Uitwerking van het tactische beleid logische toegangsbeveiliging

Documentinformatie

Hoofdauteurs:

Dorinie Edelaar – CISO

Patriek Nouwen – Ondersteunend ISO

Versie	Datum	Gewijzigd door	Wijziging
20-05	20-05-2020	Patriek Nouwen	Na afstemmen met M. Noij en D. Edelaar wijzigingen doorgevoerd.
17-07	17-07-2020	Patriek Nouwen	Opmerkingen en aanvullingen van diverse betrokkenen verwerkt en doorgevoerd.
14-08	14-08-2020	Patriek Nouwen Dorinie Edelaar	Basisversie gereed na verwerking opmerkingen en review D. Edelaar.

Inhoud

1.1. Inleiding

Om informatieveiligheid en privacy van werknemers en burgers te beheersen dient de proceseigenaar voor zijn proces in te richten wie er wanneer toegang heeft tot informatie. Dit wordt logische toegangsbeveiliging genoemd.

Deze uitwerking van het tactisch beleid voor logische toegangsbeveiliging[1] biedt de proceseigenaar, technisch beheerder, functioneel beheerder, applicatiebeheerder, Decentraal Security en Privacy Officer (DSPO) en de AOG-medewerkers die betrokken zijn in het IDU-proces een handvat om beveiligingsmaatregelen te implementeren waarmee zij informatiebeveiliging- en privacy-risico's kunnen minimaliseren tot een acceptabel niveau.

Wanneer volg je deze uitwerking?
Heb je een verantwoordelijkheid ten aanzien van de toegang tot informatie in applicaties of apparatuur? Dan is deze uitwerking logische toegangsbeveiliging van toepassing op jou. Dit houdt in dat de applicaties en apparatuur aan deze tactische uitwerking getoetst dienen te worden. Dit geldt voor zowel nieuwe als bestaande applicaties en apparatuur. Denk hierbij ook aan nieuwe ontwikkelingen binnen een proces (wat invloed kan hebben op de rollen en autorisaties).

Afwijkingen van tactische uitwerking
Het kan voorkomen dat het niet mogelijk of wenselijk is om aan alle punten van de uitwerking te voldoen. Dit brengt echter een risico met zich mee. Aan de hand van (het uitvoeren van) een risicoanalyse dient de proceseigenaar vooraf een risicoafweging te (laten) maken en wordt de proceseigenaar geadviseerd door de DSPO. De proceseigenaar bepaalt uiteindelijk of wordt afgeweken van de tactische uitwerking en stelt vast welk risico degene hierbij neemt. Dit risico dient de proceseigenaar vast te leggen. De risico's kunnen worden voorgelegd aan de directie en/of het bestuur. Op deze wijze krijgen zij inzicht in de gelopen risico's.

1.1.1. Opbouw tactische uitwerking

In deze tactische uitwerking wordt uitgelegd wat logische toegangsbeveiliging is en waarom je het toepast. Verder wordt de scope waarop het van toepassing is en de rollen en verantwoordelijkheden nader toegelicht. Vervolgens worden randvoorwaarden aangegeven om logische toegangsbeveiliging te kunnen borgen. Daarna worden onderstaande aspecten van logische toegangsbeveiliging toegelicht:

Stap	**Uitleg**
Het beheer van identiteiten	Identiteitsgegevens zijn gegevens die toebehoren aan een natuurlijk persoon en waarmee deze zich kan identificeren. Denk aan: naam, gebruikersnaam, personeelsnummer, BSN (Hoofdstuk 2).
Authenticatie en wachtwoordbeleid	Authenticatie is het proces waarbij nagegaan wordt of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Het wachtwoordbeleid geeft richting en middelen voor het omgaan met wachtwoorden. (Hoofdstuk 3).
Het beheer van autorisaties	Het proces dat zorgt dat de juiste autorisaties worden gekoppeld aan de juiste taken, functies en verantwoordelijkheden en dat deze toegekend worden aan de juiste personen. Het opstellen van de autorisatiematrix wordt hier nader toegelicht(Hoofdstuk 4).

[1] Uitwerking van het tactische informatiebeveiligingsbeleid: onderdeel logische toegangsbeveiliging.

Instroom, doorstroom & uitstroom	Het proces waarbij aan personen (intern/extern) autorisaties worden toegekend of ingetrokken omdat zij toetreden tot onze organisatie, van functie veranderen binnen onze organisatie of onze organisatie verlaten. (Hoofdstuk 5).
Controle	De borging in en op de processen van logische toegangsbeveiliging die ervoor zorgt dat de uitgegeven autorisaties juist, volledig en actueel zijn en blijven (logging en monitoring op logische toegangsbeveiliging: (Hoofdstuk 6).

1.1.2. Wat en waarom logische toegangsbeveiliging?

Logische toegangsbeveiliging is het geheel aan maatregelen die tot doel hebben de toegang tot gegevens en informatiesystemen te beheersen zodat gegevens, applicaties, apparatuur en resources worden beschermd tegen ongeautoriseerde acties. Onder acties wordt onder andere verstaan: creëren, raadplegen, verwijderen, wijzigen en gebruik.[2]

Een goed ingericht proces leidt ertoe dat oneigenlijk gebruik zoveel mogelijk wordt tegen gegaan en dat de juiste personen toegang hebben. Processen worden hierdoor voorspelbaarder en meer beheersbaar. Logische toegangsbeveiliging maakt inzichtelijk of risico's binnen processen tot een acceptabel niveau zijn geborgd, of voldaan wordt aan wetgeving en toont zorgvuldige omgang van persoonsgegevens richting burgers en ketenpartners aan. Onduidelijke of niet (voldoende) nageleefde procedures voor logische toegangsbeveiliging kunnen leiden tot:

1. Medewerkers die niet of niet tijdig de juiste autorisaties hebben, waardoor men niet of minder effectief kan werken.
2. Onbevoegden toegang tot middelen en informatie, met hierdoor hogere kans op fraude, fouten, onrechtmatige verwerkingen en datalekken.
3. Hogere licentiekosten doordat applicaties meer gebruikers hebben dan benodigd.

Dit is een bedreiging voor de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatie en is daarmee een bedreiging voor de dienstverlening van de gemeente. Dit kan leiden tot o.a. financiële en persoonlijke schade en tot schade voor het imago van de gemeente.

Daarnaast schrijft de AVG voor dat een organisatie inzichtelijk moet kunnen maken wie toegang heeft gehad tot bepaalde gegevens. Het toepassen van logische toegangsbeveiliging is hierbij een essentiële stap.

1.1.3. Scope: Waar pas je logische toegangsbeveiliging op toe?

Zoals aangegeven heeft logische toegangsbeveiliging als doel de juiste mensen toegang te geven tot de juiste middelen en gegevens. En tegelijkertijd is het doel toegang door onbevoegden te voorkomen. Deze middelen en gegevens zijn vanzelfsprekend beschikbaar in de applicaties, maar ook op minder voor de hand liggende plekken. Om logische toegangsbeveiliging in de keten te borgen pas je logische toegangsbeveiliging daarom toe op:

- De geautomatiseerde informatiesystemen (applicaties);
- De gegevens en informatie die zijn vastgelegd met behulp van deze informatiesystemen;
- De omgevingen (ontwikkeling/test/acceptatie/productie);
- De besturingssystemen en databasemanagementsysteem (DBMS);
- De hulpmiddelen (ontwikkel- en querytools);

2 IBD - Handreiking Beleid Logische Toegangsbeveiliging v2.0

- De netwerken en infrastructuur (inclusief hardware) waarmee toegang tot computersystemen wordt verkregen.

1.1.4. Rollen & Verantwoordelijkheden

Hieronder zijn de rollen en verantwoordelijkheden nader toegelicht:

- De proceseigenaar zijnde de afdelingsmanager is verantwoordelijk voor een correcte naleving van het informatiebeveiligingsbeleid door zijn medewerkers. Hierbij kan de eigenaar eventueel taken delegeren, maar blijft verantwoordelijk. De proceseigenaar is verantwoordelijk voor het veilig functioneren van de processen die een wisselwerking hebben met applicaties en andere domeinen. De proceseigenaar is daarmee ook verantwoordelijk voor de beschikbaarheid, de integriteit (juist, volledig en tijdig) en de vertrouwelijkheid van gegevens die verwerkt worden binnen zijn proces. Dit houdt ook in dat de proceseigenaar zorg moet dragen dat de vereisten voor de applicatie bekend zijn bij de applicatie-eigenaar (of eigenaren bij generieke applicaties). De applicatie-eigenaar moet zorgen dat de applicatie aan de vereisten van het proces voldoet. De proceseigenaar is verantwoordelijk voor de juiste toekenning van autorisaties in de applicatie. Een belangrijk onderdeel hiervan is dat de proceseigenaar tijdig een signaal doorgeeft indien een wijziging van autorisaties benodigd is.
- De gegevenseigenaar is verantwoordelijk voor de juistheid van de gegevens in het informatiesysteem van de onder hun vallende gegevens. Dit is momenteel de proceseigenaar.
- De functioneel beheerder (FB) is verantwoordelijk voor het tegen overeengekomen kosten en kwaliteit in stand houden van de gewenste informatievoorziening ten behoeve van de gebruikersorganisatie tijdens de gehele levenscyclus van informatiesystemen. De FB zorgt ervoor dat de applicatie goed aansluit op de processen van het betreffende domein of de afdeling.
  Voor logische toegang houdt dit in dat de functioneel beheerder zich samen met de proceseigenaar richt op de inrichting van autorisaties binnen de gestelde kaders van de proceseigenaar. Daarnaast zorgt de functioneel beheerder dat de processen zijn ingericht rondom het wijzigen en controleren van autorisaties.
- De applicatiebeheerder is verantwoordelijk voor het tegen de overeengekomen kosten en kwaliteit in stand houden en onderhouden van de bedrijfsapplicaties en de bijbehorende gegevensverzamelingen tijdens de gehele levenscyclus van de informatiesystemen.
  De applicatiebeheerder richt zich op de wijze waarop de applicatie aansluit op de behoeften van de gebruikersorganisatie. De applicatiebeheerder richt zich niet op de gegevens die in de applicatie zitten en niet op de infrastructuur waar ze op landen/geland zijn.
  Voor logische toegang houdt dit in dat de applicatiebeheerder zich richt op de technische inrichting van de wijze waarop gebruikers zichzelf authentiseren tegen de applicatie (wachtwoordinstellingen, multifactor authenticatie, Single Sign On).
  Bij SAAS-applicaties ligt (een groot deel van) het applicatiebeheer bij de applicatiebeheerder van de SAAS-leverancier en coördineert de applicatiebeheerder van de gemeente Helmond de acties en communicatie met de leverancier.
- De technisch beheerder is verantwoordelijk voor het in stand houden, beheren en onderhoud van de IT-infrastructuur. De technisch beheerder richt zich niet op de applicaties of de gegevens. De technisch beheerder zorgt ervoor dat servers beschikbaar en bereikbaar blijven. Daarmee ook de servers voor *on premise* applicaties. Bij SAAS-applicaties ligt het technisch beheer bij de SAAS-leverancier.
  Voor logische toegang betekent dit het volgende: Ook op de technische infrastructuur zijn autorisaties benodigd. Denk hierbij aan autorisaties voor op de servers, netwerk, databases, firewalls, Intrusion Detection System (IDS) / Intrusion Protection System (IPS), antimalware-applicaties, Operating System (zoals Windows) en dergelijke. Ook deze autorisaties dienen conform een proces te worden beheerd.
  Daarnaast richt de technisch beheerder zich op de technische inrichting van de wijze waarop

