan de BIO en is vooral gericht op de werking van de genomen maatregelen. Hiermee wordt de aansprakelijkheid verder aangescherpt voor organisaties en bestuurders. Accountants gaan hierop DeSom en de deelnemers auditeren.

Bij het opstellen van de begroting heeft het DB van SSC DeSom het belang van cybersecurity onderkend. In de aanbiedingsbrief van de begroting 2024 van SSC DeSom is aangegeven dat het tijdspad te kort was om de noodzakelijke maatregelen voor informatiebeveiliging in de begroting 2024 op te nemen.
Vanaf juni is in samenwerking met de deelnemers een proces van inventariseren en prioriteren doorgelopen. Gedurende dit proces en om het prioriteren van te nemen maatregelen goed te onderbouwen, heeft SSC DeSom het bureau Noordbeek gevraagd om een technische risicoanalyse geënt op de NIS2.0 uit te voeren op de huidige situatie bij SCC DeSom.

Op basis van de huidige situatie en de reeds doorgevoerde maatregelen van de afgelopen periode laat de risicoanalyse van Bureau Noordbeek een goed en positief beeld van de huidige status van informatiebeveiliging binnen de SSC DeSom zien. Ondanks het positieve beeld vanuit de risicoanalyse zijn er (altijd) nog aanvullende maatregelen nodig om te voldoen aan de (nieuwe) NIS2.0. Bureau Noordbeek heeft haar bevindingen en te nemen maatregelen met de deelnemers gedeeld.

Memo

Vertaald naar volwassenheidsniveau (1 t/m 5) op de NIS2.0 geënt, staat SSC DeSom tussen niveau 2 en 3. Gelet op de nieuwe wetgeving richt SSC DeSom zich op verdere invulling en borging op niveau 3. Hiermee voldoet SSC DeSom deels aan de wettelijke normen.

Op basis van de inventarisaties vanuit de regio en met de aanbevelingen vanuit bureau Noordbeek kunnen we u een breed gedragen advies met 15 maatregelen voor de periode 2024 en 2025 aanbieden. Deze maatregelen worden in 2024 en 2025 door de SSC DeSom uitgevoerd. Jaarlijks wordt verantwoording afgelegd middels de P&C cyclus.

Financiële gevolgen:

Voor onderdeel 1 is in 2024 incidenteel € 121.000 aan budget nodig en vanaf 2025 structureel € 48.000.
Voor onderdeel 2 moet in 2024 een krediet van € 84.500 worden uitgetrokken ten behoeve van investeringen die vanaf 2025 in vijf jaar worden afgeschreven, met als gevolg kapitaallasten van 2025 t/m 2029.
Voor onderdeel 3 moet in 2024 een krediet van € 242.000 worden uitgetrokken ten behoeve van investeringen die vanaf 2025 in vijf jaar worden afgeschreven, met als gevolg kapitaallasten van 2025 t/m 2029.
Daarnaast wordt voor onderdeel 3 vanaf 2025 nog € 181.500 aan overige structurele lasten geraamd.
Vanaf begroting 2025 wordt op basis van nieuwe ontwikkelingen en NIS2.0 jaarlijks de status gemonitord en waar nodig nieuwe maatregelen in de begroting opgenomen.

Het financieel totaaloverzicht en de dekking door de deelnemers is dan als volgt:

onderdeel	krediet	2024	2025	2026	2027	2028
1. processen, meten en sturen		121.000	48.000	48.000	48.000	48.000
2. segmentering	84.500		20.300	19.600	18.900	18.200
3. ict en basisvoorzieningen	242.000		58.100	56.200	54.300	52.400
overige structurele kosten			181.500	181.500	181.500	181.500
totaal		**121.000**	**307.900**	**305.300**	**302.700**	**300.100**
gemeente	**inwoners**	**2024**	**2025**	**2026**	**2027**	**2028**
Drechterland	19.978	17.100	43.600	43.200	42.900	42.500
Enkhuizen	18.620	16.000	40.600	40.300	39.900	39.600
Stede Broec	21.952	18.800	47.900	47.500	47.100	46.700
Opmeer	12.074	10.400	26.300	26.100	25.900	25.700
Medemblik	45.450	39.000	99.200	98.300	97.500	96.700
Koggenland	23.041	19.800	50.300	49.800	49.400	49.000
totaal	141.115	**121.000**	**307.900**	**305.300**	**302.700**	**300.100**

