# BELEID VOOR BEVEILIGEN BEDRIJFSVOERING (OPERATIONEEL)

Operationele beleidsnotitie

Bedrijfsvertrouwelijk

BIO 12.1

Gemeente Almere

| | |
|---|---|
| Status | Definitief |
| Versie | 1.0 |
| Ingangsdatum | 01-11-2022 |
| Revisiedatum | 31-10-2023 |
| Einddatum | 31-10-2023 |
| Opdrachtgever | Gemeente Almere |
| Team/taakveld | ICTAR |
| Auteur(s) | J.A. Blok, CISO<br>R.R. Snellenburg, Technisch security specialist<br>P.A. Kleinjan, Technisch applicatie beheerder<br>M. Soeting, Technisch applicatie beheerder |

# 1. INHOUD

# 2. INLEIDING

De hoofdlijnen voor het beleid over beveiliging bedrijfsvoering zijn vastgelegd in het beleidsdocument “Beleid voor beveiliging bedrijfsvoering (tactisch)”. Bij beveiliging van de bedrijfsvoering moet informatiebeveiliging op effectieve wijze worden onderkend en ingevuld worden. Dit met het oog op de bescherming van bedrijfsmiddelen van de gemeente Almere die toegankelijk zijn voor leveranciers, burgers en andere overheden. Door een adequate (veilige en correcte) bediening van informatieverwerkende faciliteiten, door goed getrainde gebruikers, beheerders en externe beheerpartijen, optimaliseert een ongestoorde en veilige informatievoorziening binnen de gemeente Almere.

## 2.1 DOELSTELLING EN DOELGROEP

Het doel van dit document is dat het (vereiste) beschermingsniveau is vastgelegd en inzichtelijk is, aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. Het is een operationele invulling van het Tactisch beleid voor beveiligen bedrijfsvoering en een onderdeel van het gehele Informatiebeveiliging managementsysteem.

De doelgroep van dit beleidsdocument is het middenmanagement (niveau teamleider en coördinator/senior) van ICTAR en de uitvoerenden functioneel en technisch beheer.

## 2.2 TOEPASSINGSGEBIED

Het beleid en richtlijnen zijn van toepassing voor alle informatie van de gemeente (o.a. gegevensverzamelingen, gegevensdragers, informatiesystemen, servers en netwerkcomponenten) en moeten worden nageleefd door alle medewerkers van de gemeente en zij die werkzaamheden verrichten ten behoeve van de gemeente. Indien er onduidelijkheid is over een onderwerp dient daarvoor contact opgenomen te worden met de CISO of afgevaardigden.

# 3. GEDOCUMENTEERDE BEDIENINGSPROCEDURES EN VERANTWOORDELIJKHEDEN

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent gedocumenteerde bedieningsprocedures en verantwoordelijkheden. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

## 3.1 BEDIENINGSPROCEDURES DOCUMENTEREN

| | |
|---|---|
| **Beschrijving** | In een bedieningsprocedure zijn bedieningsactiviteiten opgenomen die samenhangen met informatieverwerking en communicatiefaciliteiten, zoals de procedures voor het starten en afsluiten van de computer, back-up, onderhoud van apparatuur, etc.<br><br>Er kan gedacht worden om bedieningsprocedures op te stellen voor:<br><br>• de installatie en configuratie van systemen;<br>• de verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig;<br>• de back-up;<br>• de eisen voor de planning, met inbegrip van onderlinge verbondenheid met andere systemen;<br>• de voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen van het gebruik van systeemhulpmiddelen;<br>• de ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten door onverwachte bedienings- of technische moeilijkheden;<br>• het beheer van audit- en systeemlogbestandinformatie;<br>• de procedures voor het monitoren van activiteiten. |
| **Maatregel** | De volgende maatregelen zijn van toepassing op het bedieningsprocedures:<br><br>• Het is verplicht om bedieningsprocedures gedocumenteerd te hebben voor elke procedure.<br>• De bedieningsprocedures worden beschikbaar gesteld op een centrale omgeving aan alle gebruikers die ze slechts voor hun functie nodig hebben.<br>• De bedieningsprocedures worden minimaal elk jaar herzien.<br>• Bij een ingrijpende wijziging worden de bedieningsprocedures direct herzien. |
| **ID** | GA-IB-OP075 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.* |

## 3.2 PROCEDURE WIJZIGINGSBEHEER

| | |
|---|---|
| **Beschrijving** | Wijzigingsbeheer heeft tot doel om wijzigingen op een beheerste en geautoriseerde wijze te laten verlopen. Op die wijze kan voorkomen worden dat de doorgevoerde wijzigingen allerlei verstoringen veroorzaken. Veranderingen in de gemeentelijke organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging worden beheerst. Nieuwe systemen en belangrijke wijzigingen aan bestaande systemen volgen dan ook een formeel proces van indienen, prioriteren, besluiten, impactanalyse, vastleggen, specificeren, ontwikkelen, testen, kwaliteitscontrole en implementeren. |
| **Maatregel** | In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:<br>• het administreren van wijzigingen;<br>• risicoafweging van mogelijke gevolgen van de wijzigingen;<br>• goedkeuringsprocedure voor wijzigingen. |
| **ID** | GA-IB-OP076 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Wijzigingsbeheer: Veranderingen in de gemeentelijke organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging worden beheerst. In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:*<br>*het administreren van wijzigingen;*<br>*risicoafweging van mogelijke gevolgen van de wijzigingen;*<br>*goedkeuringsprocedure voor wijzigingen.* |

## 3.3 CAPACITEITSBEHEER

| | |
|---|---|
| **Beschrijving** | Het proces capaciteitsbeheer zorgt voor een optimale inzet van IT-middelen ten behoeve van met de opdrachtgever overeengekomen prestaties. Computercapaciteit (resources) zoals CPU tijd en schijfruimte worden tijdig en in voldoende mate beschikbaar gesteld. Het hoofddoel van capaciteitsbeheer is om de capaciteit van de IT-infrastructuur op peil te houden, om er voor te zorgen dat er voldoende capaciteit is en in de toekomst ook. Om een goed beeld te krijgen van de benodigde capaciteit moet er goed nagegaan worden op welke manier de capaciteit wordt en moet worden gebruikt, ook zal in de toekomst moeten worden gekeken of er wijzigingen komen die meer of misschien wel minder capaciteit vereisen. |
| **Maatregel** | Er moet capaciteitsbeheer toegepast worden waarvoor minimaal aandacht is voor de volgende onderdelen:<br>• Capaciteitsplanning: Het opstellen van een capaciteitsplan. Welke IT-middelen zijn nodig om te kunnen voldoen aan het dienstenniveau dat met de opdrachtgever is overeengekomen?<br>• Modellering: Onderzoeken van het capaciteitsplan m.b.v. scenario's.<br>• Prestatiebeheer: Monitoring en tuning van systemen om Diensten Niveau Overeenkomsten (DNO) na te kunnen komen.<br>• Middelenbeheer: Over welke middelen beschikt de IT-dienstenorganisatie om aan de vraag naar IT-diensten te voldoen? Middelenbeheer biedt inzicht in de IT-infrastructuur en het gebruik hiervan.<br>• Vraagbeheersing: Beheren van 'business' behoeften. Is er groei te verwachten in de vraag naar IT-middelen ? Vraagbeheersing speelt een sturende rol op korte en lange termijn. Op korte termijn wordt er voldaan aan de vraag bij een dreigend capaciteitstekort. Op lange termijn fungeert vraagbeheersing als beleidsinstrument om de benodigde capaciteit te verminderen en zo een verlaging van de kosten te realiseren.<br>• Werklastbeheer: Deze activiteit bepaalt en bewaakt de hoeveelheid werk die een systeem aangeboden krijgt. Op deze manier kunnen afspraken met de opdrachtgever over prestaties veilig worden gesteld.<br>• Applicatiedimensionering: Het maken van een begroting m.b.t. de IT-middelen die voor een applicatie nodig zijn. |
| **ID** | GA-IB-OP077 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Capaciteitsbeheer: Het gebruik van middelen wordt gemonitord en afgestemd, en er worden verwachtingen opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.* |