gebruikers zichzelf authentiseren in de ICT-infrastructuur (wachtwoordinstellingen, multifactor authenticatie, Single Sign On).
Voor SAAS-applicaties betekent dit dat over de maatregelen afspraken moeten zijn gemaakt met de leverancier. Vanzelfsprekend ligt deze verantwoordelijkheid niet bij de technisch beheerder, maar bij de eigenaar van het contract.

- De proceseigenaar AOG is verantwoordelijk voor de borging van de kwaliteit van de centrale registratie van (externe) medewerkers en het verwerken en doorsturen van signalen bij indiensttredingen, van wijzigingen van functies/medewerkers en uitdiensttredingen.
- De Decentrale Security en Privacy Officer (DSPO) ziet erop toe dat de rollen, verantwoordelijkheden en processen/procedures ten aanzien van logische toegangsbeveiliging zijn ingevuld en effectief zijn. Hij adviseert bij de inrichting en draagt bij aan bewustwording. Daarnaast controleert de DSPO of is voldaan aan de vereiste maatregelen en het beleid.

1.1.5. Wat zijn de randvoorwaarden?

Voor een juiste inrichting van logische toegangsbeveiliging gelden de volgende randvoorwaarden:

- Er is een overzicht van bedrijfsmiddelen (CMDB) beschikbaar[3] met de bijbehorende eigenaren (onder verantwoordelijkheid van IVA).
- Het eigenaarschap van gegevens en processen is belegd bij de proceseigenaar en is bepaald door de directie.
- Het eigenaarschap van applicaties is belegd bij de applicatie-eigenaar. Vooralsnog is dit de proceseigenaar.
- Er is een overzicht van technisch beheerders beschikbaar, met hierin zichtbaar voor welke infrastructuurcomponenten (zoals servers, databases, firewalls en beheertools (zoals voor netwerk monitoring, configuratiemanagement en gebruikersbeheer) zij het beheer uitvoeren. Hierbij dient duidelijk te zijn welke beheerder toegang heeft tot welke componenten van de ICT-infrastructuur en beheertools.
- Er is een overzicht van applicatie beheerders beschikbaar, met hierin zichtbaar voor welke applicatie zij het beheer uitvoeren (onder verantwoordelijkheid van IVA)
- Er is een overzicht van functioneel beheerders beschikbaar, met hierin zichtbaar welke functioneel beheerder gebruikers aanmaakt en toegang verleent tot welke applicaties en/of gegevens (onder verantwoordelijkheid van IVA).
- De proceseigenaar heeft een classificatie van informatie uitgevoerd[4] (proceseigenaren).
- Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van applicaties en/of gegevens. Dit is de verantwoordelijkheid van de proceseigenaren.
    - Er is een overzicht beschikbaar met daarin welke functies worden uitgevoerd door welke medewerker (onder verantwoordelijkheid van AOG).
    - De proceseigenaar leidt de bevoegdheid van een persoon af van zijn taak, functie, rol of verantwoordelijkheid.
    - De proceseigenaar accordeert het verlenen van toegang tot een applicatie / gegevens[5].
    - Er is een overzicht van wel en niet toegestane combinaties van taken en rollen beschikbaar per applicatie[6] en over verschillende applicaties heen.
- Niemand mag autorisaties hebben om een gehele cyclus van handelingen in een proces te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Hier mag alleen aan de hand van een zichtbaar uitgevoerde risicoanalyse van worden afgeweken.

3 Bron: Configuration Management Database (CMDB)

4 Zie handreiking risicomanagement

5 Functioneel beheerder houdt dit actueel voor zijn applicaties

6 Functioneel beheerder houdt dit actueel voor zijn applicaties

- Daar waar mogelijk is er functiescheiding tussen beheertaken en overige gebruikerstaken. Ook dient er scheiding te zijn voor beheertaken in productie- en testomgevingen. Het kan voor komen dat gebruikerstaken en beheertaken toch door dezelfde medewerker uitgevoerd moeten worden. Indien het technisch mogelijk is, worden beheerwerkzaamheden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.

2. Het beheer van identiteiten

Vanuit de optiek van informatiebeveiliging is identificatie de eerste stap in het autorisatieproces. De tweede stap is de authenticatie, het vaststellen van de juistheid van de opgegeven identiteit. De derde stap in dit proces is autorisatie, het vaststellen of een medewerker de rechten krijgt die hij nodig heeft voor de uitvoering van zijn functie, rol.

2.1. Identificeren (externe) medewerkers

Relevant voor: AOG-medewerker, proceseigenaar, technisch beheerder, applicatiebeheerder, functioneel beheerder, Servicedesk-medewerker.

Iedereen dient zich te kunnen identificeren met een geldig identiteitsbewijs, ook op de werkplek. Als werkgever ben je verplicht de identiteit van je (externe) medewerkers te controleren, voordat deze medewerker toegang krijgt tot gemeentelijke faciliteiten. Voor interne medewerkers dient deze identificatie plaats te vinden aan de hand van het originele identiteitsbewijs [7]. Identificatie vindt plaats door de afdeling AOG (daarnaast is AOG verplicht om een kopie te maken vanuit de wet op loonbelasting). Voor externe medewerkers geldt dat de identiteit van de medewerker bekend dient te zijn gemaakt bij het overeenkomen van de dienstverlening. Op basis hiervan kunnen het account, de applicaties en de apparatuur voorbereid worden. Hiermee is AOG het enige punt van waarheid (Single Point Of Truth (SPOT)), waardoor gewaarborgd wordt dat autorisatieprocessen centraal geregeld kunnen worden. Bij de eerste werkdag van de externe medewerker legitimeert deze zich aan de hand van een origineel identiteitsbewijs[8] bij de uitgifte van het account en de uitgifte van de apparatuur (kopie maken bij de uitgifte van apparatuur is verboden). Indien de identiteit is bepaald krijgt iemand toegang tot de apparatuur, het netwerk, de applicaties en vervolgens toegang tot informatie. De proceseigenaar bepaalt of een medewerker toegang krijgt tot deze informatie.

Het is in ieder geval niet toegestaan om een kopie van het identiteitsbewijs van de medewerker op te laten sturen of mailen (mail is überhaupt geen geschikt middel voor het uitwisselen van gevoelige documenten). Dit levert een extra risico op voor de eigenaar van het identiteitsbewijs (de kopie kan ook voor andere doeleinden gebruikt worden). Een malafide partij kan namelijk ook een identiteitsbewijs van een ander gebruiken.

2.2. Identiteit in applicatie

Relevant voor: technisch beheerder, applicatiebeheerder, functioneel beheerder.

Binnen applicaties is het van belang dat de identiteit van de gebruiker kenbaar gemaakt wordt aan de applicatie. De identiteit wordt gebruikt om de toegang van deze gebruiker tot een applicatie te beheersen (autorisatie). Het doel is dat acties van een gebruiker herleidbaar zijn naar diezelfde gebruiker. Indien meerdere gebruikers of processen hetzelfde account gebruiken, is een actie niet meer herleidbaar naar de ene gebruiker.