Memo

Toelichting:

De investeringen worden conform Activabeleid lineair afgeschreven in 5 jaar, tegen 4% rente.
De kosten worden verdeeld over de deelnemers met de verdeelsleutel uit de begroting 2024.
Vooralsnog wordt ervan uitgegaan dat WerkSaam WF niet zal bijdragen in de hier opgenomen kosten.

Namens SSC DeSom,
Maarten Vrolijk

Memo

Inleiding

Cybersecurity maakt een niet meer weg te denken deel uit van het dagelijks beheer van de ICT-infrastructuur en het hebben van een 'veilige' werkplek. SSC DeSom en onze deelnemers zien deze ontwikkelingen alleen maar toenemen en onderkennen de noodzaak tot het nemen van maatregelen om de veiligheid te vergroten en verder te borgen. Gelet op de snelle ontwikkelingen, maar bovenal de omvang en de continuïteit van dreigingen is een uitvoeringsplan niet alleen wenselijk maar ook noodzakelijk. Onze belangenvereniging, De VNG, heeft via nieuwsbrieven gemeenten ook al vaker gewezen op mogelijke gevaren en de noodzaak tot het nemen van maatregelen op het gebied van Cybersecurity en hiervoor de benodigde middelen beschikbaar te stellen.

Daarnaast zien we nieuwe wetgeving uit Europa op ons afkomen. De Baseline Informatiebeveiliging Overheid (BIO), jarenlang en nog steeds de leidraad en het normenkader voor processen en te nemen maatregelen binnen informatiebeveiliging, wordt op termijn ondersteund door nieuwe Europese wetgeving NIS2.0 ook wel Network and Information Systems genoemd wordt in 2024 in de Tweede Kamer ter besluitvorming gebracht en zal daarna in werking treden.

Bij het opstellen van de begroting heeft het DB van SSC DeSom het belang van cybersecurity reeds onderkend en heeft In de aanbiedingsbrief van de begroting 2024 van SSC DeSom de volgende passage opgenomen:

'Ander belangrijke ontwikkeling en speerpunt zijn de snel toenemende cyberdreigingen. Gelet op de landelijke adviezen en onderzoeken, maar ook gezien de dagelijkse dreigingen, vergt dit continue aanpassingen en bijbehorende investeringen in de gedeelde infrastructuur. In 2022 zijn de eerste noodzakelijke stappen geïnventariseerd. In 2023 is deze weg voortgezet en wordt en is geïnvesteerd in aanvullende maatregelen om cyberdreigingen te voorkomen. De gemeentelijke CISO's voeren hier, in nauwe samenwerking met SSC DeSom, de gezamenlijke regie op.'

Daar het tijdspad te kort was om de noodzakelijke maatregelen in de begroting 2024 op te nemen is een separaat (onderliggend) voorstel opgesteld. Het plan is om de komende jaren de te nemen maatregelen inzake cybersecurity periodiek te monitoren en middels een P&C cyclus te borgen en mee te nemen in het jaarlijkse begrotingsproces. Een separaat voorstel is dan niet meer nodig, daar het deel uitmaakt van het P&C cyclus.

Op basis van het bovenstaande kunnen wij u het onderliggende 'Uitvoeringsplan Informatiebeveiliging 2024-2025' aanbieden. Waarbij wel gezegd hebbende dat er structurele kosten aan deze incidentele investeringen zijn verbonden.

