Rapportage Verhogen digitale veiligheid

Onderdeel van ENSIA verantwoording
Gemeente Doesburg 2024

Verhogen digitale weerbaarheid

Basismaatregelen Informatieveiligheid 2024

Uit informatiebeveiligingsincidenten van de afgelopen jaren is één rode draad te ontwaren: Organisaties werden voornamelijk getroffen[1] doordat één of meerdere systemen niet voorzien waren van de benodigde beveiligingsupdates of doordat onvoldoende maatregelen waren genomen om de toegang tot deze systemen te beperken. Hacks en incidenten hebben grote impact op imago, bedrijfsvoering en kunnen behoorlijk wat tijd en geld kosten. De Informatiebeveiligingsdienst (IBD) adviseert daarom bij de implementatie van de BIO om prioriteit te geven aan het op orde krijgen en houden van basismaatregelen en basisprocessen.

Lessen uit incidenten en actuele dreigingen laten zien dat basismaatregelen essentieel zijn voor het beveiligen van informatie. Voor deze basismaatregelen geldt dat deze hoe dan ook van belang zijn, ongeacht de omvang van de organisatie en de risicocontext. Hiervoor heeft de IBD het ondersteuningstraject Verhogen Digitale Weerbaarheid (VDW) ontwikkeld, met in Module 1 de focus op de basismaatregelen en processen.[2] De basismaatregelen hebben nu ook een aparte markering gekregen in de BIO vragenlijst van de ENSIA-verantwoording. Het doel van deze markering is dat voor zowel bestuurders als professionals bij gemeenten direct inzichtelijk kan worden gemaakt of de basismaatregelen voldoende zijn geïmplementeerd. Kortom, of voldoende effectieve preventieve en impact beperkende maatregelen zijn genomen om informatiebeveiligingsincidenten in de toekomst te voorkomen.

Kanttekening
Informatiebeveiliging valt of staat bij de samenhang aan maatregelen die de daadwerkelijke beveiliging van de organisatie bepalen. Voor een effectieve beveiliging staan maatregelen niet op zichzelf. De momenteel gebruikte set aan maatregelen is specifiek gekoppeld aan de BIO vragenlijst in de ENSIA-verantwoording en bevat niet alle aspecten van de maatregelen uit de ondersteuning van VDW Module 1. Zoals bij alle onderdelen van ENSIA is een ‘afgevinkte’ maatregel nooit een garantie op veiligheid. Ook is compliance geen vervanging voor het uitvoeren van een risicoanalyse of het zelf te blijven interpreteren of risico’s afdoende worden gemitigeerd. Daarentegen is het ontbreken van een basismaatregel wel een belangrijk waarschuwingssignaal.

1 https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/
2 https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/

Managementsamenvatting

Een gedeelte van de vragen die gesteld worden in de BIO-vragenlijst zijn voorzien van het trefwoord 'VDW-1'. Deze vragen zijn geclusterd in 8 verschillende onderwerpen. In de bijlage zijn de vragen opgenomen die horen bij deze clusters. Op basis van de antwoorden in de BIO-vragenlijst wordt de volgende beoordeling gegeven over de onderwerpen die in het kader van VDW Module 1 relevant zijn:

Onderwerp	Status vorig jaar	Huidige status
1. Dringend advies IBD	😐	😐
2. Beheer en bedrijfsmiddelen	😐	😐
3. Toegangsbeveiliging	😐	😐
4. Wachtwoorden	🙂	🙂
5. Change Management	☹	☹
6. Back-up en restore	🙂	🙂
7. Beheer van informatiebeveiligingsincidenten	😐	😐
8. Technische infrastructuur	😐	😐

Legenda: 🙂 = goed 😐 = heeft t.z.t aandacht nodig ☹ = heeft dringend aandacht nodig

Toelichting CISO

1. Dringend advies (2-Factor & kritieke kwetsbaarheden tijdig patchen)

Het risico bestaat dat, als 2-factor authenticatie niet goed is ingevuld, via bruteforce of een gelekte accountinformatie een account gecompromitteerd wordt en gebruikt kan worden voor een datalek of een hack. Het niet binnen een week patchen van kwetsbaarheden met een hoge impact en een hoge kans (high/high) kan ervoor zorgen dat kwaadwillende een kwetsbaarheid misbruiken om in het gemeentelijk netwerk in te breken.

2-factor authenticatie is voor onze digitale werkomgeving de minimale standaard. Aan een loginnaam en een wachtwoord alleen heeft een hacker niet genoeg om binnen te kunnen dringen. Brute force werkt niet bij inloggen op onze werkomgeving, omdat we een limiet op inlogpogingen hebben staan.
De h/h meldingen vanuit de IBD worden door ICT Samen snel en adequaat opgepakt en software indien nodig en mogelijk z.s.m. gepatched. Bij patches die door externe leveranciers doorgevoerd moeten worden zijn we wel afhankelijk van de snelheid van handelen van die leveranciers. Afspraken op dit gebied blijven belangrijk en aandachtspunt in relatie tot leveranciersmanagement.

2. Beheer en bedrijfsmiddelen

Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, mobiele apparatuur niet Is voorzien van de juiste beveiliging en data kan worden gemanipuleerd of gestolen.