# 4. MALWARE

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent beheersmaatregelen tegen malware. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

Malware is software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software (kwaadaardige software, soms schadelijke software). Malware veronderstelt kwade opzet. Er kan gedacht worden aan een computer virus. Oorzaken van Malware kunnen als volgt zijn:

- De grootste oorzaak van een malwarebesmetting zijn kwetsbaarheden (gaten) in de software. Deze gaten kunnen via een exploit misbruikt worden, waardoor kwaadwillenden het systeem kunnen infecteren.
- De gebruiker kan ook zelf de oorzaak zijn van een malware-infectie, bijvoorbeeld door louche websites te bezoeken.
- Door gratis software zoals spyware of adware te installeren, kan men ook risico lopen op een malware-infectie.

## 4.1 ANTI-MALWARE OP SYSTEMEN

| | |
|---|---|
| **Beschrijving** | Door een systeem proactief continu te scannen op malware kunnen er reactieve en preventieve acties ondernomen ter bescherming. |
| **Maatregel** | Het is verplicht om op elk systeem anti-malware software te installeren die centraal beheerd wordt. De volgende maatregelen zijn van toepassing op de anti-malware:<br><br>- Minimaal maandelijks een volledige scan op het systeem.<br>- Automatische scan van ontvangen bestanden voor het openen. Denk hierbij aan bijlagen en downloads.<br>- Automatische scan op verwijderbare media en blokkering van bestandsopening tot de (bestand)scan afgerond is.<br>- Een gebruiker mag een (extra) scan starten.<br>- Een gebruiker mag geen acties en instellingen wijzigen van de anti-malware.<br>- Updates van de definities moeten geïnstalleerd worden zodra ze uitkomen. |
| **ID** | GA-IB-OP078 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Beheersmaatregelen tegen malware*<br>*Ter bescherming tegen malware worden beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.*<br>*Uitzonderingen op beheersmaatregelen tegen malware moeten onderbouwd, vastgelegd en regelmatig op noodzakelijkheid gecontroleerd worden.*<br>*Het downloaden van bestanden is beheerst en beperkt op basis van risico en noodzakelijkheid.*<br>*Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.*<br>*De gebruikte anti-malware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.*<br>*Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan omvat:*<br>*Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen.*<br>*Bijlagen en downloads vóór gebruik.*<br>*De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.* |

## 4.2 GECENTRALISEERDE ANTI-MALWARE OMGEVING

| | |
|---|---|
| **Beschrijving** | Door de scanners van systemen naar een centraal beheerder omgeving te laten rapporteren kan er actueel inzicht verkregen worden in de systemen, scanresultaten en status. Met dit inzicht kunnen vervolgens reactieve en preventieve acties ondernomen worden ter bescherming. |
| **Maatregel** | Het is verplicht om op elk systeem anti-malware software te installeren die centraal beheerd wordt. De volgende maatregelen zijn van toepassing op het centrale beheer systeem:<br>- Er moet inzicht verschaft worden over de status van de anti-malware en haar definities op de geïnstalleerde systemen. Maximale ouderdom van definities is 14 dagen.<br>- Er moet inzicht verschaft worden over de (ingeplande) anti-malware scans en uitkomsten. Indien een ingeplande scan niet uitgevoerd is, moet deze geforceerd gestart worden op het eerstvolgende moment.<br>- Er moet inzicht verschaft worden over de gevonden malware en de vervolgacties. Op basis van het gegeven inzicht moet er (geautomatiseerd) actie ondernomen worden door bij-voorbeeld het getroffen systeem te weren van toegang tot het netwerk en op nieuw te installeren. |
| **ID** | GA-IB-OP079 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Beheersmaatregelen tegen malware*<br>*Ter bescherming tegen malware worden beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.*<br>*De gebruikte anti-malware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.*<br>*Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitge-voerde scan omvat:*<br>*Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen.*<br>*Bijlagen en downloads vóór gebruik.* |

### 4.3 MEERDERE LEVERANCIERS PRINCIPE VAN ANTI-MALWARE

| | |
|---|---|
| **Beschrijving** | Door anti-malware van meerdere partijen af te nemen is de kans groter dat een aanval gedetecteerd wordt. Een aanvaller komt vaak binnen op een systeem van een eindgebruiker om vanaf daar servers aan te vallen. Door op beide systemen anti-malware van een andere leverancier te gebruiken is het voor een aanvaller lastiger om onopgemerkt aan te vallen. Hierop kan actie ondernomen worden om onze systemen beter te beschermen. |
| **Maatregel** | Het is verplicht om een unieke leverancier van anti malware te hebben voor:<br>- Eindgebruiker werkplek<br>- Servers |
| **ID** | GA-IB-OP080 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Beheersmaatregelen tegen malware*<br>*Ter bescherming tegen malware worden beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.*<br>*De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.* |

### 4.4 BEWEZEN GEKWALIFICEERDE ANTI-MALWARE LEVERANCIERS

| | |
|---|---|
| **Beschrijving** | Er zijn ontelbare aantal leveranciers van anti-malware. MRG Effitas voert elk kwartaal een 360 graden assessment & certificatie uit van anti-malware leveranciers. De rapportage van het assessment wordt publiekelijk gepresenteerd. De anti-malware leveranciers moeten zich bewijzen op uiteenlopende en uniforme testen. Door een leverancier te kiezen die aan het assessment en certificatie voldoet weet gemeente Almere dat het de juiste leverancier en product in huis haalt dat voldoet aan een hoge standaard. |
| **Maatregel** | Het is verplicht dat de gekozen anti-malware leverancier beschikt over een certificatie van MRG Effitas in de meest recente test. |
| **ID** | GA-IB-OP081 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Beheersmaatregelen tegen malware*<br>*Ter bescherming tegen malware worden beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.*<br>*De gebruikte anti-malware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.* |

## 4.5 DOWNLOADEN EN UITVOEREN VAN BESTANDEN BEPERKEN

| | |
|---|---|
| **Beschrijving** | Zoals beschreven in het begin van dit hoofdstuk is één van de grootste bronnen van malware downloads van louche websites. Door downloads en hun uitvoer te blokkeren van potentiële gevaarlijke bestanden, is het aanvalsvlak aanzienlijk verkleind. |
| **Maatregel** | Minimaal moeten de volgende type bestanden geblokkeerd worden om te downloaden en uit te voeren:<br><br>- Uitvoerbare bestanden<br>- Batch bestanden<br>- Scripts<br><br>De blokkade moet gepaard gaan met een beschrijvende uitleg. Applicaties moeten goedgekeurd zijn om uitgevoerd te worden door medewerkers. Er moet een uitzonderingsprocedure zijn voor medewerkers die deze functionaliteiten nodig hebben voor hun functie. |
| **ID** | GA-IB-OP082 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Het downloaden van bestanden is beheerst en beperkt op basis van risico en noodzakelijkheid.*<br>*Uitzonderingen op beheersmaatregelen tegen malware moeten onderbouwd, vastgelegd en regelmatig op noodzakelijkheid gecontroleerd worden.* |