---

[7] Artikel 1 Wet op de identificatieplicht (Wid). Bij indiensttreding is identificatie met een rijbewijs niet mogelijk omdat er de werkgever de verblijfsstatus en/of nationaliteit moet vaststellen en, deze gegevens staan niet op het rijbewijs (Wet arbeid Vreemdelingen). De inhoudsplichtige stelt de identiteit vast en houdt een afschrift ter controle beschikbaar bij de administratie. (artikel 7.5 lid 1 Uitvoeringsregeling loonbelasting 2011)

[8] Artikel 1 Wet op de identificatieplicht (Wid). Bij indiensttreding is identificatie met een rijbewijs niet mogelijk omdat de inlener de verblijfsstatus en/of nationaliteit moet vaststellen en, deze gegevens staan niet op het rijbewijs (Wet arbeid Vreemdelingen 2011). Als inlener ben je aansprakelijk voor niet door de uitlener betaalde loonheffing (inlenersaansprakelijkheid). De aansprakelijkheid wordt gematigd als (o.a.) de identiteit van de werknemer kan worden aangetoond (zie artikel 34.8.2 van de Leidraad invordering)

2.2.1. Voorwaarden identiteit:

- Binnen Helmond is iedere gebruiker naar een unieke identiteit te herleiden.
    - Technisch beheer: Dit geldt voor het centrale account waarmee alle gebruikers van gemeente Helmond in loggen ((Azure) Active Directory). Daarnaast geldt dit voor accounts van centrale beheerders voor componenten in de technische ICT-infrastructuur (o.a. servers, databases, netwerkcomponenten, firewall). Ook hier dienen (acties van) de gebruikers (in dit geval beheerders) te herleiden zijn naar een uniek persoon.
    - Applicatiebeheer / Functioneel beheer: Dit betekent dat in een applicatie ieder gebruikersaccount naar een uniek persoon ter herleiden moet zijn. Groepsaccounts zijn niet toegestaan.
- Het kenbaar maken van de identiteit mag op verschillende manieren ingericht worden. Dit kan door:
    - in een inlogscherm invoeren van een unieke gebruikersnaam/-nummer/userid.
    - gebruik van een vingerafdruk of een ander biometrisch kenmerk (hiervoor dient er een beoordeling plaats te vinden door de Functionaris Gegevensbescherming).
    - gebruik van een token (bijvoorbeeld een authenticator app of een smartcard)

Zie voor de identiteit en het identificeren van externe leveranciers het gedeelte bij 3.3 over authenticatie van leveranciers. Verder zijn in paragraaf 4.3 accounts toegelicht die extra aandacht vergen.

3. Authenticatie en wachtwoordbeleid

Relevant voor: technisch beheerder, applicatiebeheerder, functioneel beheerder.

Authenticatie is de methodiek / het proces waarbij gecontroleerd wordt of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs. Er zijn verschillende vormen van authenticatie die eventueel gecombineerd kunnen worden om een hoger of lager niveau van beveiliging op te leveren. Daarbij zijn drie vormen van bewijs bruikbaar:

- iets wat je weet (kennis) bijvoorbeeld een wachtwoord;
- iets wat je bezit bijvoorbeeld een token, pasjes, calculator, authenticatie-app, SMS met code, geauthentiseerde apparatuur (laptop, telefoon, applicatie), IP-adres, certificaat;
- iets wat je bent (persoonlijke eigenschap biometrie). Bijvoorbeeld een vingerafdruk. (hiervoor dient er een beoordeling plaats te vinden door de Functionaris Gegevensbescherming).

Authenticatie vindt plaats op verschillende niveaus:

- Apparatuur en onderliggend operating systeem (laptop, telefoon, tablet: paragraaf (3.1);
- Authenticatie in applicatie (paragraaf 3.2);
- Authenticatie van leverancier (paragraaf 3.3);
- Burgers en bedrijfsleven (paragraaf 3.4).

3.1. Authenticatie apparatuur en onderliggend operating systeem

De door Helmond beheerde apparatuur voor eindgebruikers dient te zijn afgeschermd voor onbevoegde toegang. Denk hierbij aan PC's, laptops, telefoons en tablets.

3.1.1. PC's / Laptops

Relevant voor: proceseigenaar Beheren Veiligheid, DSPO, technisch beheerder.

Voor PC's en laptops geldt dat deze logisch afgeschermd dienen te zijn. Dit betekent onder meer dat deze voorzien zijn van een authenticatiemechanisme. Dit houdt in dat alleen geregistreerde en met een authenticatiemechanisme uitgeruste apparatuur toegang mag krijgen tot de vertrouwde zone van de gemeente (waaronder het interne (wifi-)netwerk). Gemeente Helmond heeft authenticatiemechanisme ingericht voor PC's en laptops (token).

Doordat de fysieke en logische beveiliging in de kantoren van de gemeente Helmond doorbroken kan worden, kunnen onbevoegden toegang krijgen tot een onbeheerde PC of laptop binnen de beveiligde zone. Dit betekent dat de volgende maatregelen dienen te zijn ingericht om het risico te verminderen:

- Iedere PC/laptop die toegang mag krijgen tot de interne infrastructuur van Helmond (vertrouwde zone), moet zijn geauthentiseerd. Apparatuur die tot de onvertrouwde zone (gastennetwerk) toegang krijgt, hoeft niet te zijn geauthentiseerd.
- Gebruikers met eigen of geauthentiseerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten[9].
- Verder geldt dat de gegevensdrager (harde schijf) versleuteld dient te zijn.

[9] Zie BIO 11.2.9.2

Overigens geldt dat iedere gebruiker de PC of laptop dient te vergrendelen (locken) zodra de gebruiker het apparaat onbeheerd achterlaat. De DSPO stimuleert het actief vergrendelen van het apparaat.

3.1.2. Telefoon, tablet

Relevant voor: technisch beheerder, Servicedesk-medewerker.

Bedrijfsinformatie die op mobiele apparatuur staat, dient te zijn afgeschermd. Zakelijke gegevens mogen in ieder geval niet in contact komen met privégegevens of privé-applicaties Zie hiervoor ook het beleid voor mobiele apparatuur en locatie-onafhankelijk werken. Ten aanzien van logische toegang geldt dat voor de telefoon/tablet het volgende technisch afgedwongen dient te zijn:

- De telefoon/tablet is toegankelijk door middel van een 6-cijferige pincode, wachtwoord[10], vingerafdruk of andere vorm van biometrie (DPIA benodigd en afstemmen met FG).
- Bij voorkeur is voor het inrichten/instellen van gemeentelijke mail op de telefoon/tablet een eenmalige of periodieke multifactor authenticatie ingericht. Bij gebruik is de gemeentelijke mail-inbox direct beschikbaar na een eerste authenticatie op deze telefoon. Als opnieuw verbinding wordt gemaakt met exchange en bijvoorbeeld opnieuw opstarten telefoon/tablet is multifactor authenticatie van toepassing d.m.v. ingeven wachtwoord.
- Voor toegang tot gemeentelijke applicaties en andere gemeentelijke informatie via de telefoon/tablet dient multifactor authenticatie te zijn ingericht.
- Telefoons en tablets (ook indien uitgegeven/beheerd door Helmond) maken geen connectie met het gemeentelijke interne (wifi-)netwerk (vertrouwde zone) waar ook de laptops op zijn aangesloten. Medewerkers kunnen namelijk eigen applicaties installeren en het internetgebruik is in mindere mate gecontroleerd/beheerst. Dit vergroot het risico op telefoons en tablets als aanvalsvector.
- Op het openbare netwerk (waar ook gast-accounts zijn aangesloten) is verkeer van gebruikers (clients) van elkaar geïsoleerd.

3.1.3. Bring Your Own Device (BYOD)

Relevant voor: Technisch beheerder.

BYOD is alleen toegestaan indien Enterprise Mobility Management (EMM) wordt ingezet. Zonder EMM-maatregelen is BYOD in combinatie met bedrijfsgegevens niet toegestaan.
Voor BYOD geldt dat ten aanzien van logische toegang het volgende technisch afgedwongen dient te zijn:

- Gemeentelijke informatie op de BYOD-apparatuur dient logisch gescheiden te zijn van andere informatie op de apparatuur. Dit geldt expliciet niet voor contacten (dit zou het gebruik van het apparaat teveel beperken). Dit geldt expliciet wel voor informatie in gemeentelijke applicaties. Dit houdt in dat informatie uit gemeentelijke applicaties niet toegankelijk mag zijn voor applicaties uit de onbeheerde omgeving van de telefoon.
- E-mail is alleen middels multifactor authenticatie te benaderen. E-mail is daarnaast logisch gescheiden. De authenticatie van het apparaat is hierbij een mogelijkheid. Denk bijvoorbeeld aan een certificaat op het apparaat of een unieke key van het apparaat dat geregistreerd is.

[10] Zie het wachtwoordbeleid voor de wachtwoordvereisten en voor multifactor authenticatie voor mobiele gegevensdragers.

- Gebruikers met eigen of geauthentiseerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone. Voor toegang tot de vertrouwde zone zie 3.2.1.

3.2. Authenticatie in applicatie

Relevant voor: proceseigenaar, DSPO, technisch beheerder, applicatiebeheerder, functioneel beheerder.

Voor de toegang tot applicaties geldt dat de gebruiker dient te worden geauthentiseerd. Hiervoor zijn een aantal voorwaarden die in dit onderdeel zijn uitgewerkt.

3.2.1. Onvertrouwde omgeving en multifactor authenticatie

Multifactor authenticatie geldt altijd als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone. Een onvertrouwde omgeving betreft iedere omgeving die niet door de gemeente Helmond beheerd wordt. Denk hierbij aan:

- Internet.
- Wifi en netwerk van thuis, burgers, bedrijven, andere gemeenten, restaurants, hotels etc.
- Een PC / laptop die niet door de gemeente Helmond is geauthentiseerd.

Een applicatie die als online dienst wordt aangeboden (Software as a Service, SaaS) bevindt zich in principe in een onvertrouwde omgeving, namelijk het internet. De SaaS-applicatie dient dus te zijn voorzien van multifactor authenticatie waardoor gewaarborgd wordt dat alleen bevoegde gebruikers toegang hebben tot de applicatie. Dit kan op verschillende manieren worden ingericht:

- iets wat je weet (kennis). Bijvoorbeeld een wachtwoord.
- iets wat je bezit. Bijvoorbeeld een token, pasjes, calculator, authenticatie-app, SMS met code, geauthentiseerde apparatuur (laptop, telefoon, applicatie), IP-adres, MAC-adres, certificaat.
- iets wat je bent (persoonlijke eigenschap biometrie). Bijvoorbeeld een vingerafdruk. Hier wordt alleen gebruik van gemaakt als de noodzaak tot beveiliging zo groot is dat een minder ingrijpende manier van beveiliging niet passend is of als biometrie hier geen bezwaar oplevert. Naast deze afweging wordt een DPIA uitgevoerd, beiden worden ter advisering aan de Functionaris Gegevensbescherming voorgelegd, voordat wordt besloten om over te gaan op deze manier van identificatie.