Informatie op de door ons beheerde werkapparatuur is goed beveiligd en versleuteld. Patchmanagement en verwijderinstructies op onze apparatuur voldoen aan de norm. Wordt informatie tegen instructies in toch gebruikt op andere apparatuur (bijvoorbeeld in een thuissituatie of bij inhuur externen) dan is dat mogelijk wel een kwetsbaarheid. Advies is daarom om, zoveel als mogelijk, te voorkomen dat er met onbeheerde apparatuur ingelogd wordt op onze werkomgeving. Binnen onze ICT-samenwerking wordt gewerkt aan een gezamenlijke afspraak om bring your own device niet langer toe te staan.

3. Toegangsbeveiliging

Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, onbevoegde toegang krijgen tot gemeentelijke data en een datalek veroorzaken. Daarnaast kunnen medewerkers met te veel rechten

(onbedoeld) veel schade veroorzaken door verkeerde handelingen uit te voeren of, als het account is overgenomen, kan een kwaadwillende de organisatie bewust schade toebrengen.

De toegangsrechten van nieuwe medewerkers zou meer afhankelijk moeten zijn van de functie. De verantwoordelijke teamleider of manager zou moeten kunnen aangeven waartoe een medewerkers toegang nodig heeft. In de praktijk wordt er nu nog veel gewerkt op basis van een profiel van collega's met een vergelijkbare functie. Daarna wordt evt. bekeken of iemand mogelijk te veel rechten heeft. Dit kan beter ingeregeld worden, meer conform roll based acces. Er wordt gewerkt aan een aangepast proces voor toewijzen van rechten voor nieuwe accounts dat in 2025 uitgerold gaat worden.

4. Wachtwoorden
Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, wachtwoorden niet sterk genoeg zijn en accounts daardoor onvoldoende beschermd zijn. Dit kan leiden tot een datalek of een hack.

De maatregelen rondom wachtwoorden in onze werkomgeving voldoet aan de eisen. Steeds meer leveranciers dwingen ook sterke wachtwoorden af om in te kunnen loggen op hun portal. Bovendien werken we ook standaard met 2 factor authenticatie als extra check en waar mogelijk zelfs met MFA. Wel wordt er ook gekeken nog betere en gebruikersvriendelijke methoden om in te loggen op onze werkomgeving.

5. Change Management
Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, wijzigingen niet of onvoldoende getest zijn waardoor de dienstverlening mogelijk (langdurige) niet beschikbaar is en/of (onbedoeld) er kwetsbaarheden in de productieomgeving geïntroduceerd worden.

Er wordt voor de grote en belangrijke systemen gewerkt met gescheiden test- en productieomgeving. Voor wijzigingen in onze informatievoorziening hebben we een Architectuurteam opgericht. Hier worden echter niet alle wijzigingen aangemeld en worden ook niet alle nieuwe systemen van tevoren besproken. Het is noodzakelijk om centraal zicht hebben en houden op alle (significante) wijzigingen in de Informatievoorziening, om risico's te kunnen signaleren en indien nodig maatregelen te kunnen nemen.

6. Back-up en restore
Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, back-ups niet voldoen aan de gewenste eisen en daardoor data onvoldoende teruggezet kan worden, waardoor gegevens verloren gaan. Hierdoor kan de dienstverlening bij een incident potentieel niet voldoende hersteld worden.

Op basis van de verstrekte informatie van ICT Samen kunnen we stellen dat de Backup en Restore maatregelen voldoen aan de gestelde normen. Ook wordt hier nog verder in geïnvesteerd.

7. Beheer van informatiebeveiligingsincidenten.
Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, informatiebeveiligingsincidenten onvoldoende gemeld, opgepakt en geëvalueerd worden om de incidenten in de toekomst te voorkomen. Het gevolg van het niet tijdig aanpakken van informatiebeveiligingsincidenten is dat dit de impact van datalekken en incidenten kan vergroten en zodoende leidt tot reputatieschade en (langdurig) uitvallen van de dienstverlening.

Goede ontwikkeling is dat er steeds meer gegevens beschikbaar komen over beveiligingsincidenten die gemeld of geconstateerd en geregistreerd worden. Aandachtspunt voor de organisatie is dat het soms erg lang duurt, voordat verbetervoorstellen n.a.v. een incident daadwerkelijk uitgevoerd worden. Dat geldt zowel voor technische- als voor procesverbeteringen.

8. Technische infrastructuur.
Het risico bestaat dat, als deze maatregelen niet goed zijn ingevuld, de technische infrastructuur onvoldoende beschermd is en een kwaadwillende zich door het hele netwerk kan verplaatsen. Als logging niet juist is toegepast kan niet worden nagegaan wat er is gebeurd op het moment dat dit nodig is.

ICT Samenwerking heeft besloten om beleid rondom logging op te stellen om meer grip op de uitvoering hiervan te krijgen. Ook liggen er inmiddels adviezen op gebied van netwerksegmentatie en wordt komend jaar mogelijk een complete SIEM/ SOC omgeving in gebruik genomen voor monitoren en beveiligen van onze ICT-infrastructuur. Bij de inrichting nieuw datacentrum in 2025 wordt hier ook aandacht aan besteed om tot verbetering te komen.