# 5. BACK-UP

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent back-up van informatie. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

## 5.1 BACK-UP FREQUENTIE

| | |
|---|---|
| **Beschrijving** | Om dataverlies te beperken en/of voorkomen, is het hebben van een goede kopie noodzakelijk. Met deze backup kan de data hersteld worden. Door op frequente tijdstippen een backup te maken is er een minimaal dataverlies. Deze afweging heet 'Recovery Point Objective' (RPO). |
| **Maatregel** | De volgende maatregelen zijn van toepassing omtrent de frequentie van back-ups:<br>- Maximale dataverlies is 28 uur, op basis van een risicoanalyse kan dit verlaagd worden voor kritieke systemen.<br>- Dagelijks wordt er minimaal een incrementele back-up gemaakt.<br>- Wekelijks wordt er een volledige back-up gemaakt. |
| **ID** | GA-IB-OP083 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Back-up van informatie*<br>*Regelmatig worden back-upkopieën van informatie, software en systeemafbeeldingen gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid*<br>*Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld*<br>*Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.*<br>*In het back-upbeleid staan minimaal de volgende eisen:*<br>*Dataverlies bedraagt maximaal 28 uur.* |

## 5.2 BACK-UP RETENTIE

| | |
|---|---|
| **Beschrijving** | De zogenoemde retentie van een back-up geeft aan hoe ver terug gegaan worden kan in de geschiedenis van een back-up. Dit kan van belang zijn wanneer bijvoorbeeld een bestand terug gezet moet worden wat een jaar geleden is verwijderd. In dat geval zou een backup die een retentie van een maand heeft geen oplossing bieden. Een langere retentie zal meer opslag vergen waardoor een onbeperkte retentie misschien 'handig om te hebben' klinkt, maar kan wel onnodig in de kosten oplopen. |
| **Maatregel** | De minimale retentietermijn van back-ups zijn als volgt:<br>• Voor wekelijkse back-ups 3 weken.<br>• Voor de maandelijkse back-ups 18 maanden. Hierbij is het toegestaan om na 6 maanden, per kwartaal één back-up te bewaren zolang de 18 maanden retentie gewaarborgd blijft. |
| **ID** | GA-IB-OP084 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Back-up van informatie*<br>*Regelmatig worden back-upkopieën van informatie, software en systeemafbeeldingen gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid*<br>*Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld*<br>*Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.* |

## 5.3 BACK-UP HERSTEL

| | |
|---|---|
| **Beschrijving** | Wanneer een incident plaatsvindt waardoor (kritieke)bedrijfsprocessen worden geraakt, is het belangrijk om te weten hoe lang het duurt voordat data en applicatie(s) weer beschikbaar zijn. Meerdere factoren hebben impact op de hersteltijd zoals de hoeveelheid data, de gebruikte techniek of de snelheid van de back-up media. Het kan zijn dat er afwegingen gemaakt moeten worden wat wanneer herstelt wordt om zo snel mogelijk weer aan het werk te kunnen. Deze afweging heet 'Recovery Time Objective' (RTO). Binnen zo'n afweging zullen prioriteiten gesteld moeten stellen zodat belangrijke onderdelen eerder hersteld worden dan andere. |
| **Maatregel** | De hersteltijd bedraagt maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen. Prioriteit van het herstel ligt bij de meest kritische systemen volgens classificatie. |
| **ID** | GA-IB-OP085 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Back-up van informatie*<br>*Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.*<br>*In het back-upbeleid staan minimaal de volgende eisen:*<br>*Dataverlies bedraagt maximaal 28 uur.*<br>*Hersteltijd in geval van incidenten is max 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.* |

## 5.4 BACK-UP TESTEN

| | |
|---|---|
| **Beschrijving** | Het testen van back-ups wordt soms alleen gedaan wanneer er daadwerkelijk iets hersteld moet worden. Dit heeft er mede mee te maken dat het testen vaak geld en veel tijd kost. Sommige back-up applicaties bieden de mogelijkheid om een verificatietest te draaien. Zo'n verificatietest kijkt of de back-up data in orde zijn. Beter is periodiek de backup herstellen en vervolgens te verifiëren of de data intact is. Een hersteltest kan plaats vinden door steekproefsgewijs bestanden te herstellen, of zelfs een geheel systeem te herstellen om ook de functionaliteit van applicaties te testen. |
| **Maatregel** | De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden. Van deze test wordt een evaluatie en een verslag opgemaakt. Verbeterpunten moeten verholpen zijn voor de eerstvolgende test. |
| **ID** | GA-IB-OP086 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Back-up van informatie*<br>*De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.* |

## 5.5 BACK-UP MONITORING

| | |
|---|---|
| **Beschrijving** | Wanneer de back-up is ingeregeld, is het van belang dat de back-up gemonitord wordt. Op basis van rapportage kan dagelijks nagegaan worden of de back-ups daadwerkelijk draaien en of er geen fouten zijn opgetreden. Het is belangrijk dat fouten tijdig worden hersteld zodat de bescherming in orde is. |
| **Maatregel** | Er moet dagelijks actuele rapportage van de back-ups beschikbaar zijn. Deze rapportage moet dagelijks gemonitord worden. |
| **ID** | GA-IB-OP087 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Back-up van informatie*<br>*Regelmatig worden back-upkopieën van informatie, software en systeemafbeeldingen gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid*<br>*Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld*<br>*Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.* |

## 5.6 BACK-UP BESCHERMING

| | |
|---|---|
| **Beschrijving** | De systemen van gemeente Almere bevatten gevoelige informatie. Deze data komt terecht in de back-up en moet adequaat beveiligd worden. De toegang tot de data moet afgeschermd zijn en versleuteld. Tevens moet de data opgeslagen worden zodat de beschikbaarheid van de data gewaarborgd is. |
| **Maatregel** | De volgende maatregelen zijn van toepassing op bescherming van back-ups:<br>- Toegang tot backups is beperkt tot de strikt noodzakelijke medewerkers.<br>- De backup is versleuteld opgeslagen.<br>- Van een backup bestaan meerdere kopieën verspreid over meerdere fysiek gescheiden locaties. De afstand tussen de verschillende locaties moet dusdanig zijn dat bij een calamiteit van één locatie bij de ander niet leid tot een calamiteit bij een andere locatie. Twee locaties is minimaal benodigd. |
| **ID** | GA-IB-OP088 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Back-up van informatie*<br>*Regelmatig worden back-upkopieën van informatie, software en systeemafbeeldingen gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid*<br>*Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld*<br>*Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.*<br>*In het back-upbeleid staan minimaal de volgende eisen:*<br>*Dataverlies bedraagt maximaal 28 uur.*<br>*Hersteltijd in geval van incidenten is max 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.*<br>*Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.*<br>*De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.* |