Het is hierbij als extra factor ook mogelijk om via de Active Directory / ADFS (federation service voor SaaS) te authentiseren. Indien de applicatie zo is ingeregeld dat de gebruiker zich via Active Directory /ADFS kan authentiseren, betekent dit dat alleen gebruikers die in Active Directory staan toegang kunnen krijgen tot de applicatie. Het voordeel hiervan is dat bij het intrekken van autorisaties in de Active Directory ook alle toegang tot SaaS-applicaties wordt geblokkeerd. Ook is ADFS de plek waar multifactor authenticatie ingesteld kan worden. Echter, indien Active Directory niet beschikbaar is, is de toegang tot SaaS-applicaties ook geblokkeerd.

Hiernaast dienen de verbindingen ook versleuteld te zijn volgens de meest recente beveiligingsstandaarden (zie website Forum Standaardisatie voor open standaarden. Denk hierbij bijvoorbeeld ook aan het gebruik van een VPN. Ontsluit ook nooit Direct Management Interfaces zoals Remote Desktop Protocol[11] (RDP) direct via het internet voor onderhoud op afstand (bijvoorbeeld vanuit thuis of vanuit de leverancier). Dit is een veelgebruikte manier voor hackers om binnen te dringen in systemen. Mocht dit toch noodzakelijk zijn, richt deze dan in volgens de laatste beveiligingsstandaarden.

[11] Dankzij het Remote Desktop Protocol kunnen mensen van op afstand een andere computer besturen, zonder hierbij fysiek aanwezig te zijn.

Om de toegang (IDU) tot een SAAS applicatie te beheersen is het van belang dat SaaS-applicaties niet vanuit onbeheerde apparatuur benaderd worden. Indien dit technisch afgedwongen kan worden, moet dit worden ingericht. Een mogelijke oplossing is hierboven toegelicht (ADFS).

3.2.2. Wachtwoordbeleid

Indien authenticatie in de applicatie plaats vindt met een wachtwoord, dan voldoet het wachtwoord aan de hieronder opgenomen wachtwoordeisen.

Applicatie mét multifactor authenticatie	**Applicatie zonder multifactor authenticatie**
De eisen aan wachtwoorden dienen geautomatiseerd te worden afgedwongen.	De eisen aan wachtwoorden dienen geautomatiseerd te worden afgedwongen.
De wachtwoordlengte is minimaal **8** posities en de samenstelling voldoet aan de complexiteitseis:tenminste 3 van de 4: 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken.	De wachtwoordlengte is minimaal **12** posities en de samenstelling voldoet aan de complexiteitseis: tenminste 3 van de 4: 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken.
Vanaf een wachtwoordlengte van **12** posities vervalt de complexiteitseis.	Vanaf een wachtwoordlengte van **20** posities vervalt de complexiteitseis.
Het aantal foutieve inlogpogingen is maximaal **10** of het is technisch afgedwongen dat iedere extra inlogpoging een extra vertraging heeft. Dit loopt op tot minimaal 10 minuten.	Het aantal foutieve inlogpogingen is maximaal **10** of het is technisch afgedwongen dat iedere extra inlogpoging een extra vertraging heeft. Dit loopt op tot minimaal 10 minuten.
Wachtwoorden niet binnen 6 keer herhalen.	Wachtwoorden niet binnen 6 keer herhalen.
Een vergrendeld/gelocked account mag alleen na identificatie van de gebruiker worden ontgrendeld / gereset.	Een vergrendeld/gelocked account mag alleen na identificatie van de gebruiker worden ontgrendeld / gereset.
Een geblokkeerd account mag alleen na goedkeuring door AOG worden ontgrendeld / gereset.	Een geblokkeerd account mag alleen na goedkeuring door AOG worden ontgrendeld / gereset.
Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en dienen bij het eerste gebruik te worden gewijzigd.	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en dienen bij het eerste gebruik te worden gewijzigd.
Het wachtwoord heeft een maximale geldigheidsduur van een **jaar**. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van een half jaar.	Het wachtwoord heeft een maximale geldigheidsduur van een **half jaar**.
Wachtwoorden mogen niet in plain text worden opgeslagen.	Wachtwoorden mogen niet in plain text worden opgeslagen.

Let op: Bepaalde wet- en regelgeving kan andere (strengere) eisen hebben. Deze eisen dienen dan gevolgd te worden.

3.2.3. Single Sign On

Applicaties kunnen gebruik maken van Single Sign On (SSO). De voordelen voor de gebruiker zijn:

- De gebruiker hoeft slechts één wachtwoord te onthouden.
- De gebruiker vult het wachtwoord op één plek in, in plaats van op verschillende inlogpagina's.

De voordelen voor de applicatie / functioneel beheerder zijn:

- Indien een gebruiker geen toegang meer hoort te hebben, kunnen alle gelinkte accounts direct vanuit één plek geblokkeerd worden.
- Je kunt op één plaats multifactor authenticatie implementeren.

De nadelen van SSO zijn:

- Indien het wachtwoord bekend is bij een onbevoegde, heeft de onbevoegde toegang tot niet één applicatie, maar tot alle gelinkte applicaties.
- Niet iedere applicatie kan omgaan met SSO. Zo hebben verschillende applicaties verschillende wachtwoordvereisten en dient de applicatie technisch aangesloten te kunnen worden op onze infrastructuur. Dit is niet altijd mogelijk.
- Het kan relatief duur zijn om SSO in te richten op een applicatie.

Er zijn applicaties waarbij met name de mogelijkheid tot onbevoegde toegang tot een hoog risico leidt. Dit geldt voor applicaties waarbij:

- Bijzondere persoonsgegevens verwerkt worden (o.a. medische gegevens, politieke opvattingen, geloof, ras, vakbondslidmaatschap, biometrische gegevens voor identificatie, seksuele leven (geaardheid), strafrechtelijk verleden);
- Gevoelige gegevens verwerkt worden. Denk hierbij bijvoorbeeld aan Burgerservicenummer (BSN), geheim fraudeonderzoek, WOB-verzoek, grondposities en verandering bestemmingsplan;
- Financiële transacties worden gedaan of financiële gegevens kunnen worden aangepast (zoals bankrekeningnummers).

Voor deze applicaties wil de gemeente dat deze extra goed moeten worden beschermd. Aan de volgende voorwaarden moeten worden voldaan om deze applicaties van SSO gebruik te laten maken:

- General IT Controls (zoals toegangsrechten en autorisaties, wijzigingenbeheer en incidentmanagement) dient goed ingericht te zijn waarbij opzet, bestaan en werking aantoonbaar is (vanaf een volwassenheidsniveau[12] van 3).
- Een vorm van multifactor authenticatie moet zijn ingericht om toegang te kunnen krijgen tot de applicaties. Dit mag zijn ingericht op het niveau van de applicatie zelf. Het mag ook centraal (bijvoorbeeld op netwerkniveau) zijn ingericht zodat de authenticatie voor meerdere applicaties tegelijkertijd werkt. De centrale wijze geniet de voorkeur, omdat deze ook gebruiksvriendelijker is.

Is voor deze applicaties geen multifactor authenticatie ingericht en/of voldoet de applicatie niet aan de General IT Controls, dan stelt de gemeente dat hiervoor dus geen SSO voor ingericht mag zijn.

3.2.4. De gebruiker en het veilig gebruik van wachtwoorden

Relevant voor: technisch beheerder, applicatiebeheerder, functioneel beheerder, DSPO.

Als functioneel beheerder zorg je dat de volgende gedragsregels ten aanzien van wachtwoorden afdoende bekend zijn bij gebruikers en reik je deze uit bij het aanmelden van de medewerker tot de applicatie:

- wijzig standaard wachtwoorden altijd bij het eerste gebruik;

[12] NOREA NBA-LIO volwassenheidsmodel

- gebruik in ieder geval een uniek wachtwoord voor belangrijke applicaties (zoals bankieren);
- gebruik geen opvolgend wachtwoord;
- wissel je wachtwoord regelmatig, maar tenminste één keer per jaar;
- gebruik geen privé-wachtwoorden op het werk;
- deel je wachtwoord niet;
- schrijf je wachtwoord niet op;
- maak GEEN gebruik van de 'wachtwoord onthoud'-functie van sommige webbrowsers;
- maak GEEN gebruik van de functie om ingelogd te blijven;
- wijzig een wachtwoord direct bij vermoeden van misbruik;
- meldt misbruik van wachtwoorden als beveiligingsincident aan de Servicedesk.

Attendeer medewerkers op het aanvragen van een wachtwoordkluis bij de servicedesk. Als DSPO zorg je voor de continue bewustwording ten aanzien van bovenstaande gedragsregels.

Technisch beheerders en applicatiebeheerders moeten zich vanzelfsprekend ook aan bovenstaande gedragsregels houden.

3.2.5. Wachtwoordmanager

Relevant voor: technisch beheerder, DSPO.

Het onthouden van wachtwoorden is niet eenvoudig voor een gebruiker. Deze heeft al snel een tiental accounts waarvoor telkens een ander wachtwoord geldt. Single Sign On (SSO) kan hierbij helpen. Echter zijn niet alle applicaties hiervoor geschikt en is er een gevaar dat een onbevoegde toegang krijgt tot alle accounts indien degene het primaire wachtwoord kent.