Verbetervoorstel CISO

Verbeterpunten voor de organisatie n.a.v. deze rapportage:

• Besteedt meer aandacht aan afspraken met externe softwareleveranciers om te borgen dat zij hun omgeving veilig houden. Denk hierbij o.a. aan afspraken rondom patchen bij kwetsbaarheden.
• Probeer zoveel als mogelijk te voorkomen dat er met onbeheerde apparatuur in onze werkomgeving gewerkt wordt.
• Richt het proces voor het toekennen van rechten van nieuwe medewerkers in conform uitgangspunten van rol based acces zodat we voorkomen dat medewerkers te veel rechten krijgen
• Zorg dat wijzigingen aan onze IV tijdig doorgesproken worden met het Architectuurteam om te voorkomen dat er kwetsbaarheden ontstaan in onze informatievoorziening.
• Verbeterpunten n.a.v. gemelde incidenten blijven nu soms te lang liggen, dat kan beter.
• Vinger aan de pols houden bij ICT Samen op aantal onderwerpen:
    o Vast gaan stellen van een loggingbeleid en de uitvoering daarvan
    o Meer netwerksegmentatie doorvoeren
    o Implementeren van een volledig SIEM SOC systeem

Bijlage: Antwoorden op de vragen

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
1. Dringend advies van de IBD				
9.4.2.1	Worden inlogschermen die publiek of openbaar toegankelijk zijn minimaal afgeschermd met tenminste een 2FA-toegangscontrole mechanisme?	Ja	Door 2-factorauthenticatie (2FA/MFA) af te dwingen wordt de kans op een incident aanzienlijk verkleind. Kwaadwillenden hebben zo niet voldoende aan het enkel verkrijgen van een combinatie van wachtwoord en gebruikersnaam, bijvoorbeeld middels phishing of toepassing van een elders hergebruikt wachtwoord. De Informatiebeveiligingsdienst adviseert gemeenten dringend om per direct 2-factorauthenticatie (2FA/MFA) af te dwingen* op ten minste: • Alle beheeraccounts (intern en extern) • De kantoorautomatisering • E-mailaccounts incl. webmail en webapps • Cloud-toepassingen. *Afdwingen wil zeggen dat inloggen met slechts een gebruikersnaam en wachtwoord niet meer mogelijk is.	
12.6.1.1.a	Worden bij een hoge kans op misbruik en een hoge kans op schade patches uiterlijk binnen een week geïnstalleerd?	Ja	Spoedpatches dienen zo spoedig mogelijk geïnstalleerd te worden om te voorkomen dat de kwetsbaarheden worden misbruikt door kwaadwillende. Bij spoedpatches is de kans op misbruik hoog en is de mogelijke schade ook hoog, ofwel High/High (classificering NCSC). Deze patches dienen zo spoedig mogelijk doorgevoerd, echter maximaal binnen één week (zoals de in BIO vastgelegd). Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerstvolgende onderhoudsronde van het systeem. Bij spoedpatches met de classificering High/High zal de IBD-CERT naast de reguliere waarschuwingen waar nodig ook een SMS versturen. Bij het ontvangen van een dergelijke SMS moet bij de gemeente direct het proces voor spoedpatches worden ingezet. Zorg ervoor dat het proces voor patchmanagement is ingericht en	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			wordt nageleefd. De minimale maatregelen die men met betrekking tot patchmanagement dient te nemen zijn: • Zorg dat er een proces is voor spoedpatches. • Leg afspraken voor patches vast in Sla's. • Volg het Change Managementproces voor de uitrol van patches. • Controleer regelmatig voor relevante patches. Zie voor meer informatie ook de factsheet patchmanagement.	
2. Beheer en bedrijfsmiddelen				
6.2.1.1.c	Worden vertrouwelijke gegevens op mobiele apparatuur versleuteld?	Ja	Het versleutelen van vertrouwelijke gegevens op mobiele apparatuur zorgt ervoor dat de vertrouwelijkheid en integriteit van de data beschermd is. Bij verlies van mobiele apparatuur is de data beschermd tegen onbevoegde inzage. Zie ook de Handreiking telewerkbeleid.	
6.2.1.2.b	Wordt patchmanagement en hardening toegepast op mobiele apparatuur?	Ja, er wordt patchmanagement en hardening toegepast	Door tijdig te updaten en op structurele basis de juiste patches door te voeren kan worden voorkomen dat bekende kwetsbaarheden in software, hardware en besturingssystemen worden misbruikt. Kwetsbaarheden worden in toenemende mate geautomatiseerd misbruikt. Online scans vinden kwetsbare systemen en deze worden met behulp van eenvoudige tools geëxploiteerd. De gevolgen kunnen verstrekkend zijn voor de beschikbaarheid, integriteit en vertrouwelijkheid van systemen. Informatie kan worden gestolen, gewijzigd of versleuteld (ransomware), met alle financiële – en imagoschade van dien. Het is daarom zaak om een kwetsbaarheid zo snel mogelijk te verhelpen zodra een patch beschikbaar is gesteld. Gemeenten kunnen door hun systemen up-to-date te houden veel grote en kleine incidenten voorkomen. Door overbodige software, services en gebruikersaccounts uit te schakelen en/of van de systemen te verwijderen kunnen de aanvalsmogelijkheden op het systeem worden verkleind en nemen de risico's op achterstallige patches af. Dit proces wordt ook wel hardening genoemd. Meer hierover is verder uitgewerkt in het hardeningsbeleid voor gemeenten.	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			Zorg ervoor dat het proces voor patchmanagement is ingericht en wordt nageleefd. Zie voor meer informatie ook de factsheet patchmanagement.	