# 6. VERSLAGLEGGING EN MONITOREN

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent verslaglegging en monitoring. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

## 6.1 GEBEURTENISSEN REGISTREREN

| | |
|---|---|
| **Beschrijving** | Veel gebeurtenissen die voor het beheer van IT-voorzieningen van belang zijn, hebben tevens betekenis voor informatiebeveiliging en worden daarom vastgelegd ofwel gelogd. Loggegevens kunnen zowel betrekking hebben op handelingen van natuurlijke personen als op het gedrag van informatiesystemen. Daarnaast zijn er andere doelen zoals technisch beheer, productiebesturing, capacitymanagement, configurationcontrol, SLA compliancemonitoring etc.<br><br>Loggegevens over personen kunnen dienen als wettig bewijsmateriaal, waarmee onwettige handelingen aangetoond kunnen worden. Loggegevens kunnen ook betrekking hebben op ongewenste handelingen, die niet in overeenstemming zijn met het organisatiebeleid. Deze gegevens worden daarom zeer vertrouwelijk behandeld.<br><br>Bij elke actie die een medewerker in een applicatie, database of systeem uitvoert dient er registratie plaats te vinden. Deze gebeurtenissen worden weggeschreven in een logbestand. Hiermee kan er controle en signalering toegepast worden. Acties zijn daarmee herleidbaar naar een persoon. |
| **Maatregel** | Afhankelijk van het systeem worden er gegevens vastgelegd. Minimaal worden de volgende gegevens gelogd: datum en tijdstip, gebruiker, apparaat, gebeurtenis, resultaat gebeurtenis. Bij apparaat voldoet een IP-adres als de systeemnaam niet bekend is. De logbestanden moeten niet manipuleerbaar zijn.<br><br>Er mag geen gevoelige informatie in een logbestand staan zoals wachtwoorden of teksten uit een persoonlijk dossier. De beveiliging van de applicatie of het systeem mag niet op basis van logbestanden in het geding komen. |
| **ID** | GA-IB-OP089 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Gebeurtenissen registreren*<br>*Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig beoordeeld.*<br>*Een logregel bevat minimaal:*<br>*de gebeurtenis;*<br>*de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;*<br>*het gebruikte apparaat;*<br>*het resultaat van de handeling;*<br>*een datum en tijdstip van de gebeurtenis.*<br>*Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.* |

## 6.2 LOGBESTANDEN VAN BEHEERDERS EN OPERATORS

| | |
|---|---|
| **Beschrijving** | Logbestanden van beheerders zijn specifiek benoemd omdat beheerders verregaande rechten hebben. Beheerders kunnen logfiles wissen. Configuratiefouten of misbruik door beheerders kunnen worden gemaskeerd omdat beheerders logfiles in systemen kunnen wissen. |
| **Maatregel** | De volgende maatregelen gelden rondom logbestanden van beheerders:<br>• Beheeracties worden altijd gelogd worden.<br>• De logbestanden moeten niet manipuleerbaar zijn door de beheerders. |
| **ID** | GA-IB-OP090 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident (via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16).*<br>*Logbestanden van beheerders en operators*<br>*Activiteiten van systeembeheerders en -operators worden vastgelegd en de logbestanden worden beschermd en regelmatig beoordeeld.* |

## 6.3 CENTRALE LOGOMGEVING (SIEM)

| | |
|---|---|
| **Beschrijving** | Gebeurtenissen worden weggeschreven in een logbestand. Voor de integriteit is het belangrijk dat de data niet aanpasbaar is. Om deze data te beschermen en te kunnen correleren is er een centrale Security Incident en Event Management (SIEM) omgeving. Het Security Operations Center (SOC) bedient de SIEM omgeving. |
| **Maatregel** | Alle loggebeurtenissen van applicaties, systemen en infrastructuur moeten geautomatiseerd naar de centrale logomgeving (SIEM) doorgezet worden. In de SIEM omgeving is het onmogelijk om log-gebeurtenissen aan te passen. |
| **ID** | GA-IB-OP091 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Gebeurtenissen registreren*<br>*Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig beoordeeld.*<br>*De informatieverwerkende omgeving wordt gemonitord door Security Information & Event Management (SIEM) tooling en een Security Operations Center, middels detectie-voorzieningen. Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.*<br>*De SIEM en SOC hebben beheerste processen met betrekking tot het beheer van incidenten, voor zowel respons en escalatie als de rapportage aan het verantwoordelijk management.*<br>*Beschermen van informatie in logbestanden*<br>*Logfaciliteiten en informatie in logbestanden worden beschermd tegen vervalsing en onbevoegde toegang.*<br>*Beschermen van informatie in logbestanden*<br>*Logfaciliteiten en informatie in logbestanden worden beschermd tegen vervalsing en onbevoegde toegang.* |

## 6.4 Security Operations Center (SOC)

| | |
|---|---|
| **Beschrijving** | In de praktijk monitort een Security Operations Centre de computer- en netwerkactiviteiten in een organisatie. Log-informatie van applicaties en apparaten in het bedrijfsnetwerk wordt verzameld en onderzocht op afwijkende zaken. De log-informatie kan afkomstig zijn van servers, firewalls, webapplicaties, antivirus-software en zelfs van industriële controlesystemen. Het draait dus om relevante informatie over de beveiliging van alle systemen en apparaten. Alle informatie leidt tot inzicht in hoe veilig het netwerk, de systemen en hard- en software functioneert in de organisatie<br><br>Om log-informatie vanuit verschillende bronnen te interpreteren en de samenhang met wat zich digitaal afspeelt te duiden, zal een Security Information & Event Management-systeem (SIEM) gebruikt worden. Naast informatie over systemen, hard- en software en het netwerk, gebruikt een SOC ook 'threat intelligence'. Dit is informatie over kwetsbaarheden en dreiging in cybersecurity, afkomstig uit andere bronnen. Met deze informatie beoordeelt het SOC gebeurtenissen in systemen en op alle aangesloten apparaten. |
| **Maatregel** | De volgende maatregelen zijn van toepassing rondom een Security Operations Center (SOC):<br><br>• Het SOC heeft toegang tot de Security Information & Event Management-systeem (SIEM) omgeving.<br>• Het SOC heeft overzicht in alle logbronnen en monitort actief de systemen en infrastructuur op securityincidenten.<br>• Het SOC grijpt preventief en reactief in bij incidenten.<br>• Bij aanvallen deelt het SOC bekende informatie met de IBD, het CERT van gemeentes in Nederland.<br>• Minimaal elk jaar wordt elke logbron gecontroleerd |
| **ID** | GA-IB-OP092 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*De informatieverwerkende omgeving wordt gemonitord door Security Information & Event Management (SIEM) tooling en een Security Operations Center, middels detectie-voorzieningen. Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.*<br>*Bij ontdekte nieuwe dreigingen (aanvallen) worden deze binnen geldende juridische kaders verplicht gedeeld met de IBD als sectorale CERT, middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.*<br>*De SIEM en SOC hebben beheerste processen met betrekking tot het beheer van incidenten, voor zowel respons en escalatie als de rapportage aan het verantwoordelijk management.*<br>*Beschermen van informatie in logbestanden*<br>*Logfaciliteiten en informatie in logbestanden worden beschermd tegen vervalsing en onbevoegde toegang.*<br>*Er is een overzicht van logbestanden die worden gegenereerd.* |

| | |
|---|---|
| | *Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.*<br>*Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident (via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16).*<br>*Logbestanden van beheerders en operators*<br>*Activiteiten van systeembeheerders en -operators worden vastgelegd en de logbestanden worden beschermd en regelmatig beoordeeld.* |