Een oplossing voor het onthouden van vele wachtwoorden is een wachtwoordmanager. Dit is een digitale kluis waarin de wachtwoorden voor de diverse applicaties zijn opgeslagen. Deze kluisapplicatie is erop gericht juist deze belangrijke informatie op te slaan, maar helpt ook bij het genereren van nieuwe, moeilijk te kraken wachtwoorden en bij het invullen van deze wachtwoorden in (online) applicaties. Het grote voordeel van een wachtwoordmanager is dat op iedere applicatie een ander, sterk wachtwoord kan worden gebruikt, en dat dit toch redelijk gebruikersvriendelijk is. Indien een wachtwoord van één applicatie alsnog gekraakt wordt, is de beveiliging van andere applicaties niet in gevaar.

De Servicedesk dient de medewerkers te ondersteunen in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordmanager[13]. Het dient daarbij technisch afgedwongen te zijn dat de gebruiker multifactor authenticatie dient te gebruiken voor het inloggen op de wachtwoordmanager. Anders bestaat alsnog het gevaar dat de wachtwoorden beschikbaar zijn voor onbevoegden.

3.3. Authenticatie van leverancier

Relevant voor: technisch beheerder, applicatiebeheerder.

Leveranciers van (online) applicaties dienen met regelmaat onderhoud uit te voeren op deze applicaties. Het is voor de gemeente Helmond niet noodzakelijk dat het account van een leverancier tot een persoon herleidbaar dient te zijn. De acties van de leverancier dienen in ieder geval wel altijd herleidbaar te zijn naar diezelfde leverancier. Dit betekent dat de leverancier onder een eigen

[13] BIO 9.3.1.1

accountnaam werkt. Voor gemeente Helmond is het belangrijk dat acties herleidbaar zijn naar de leverancier zodat eventuele schade op de leverancier verhaald kunnen worden. De leverancier is zelf verantwoordelijk voor hun interne authenticatie. Hiermee wijkt de gemeente bewust af van de BIO 9.2.1.2 waarin staat dat groepsaccounts niet zijn toegestaan.

3.3.1. Toegang tot on premise applicaties

Bij een *on premise* applicatie moet de leverancier vooraf toestemming vragen om in te loggen op onze applicatie. Dit legt de beheerder vast in een registratie zodat achteraf kan worden beoordeeld of de acties terecht zijn. Om dit proces in goede banen te leiden heeft IVA AD is hiervoor een procedure opgesteld en vastgesteld.
In het geval dat de leverancier op afstand moet inloggen vanuit een onvertrouwde zone, dient een vorm van multifactor authenticatie te worden toegepast. Is dit niet mogelijk, dan geldt de opgestelde/ vastgestelde procedure van IVA AD.

3.3.2. Voorwaarden meekijksoftware

Voor meekijk-software is het van belang dat de leverancier conform de procedure geauthentiseerd wordt op het moment dat de leverancier mee kijkt en/of overneemt. Het is dan niet noodzakelijk dat de leverancier een eigen account heeft. Degene kijkt immers mee met een medewerker van Helmond. Wel dient de medewerker van Helmond te kunnen nagaan welke acties de leverancier uitvoert. Dit kan ingericht worden door bijvoorbeeld:

- Direct mee te kijken met de acties;
- Logging van acties;
- Opnamen te maken van alle acties. Het maken van opnamen mag alleen worden toegepast indien andere, minder ingrijpende methodes niet voldoende beveiliging bieden of niet mogelijk zijn. Bij opnamen dient de leverancier van tevoren geïnformeerd te worden en dienen er afspraken gemaakt te worden over de beveiliging, de toegang en de bewaartermijn van opnamen. Indien het de bedoeling is dat structureel opnamen worden gemaakt, moet eerst een DPIA worden uitgevoerd en worden voorgelegd aan de Functionaris Gegevensbescherming.

3.3.3. Toegang SAAS

Voor SaaS-applicaties moet toegang door de leverancier tot de applicatie en onderliggende databases zijn vastgelegd in afspraken (bijvoorbeeld SLA of DAP).

Zoals eerder vermeld: het is niet toegestaan om een Remote Desktop Protocol (RDP) aan het internet gekoppeld te hebben. Indien het geen optie is om RDP uit te schakelen, dient RDP te zijn gekoppeld aan multifactor authenticatie. Ook moet dan worden vastgelegd waarom van deze regel wordt afgeweken.

3.4. Identificatie / authenticatie burgers en bedrijfsleven

Relevant voor: technisch beheerder, applicatiebeheerder, functioneel beheerder, DSPO, proceseigenaar.

In veel gevallen is het is van belang dat de gemeente zeker weet met wie zij zaken doet. Onder de volgende voorwaarden dient de burger of organisatie geïdentificeerd te worden:

- Indien de gemeente gevoelige gegevens en/of bijzondere persoonsgegevens dient uit te wisselen;
- Indien de andere partij een product of dienst van de gemeente nodig heeft;
- Indien de andere partij een betaling dient uit te voeren.

Indien een burger of iemand van een organisatie fysiek aanwezig is bij de gemeente, kan deze zich legitimeren (authentiseren) via een paspoort, identiteitsbewijs of rijbewijs. Ook zijn nader identificerende vragen mogelijk. De burgers en organisaties (waaronder bedrijven) gebruiken echter steeds meer de digitale weg om zaken te regelen met de gemeente Helmond. Het grote voordeel is dat veel processen (deels) geautomatiseerd en/of op afstand kunnen plaatsvinden. Dit kan op verschillende manieren:

- Telefonisch;
- Via een digitaal kanaal (portaal / applicatie);
- Per e-mail.

Iedere manier brengt andere risico's en andere oplossingen voor identificatie en authenticatie met zich mee. Het uitgangspunt is dat naarmate de informatie gevoeliger wordt, er sterkere methodes van identificatie en authenticatie moeten worden toegepast.[14]

3.4.1. Telefonie

Het kan voorkomen dat communicatie met burgers of organisaties en de gemeente telefonisch plaatsvindt. Omdat de gemeente met gevoelige gegevens werkt, kan niet alle informatie telefonisch verstrekt worden. Het is namelijk moeilijker om vast te stellen wie de persoon is aan de andere kant van de telefoon.
Indien de andere partij geïdentificeerd en geauthentiseerd dient te worden (zie voorwaarden hierboven) is het van belang dat het bedrijfsonderdeel hiervoor de volgende punten heeft uitgewerkt:

- Welke informatie wel telefonisch mag worden vrijgegeven;
- Welke informatie nooit telefonisch mag worden vrijgegeven;
- De wijze waarop de medewerker de identiteit kan vaststellen van degene aan de telefoon. Opties hiervoor zijn:
    - De medewerker belt degene zelf op een vooraf vastgesteld nummer (in plaats van dat de medewerker zelf gebeld wordt).
    - Controlevragen om de identiteit vast te stellen. Denk aan vragen over adres, geboortedatum, maar ook juist over specifieke onderdelen uit een dossier die anderen niet kunnen weten. Dus een geboortedatum of adres is niet voldoende.
    - Vraag tijdens het gesprek om een controlemail indien je al eerder per mail contact hebt gehad. Een onbevoegde kan namelijk niet zo makkelijk namens iemand anders mailen.
    - Een app die de identiteit verifieert van de beller. In dit geval worden telefonie en (authenticatie via) een digitaal kanaal met elkaar vermengd. Zie hiervoor 3.4.2 "Digitaal kanaal".

[14] Zie ook "Procedure verificatie en vaststellen identiteit"

3.4.2. Digitaal kanaal

Indien de gemeente digitaal met de burger of organisatie communiceert kan ook hier authenticatie van belang zijn (zie voorwaarden onder 3.4).

Burgers en bedrijven kunnen via websites van overheidsorganisaties diensten afnemen. Hierbij valt te denken aan elektronische formulieren waarmee diensten of producten aangevraagd kunnen worden, MijnOverheid en een gemeentelijke persoonlijke internet pagina (PIP). Deze diensten worden in dit document “elektronische diensten” genoemd. Het vereiste niveau van het authenticatiemiddel hangt af van de aard van de transactie en de gevolgen van die elektronische dienst (zoals financiële of juridische gevolgen).

Het uitgangspunt is: het authenticatiemiddel wat door een burger of bedrijf wordt gebruikt, moet conform wet- en regelgeving aan sluiten bij het betrouwbaarheidsniveau van de dienst. Bij een dienst die het betrouwbaarheidsniveau 'Substantieel’ heeft, moet dus een authenticatiemiddel gebruikt worden wat ten minst van het niveau Substantieel[15] is.

In zulke gevallen maak je gebruik van de bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatiebeveiliging. Voor burgers die via een digitaal kanaal geauthentiseerd dienen te worden, is authenticatie middels *DigiD* de sterkste methode. Voor ondernemers is authenticatie middels *eHerkenning* de sterkste methode.

Alternatieven voor authenticatie

Alternatieven voor authenticatie van burgers en bedrijfsleven zijn toegestaan, indien deze aantoonbaar aan dezelfde of vergelijkbare beveiligingseisen voldoen als DigiD. Met Electronic Identities And Trust Services (eIDAS) hebben de Europese lidstaten afspraken gemaakt over onder meer het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. De Europese eIDAS-verordening stelt dat het voor burgers en organisaties mogelijk moet zijn om met de nationale, genotificeerde (door Europa erkende) middelen in te loggen bij alle overheidsorganisaties binnen de Europese Unie. De (Nederlandse) overheidsdiensten moeten ervoor zorgen dat alle EU-ingezetenen zo toegang hebben tot hun dienstverlening. Deze verplichting geldt o.a. voor organisaties die gebruik maken van DigiD en eHerkenning en diensten bieden op niveau substantieel.[16]

Alternatieven zijn dus mogelijk en zelfs gewenst. Het moeten dan wel nationale genotificeerde en/of door Europa erkende middelen zijn om in te loggen. Daarnaast dient er een zichtbare risicoafweging te worden gemaakt. Deze alternatieven en vereisten dienen te zijn afgestemd met de DSPO en de CISO.