6.2.1.2.c	Wordt mobiele apparatuur daar waar mogelijk beheerd en beveiligd via een MDM- of MAM-oplossing?	Ja, voor beheer en beveiliging	Door mobiele apparatuur te beheren en beveiligen via een Mobile Device Management of een Mobile Application Management-oplossing, wordt de informatie beschermd. Het is mogelijk om eisen te stellen aan het beheerde apparaat wat ervoor zorgt dat alleen bevoegden toegang krijgen tot de informatie.	
8.3.1.1	Beschikt uw organisatie over een verwijderinstructie voor het verwijderen van gegevens op media die de organisatie verlaten?	Ja	Voorkom hiermee dat vertrouwelijke informatie die op media staat per ongeluk uitlekt door het ontbreken van een duidelijke instructie. Richt het proces voor configuratiemanagement in: • Zorg dat alle configuratiewijzigingen worden gelogd. • Zorg voor een actueel, volledig overzicht van alle configuratie items (CI). Als het inzicht ontbreekt in de hardware en software in de organisatie kan 'shadow-IT' ontstaan, d.w.z. apparatuur en programmatuur die zonder expliciete organisatorische goedkeuring worden gebruikt, waardoor onbekende personen, apparaten of kwetsbaarheden schade kunnen aanrichten binnen het netwerk en de gemeente-organisatie. Zie voor meer informatie ook de factsheet configuratiemanagement.	
3. Toegangsbeveiliging				
6.2.1.1.a	Is de mobiele apparatuur zo ingericht dat geen bedrijfsinformatie op het apparaat wordt opgeslagen (zero footprint)?	Dit is (nog) niet zo ingericht	Door apparaten zo in te richten dat er geen bedrijfsinformatie lokaal wordt opgeslagen, wordt het risico verkleind dat deze informatie bij onbevoegden bekend wordt. Als bedrijfsinformatie niet lokaal wordt opgeslagen, kunnen onbevoegden ook geen toegang krijgen tot deze informatie.	
6.2.1.1.b	Biedt een mobiel apparaat bij het ontbreken van zero footprint, de mogelijkheid om toegang te beschermen door een toegangsbeveiligingsmechanisme en/of versleuteling van de gegevens?	Ja, met een toegangsbeveiligingsmechanisme en versleuteling (van vertrouwelijke	Als het niet mogelijk is om gebruik te maken van zero footprint dan moeten andere maatregelen genomen worden om de kans, dat onbevoegden bij de data komen, wordt verkleind. Door gebruikt te maken van toegangsbeveiligingsmechanismen (bijv. vingerafdruk, pincode of wachtwoordzin) en/of door de informatie te versleutelen	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
		gegevens op apparaat)	wordt de kans dat de informatie wordt ingezien door onbevoegden sterk verkleind.	
6.2.1.1.d	Is het mogelijk om vertrouwelijke informatie op mobiele apparatuur 'op afstand ' te wissen?	Ja	Bij verlies van mobiele apparatuur moet vertrouwelijk informatie op afstand gewist kunnen worden. Indien een apparaat verloren of gestolen is, kan het wissen van deze informatie ervoor zorgen dat de impact van een mogelijk incident verkleind wordt.	
9.1.1.1	Is er vastgesteld beleid voor logische toegangsbeveiliging op basis van need-to-know en need-to-use? De control kent geen verplichte overheidsmaatregelen. Deze maatregel is richtinggevend.	Ja	Medewerkers dienen alleen de rechten te hebben die ze minimaal nodig hebben voor hun werkzaamheden. Te veel rechten kunnen ook door kwaadwillende (intern & extern) misbruikt worden. Beleid zorgt ervoor dat er eenduidige richtlijnen zijn en deze kunnen worden nageleefd. Beheer toegangsrechten en neem maatregelen op in het beleid voor toegangsbeveiliging. De minimale eisen in beleid voor logische toegangsbeveiliging die moeten worden opgenomen zijn: • Gebruik unieke, naar personen herleidbare accounts. • Ken alleen de noodzakelijke rechten toe per rol/account. • Zorg dat het wachtwoord regelmatig moet worden gewijzigd. • Zorg dat het wachtwoord pas na 6 andere wachtwoorden weer mag worden hergebruikt. • Zorg dat op reguliere basis de accounts en bijbehorende rechten worden gecontroleerd. Zie voor meer informatie ook het webinar beheer toegangsbeveiliging op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.1.2.1	Krijgt alleen geauthenticeerde apparatuur toegang tot een vertrouwde zone?	Ja	Alleen geauthentiseerde apparatuur dient toegang te krijgen tot een vertrouwde zone. Dit voorkomt dat apparaten die niet beheerd worden toegang krijgen en daarmee risico's introduceren.	