## 6.5 KLOKSYNCHRONISATIE

| | |
|---|---|
| **Beschrijving** | Om gebeurtenissen uit verschillende componenten te correleren, worden de klokken van de verschillende systemen gelijkgericht en waarmee de timestamps van gebeurtenissen zijn gesynchroniseerd. Dit synchroniseren is het effect van de juiste instelling van tijd op betreffende componenten. Dit is gewenst om de correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere geregistreerde gegevens mogelijk te maken en om onderzoeken naar informatiebeveiligingsincidenten te ondersteunen. |
| **Maatregel** | Er is één tijdbron waarmee alle systemen gesynchroniseerd moeten worden. |
| **ID** | GA-IB-OP093 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Kloksynchronisatie*<br>*De klokken van alle systemen van de gemeentelijke organisatie worden gesynchroniseerd met één referentietijdbron.* |

# 7. BEHEER VAN OPERATIONELE SOFTWARE

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent beheren op operationele systemen. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

## 7.1 SCHEIDING VAN ONTWIKKEL-, TEST- EN PRODUCTIEOMGEVINGEN

| | |
|---|---|
| **Beschrijving** | Ontwikkel- en testactiviteiten kunnen ernstige problemen veroorzaken, bijv. ongewenste wijziging van bestanden of systeemomgeving, of storingen in het systeem. Het is nodig een bekende en stabiele omgeving te onderhouden voor het uitvoeren van zinvolle tests en om ongepaste toegang tot de productieomgeving te voorkomen. In bepaalde systemen kan deze mogelijkheid worden misbruikt om fraude te plegen of om niet-geteste of kwaadaardige codes in te voeren, wat ernstige operationele problemen kan veroorzaken.<br><br>Ontwikkel- en testactiviteiten kunnen onbedoelde veranderingen aan software of informatie veroorzaken als ze dezelfde informatie verwerkende omgeving delen. Het is daarom wenselijk om ontwikkel-, test- en productieomgevingen te scheiden. Hiermee wordt het risico van onbedoelde verandering of onbevoegde toegang tot operationele software en bedrijfsgegevens verlaagd. |
| **Maatregel** | Het is verplicht om ontwikkel-, test en productiesystemen logisch te scheiden. Routering tussen deze gescheiden systemen is niet toegestaan.<br><br>Voor beheerdoeleinden zoals applicatie installatiebestanden is er een centrale opslag die benaderbaar is vanuit de hele OTAP omgeving toegestaan. |
| **ID** | GA-IB-OP094 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Scheiding van ontwikkel-, test- en productieomgevingen*<br>*Ontwikkel-, test- en productieomgevingen worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.*<br><br>Tactisch beleid OTAP<br><br>- Sectie Beleid voor systeemlandschap:<br>*Ontwikkelingsomgeving: een omgeving voor ontwikkeling en onderhoud van applicaties en systemen (meestal in beheer bij de dienstverlener verantwoordelijk voor ontwikkeling en onderhoud).*<br>*Testomgeving: een aparte omgeving waarop de voorbereidingen van installaties worden uitgevoerd t.b.v. de acceptatieomgeving. Daarnaast worden (technische) testen uitgevoerd op de applicaties en systemen.*<br>*Acceptatieomgeving: een omgeving voor de acceptatie van applicaties en systemen en eventueel onderhoud. Deze omgeving is technisch gelijk aan de productieomgeving (kopie) waarop getest kan worden in een realistische omgeving met data die niet te herleiden is naar persoonsgegevens.*<br>*Productieomgeving: een omgeving waarop alle actuele en juiste informatie en gegevens staan, die veilig, in beheer is en geborgd tegen fouten van systeemontwikkelaars.* |

## 7.2 GEAUTORISEERD PERSONEEL KAN FUNCTIES EN SOFTWARE INSTALLEREN OF ACTIVEREN

| | |
|---|---|
| **Beschrijving** | Het installeren van software op operationele systemen is beperkt. Alleen de medewerkers die applicaties beheren kunnen volgens het vastgestelde (wijzigings)proces software installeren op operationele systemen. |
| **Maatregel** | Alleen geautoriseerd personeel kan functies en software installeren of activeren op operationele systemen. |
| **ID** | GA-IB-OP095 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.*<br>*Beperkingen voor het installeren van software*<br>*Voor het door gebruikers installeren van software worden regels vastgesteld en geïmplementeerd.*<br>*Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat door ICTAR wordt aangeboden.*<br>*Om het op operationele systemen installeren van software te beheersen worden procedures geïmplementeerd.*<br><br>Tactisch beleid OTAP<br><br>- Sectie Beleid voor systeemlandschap:<br>*Productieomgeving: een omgeving waarop alle actuele en juiste informatie en gegevens staan, die veilig, in beheer is en geborgd tegen fouten van systeemontwikkelaars.* |

## 7.3 INSTALLATIE OP PRODUCTIEOMGEVING NA EEN SUCCESVOLLE TEST EN ACCEPTATIE

| | |
|---|---|
| **Beschrijving** | Om een goede beheersing van software te waarborgen, is het vanuit best practices noodzakelijk de verschillende stappen en testen uit te voeren in een geïsoleerde eigen omgeving. Dit is zodat er gegarandeerd kan worden dat het primaire proces niet wordt verstoord. Daarbij vindt een expliciete afsluiting van een test plaats zodat een gecontroleerde overgang mogelijk wordt. Dit concept wordt een OTAP-straat genoemd. OTAP staat voor Ontwikkel, Test, Acceptatie en Productie. |
| **Maatregel** | De volgende maatregelen zijn van toepassing bij het installeren van software in de productieomgeving:<br><br>- Installatie van software in de productieomgeving moet het wijzigingsproces gevolgd hebben inclusief een succesvolle installatie in de test en acceptatie omgeving.<br>- De integriteit van de installatiebestanden wordt gewaarborgd door een hash-controle.<br>- Installatie vind plaats via het juiste en specifiek aangevraagde beheerdersaccount.<br>- Documentatie wordt bijgewerkt als onderdeel van het installeren van software. |
| **ID** | GA-IB-OP096 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.*<br>*Scheiding van ontwikkel-, test- en productieomgevingen*<br>*Ontwikkel-, test- en productieomgevingen worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.*<br>*In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan incidenteel worden afgeweken.*<br>*Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.*<br>*Beperkingen voor het installeren van software*<br>*Voor het door gebruikers installeren van software worden regels vastgesteld en geïmplementeerd.*<br>*Om het op operationele systemen installeren van software te beheersen worden procedures geïmplementeerd.*<br><br>Tactisch beleid OTAP<br><br>- Sectie Beleid voor systeemlandschap:<br>*Productieomgeving: een omgeving waarop alle actuele en juiste informatie en gegevens staan, die veilig, in beheer is en geborgd tegen fouten van systeemontwikkelaars.*<br><br>Tactisch beleid beheer technische kwetsbaarheden<br><br>- Sectie Beleidsuitgangspunten |

| | |
|---|---|
| | *Alle patches dienen voor installatie te worden getest.*<br>*Als een systeem gepatched is wordt de systeem documentatie bijgewerkt naar de laatste stand van zaken, de configuratie management database wordt geupdate met de nieuwe versienummers van componenten.*<br>*De technische integriteit van programmapakketten en infrastructurele programmatuur wordt gecontroleerd door middel van een hashing mechanisme en een controlegetal van de leverancier, dat via een vertrouwd kanaal is verkregen.* |