3.4.3. E-mail

Onze organisatie wisselt veel informatie uit via e-mail. Je weet echter niet altijd wie er achter een e-mailadres zit.

> *Voorbeeld: Een e-mailadres w.a.alexander@gmail.com is zo gemaakt. Dat wil niet zeggen dat je dan met onze koning mailt.*

Er zijn vele gevallen bekend waarbij iemand zich voordoet als iemand anders om informatie te achterhalen of om je te verleiden tot een bepaalde actie:

[15] Door het Forum Standaardisatie is een handreiking opgesteld die helpt bij het maken van een heldere en transparante keuze voor het betrouwbaarheidsniveau van een digitale dienst. Zie ook “GEMMA_Gegevenslandschap_-_Autorisatie_en_authenticatie_v1.0”.

[16] GEMMA_Gegevenslandschap_-_Autorisatie_en_authenticatie_v1.0

- een “Microsoft-medewerker” die belt omdat je computer besmet zou zijn;
- een “directeur” die aangeeft dat er snel geld overgemaakt dient te worden (CEO-fraude);
- iemand die persoonlijke informatie van burgers probeert te achterhalen. Bijvoorbeeld van de ex-partner.

Als eerste is het dus van belang om zeker te weten wie er bij een bepaald e-mailadres hoort. Dit kan bijvoorbeeld indien degene zich eerder fysiek heeft gelegitimeerd of via een digitaal kanaal is geauthentiseerd (zie 3.4.2 hierboven) en daar het e-mailadres heeft achtergelaten. Let ook dan op of met zekerheid valt te stellen of het e-mailadres nog actueel is. Bij een online aanvraagformulier dat direct afgehandeld wordt, kan het adres bijvoorbeeld worden gebruikt. Indien al een langere tijd niet naar het e-mailadres is gemaild, kan het zijn dat dit adres niet meer juist is, of dat het adres niet meer aan de juiste persoon gekoppeld is. Een separate verificatie van het e-mailadres is dan noodzakelijk.

Is er alleen gecommuniceerd via e-mail? Dan kan er geen goede verificatie plaats hebben gevonden van de identiteit. Er zijn dan onwenselijke risico’s verbonden aan de uitwisseling van gevoelige informatie, het leveren van een dienst of product, of uitwisseling van financiële gegevens. E-mail kan wel gerust gebruikt worden voor de uitwisseling van niet-gevoelige informatie.

Versleuteling berichten
E-mail is daarnaast geen veilige manier om informatie uit te wisselen. Een e-mail kun je vergelijken met een postkaart. Dit betekent dat tussenliggende partijen het bericht kunnen lezen. Daarom dient gevoelige informatie in een e-mail ook versleuteld te worden en dient de sleutel (meestal het wachtwoord) via een ander kanaal (bijvoorbeeld via SMS) te worden verzonden. Door het invoeren van het wachtwoord vindt authenticatie plaats van de juiste ontvanger om de informatie te kunnen zien. Zo is het zeker dat alleen de juiste ontvanger toegang krijgt tot de informatie.

3.4.4. Geen kopie identiteitsbewijs
Bij digitale authenticatie is het in ieder geval niet toegestaan om een kopie van het identiteitsbewijs door de andere partij op te laten sturen. Een kopie mag overigens nooit opgestuurd worden. Dit levert een extra risico op voor de eigenaar van het identiteitsbewijs (de kopie kan onderschept worden of door de ontvanger ook voor andere doeleinden gebruikt worden) en levert geen authenticatie op. Ook kan een malafide partij een identiteitsbewijs van een ander gebruiken om zich daarmee als die ander voor te doen. De kopie van een identiteitsbewijs is dus geen geschikte authenticatiemethode en is dus niet toegestaan.

3.4.5. Identificatie / Authenticatie niet altijd nodig of wenselijk
Identificatie en authenticatie van de burger is niet altijd nodig en soms zelfs niet wenselijk. Deze is bijvoorbeeld niet noodzakelijk bij een algemene vraag aan de gemeente. Een ander voorbeeld is een melding openbare ruimte of een melding die gaat over openbare orde en veiligheid. Dan is het zelfs mogelijk niet wenselijk dat authenticatie plaats vindt omdat de melder het recht heeft anoniem te blijven.

4. Het beheer van autorisaties

Relevant voor: AOG-medewerker, proceseigenaar, DSPO, technisch beheerder, applicatiebeheerder, functioneel beheerder.

In het vorige hoofdstuk is beschreven hoe personen, applicaties en apparatuur zich kunnen legitimeren/identificeren door middel van authenticatie. We weten nu zeker wie degene is, dat de applicatie de juiste applicatie is en dat een apparaat het juiste apparaat is. Op basis hiervan mag bepaald worden waartoe deze persoon, applicatie of apparaat toegang heeft. Dit wordt geregeld via autorisatiebeheer. Dit hoofdstuk behandelt het autorisatiebeheer voor personen en gaat niet verder in op het autoriseren van applicaties en apparatuur zelf.

Autorisatiebeheer is in te delen in de volgende processen: aanvragen, goedkeuren, toekennen, wijzigen, intrekken van rechten (autorisaties). Van belang is dat alleen geautoriseerde personen toegang krijgen tot een autorisatie.

Om te borgen dat medewerkers toegang hebben tot gegevens die zij nodig hebben voor hun rol dient de bevoegdheid van deze medewerker te worden afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon. Anders is het mogelijk dat een medewerker toegang krijgt tot ofwel teveel ofwel te weinig data en functionaliteit voor de uitoefening van de taak, functie of verantwoordelijkheid.

4.1. Centrale registratie

Om te waarborgen dat iedere (externe) medewerker is gekoppeld aan een taak, functie en/of verantwoordelijkheid dient deze koppeling centraal geregistreerd te zijn. Net als bij identificatie geldt ook hier dat de afdeling AOG de single point of truth (SPOT) is.

Op centraal niveau is dan inzichtelijk gemaakt welke medewerker is gekoppeld aan een taak, functie en/of verantwoordelijkheid. Afhankelijk van deze taak, functie en/of verantwoordelijkheid is de medewerker gekoppeld aan bepaalde applicaties, toegang tot informatie, ruimten en middelen.

In het geval van direct/automatische provisioning kunnen specifieke autorisaties vanuit het centrale punt gewijzigd worden. Dit moet wel decentraal worden gevoed. Op decentraal niveau moet namelijk bepaald worden welke specifieke autorisaties een gebruiker krijgt. Indien direct/automatische provisioning niet is toegepast, dan moeten autorisaties op decentraal niveau worden gewijzigd.

4.2. Hoe bepaalt een proceseigenaar de autorisaties?

Wat een medewerker mag vanuit zijn rol is afhankelijk van:

- Welke functies door AOG worden onderkend binnen de gemeente;
- Welke processen een (externe) medewerker aan gekoppeld is en welke rol/functie de medewerker heeft binnen dat proces;
- Van welk organisatieonderdeel de medewerker onderdeel uitmaakt;
- Welke taken en verantwoordelijkheden bij een specifieke functie horen;
- Welke applicaties benodigd zijn om deze taken uit te voeren en verantwoordelijkheden te kunnen nemen;
- De benodigde autorisaties die deze medewerker met deze functie dient te hebben om deze taken te kunnen uitvoeren.

    - Autorisaties voor toegang tot folders met informatie;
    - Autorisaties voor toegang tot functionaliteiten en informatie in applicaties (waar mogelijk middels rollen);
- Waar functiescheiding benodigd is om fraude en fouten te voorkomen;
    - Zowel welke functies niet gecombineerd mogen worden; als,
    - Welke autorisaties niet gecombineerd mogen worden.
- Autorisaties op basis van een mandaat. In sommige gevallen dient het formeel te zijn vastgesteld dat degene mag beschikken over deze rechten;
- Wettelijk kaders en met inachtneming doelbinding;
- "Need to know, need to have-principe" (en daarmee dus niet het "Open, tenzij"-principe;
- Maatregelen om goed gebruik van autorisaties te borgen. Denk bijvoorbeeld aan:
    - (technisch afgedwongen) vierogen-principe;
    - (technisch afgedwongen) functiescheiding (bijvoorbeeld tussen invoeren en goedkeuren)
    - controle van lijstwerk;
    - controle van logging van acties van medewerkers.

Zoals gesteld bij 1.5 in de randvoorwaarden: niemand mag autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd.

Het opzetten van rol-gebaseerde autorisaties doe je niet alleen en is een samenspel.

4.3. Welke accounts vergen extra aandacht?

Accounts met speciale bevoegdheden vormen extra risico voor misbruik. Het toekennen en beheer op deze speciale bevoegdheden verdient daarmee extra aandacht.

Kritische accounts zijn:
- Beheerdersaccounts (technisch, applicatief, functioneel)
- Groepsaccounts (Admin rechten, root, gastaccounts);
- Systeem en batchaccounts.

4.3.1. Rol van beheerder (technisch, applicatie, functioneel)

Voor beheerders gelden de volgende afspraken:
- Er is een scheiding tussen beheertaken en overige gebruikstaken[17].
    - Voer je beheerwerkzaamheden uit dan log je in als beheerder.
    - Voer je normale gebruikstaken uit dan log je in als gebruiker.
- Regel multifactor authenticatie in.
- Sla wachtwoorden op in een digitale kluis en wijzig bij personeelsmutaties.
- Beoordeel speciale bevoegdheden minimaal ieder kwartaal (half jaar afhankelijk van verloop) en leg vast dat je deze beoordeling hebt uitgevoerd.