9.2.1.1	Beschikt uw organisatie over een formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties?	Ja	Om accounts van medewerkers en externe goed te beheren is het nodig dat er een formele procedure is voor het beheren van gebruikersidentificatie. Dit voorkomt dat accounts niet goed geregistreerd worden en accounts niet worden dichtgezet als het niet meer nodig is. Zie voor meer informatie ook het webinar “Beheer	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			toegangsbeveiliging" op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.2.1.2	Is het gebruik van groepsaccounts gemotiveerd en vastgelegd?	Ja	Een groepsaccount wordt door meerdere medewerkers gebruikt en het is erg lastig terug te vinden wie een actie heeft doorgevoerd. Daarom is het van belang het gebruik hiervan te minimaliseren en als het gebruik nodig wordt geacht, dient dit gemotiveerd te worden en dienen deze uitzonderingen centraal te worden gedocumenteerd. Zie voor meer informatie ook het webinar "Beheer toegangsbeveiliging" op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.2.2.1	Wordt toegang tot informatiesystemen alleen verleend na autorisatie door een bevoegd functionaris?	Ja	Door toegang tot informatiesystemen alleen te verlenen nadat deze geautoriseerd is door een bevoegd functionaris wordt er gebruik gemaakt van het need-to-know principe. Het zorgt ervoor dat medewerkers alleen toegang hebben tot systemen waar dat nodig is voor de uitvoering van hun functie.	
9.2.3.1	Worden speciale bevoegdheden minimaal ieder kwartaal beoordeeld?	Nee	Door speciale bevoegdheden te controleren wordt de kans op intern en extern misbruik verkleind. Dit zijn speciale bevoegdheden waarvan de gebruikers moeten weten dat ze extra rechten hebben en die voor meer impact kunnen zorgen dan normale gebruikersaccounts. Geef enkel toegang tot de noodzakelijke set van applicaties en commando's. Maak waar nodig zoveel mogelijk gebruik van two-factor authenticatie. Zie voor meer informatie ook het webinar "Beheer toegangsbeveiliging" op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.2.5.1	Worden voor BBN 1-systemen de toegangsrechten minimaal eenmaal per jaar beoordeeld?	Ja	Controleer de accounts en bijbehorende toegangsrechten frequent en zorg ervoor dat alleen de noodzakelijke rechten per account zijn toegekend om de kans op misbruik met accounts te verkleinen. Zie voor meer informatie ook het webinar "Beheer toegangsbeveiliging" op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.2.5.3	Worden, voor systemen met BBN 2 of hoger, de toegangsrechten minimaal eenmaal per halfjaar beoordeeld?	Ja	Controleer de accounts en bijbehorende toegangsrechten frequent en zorg ervoor dat alleen de noodzakelijke rechten per account zijn toegekend om de kans op misbruik met accounts te verkleinen.	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			Zie voor meer informatie ook het webinar “Beheer toegangsbeveiliging” op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.2.6.1	Worden de toegangsrechten van gebruikers bij wijziging van functie aangepast?	Ja	Medewerkers die van functie wijzigen houden veelal hun oude rechten. Hierdoor kan de impact bij misbruik van een account vergroot worden. Zorg dat er een in de organisatie ingebed proces is voor nieuwe medewerkers, medewerkers die van functie wijzigen en medewerkers die de organisatie verlaten. Zie voor meer informatie ook het webinar “Beheer toegangsbeveiliging” op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
9.4.1.2	Is de toegang tot informatie met een specifiek belang beperkt tot medewerkers die deze informatie nodig hebben voor de uitoefening van hun taak?	Ja	Gebruikers alleen toegang te geven tot informatie als ze dat nodig hebben voor de uitoefening van hun taak, is een onderdeel van het least-privilege-principe. De impact bij misbruik van een account wordt zo verlaagd.	
9.4.4.1	Heeft alleen bevoegd personeel toegang tot systeemhulpmiddelen?	Ja	Geef enkel toegang tot de noodzakelijke set van applicaties en commando’s die personeel nodig heeft om zijn of haar werk te kunnen uitoefenen. Door toegang te beperken kan de kans op incidenten sterk worden verkleind doordat bestaande controles in systemen en applicaties niet eenvoudig kunnen worden omzeild. Zie voor meer informatie ook het webinar “Beheer toegangsbeveiliging” op de webpagina voor het ondersteuningstraject Verhogen Digitale Weerbaarheid.	
4. Wachtwoorden				
9.4.3.1.a	Wordt afgedwongen dat, als two-factor authenticatie niet mogelijk is, dat wachtwoorden voldoen aan aanvullende complexiteitseisen?	Ja	Zwakke wachtwoorden kunnen door middel van bijvoorbeeld het (al dan niet geautomatiseerd) raden van wachtwoorden een kwetsbaarheid vormen met potentieel veel impact op de organisatie. Door minimaal een sterk, uniek wachtwoord af te dwingen kan de kans op een incident verkleind worden. Zie voor meer informatie over wachtwoordbeleid ook de handreiking van de Informatiebeveiligingsdienst.	
9.4.3.3	Worden de eisen aan wachtwoorden geautomatiseerd afgedwongen?	Ja	Door technisch af te dwingen dat wachtwoorden voldoen aan de gestelde eisen is het onmogelijk om een zwak wachtwoord te	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			gebruiken en zal dit niet een kwetsbaarheid vormen met potentieel veel impact op de organisatie. Zie voor meer informatie over wachtwoordbeleid ook de handreiking van de Informatiebeveiligingsdienst.	