### 7.4 GEÏNSTALLEERDE PROGRAMMATUUR, CONFIGURATIES EN DOCUMENTATIE VASTLEGGEN IN DE CONFIGURA-

| | |
|---|---|
| **Beschrijving** | Om een goede beheersing van software te waarborgen, is het vanuit best practices noodzakelijk actuele verslaglegging te leggen van de software en gerelateerde informatie. Daarbij is het van belang om nuttige en noodzakelijke informatie vast te leggen zoals de softwareversie, leverancier, beheerder en eigenaar. |
| **Maatregel** | De volgende maatregelen zijn van toepassing over de Configuratie Management Database (CMDB):<br>- De volgende details moeten vastgelegd zijn in de CMDB:<br>  o Software naam<br>  o Software versie<br>  o Geïnstalleerde systemen<br>  o Status<br>  o Beheerders<br>  o Applicatie eigenaar<br>  o Software leverancier<br>  o Contractinformatie inclusief contactpersoon<br>- De CMDB moet bijgewerkt worden bij elke wijziging aan de software. |
| **ID** | GA-IB-OP097 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.*<br>*Beperkingen voor het installeren van software*<br>*Voor het door gebruikers installeren van software worden regels vastgesteld en geïmplementeerd.*<br>*Om het op operationele systemen installeren van software te beheersen worden procedures geïmplementeerd.*<br><br>Tactisch beleid OTAP<br>- Sectie Beleid voor systeemlandschap:<br>*Productieomgeving: een omgeving waarop alle actuele en juiste informatie en gegevens staan, die veilig, in beheer is en geborgd tegen fouten van systeemontwikkelaars.* |

TIEDATABASE

## 7.5 LEVERANCIER ONDERSTEUNDE SOFTWARE

| | |
|---|---|
| **Beschrijving** | Software heeft een product cyclus die eindigt met een End Of Life (EOL) datum. Vanaf dat moment is er geen ondersteuning meer van de leverancier. Fouten zoals security kwetsbaarheden worden dan niet meer verholpen. Het is van belang dat de organisatie in controle is van de software en alleen software gebruikt die ondersteuning heeft van de leverancier. |
| **Maatregel** | De volgende maatregelen zijn van toepassing op leverancier ondersteunde software:<br>- Installatie van software in de productieomgeving moet ondersteund worden door een leverancier die de security van de software waarborgt.<br>- Aanpassingen of toevoegingen die de leverancier niet ondersteund of goedkeurt worden niet toegepast. |
| **ID** | GA-IB-OP098 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.*<br>*Beperkingen voor het installeren van software*<br>*Voor het door gebruikers installeren van software worden regels vastgesteld en geïmplementeerd.*<br>*Om het op operationele systemen installeren van software te beheersen worden procedures geïmplementeerd.*<br>Tactisch beleid OTAP<br>- Sectie Beleid voor systeemlandschap:<br>*Productieomgeving: een omgeving waarop alle actuele en juiste informatie en gegevens staan, die veilig, in beheer is en geborgd tegen fouten van systeemontwikkelaars.*<br>Tactisch beleid beheer kritische kwetsbaarheden<br>- Sectie Beleidsuitgangspunten:<br>*Behoudens de door de leverancier goedgekeurde updates worden er geen wijzigingen aangebracht in programmapakketten en infrastructurele programmatuur.* |

## 7.6 N-1 PRINCIPE EN UPDATES EVALUATIE

| | |
|---|---|
| **Beschrijving** | Het uitgangspunt voor softwareversies is het N-1 principe. Hierbij wordt de op één na laatste versie geïnstalleerd. Een uitzondering is dat indien er een securitypatch beschikbaar is, dan de meest recente versie voor het principe gaat. Het is een gegeven dat er voor software updates uitgegeven gaan worden door leveranciers. Elke update moet dan ook geëvalueerd worden op mogelijke impact. Zowel op gebruikerservaring, stabiliteit en security. |
| **Maatregel** | De volgende maatregelen zijn van toepassing op het N-1 principe en evaluatie van updates:<br>• Beheerders volgen software en patch releases op van applicaties die onder hun beheer vallen.<br>• De meest recente versie van de software is geïnstalleerd, N-1 is het uitgangspunt indien er geen securityverbeteringen in de laatste versie zitten.<br>• Nieuwe versies worden geëvalueerd binnen uiterlijk twee werkdagen met daarbij aandacht voor securityverbeteringen.<br>• Elke update moet getest worden volgens het normale wijzigingsproces, in uitzonderlijke gevallen kan het beveiligingsrisico groter zijn dan het risico van niet testen. Dit blijkt uit de evaluatie<br>• Op basis van de evaluatie wordt de update ingepland. Bij securityverbeteringen zal dit op een zo kort mogelijk termijn zijn. |
| **ID** | GA-IB-OP099 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.*<br>*Beperkingen voor het installeren van software*<br>*Voor het door gebruikers installeren van software worden regels vastgesteld en geïmplementeerd.*<br>*Om het op operationele systemen installeren van software te beheersen worden procedures geïmplementeerd.*<br>Tactisch beleid OTAP<br>- Sectie Beleid voor systeemlandschap:<br>*Productieomgeving: een omgeving waarop alle actuele en juiste informatie en gegevens staan, die veilig, in beheer is en geborgd tegen fouten van systeemontwikkelaars.*<br>Tactisch beleid beheer technische kwetsbaarheden<br>- Sectie Beleidsuitgangspunten<br>*Alle patches dienen voor installatie te worden getest.* |

| | |
|---|---|
| **Beschrijving** | Om een goede beheersing van software te waarborgen, is het vanuit best practices noodzakelijk om een rollback strategie te hebben. In het geval een wijziging, ondanks zorgvuldig testen en acceptatie, niet succesvol is in de productieomgeving moet de omgeving hersteld worden naar de voorgaande staat. Als onderdeel van het implementatieplan moet de rollback beschreven zijn in een stappenplan inclusief de benodigde acties en middelen. Op basis van een risicoanalyse wordt er bepaald wat het juiste moment is om de rollback in te starten. Er kan bijvoorbeeld gedefinieerd zijn dat na een uur na het eerste falen er per definitie een rollback moet starten. In de planning van de wijziging moet hiermee rekening gehouden worden. |
| **Maatregel** | Voorafgaand aan de installatie van software in de productieomgeving moet het wijzigingsproces gevolgd worden inclusief een opgesteld implementatieplan. De volgende maatregelen zijn hierbij van toepassing:<br>• Er moet een rollback strategie beschreven zijn inclusief stappenplan en de benodigde acties en middelen.<br>• Op basis van een risicoacceptatie moeten de criteria om een rollback uit te rollen beschreven.<br>• Met de planning van de implementatie moet er rekening gehouden zijn met de doorlooptijd van de rollback. |
| **ID** | GA-IB-OP100 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Gedocumenteerde bedieningsprocedures: Bedieningsprocedures worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze slechts voor hun functie nodig hebben.*<br>*Wijzigingsbeheer: Veranderingen in de gemeentelijke organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging worden beheerst. In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:*<br>*het administreren van wijzigingen;*<br>*risicoafweging van mogelijke gevolgen van de wijzigingen;*<br>*goedkeuringsprocedure voor wijzigingen*<br>*Beperkingen voor het installeren van software*<br>*Voor het door gebruikers installeren van software worden regels vastgesteld en geïmplementeerd.*<br>*Om het op operationele systemen installeren van software te beheersen worden procedures geïmplementeerd.* |