Ter verduidelijking en ter aanvulling, naar aanleiding van het rekenkameronderzoek in 2022 bij twee deelnemers is in 2022 een start gemaakt met het opstellen van een regionaal meerjarig informatiebeleidsplan (MIB). Dit is destijds met behulp van een externe partner opgesteld. Daar er onvoldoende draagvlak

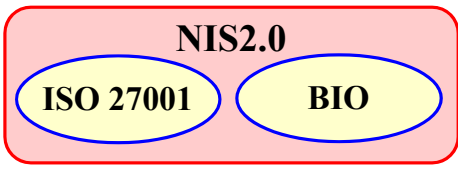
Memo

bestond voor het MIB is deze niet door het AB van SSC DeSom behandeld c.q. vastgesteld. In overleg met de deelnemers is besloten het MIB niet meer te behandelen, maar die elementen uit het MIB te gebruiken welke (nog) actueel zijn en deze mee te nemen in het onderliggende advies.

NIS2.0

Zoals gememoreerd is de BIO, baseline Informatiebeveiliging Overheid, de facto de standaard van het basis-normenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en water-schappen). Buiten de overheid wordt met ISO27001 en ISO27002 normenkader gewerkt. De BIO is het ge-meenschappelijk normkader, gebaseerd op de internationale norm ISO27001 en ISO27002 het is een con-cretisering van een aantal normen tot verplichte overheidsmaatregelen. Zowel de BIO als de ISO- normen-kaders blijven van kracht en zijn te gebruiken als opmaat tot de invoering van de NIS2.0.

De NIS2.0 staat voor Netwerk- en Informatiesystemen en is de eerste EU-wetgeving op het gebied van cyberbeveiliging. De verwachte besluit-vorming door de Tweede Kamer vindt in 2024 plaats.



De belangrijkste wijziging of beter gezegd toevoeging aan de invoering van de NIS2.0 ten opzichte van de BIO en ISO27001, is dat de ISO 27001 en de BIO zich richten op **opzet** en **bestaan** van maatregelen. De NIS2.0 vraagt deels ook om **werking.** Een andere belangrijke voorgestelde wijziging is de inrichting van de aansprakelijkheid. Deze wordt meer 'verlegd' naar organisaties en bestuurders. Hoe e.e.a. precies wordt verwerkt in de (nieuwe) wetgeving is nog onduidelijk. Dat zal t.z.t. bij de aanbieding van de NIS2.0 duidelijk gaan worden.

De belangrijkste aandachtspunten van de NIS2.0 nog even op een rij:

- De EU 'Netwerk- en Informatiesysteem Beveiliging' (NIS2) Richtlijn probeert het cybersecurityniveau te verbeteren
  - De richtlijn scherpt opgelegde beveiligingseisen aan, richt zich op het aanpakken van de beveili-ging van supply chains (de productie- of toeleveringsketen), het stroomlijnen van rapportage-verplichtingen, strengere toezichtmaatregelen en het invoeren van handhavingsvereisten met geharmoniseerde sancties in alle lidstaten.
  - Daarbij wordt ook het belang van informatie delen en (inter)nationale samenwerking op het gebied van crisismanagement benoemd.
- Met de invoering van de NIS2-richtlijn verandert tevens de wijze waarop aansprakelijkheid is ingericht
  - NIS2 kan rechtspersonen direct aansprakelijk stellen voor niet-naleving van de maatregelen voor cybersecurity van de entiteit.
  - Uitzondering: NIS2 stelt dat deze bepaling geen afbreuk doet aan nationale wetgeving. In het Nederlandse Pikmeerarrest II is bepaald dat overheidsinstanties, waaronder ambtenaren, niet aansprakelijk kunnen worden gesteld als het de uitvoering betreft van specifieke overheidsta-ken.
  - Gemeenten en gemeentelijke samenwerkingsverbanden vallen hier ook onder.

  - Het is nog niet duidelijk hoe de wetgever dit verwerkt in de nieuwe Wet beveiliging netwerk- en informatiesystemen 2 (afgekort Wbni 2) (oktober 2024).