9.4.3.4.a	Voldoen initiële wachtwoorden aan de gestelde eisen?	Ja	Initiële wachtwoorden die voor nieuwe accounts worden gemaakt, moeten voldoen aan de gestelde eisen. Hierdoor zal dit niet zo snel een kwetsbaarheid vormen met potentieel veel impact op de organisatie. Zie voor meer informatie over wachtwoordbeleid ook de handreiking van de Informatiebeveiligingsdienst.	
9.4.3.4.b	Voldoen geresette wachtwoorden aan de gestelde eisen?	Ja	Wachtwoorden die zijn gereset moeten voldoen aan de eisen. Hierdoor zal dit niet zo snel een kwetsbaarheid vormen met potentieel veel impact op de organisatie. Zie voor meer informatie over wachtwoordbeleid ook de handreiking van de Informatiebeveiligingsdienst.	
5. Change Management				
12.1.2.1	Beschikt uw organisatie over een procedure voor wijzigingenbeheer die voldoet aan de gestelde eisen?	Ja	Alle IT-systemen en applicaties zijn de gehele levensduur aan wijzigingen onderhevig. Om de ICT-omgeving te vernieuwen zonder disrupties is een goed Change Managementproces van belang. Change Management kan worden toegepast om patchmanagement op een gecontroleerde wijze te organiseren. Daarmee kunnen ICT-systemen up-to-date gehouden en schade aan of misbruik van ontstane kwetsbaarheden in software en hardware worden voorkomen. De mogelijke schade hierbij kan variëren van een kleine verstoring tot serieuze incidenten als ransomware of datalekken, met grote financiële en imagoschade tot gevolg. Change Management kan ook toegepast worden voor het uitfaseren van oude software of hardware, maar ook het implementeren van verschillende beveiligingsmaatregelen in bijvoorbeeld het netwerk van de organisatie. De toepassing is veelzijdig en het is van groot belang voor het verhogen van de digitale weerbaarheid.	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			Zorg voor een passende inrichting van het Change Managementproces. Zie voor meer informatie ook de factsheet Change Management.	
12.1.4.1	Wordt er getest in een andere omgeving dan de productieomgeving?	Ja, er wordt niet in de productieomgeving getest	Door wijzigingen in een andere omgeving te testen dan de productieomgeving wordt de kans op een incident in de productieomgeving verkleind. Zo hebben fouten in de ene omgeving geen directe gevolgen voor de productieomgeving. Corruptie van gegevens of verstoringen kunnen daarmee in het proces van wijzigingsbeheer worden voorkomen. Deze scheiding wordt in de ICT ook wel OTAP-genoemd (Ontwikkeling, Test, Acceptatie en Productie). Soms is dit alleen een acceptatie- en een productieomgeving. Ook dan is scheiding van beide omgevingen beter dan een wijziging direct uit te rollen in de productieomgeving, met alle mogelijke verstoringen en fouten van dien. Zie voor meer informatie ook de factsheet Change Management.	
12.1.4.2	Worden wijzigingen in de productieomgeving getest voordat ze in productie worden genomen?	Ja	Door wijzigingen in een andere omgeving te testen dan de productieomgeving wordt de kans op een incident in de productieomgeving verkleind. Zo hebben fouten in de ene omgeving geen directe gevolgen voor de productieomgeving. Corruptie van gegevens of verstoringen kunnen daarmee in het proces van wijzigingsbeheer worden voorkomen. Deze scheiding wordt in de ICT ook wel OTAP-genoemd (Ontwikkeling, Test, Acceptatie en Productie). Soms is dit alleen een acceptatie- en een productieomgeving. Ook dan is scheiding van beide omgevingen beter dan een wijziging direct uit te rollen in de productieomgeving, met alle mogelijke verstoringen en fouten van dien. Zie voor meer informatie ook de factsheet Change Management.	
14.1.1.1	Vindt een expliciete risicoafweging plaats bij nieuwe informatiesystemen en wijzigingen op bestaande informatiesystemen?	Ja	Door een expliciete risicoafweging te maken bij nieuwe informatiesystemen en wijzigingen op bestaande informatiesystemen kan worden gekeken naar mogelijk risico's die voor kunnen komen en kunnen daarop passende maatregelen worden genomen. Voor nieuwe informatiesystemen is het inkoopproces van belang. Voor wijzigingen is het Change Managementproces van belang. Zorg ervoor dat het Change Advisory Board (CAB) voldoende betrokken is bij het Change Managementproces. Mocht deze nog niet afdoende	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			zijn aangewezen, dan is het van belang dat een goed functionerend CAB alsnog wordt opgezet of dat op een andere wijze expliciete risicoafwegingen plaatsvinden bij nieuwe informatiesystemen en wijzigingen op bestaande systemen. In dit CAB is alle expertise aanwezig om wijziging te goed kunnen beoordelen. Wijzigingen hebben steeds goedkeuring nodig van het CAB voordat deze doorgevoerd kunnen worden. Maak hier eenduidige afspraken over die binnen de organisatie ook praktisch uitvoerbaar zijn en daadwerkelijk worden nageleefd. Zie voor meer informatie ook de factsheet Change Management.	