## 7.7 IMPLEMENTATIEPLAN EN ROLLBACKSTRATEGIE

# 8. BEHEER VAN TECHNISCHE KWETSBAARHEDEN

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent beheer van technische kwetsbaarheden. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

## 8.1 GEAUTOMATISEERD SCANNEN NAAR TECHNISCHE KWETSBAARHEDEN

| | |
|---|---|
| **Beschrijving** | Het geautomatiseerd scannen naar technische kwetsbaarheden is een controleslag op de uitvoering van het patchbeleid. De meeste technische kwetsbaarheden komen voort uit het ontbreken van patches. Het beheer van kwetsbaarheden in een bedrijfsnetwerk is dan ook een taak die nooit stopt. Er zijn gemiddeld tien kwetsbaarheden per IT-asset, wat neerkomt op een gemiddelde van ongeveer 20.000 kwetsbaarheden die een middelgroot bedrijf op een bepaald moment moet beheren. Met kwetsbaarheden management is het mogelijk om grip te krijgen. Het is echter praktisch onmogelijk om elke kwetsbaarheid op te lossen, wel is het mogelijk om zorg te dragen voor de kwetsbaarheden met het grootste risico voor de organisatie. Dit kan met behulp van automatisering en door de juiste prioriteiten te stellen. Alle systemen moeten dan ook geautomatiseerd gescand worden met een kwetsbaarheden scanner op bekende kwetsbaarheden. |
| **Maatregel** | De volgende maatregelen zijn van toepassing op geautomatiseerd kwetsbaarheden controleren:<br>- Het is verplicht om alle systemen in de productieomgeving minimaal wekelijks geautomatiseerd te scannen met een kwetsbaarheden scanner.<br>- De scan moet uitgevoerd worden op alle netwerkverbindingen van een systeem.<br>- De scan moet geauthentiseerd uitgevoerd worden op het systeem.<br>- Van een gevonden kwetsbaarheid moet een ticket uitgezet worden via het incidentproces naar de juiste beheerder. |
| **ID** | GA-IB-OP101 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en passende maatregelen worden genomen om het risico dat ermee samenhangt aan te pakken.*<br>Tactisch beleid beheer technische kwetsbaarheden<br>- Sectie Beleidsuitgangspunten:<br>*Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch). Bij deze evaluatie wordt minimaal de systeemeigenaar betrokken. Bij vermoeden van hoog risico wordt de CISO geconsulteerd.* |

## 8.2 EVALUATIE EN RISICO INSCHATTING KWETSBAARHEID

| | |
|---|---|
| **Beschrijving** | Een kwetsbaarheid heeft inherent een bepaald risico. Dit risico moet geëvalueerd worden en bepaalt het vervolg traject. Een kwetsbaarheid met een hoog risico zal op een korter termijn verholpen moeten worden om de veiligheid van de organisatie te waarborgen. |
| **Maatregel** | De volgende maatregelen zijn van toepassing rondom de evaluatie en risico inschatting van een kwetsbaarheid:<br><br>- De beheerder van de applicatie is verantwoordelijk voor het opvolgen en oplossen van de kwetsbaarheid.<br>- Een kwetsbaarheid moet binnen 24 uur na bekendmaking geëvalueerd zijn, in achtneming van kantoortijden. Hierbij worden alle stakeholders meegenomen.<br>- Bij een kwetsbaarheid met een P1 priorisering binnen het incidentproces moet binnen 24 uur een oplosscenario gekozen zijn die vervolgens binnen één week geïmplementeerd wordt.<br>- Het oplosscenario volgt het wijzigingsproces.<br>- Alle stappen worden vastgelegd zijn in het bijhorende ticket in het incident proces. |
| **ID** | GA-IB-OP102 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Beheer van technische kwetsbaarheden*<br>*Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en passende maatregelen worden genomen om het risico dat ermee samenhangt aan te pakken.*<br>*Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.*<br><br>Tactisch beleid beheer technische kwetsbaarheden<br><br>- Sectie Beleidsuitgangspunten:<br>*Er is een proces ingericht voor het beheer van kwetsbaarheden en patching van (systeem) software binnen de gemeente Almere. Patches volgen het wijzigingsbeheer proces.*<br>*Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch). Bij deze evaluatie wordt minimaal de systeemeigenaar betrokken. Bij vermoeden van hoog risico wordt de CISO geconsulteerd.*<br>*Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter maximaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde van het systeem.* |

| | |
|---|---|
| | *Van alle uitgevoerde en niet uitgevoerde patches wordt door de ICT beheerders een log-boek bijgehouden.* |

## 8.3 NCSC EN IBD BEVEILIGINGSADVIEZEN

| | |
|---|---|
| **Beschrijving** | Een beveiligingsadvies wordt door het NCSC gepubliceerd naar aanleiding van een recent gevonden kwetsbaarheid of geconstateerde dreiging. In een beveiligingsadvies staat de beschrijving, de mogelijke gevolgen en mogelijke oplossingen van de kwetsbaarheid of dreiging. De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen; kans en impact. Beide elementen worden ingeschaald op low, medium of high.<br><br>Op basis van ervaringen bij andere gemeentes en door de gemeente ingestuurde 'IBD foto' kan het IBD CERT een beveiligingsadvies uitgeven.<br><br>Gemeente Almere moet beide adviezen opvolgen en evalueren. In het geval van een kritisch beveiligingsadvies, bijvoorbeeld een High-High beveiligingsadvies van de NCSC is er direct actie nodig om het risico in te schatten dat de gemeente loopt. |
| **Maatregel** | De volgende maatregelen zijn van toepassing bij beveiligingsadviezen van de IBD en NCSC:<br><br>- Een beveiligingsadvies moet binnen 8 uur na bekendmaking geëvalueerd zijn, in achtneming van kantoortijden. Hierbij worden alle stakeholders meegenomen.<br>- Bij een kwetsbaarheid met een P1 priorisering binnen het incidentproces moet binnen 8 uur een oplosscenario gekozen zijn die vervolgens binnen één week geïmplementeerd wordt.<br>- Het oplosscenario volgt het wijzigingsproces.<br>- Alle stappen worden vastgelegd zijn in het bijhorende ticket in het beveiligingsincident proces. Van adviezen die niet van toepassing zijn is geen ticket vereist. |
| **ID** | GA-IB-OP103 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br>*Beheer van technische kwetsbaarheden*<br>*Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en passende maatregelen worden genomen om het risico dat ermee samenhangt aan te pakken.*<br>*Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.*<br><br>Tactisch beleid beheer technische kwetsbaarheden<br><br>- Sectie Beleidsuitgangspunten:<br>*Er is een proces ingericht voor het beheer van kwetsbaarheden en patching van (systeem) software binnen de gemeente Almere. Patches volgen het wijzigingsbeheer proces.*<br>*Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd.* |

| | |
|---|---|
| | *Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter maximaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde van het systeem.*<br>*Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatie-beveiligingsdienst voor gemeenten of een CERT zoals het NCSC.* |