- NIS2 legt entiteiten extra verplichtingen op in hun informatiebeveiligingsbeleid, namelijk
  - **Meldplicht**: voor significante incidenten;
  - **Zorgplicht**: verplichting om maatregelen te nemen om risico's voor netwerk- en informatiesystemen te beheersen;
  - **Informatieplicht**: van een incident en de gevolgen aan de betrokkenen (burgers, medewerkers etc.);
  - ISO 27001 en BIO richten zich op opzet en bestaan**, NIS2** vraagt deels ook om **werking.**

De aanstaande invoering van de NIS2.0 maakt dat overheden zich moeten voorbereiden. Veel is al gedaan en opgepakt in de BIO en/of ISO27001 en ISO27002. Zoals gesteld: de NIS2.0 gaat verder. Voor SSC DeSom en haar deelnemers is het een nieuw meetpunt (SOLL) om zich op te richten en de maatregelen op te pakken welke noodzakelijk zijn.

Aanpak:

Er is in de afgelopen jaren al veel gedaan op het terrein van cybersecurity binnen SSC DeSom. In de voorjaarsnota 2022 zijn middelen beschikbaar gesteld om een aantal maatregelen te nemen om de security op het juiste niveau te brengen. Deze worden nu opgepakt of zijn al deels uitgevoerd. De deelnemers worden hiervan periodiek op de hoogte gesteld.

Ontwikkelingen inzake cybersecurity staan niet stil en dit wordt door alle deelnemers en SSC DeSom ook onderkend. Om te bepalen wat (nu) noodzakelijk is, in de aan te nemen maatregelen, is het van belang te weten waar we staan en waar we heen moeten. Ook kan niet alles gelijktijdig worden opgepakt en soms is er sprake van een volgordelijkheid in het nemen van beoogde maatregelen.

In overleg met de deelnemers is in juni gestart met een inventarisatie door de CISO's. Deze inventarisatie gaf een goed beeld van eisen en wensen op het gebied van informatiebeveiliging en benodigde maatregelen.

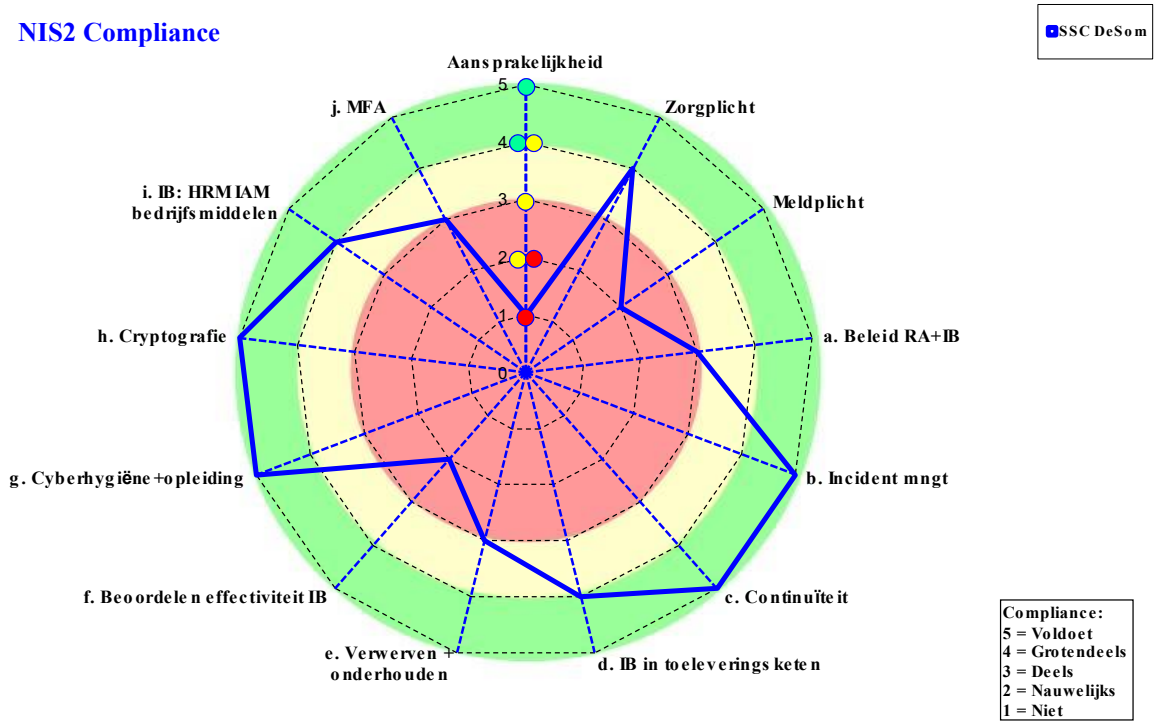
Om de prioritering mede vorm te geven was een nulmeting meer dan wenselijk. Waar staan we nu en in het bijzonder SSC DeSom. Met deze informatie is de IST, zeg maar het eerste ijkpunt, in beeld gebracht. Vervolgens kennen we het tweede ijkpunt (de SOLL), al te weten NIS2.0. Goed te benoemen is dat er aanvullende kaders zijn benoemd. De belangrijkste is het in 2022 uitgevoerde rekenkameronderzoek. Direct na het onderzoek zijn de belangrijkste aanbevelingen opgepakt, maar nog niet allemaal en nog onvoldoende geprioriteerd.