14.2.2.1	Vindt wijzigingsbeheer plaats op basis van een algemeen geaccepteerd beheerframework?	Ja	Door gebruik te maken van een geaccepteerd beheerframework wordt de kans op fouten bij wijzigingen verkleind. Alle IT-systemen en applicaties zijn de gehele levensduur aan wijzigingen onderhevig. Om de ICT-omgeving te vernieuwen zonder disrupties is een goed Change Managementproces van belang. Zijn de voorgestelde changes wel getest en werkt alles naar verwachting? Controleer hierop en verbeter waar nodig bestaande processen en procedures. Zie voor meer informatie ook de factsheet Change Management.	
6. Back-up en restore				
12.3.1.1	Is er een vastgesteld back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd?	Ja	Een goed back-up en recoveryproces zorgt ervoor dat er na een incident snel weer de juiste informatie teruggeplaatst kan worden en er zo min mogelijk informatie verloren gaat. Waarna de normale werkzaamheden weer hervat kunnen worden. Back-ups kunnen de impact van een incident drastisch verlagen en de hersteltijd van een incident sterk verkorten waardoor de gemeente snel weer door kan met de bedrijfsvoering. Goede back-ups zijn ook een zeer belangrijke maatregel tegen ransomware. Zie voor meer informatie ook de handreiking back-up en recovery gemeente.	
12.3.1.2	Is op basis van een expliciete risicoafweging bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident?	Ja	De omvang en frequentie van de back-ups dient in overeenstemming te zijn met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens en systemen.	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			Zie voor meer informatie ook de handreiking back-up en recovery gemeente.	
7. Beheer van informatiebeveiligingsincidenten				
7.2.1.1	Is iedereen in staat om anoniem en veilig beveiligingsissues te kunnen melden?	Ja	Het is belangrijk dat beveiligingsissues vertrouwelijk gemeld kunnen worden en dat medewerkers zich niet belemmerd voelen in het doen van meldingen. Zo wordt er een cultuur gecreëerd waar continu verbeteringen kunnen worden doorgevoerd. Bij twijfel dient er altijd te worden gemeld.	
16.1.2.1	Beschikt uw organisatie over een meldloket waar beveiligingsincidenten kunnen worden gemeld?	Ja	Als medewerkers incidenten snel kunnen melden, dan kunnen incidenten en kwetsbaarheden sneller worden opgemerkt en verholpen. Hiermee kan potentiële schade bij misbruik van een kwetsbaarheid aanzienlijk worden beperkt. Zorg ervoor dat er altijd melding wordt gedaan bij vermoeden van een informatiebeveiligingsincident. Dit kan in veel gevallen in eerste instantie bij de ICT-servicedesk en bij vermoedens van incidenten met een grote impact ook rechtstreeks bij de CISO. Zie voor meer informatie ook de factsheet incidentmanagement.	
16.1.2.2	Beschikt uw organisatie over een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven?	Ja	Doordat het duidelijk is wie welke taken en verantwoordelijkheden hebben binnen de organisatie, kunnen mogelijk incidenten snel opgelost worden en blijven er geen zaken liggen omdat verantwoordelijkheden onvoldoende duidelijk zijn belegd. Zie voor meer informatie ook de factsheet incidentmanagement.	
16.1.2.3	Zijn interne en externe medewerkers op de hoogte van de meldingsprocedure van incidenten?	Ja	Als medewerkers incidenten snel kunnen melden, dan kunnen incidenten en kwetsbaarheden sneller worden opgemerkt en verholpen. Hiermee kan potentiële schade bij misbruik van een kwetsbaarheid aanzienlijk worden beperkt. Belangrijk is dat voor iedere medewerker duidelijk is waar incidenten kunnen worden gemeld en dat er een open cultuur is om te melden. Laat bij twijfel altijd iemand melden. Zie voor meer informatie ook de factsheet incidentmanagement.	
16.1.2.5	Is de proceseigenaar gewezen op zijn verantwoordelijkheid voor het oplossen van beveiligingsincidenten?	Ja	Door een proceseigenaar te wijzen op zijn verantwoordelijkheid zal het mitigeren van beveiligingsincidenten sneller opgelost worden en kunnen eventuele structurele oplossingen doorgevoerd worden, waardoor dezelfde incidenten minder vaak zullen voorkomen. Zorg er	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			daarom voor dat het proces voor Incident Management voor informatiebeveiligingsincidenten is ingericht, dat deze regelmatig wordt geoefend en waar dat deze waar nodig wordt aangescherpt: Weet wie de proceseigenaar nodig heeft bij het oplossen van een informatiebeveiligingsincident, denk aan leveranciers, dienstverleners en collega's. Zorg ook dat deze mensen bekend zijn en kunnen worden bereikt. Zorg ook dat relevante stakeholders tijdig worden geïnformeerd. Dit zal in veel gevallen in ieder geval de Chief Information Security Officer (CISO) zijn. Maar in veel gevallen is dit bij grotere incidenten ook het management en bijvoorbeeld de gemeentesecretaris. Ook relevante functionarissen van de ICT-afdeling dienen tijdig betrokken te worden bij het afhandelen van het incident. Maak hierover duidelijke afspraken, dan weet men elkaar sneller te vinden als er daadwerkelijk sprake is van een incident met mogelijk hoge impact. Zie voor meer informatie ook de factsheet incidentmanagement.	