## 8.4 INCIDENT DOORGEVEN AAN DE IBD CERT

| | |
|---|---|
| **Beschrijving** | De IBD is de sectorale CERT / CSIRT (Computer Emergency Response Team / Computer Security Incident Response Team) voor alle Nederlandse gemeenten en ondersteunt bij incidenten op het gebied van informatiebeveiliging. De IBD-CERT ondersteunt gemeenten, gemeentelijke ICT-samenwerkingen, belastingsamenwerkingen en intergemeentelijke sociale diensten bij (dreigende) informatiebeveiligingsincidenten en helpt om incidenten te herkennen en te voorkomen.<br><br>Bij een acuut incident ondersteunt de IBD de gemeente tijdens het incident. Door beveiligingsincidenten door te geven aan de IBD kan de IBD een (trend)analyse maken en eventuele andere gemeentes proactief informeren. |
| **Maatregel** | De volgende maatregelen zijn van toepassing rondom meldingen doorgeven aan de IBD CERT.<br><br>- Bij een detectie van een inbraak wordt direct het IBD CERT gecontacteerd.<br>- Minimaal maandelijks wordt een overzicht gedeeld van alle beveiligingsincidenten met de IBD. |
| **ID** | GA-IB-OP104 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br><br>- Sectie Beleidsuitgangspunten:<br><br>*Beheer van technische kwetsbaarheden*<br>*Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en passende maatregelen worden genomen om het risico dat ermee samenhangt aan te pakken.*<br><br>Tactisch beleid beheer technische kwetsbaarheden<br><br>- Sectie Beleidsuitgangspunten:<br>*Er is een proces ingericht voor het beheer van kwetsbaarheden en patching van (systeem) software binnen de gemeente Almere. Patches volgen het wijzigingsbeheer proces.*<br>*Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd.* |

# 9. BEHEERSMAATREGELEN BETREFFENDE AUDITS VAN INFORMATIESYSTEMEN

Dit hoofdstuk beschrijft op operationeel niveau de maatregelen die getroffen moeten worden omtrent beheersmaatregelen betreffende audits van informatiesystemen. Indien er afwijkingen zijn van het gebruik van dit beleid, dan zal dit onder verantwoording van de dataeigenaar vastgelegd worden in een register door de CISO. Hierop moet vooraf goedkeuring verleend worden na een impact analyse.

## 9.1 VERSTORING BEDRIJFSPROCESSEN DOOR AUDIT BEPERKEN

| | |
|---|---|
| **Beschrijving** | Met een audit wordt een controle gedaan worden op de uitvoering van beheerprocessen. Fouten kunnen ontdekt worden en verbeteringen opgemerkt. Voor enkele processen is een audit vereist, denk hierbij aan de Ensia audit. Ondanks de meerwaarde van een audit, is het van belang dat een audit de productie werkzaamheden niet verstoort. |
| **Maatregel** | De volgende maatregelen zijn van toepassing bij audits:<br>• Auditeisen voor toegang tot systemen en gegevens behoren met de juiste managers te worden overeengekomen;<br>• Het toepassingsgebied van technische audittests behoort te worden afgesproken en te worden gecontroleerd;<br>• Audittests behoren te worden beperkt tot alleen-lezen-toegang tot software en gegevens;<br>• Toegang anders dan 'alleen lezen' behoort alleen te worden toegelaten voor geïsoleerde kopieën van systeembestanden, die behoren te worden verwijderd als de audit is uitgevoerd, of ze behoren voldoende te worden beschermd indien het verplicht is deze bestanden bij de vereiste auditdocumenten te bewaren;<br>• Eisen voor speciale of extra verwerkingsactiviteiten behoren te worden vastgesteld en overeengekomen;<br>• Audittests die de beschikbaarheid van systemen kunnen beïnvloeden, behoren buiten werkuren plaats te vinden;<br>• Alle toegangshandelingen behoren te worden gemonitord en vastgelegd in een logbestand om een referentietraject te produceren. |
| **ID** | GA-IB-OP105 |
| **Versie** | 1.0 |
| **Datum** | 01-11-2022 |
| **Rationale** | Tactisch beleid beveiliging bedrijfsvoering<br>- Sectie Beleidsuitgangspunten:<br>*Beheersmaatregelen betreffende audits van informatiesystemen*<br>*Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, worden zorgvuldig gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.* |

# 10. Bijlage 1: Hoofdstuk 12: Beveiliging bedrijfsvoering (Baseline Informatiebeveiliging Overheid versie 1.04)

**12.1 Bedieningsprocedures en verantwoordelijkheden**

Doelstelling: Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.

12.1.1 Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.

12.1.2 Wijzigingsbeheer

Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.

12.1.2.1 In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan:

(a) het administreren van wijzigingen;

(b) risicoafweging van mogelijke gevolgen van de wijzigingen;

(c) goedkeuringsprocedure voor wijzigingen.

12.1.3 Capaciteitsbeheer

Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.

12.1.4 Scheiding van ontwikkel-, test- en productieomgevingen

Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.

12.1.4.1 In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.

12.1.4.2 Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.

**12.2 Bescherming tegen malware**

Doelstelling: Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.

12.2.1 Beheersmaatregelen tegen malware

Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.

12.2.1.1 Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.

12.2.1.2 Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.

12.2.1.3 De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.

12.2.1.4 Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten:

(a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen.

(b) Bijlagen en downloads vóór gebruik.

12.2.1.5 De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.

**12.3 Back-up**

Doelstelling: Beschermen tegen het verlies van gegevens.

12.3.1 Back-up van informatie

Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.

12.3.1.1 Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld

12.3.1.2 Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.

12.3.1.3 In het back-upbeleid staan minimaal de volgende eisen:

(a) Dataverlies bedraagt maximaal 28 uur.
(b) Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.

12.3.1.4 Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.

12.3.1.5 De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.

**12.4 Verslaglegging en monitoren**

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.4.1 Gebeurtenissen registreren

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

12.4.1.1 Een logregel bevat minimaal:
(a) de gebeurtenis;
(b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;
(c) het gebruikte apparaat;
(d) het resultaat van de handeling;
(e) een datum en tijdstip van de gebeurtenis.

12.4.1.2 Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.

12.4.1.3 De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.

12.4.1.4 Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.

12.4.1.5 De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.

12.4.2 Beschermen van informatie in logbestanden

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

12.4.2.1 Er is een overzicht van logbestanden die worden gegenereerd.

12.4.2.2 Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.

12.4.2.3 Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.

12.4.2.4 Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.

12.4.3 Logbestanden van beheerders en operators

Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.

12.4.4 Kloksynchronisatie

De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

**12.5 Beheersing van operationele software**

Doelstelling: De integriteit van operationele systemen waarborgen.

12.5.1 Software installeren op operationele systemen

Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.

12.6 Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

12.6.1 Beheer van technische kwetsbaarheden

Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.

12.6.1.1 Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.

12.6.2 Beperkingen voor het installeren van software

Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.

12.6.2.1 Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).

**12.7 Overwegingen betreffende audits van informatiesystemen**

Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen

Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.