Memo

Status SSC DeSom (IST)

Om de twee 'ijkpunten' te kunnen bepalen is bureau Noordbeek gevraagd een risicoanalyse voor SSC De-Som uit te werken en duiding c.q. richting te geven aan de te nemen maatregelen om voorbereid te zijn op de implementatie van NIS2.0 (en aanvullende kaders).

Medio augustus heef Bureau Noordbeek een risicoanalyse SSC DeSom opgeleverd en deze getoetst aan de NIS2.0 (art 21, lid 2, a tm j) Deze is uitgewerkt in een presentatie waarin de risicomitigatie, bruto en netto risico's zijn benoemd. Bureau Noordbeek heeft naar aanleiding van haar risicoanalyse de onderstaande spider opgesteld.



Op basis van de risicoanalyse kan gesteld worden dat SSC DeSom al veel heeft gedaan om te voldoen aan de NIS2.0. Met de deelnemers zijn de uitkomsten van de risicoanalyse en de voorgestelde maatregelen door Noordbeek gedeeld.

Vertaald naar volwassenheidsniveau (1 t/m 5) op de NIS2.0 geënt, staat SSC DeSom tussen niveau 2 en 3. Gelet op de nieuwe wetgeving richt SSC DeSom zich op verdere invulling en borging op niveau 3. Hiermee voldoet SSC DeSom deels aan de geëiste normen. Middels de jaarlijkse P&C cyclus, beginnend bij het opstellen van de begroting 2025, wordt de status van de genomen maatregelen geëvalueerd en bijgesteld. De wenselijkheid of eis van verdere doorgroei naar helemaal volwassenheidsniveau 4 of mogelijk 5 en in welk tempo wordt in overleg met de deelnemers ingevuld. Hierbij wel de aantekening, ook op volwassenheidsniveau 5 bestaan er altijd nog risico's.

Memo

Nadere uitwerking IST – SOLL

De uitkomsten van de risicoanalyse van bureau Noordbeek (IST) en het normenkader van de NIS2.0 (SOLL) zijn in gezamenlijkheid beoordeeld en hebben geleid tot een matrix van geprioriteerde maatregelen voor de periode 2024 en 2025. Vervolgens zijn hier de benodigde middelen aan gekoppeld.

THEMATISCHE INDELING MAATREGELEN	N	INCIDENTEEL	STRUCTUREEL
1: PROCESSEN, METEN EN STUREN	5	€ 121.000	€ 48.000
2. SEGMENTERING	3	84.500	-
3. ICT EN BASISVOORZIENINGEN BASISINFRASTRUCTUUR	7	242.000	181.500
TOTAAL	15	€ 447.500	€ 229.500