16.1.4.1	Worden beveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beveiliging (BIV) van informatieverwerkende systemen, uiterlijk binnen 72 uur gemeld aan de sectorale CERT?	Ja	Meld (grote) informatiebeveiligingsincidenten via de vertrouwde contactpersoon van de gemeente (VCIB) bij de Informatiebeveiligingsdienst. Doe dit uiterlijk binnen 72 uur. Eventueel kan dit ook iemand anders zijn als bijvoorbeeld de CISO. Daarbij kan de IBD-CERT (Computer Emergency Response Team) direct voorzien van advies in het afhandelen van het incident en waar nodig escaleren naar andere gemeenten. Mochten meerdere gemeenten last hebben van hetzelfde incident dan kan de IBD optreden als contactpersoon richting de leverancier. Zie de webpagina Ondersteuning aan gemeenten bij incidenten over de ondersteuning die de IBD aan gemeenten kan bieden als zich een incident voordoet.	
16.1.6.1	Wordt de informatie verkregen uit het beoordelen van beveiligingsmeldingen, geëvalueerd met als doel beheersmaatregelen te verbeteren?	Ja	Incidenten zijn nooit helemaal te voorkomen. Daarom is het van groot belang dat de gemeentelijke organisatie is voorbereid voor als het toch mis gaat en dat wordt geleerd van informatiebeveiligingsincidenten die al hebben plaatsgevonden. Dit voorkomt ook dat medewerkers (veel) tijd kwijt zijn met dezelfde incidenten of dat dezelfde incidenten op een andere manier worden behandeld. • Leer van (grote) informatiebeveiligingsincidenten in bespreking met het team en in rapportage. Welke vervolgstappen en	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			maatregelen dienen te worden genomen om het incident in de toekomst te voorkomen? Hoe kan het Incident Managementproces worden verbeterd? Belangrijk is dat incidenten op een centrale plek worden gedocumenteerd. • Maak gebruik van trends om verbeteringen te initiëren. • Leer ook van beveiligingsincidenten die al hebben plaatsgevonden. Goede voorbeelden hiervan bij gemeenten zijn de lessen van de hack bij de gemeente Lochem juni 2019, de hack bij de gemeente Hof van Twente, maar ook de Citrix-crisis januari 2020. Van deze incidenten zijn factsheets opgesteld met beschrijvingen en adviezen op deze incidenten. Maak handig gebruik van wat anderen al hebben geleerd. Links naar deze documenten zijn te vinden in de factsheet Incident Management. Zie voor meer informatie ook de factsheet Incident Management.	
8. Technische infrastructuur				
12.4.1.1	Is logging zo ingericht dat de logregels voldoen aan het logbeleid?	Nee	Wordt er voldoende gelogd? Logging is nodig om te controleren wat er is gebeurd. Vooral tijdens een incident is het belangrijk dat alle informatie beschikbaar is zodat duidelijk is welke acties zijn uitgevoerd en wat er precies is geraakt. Als periodiek naar de logging wordt gekeken kunnen eventuele verdachte situaties gedetecteerd worden (zowel van de medewerkers als kwaadwillende). Tevens is dit een vereist voor monitoring en response.	
12.4.1.3	Maakt uw organisatie gebruik van voorzieningen voor het detecteren van aanvallen, waarbij dit gebruik gebaseerd is op een risico-inschatting?	Ja	Het detecteren van aanvallen is van zeer groot belang bij het verkleinen van de impact van een aanval. Door tijdig te signaleren dat kwaadwillenden inbreken op systemen van gemeenten, kan hier snel tegen worden opgetreden en kan zelfs de aanval grotendeels worden tegengehouden. Het is erg belangrijk om gebruik te maken van en te acteren op de signalen die uit de detectie komen.	
13.1.2.1	Wordt het in- en uitgaande dataverkeer bewaakt / geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen zoals de toelichting uit de maatregel voorschrijft?	Ja	IDS/IPS-systemen zijn belangrijke maatregelen om netwerk en computersystemen te beschermen tegen schadelijke activiteiten en aanvallen. Het vermindert de kans op gegevensdiefstal, systeemcompromissen en andere cyberaanvallen. Daarnaast biedt het de mogelijkheid om snel te reageren op aanvallen en bedreigingen	

Vraagnr	Vraag	Antwoord	Toelichting	Opmerking CISO
			waardoor de schade, die aan systemen en gegevens kan worden toegebracht, wordt geminimaliseerd.	
13.1.3.1	Wordt segmentatie toegepast in netwerken om verschillende groepen van elkaar te scheiden?	Ja	Netwerksegmentatie is het opknippen van het totale netwerk in kleinere segmenten, met tussen de segmenten een beveiligd koppelvlak. Dit zorgt ervoor dat kwaadwillende die zich in een netwerksegment bevindt niet direct ongehinderd toegang heeft tot andere netwerksegmenten. Een belangrijke maatregel die de impact van een kwaadwillende sterk verkleind.	