4.3.2. Groepsaccounts (zoals Admin, root, guest)

Zoals bij 2.2.1 al is gesteld zijn groepsaccounts niet toegestaan. In enkele gevallen kan hiervan worden afgeweken. Voor groepaccounts gelden de volgende afspraken:

[17] Zie ook 1.1.5 "Wat zijn de randvoorwaarden?"

- Het gebruik van groepsaccounts is alleen toegestaan indien noodzakelijk gebruik wordt vastgelegd door de proceseigenaar[18];
- Gebruik het groepsaccount alleen indien de werkzaamheden erom vragen. *Zie hiervoor ook 3.3 Authenticatie van leverancier*;
- Regel voor administrator-rechten multifactor authenticatie in;
- Ken minimale rechten toe aan guest accounts;
- Sla wachtwoorden op in een digitale kluis, en wijzig bij personeelsmutaties;
- Beoordeel groepsaccounts minimaal ieder kwartaal (bij verhoogde rechten) / half jaar en leg vast dat je deze beoordeling hebt uitgevoerd en leg de conclusie vast;
- Om het risico op onrechtmatig gebruik te minimaliseren moet het aanvragen van groepsaccounts in IT Service Management-software[19] zijn aangevraagd via een service request..

4.3.3. Systeem en batch accounts

Verschillende applicaties kennen systeemgebruikers. Dit zijn technische accounts die een technische taak uitvoeren. Denk bijvoorbeeld aan het verzenden van een batch. Het zijn dus geen accounts van een natuurlijk persoon. Vaak hebben deze accounts verhoogde rechten. Dit soort accounts kennen daarom een aantal regels en uitzonderingen:

- Gebruik unieke accounts die specifiek zijn benoemd naar de service die het account levert: deze zijn herleidbaar naar specifieke services bij een storing.
- Deze accounts mogen nooit zijn gekoppeld aan een echt persoon. Het mag dus technisch niet mogelijk zijn om als persoon met deze accounts in te loggen (deze account beschikken namelijk vaak over verhoogde rechten. Dit biedt extra risico en dan is niet te herleiden of de persoon een actie heeft uitgevoerd, of dat een actie door het systeemaccount zelf is geïnitieerd).
- Van alle systeemgebruikersaccounts is vastgelegd en hiermee inzichtelijk waarvoor deze gebruikt worden. Hierdoor hoeft niet bij iedere controle van de autorisaties te worden verklaard waarom deze autorisaties zijn uitgegeven.
- De autorisaties voor systeemgebruikers zijn beperkt tot wat noodzakelijk is voor de uitvoering van de taak van de systeemgebruiker. Dus minimale rechten voor die specifieke taak.
- Sla wachtwoorden op in een digitale kluis.
- Wachtwoorden van systeemgebruikers hoeven niet te verlopen omdat een verlopen wachtwoord kan leiden tot incidenten.
- Beoordeel systeem en batchaccounts daarom minimaal ieder kwartaal. Check op: Hebben de accounts de juiste rechten, bestaat de service nog?

4.4. Functiescheidingsmatrix

Voor bepaalde taken is het niet wenselijk als deze door dezelfde medewerker worden uitgevoerd. Er is dan een verhoogde kans op fouten of fraude. We willen daarom deze taken scheiden over verschillende functies. Niet verwonderlijk wordt dit functiescheiding genoemd. Voorbeelden hiervan zijn:

Taak 1	**Taak 2**	**Risico**

[18] zie hiervoor ook bij “1.1 Inleiding” de mogelijkheid om af te wijken van deze tactische uitwerking.

[19] Een IT Service Management-applicatie ondersteunt de organisatie bij de taken, registratie, planning en controle van te leveren producten en diensten van de IT-afdeling. In de applicatie worden service requests geregistreerd waarbij inzichtelijk kan worden gemaakt wie deze aanvraagt, wie deze goedkeurt en wie deze wanneer afhandelt.

Invoeren van betaling	Goedkeuren van betaling	Het risico bestaat dat een gemaakte fout niet wordt opgemerkt of dat iemand een ongeoorloofde betaling doet.
Aanpassen bankrekeningnummer	Opvoeren van factuur	Het risico bestaat dat een medewerker een bankrekeningnummer aanpast en vervolgens geld naar zichzelf overmaakt.
Opvoeren nieuwe leverancier	Toekennen budget aan leverancier	Het risico bestaat dat een medewerker een nep-leverancier opvoert en hieraan budget toekent.

Om te bepalen welke combinaties van taken (autorisaties binnen een applicatie) wel en niet mogen worden toegekend aan één functie (medewerker) is een procesbeschrijving van belang. Aan de hand van deze procesbeschrijving is het handig om een functiescheidingsmatrix op te stellen. In deze matrix stel je de taken op zowel de x-as als de y-as. In de matrix geef je aan welke combinaties van taken niet zijn toegestaan. Autorisaties waarmee de applicatie alleen geraadpleegd kan worden (rapporten afdrukken, schermen bekijken) mogen met andere autorisaties worden gecombineerd.

Zie hieronder een voorbeeld van een functiescheidingsmatrix met wel en niet toegestane combinaties van taken.

X = niet toegestane combinatie van autorisaties, zwarte veld is wel toegestane combinatie	Bestellen	Controleren factuur	Registreren factuur	Verklaren prestatie	Goedkeuren factuur	Boeken factuur	Betalen factuur
Bestellen		X	X	X		X	X
Controleren factuur	X		X	X	X	X	X
Registreren factuur	X	X		X	X		X
Verklaren prestatie	X	X	X		X	X	X
Goedkeuren factuur		X	X	X		X	X
Boeken factuur	X	X		X	X		X
Betalen factuur	X	X	X	X	X	X	

Deze functiescheidingsmatrix maakt direct inzichtelijk welke combinatie van taken *wel* (groene vlakken) en *niet* is toegestaan (kruisjes). Het is dus van belang dat deze taken over verschillende functies worden verdeeld. Voor applicaties waarbij misbruik en/of foutkans absoluut voorkomen moet worden is het noodzakelijk dat deze matrix wordt opgesteld. Denk hierbij aan processen met een financiële component of daar waarbij de juist registratie van brondocumenten essentieel is (o.a. basisregistraties).

Ook kan deze matrix opgesteld worden voor bepaalde functies die niet door dezelfde persoon uitgevoerd mogen worden. Dit kan dan ook applicatie- en afdelingsoverstijgend zijn.

4.5. Autorisatiematrix

Een autorisatiematrix helpt om eenvoudig inzicht te krijgen en te behouden over welke medewerker toegang heeft tot welke informatie en/of middelen.

4.5.1. Centraal – Koppeling gebruikers met applicaties

Op centraal niveau is het raadzaam om een autorisatiematrix op te stellen waarbij aangegeven is welke rollen, taken, functies en/of verantwoordelijkheden gekoppeld zijn aan welke applicaties. Om deze te kunnen opstellen is inzicht in de functiescheidingmatrix zoals opgenomen onder 4.4 noodzakelijk.

4.5.2. Decentraal - applicatieniveau

Op decentraal niveau gelden de volgende punten:

1. Voor vastgestelde kritische applicaties dienen autorisatiematrices te zijn opgesteld, waarbij de relatie tussen een taak, functie en/of verantwoordelijkheid en de autorisatie is te leggen. Voor niet-kritische applicaties is het sterk aan te raden om hiervoor een autorisatiematrix op te stellen[20].
2. Deze matrices dienen door de DSPO te zijn beoordeeld en door de applicatie-eigenaar (in dit geval proceseigenaar) te zijn goedgekeurd.
3. Medewerkers krijgen alleen autorisaties voor rollen gebaseerd op de autorisatiematrix.

Een manier om een autorisatiematrix op te stellen is het volgende:

1. Je maakt een tabel (bijvoorbeeld in Excel).
2. As 1: Alle rollen, taken, functies en/of verantwoordelijkheden zet je onder elkaar in één kolom.
3. As 2: Alle autorisaties (of functionaliteiten) zet je achter elkaar op één rij.
4. Je zet een vinkje (of een V) daar waar een autorisatie toegekend dient te zijn aan een taak / functie / verantwoordelijkheid.
5. Optioneel: je legt vast welke functies nooit gecombineerd mogen worden met een X. Als basis kun je hiervoor de functiescheidingsmatrix gebruiken.
6. In een andere tabel leg je vast welke medewerker is gekoppeld aan welke taak / functie / verantwoordelijkheid.

Voorbeeld:

Autorisaties/functionaliteiten *Functie/Rol/verantwoordelijkheid*	(Autorisaties behorende bij) **Aanmaken gebruiker**	(Autorisaties behorende bij) **Invoeren inkooporder**	(Autorisaties behorende bij) **Goedkeuren inkooporder**
Functioneel beheerder	V	X	X
Inkoopmedewerker A		V	
Inkoopmedewerker B		V	
Senior medewerker Inkoop	X	X	V

Naam	**Taak/Functie/Verantwoordelijkheid**
Hans Seerden	Functioneel beheerder
Vicky Coolen	Inkoopmedewerker A

[20] Proceseigenaren bepalen kritische processen en hiermee de kritische applicaties

Yasmina Beelen	Inkoopmedewerker A
Karen Janssen	Inkoopmedewerker A
Saïd el Ahmadi	Inkoopmedewerker B
Harold Pijnacker	Inkoopmedewerker B
Rebecca Hazelton	Senior medewerker Inkoop

In principe blijft de autorisatiematrix gelijk. Alleen de lijst met naam en taak / functie / verantwoordelijkheid zou wijzigen als iemand van functie wijzigt. Zoals je ziet zijn er meerdere medewerkers met dezelfde rol.