Toelichting thema 1: PROCESSEN, METEN EN STUREN
Binnen hoofdthema 1 is het vastleggen en borgen van procedures binnen de organisatie van belang. Jaarlijks worden de eisen aangescherpt. Om te 'bewijzen' dat een organisatie voldoet aan de laatste eisen is de verkrijgen van certificeringen. Ook vanuit de accountant wordt hierop nadrukkelijk getoetst. DeSom gaat voor de (laatste) ISO-certificering 27001 en 27002 en wordt hierop ook geauditeerd. Deze certificering sluit aan op de BIO, wordt onderschreven door de NIS2.0 en de verplichting vanuit de accountants voor het aantonen van certificering. De voorgestelde certificering is op advies van Noordbeek en Rekenkameronderzoek.
Voldoen aan de eisen voor deze certificering betekent dat de risico's op dataverlies en uitval van de IT-voorzieningen conform een erkende standaard worden gemitigeerd. Dat geldt ook voor de bijbehorende financiële risico's als herstelkosten en eventuele boetes van bijvoorbeeld de Autoriteit Persoonsgegevens. Een ISO27001-certificering verkleint de kans op imagoschade als gevolg van grote verstoringen, als deze toch voorkomen is het niet te wijten aan ontoereikende beveiligingsmaatregelen.

Toelichting thema 2: SEGMENTERING
Binnen hoofdthema 2 is de belangrijkste doelstelling het verkleinen van het aanvalsoppervlak. Dit heet 'segmenteren' of te wel de verbindingen/relaties die er tussen de deelnemers liggen zoveel mogelijk op te heffen. Deze aanbeveling komt ook voort uit het rekenkameronderzoek van 2022. Met de segmentering is vanaf eind 2022 een start gemaakt, er zijn nog aanvullende maatregelen nodig om te voldoen aan alle aanbevelingen.
Verkleining van het aanvalsoppervlak door middel van segmentering houdt in dat kwetsbaarheden die in het rekenkameronderzoek zijn aangetroffen niet meer gebruikt kunnen worden om onbedoeld toegang te krijgen tot data en systemen. Het risico dat hackers dataverlies en uitval van de IT-systemen veroorzaken wordt aanzienlijk verkleind.

Toelichting thema 3: ICT EN BASISVOORZIENINGEN BASISINFRASTRUCTUUR
Binnen hoofdthema 3 worden technische hulpmiddelen ingezet om processen verder te automatiseren en om 'ongewenst' gedrag van gebruikers te minimaliseren. Meest voorkomend 'ongewenst' gedrag komt

Memo

voort uit 'fouten' van gebruikers. Bij de implementatie van technische hulpmiddelen moet u denken aan veilige wifi en het inzetten van een wachtwoordenkluis voor gebruikers.
Door de kans op gebruikersfouten te verkleinen nemen de bijbehorende risico's op dataverlies en uitval van de IT-systemen af. Daarnaast wordt het hackers moeilijker gemaakt om gebruikers informatie afhandig te maken waarmee ze toegang krijgen tot vertrouwelijke informatie.

In totaal worden voor de jaren 2024 en 2025 15 maatregelen/ activiteiten opgepakt en uitgevoerd. Hierin zijn zowel technische als proces maatregelen benoemd.

Voor alle duidelijkheid, het betreft hier maatregelen waar SSC DeSom de verantwoording voor 2024 en 2025 neemt. Maatregelen door de deelnemers zelf te nemen, zijn niet meegenomen. Dit zal elke deelnemer zelf moeten oppakken.

Financiële gevolgen

Voor onderdeel 1 is in 2024 incidenteel € 121.000 aan budget nodig en vanaf 2025 structureel € 48.000.
Voor onderdeel 2 moet in 2024 een krediet van € 84.500 worden uitgetrokken ten behoeve van investeringen die vanaf 2025 in vijf jaar worden afgeschreven, met als gevolg kapitaallasten van 2025 t/m 2029.
Voor onderdeel 3 moet in 2024 een krediet van € 242.000 worden uitgetrokken ten behoeve van investeringen die vanaf 2025 in vijf jaar worden afgeschreven, met als gevolg kapitaallasten van 2025 t/m 2029.
Daarnaast wordt voor onderdeel 3 vanaf 2025 nog € 181.500 aan overige structurele lasten geraamd.
Vanaf begroting 2025 wordt op basis van nieuwe ontwikkelingen en NIS2.0 jaarlijks de status gemonitord en waar nodig nieuwe maatregelen in de begroting opgenomen.

Het financieel totaaloverzicht en de dekking door de deelnemers is dan als volgt:

onderdeel	krediet	2024	2025	2026	2027	2028
1. processen, meten en sturen		121.000	48.000	48.000	48.000	48.000
2. segmentering	84.500		20.300	19.600	18.900	18.200
3. ict en basisvoorzieningen	242.000		58.100	56.200	54.300	52.400
overige structurele kosten			181.500	181.500	181.500	181.500
totaal		**121.000**	**307.900**	**305.300**	**302.700**	**300.100**
gemeente	**inwoners**	**2024**	**2025**	**2026**	**2027**	**2028**
Drechterland	19.978	17.100	43.600	43.200	42.900	42.500
Enkhuizen	18.620	16.000	40.600	40.300	39.900	39.600
Stede Broec	21.952	18.800	47.900	47.500	47.100	46.700
Opmeer	12.074	10.400	26.300	26.100	25.900	25.700
Medemblik	45.450	39.000	99.200	98.300	97.500	96.700
Koggenland	23.041	19.800	50.300	49.800	49.400	49.000
totaal	141.115	**121.000**	**307.900**	**305.300**	**302.700**	**300.100**

Memo

Toelichting:

De investeringen worden conform Activabeleid lineair afgeschreven in 5 jaar, tegen 4% rente.
De kosten worden verdeeld over de deelnemers met de verdeelsleutel uit de begroting 2024.
Vooralsnog wordt ervan uitgegaan dat WerkSaam WF niet zal bijdragen in de hier opgenomen kosten.

Cybersecurity is een essentieel en niet meer weg te denken onderdeel van de bedrijfsvoering van SSC De-Som, maar ook van de deelnemers, verworden. Dit maakt ook dat in de P&C cyclus standaard aandacht voor cybersecurity gevraagd zal worden. De VNG en ook de NIS2.0 is daarin ook duidelijk. Denk hierbij in het bijzonder de meldplicht, zorgplicht en informatieplicht, aansprakelijkheid en de toetsing daarop.

Voorgesteld wordt om vanaf de begroting 2025, vast te stellen in 2024, en verder (de P&C-cyclus) op basis van de NIS2.0 verantwoording af te leggen en waar nodig de te nemen maatregelen te benoemen en hiervoor de benodigde middelen beschikbaar te stellen.

Resumerend

In goede samenwerking en breed gedragen door alle betrokken deelnemers kunnen wij u heet onderliggende advies, uitvoeringsplan informatiebeveiliging (UIB) 2024-2025, aanbieden. Het advies is unaniem gedragen van en door alle CISO's en IM-ers van de deelnemers en SSC DeSom.

Resumerend vragen wij het AB in te stemmen met:

- Het onderliggende advies en de voorgestelde uitvoering in 2024 en 2025 van de voorgestelde maatregelen door SSC DeSom;
  De hiervoor beschikbare middelen beschikbaar stellen conform het onderstaande financieel totaaloverzicht en de dekking door de deelnemers:

onderdeel	krediet	2024	2025	2026	2027	2028
1. processen, meten en sturen		121.000	48.000	48.000	48.000	48.000
2. segmentering	84.500		20.300	19.600	18.900	18.200
3. ict en basisvoorzieningen	242.000		58.100	56.200	54.300	52.400
overige structurele kosten			181.500	181.500	181.500	181.500
totaal		**121.000**	**307.900**	**305.300**	**302.700**	**300.100**
gemeente	**inwoners**	**2024**	**2025**	**2026**	**2027**	**2028**
Drechterland	19.978	17.100	43.600	43.200	42.900	42.500
Enkhuizen	18.620	16.000	40.600	40.300	39.900	39.600
Stede Broec	21.952	18.800	47.900	47.500	47.100	46.700
Opmeer	12.074	10.400	26.300	26.100	25.900	25.700
Medemblik	45.450	39.000	99.200	98.300	97.500	96.700
Koggenland	23.041	19.800	50.300	49.800	49.400	49.000
totaal	141.115	**121.000**	**307.900**	**305.300**	**302.700**	**300.100**

Memo

- Vanaf begroting 2025 wordt op basis van nieuwe ontwikkelingen en NIS2.0 jaarlijks de status gemonitord en waar nodig nieuwe maatregelen in de begroting opgenomen.