Let op: Als de senior medewerker in dit voorbeeld wel zou kunnen invoeren én kan goedkeuren, betekent dit dat een extra maatregel nodig zou zijn om er zeker van te zijn dat deze niet de eigen ingevoerde order goedkeurt. Hetzelfde geldt voor de applicatiebeheerder en/of functioneel beheerder. Omdat deze ook gebruikers aan kan maken, is er bij verschillende applicaties de mogelijkheid om gebruikers voor zichzelf aan te maken en zo de functiescheiding te doorbreken. Het is daarom van belang dat de DSPO kritisch mee kijkt welke risico's in het proces aanwezig zijn en waar het juist inrichten van autorisaties deze risico's kunnen beperken. De proceseigenaar bepaalt uiteindelijk welk risico acceptabel is voor het proces.

In hoofdstuk 6 zijn periodieke controles beschreven ten aanzien van de autorisatiematrix en autorisaties in applicaties.

4.5.1. Applicatie en afdeling overstijgend

Voor bepaalde combinaties van rollen, taken, functies en/of verantwoordelijkheden geldt dat deze een risico vormen als deze zijn toegekend aan één gebruiker. Denk bijvoorbeeld aan:

- Een medewerker die nieuwe zorgaanbieders opvoert (Sociaal Domein) en geld over maakt naar zorgaanbieders (Financiën);
- Budget toekennen (Financiën) en beslissen waar budget naar toe gaat (leidinggevende);
- Controle van uitgaven (Concern Control) en het doen van uitgaven (leidinggevende);

Als leidinggevende en beheerder (applicatie, functioneel) word je gevraagd hier rekening mee te houden, maar wordt nog geen richtlijn meegegeven. De focus ligt voor nu op een beheersing op applicatieniveau. In een later stadium wordt deze focus mogelijk verlegd naar applicatie en afdeling overstijgend niveau.

4.6. Wijzigingen autorisaties bij gelijkblijvende functie

Ook als iemand op dezelfde functie blijft, kunnen aanpassingen in autorisaties (tijdelijk) benodigd zijn. Indien een medewerker andere autorisaties nodig heeft dan de autorisaties die conform de autorisatiematrix zijn gekoppeld aan de taak, functie en/of verantwoordelijkheid, zijn er twee opties:

1. *Exceptie*
   Excepties zijn bedoeld voor situaties waarbij een medewerker tijdelijk autorisaties krijgt toegewezen die buiten de reguliere taak, functie en/of verantwoordelijkheid valt. Dit betekent dat het volgende:
   a. De proceseigenaar dient ervoor te zorgen dat een afweging gemaakt wordt welke risico's de afwijking op de autorisatiematrix met zich mee brengt. Indien er risico's zijn, dient de eigenaar de risico's schriftelijk te accepteren. Een DSPO kan hier bij ondersteunen.

b. De functioneel beheerder kent de autorisaties toe na expliciete goedkeuring van de exceptie door de proceseigenaar via het autorisatiewijzigingsproces. Hierbij wordt de autorisatiewijziging geregistreerd als een service request in de IT service management-applicatie.
c. De functioneel beheerder houdt een aparte registratie bij van alle excepties en registreert hierbij de einddatum.
d. De functioneel beheerder waarborgt dat op de einddatum de rechten ingetrokken worden.
e. De excepties dienen ieder kwartaal verlengd te worden door de proces-eigenaar. Indien deze exceptie-autorisaties niet tijdig verlengd worden, moeten deze (automatisch) worden ingetrokken.

2. *Aanpassing autorisatiematrix*
   Indien de medewerker structureel autorisaties nodig heeft, dient een aanpassing te worden doorgevoerd in de autorisatiematrix. Deze aanpassing dient centraal te worden geregistreerd als een service request en doorloopt het wijziging beheer/ change management-proces aan de business-zijde. Dit betekent het volgende:
   a. De proceseigenaar dient ervoor te zorgen dat een afweging gemaakt wordt welke risico's de afwijking op de autorisatiematrix met zich mee brengt. De DSPO ondersteunt hierbij. De eigenaar dient de risico's schriftelijk te accepteren.
   b. Op basis van deze risicoacceptatie zorgt de proceseigenaar dat een service request wordt ingediend. Hieruit wordt duidelijk welke aanpassing (change in de IT Service Management-tool) benodigd is in de autorisatiematrix.
   c. De applicatiebeheerder en/of functioneel beheerder voegt op basis van het service request in de autorisatiematrix de autorisaties toe (of verwijdert deze) aan de bestaande taak, functie en/of verantwoordelijkheid; of,
   d. Als de taak, functie en/of verantwoordelijkheid nog niet bestaat, voegt de applicatiebeheerder en/of functioneel beheerder deze op basis van het service request toe aan de autorisatiematrix (of verwijdert deze). Hier wordt vervolgens in de matrix de autorisatie aan gekoppeld.
   e. De verantwoordelijke proceseigenaar geeft goedkeuring aan de wijziging in de matrix middels de service management-applicatie.
   f. Nadat de wijziging van de matrix is goedgekeurd, kan de applicatiebeheerder (of functioneel beheerder) de autorisaties van de gebruiker aanpassen.

5. Instroom, doorstroom & uitstroom

<u>Relevant voor: AOG medewerker, proceseigenaar, DSPO, technisch beheerder, functioneel beheerder.</u>

- Voor interne en externe medewerkers vindt registratie van de instroom, doorstroom en uitstroom gecentraliseerd plaats. Dit geldt ook voor externen zoals adviseurs indien deze toegang nodig hebben tot de IT-omgeving van de gemeente.
- Iedere wijziging van autorisaties dient te zijn geregistreerd. Voor kritische applicaties dient deze te zijn geregistreerd in een service management-applicatie. Voor autorisatiewijzigingen als gevolg van instroom, doorstroom en uitstroom moet dit in de service management-applicatie als een service request worden geregistreerd..

- Een leidinggevende zorgt ervoor dat een personeelswijziging (instroom, doorstroom, uitstroom) door wordt gegeven aan AOG.
- AOG checkt de personeelswijzigingsaanvraag op validiteit (o.a. geldig contract, beoordeling, promotie). AOG checkt niet op inhoud van de autorisaties.
- Alleen de proceseigenaar mag de aanvraag van een wijziging goedkeuren. De goedkeuring moet zijn vastgelegd en gemakkelijk zijn te koppelen aan de wijziging. Deze mag ook blijken uit een combinatie van een eerder goedgekeurde overeenkomst (contract, aanstelling, promotie, demotie) in combinatie met een eerder goedgekeurde autorisatiematrix.
- Een Servicedesk-medewerker, technisch beheerder, applicatiebeheerder of functioneel beheerder voert alleen geregistreerde en goedgekeurde wijzigingen door. De Servicedesk-medewerker of beheerder dient achteraf te kunnen aantonen dat de wijziging is geregistreerd en goedgekeurd.
- Een Servicedesk-medewerker, technisch beheerder, applicatiebeheerder of functioneel beheerder kent autorisaties aan gebruiker alleen toe op basis van de autorisatiematrix. Indien de autorisatiematrix niet voldoet, zie “Wijzigingen autorisaties bij gelijkblijvende functie”.

Noot:
Verzoeken die op een andere manier binnenkomen dan via de service management-applicatie, dienen te worden teruggestuurd. Is dit geen optie, dan dient de noodprocedure te worden gestart (zie 5.1 hieronder).

5.1. Noodprocedure

Een noodprocedure kan gestart worden indien autorisaties per direct toegekend of ingetrokken dienen te worden. Hierdoor mogen per direct mutaties doorgevoerd worden.
Vanzelfsprekend is een noodprocedure niet bedoeld om deze te gebruiken om de reguliere autorisatiemanagementprocessen te omzeilen. Om misbruik te voorkomen dient een verantwoording achteraf inclusief risicoanalyse opgesteld te worden door degene die de noodprocedure in gang zet (vaak de leidinggevende of AOG). De mutaties als gevolg van een noodprocedure worden per kwartaal gecontroleerd door de DSPO en doorgegeven aan de CISO.

6. Controle

Zonder controle op autorisaties heeft de organisatie geen grip op het autorisatiemanagementproces. Je weet dan niet zeker of de aan gebruikers uitgegeven autorisaties nog terecht zijn. In het autorisatiemanagementproces zijn daarom verschillende controles benodigd om te borgen dat autorisaties alleen zijn toegekend aan geautoriseerde gebruikers. In de voorgaande hoofdstukken zijn de meeste procescontroles al opgenomen. Het is van belang dat deze procescontroles ook daadwerkelijk toegepast worden, anders weet de organisatie niet zeker of het proces ook daadwerkelijk werkt en of de risico's beheerst worden. In dit hoofdstuk zijn controles opgenomen die dat waarborgen.

6.1. Identificatie

1. De beheerder (technisch, functioneel) zorgt jaarlijks voor een overzicht van alle gebruikers in de applicatie.
2. De DSPO'er controleert of alle gebruikers uniek zijn en te zijn herleiden naar een persoon. Afwijkingen (o.a. gebruik groepsaccounts) moeten op basis van een risicoafweging door de proceseigenaar zijn goedgekeurd of worden opgelost.
3. Bij het opstellen en controleren van de lijst moet zorggedragen worden dat alleen die persoonsgegevens opgenomen zijn die noodzakelijk zijn voor deze controle. Een naam of een identificatienummer zou dus al voldoende zijn.

6.2. Authenticatie

1. De beheerder (Servicedesk, technisch, applicatie) maakt jaarlijks een vergelijking met de wachtwoordvereisten (inclusief multifactor authenticatie) van de gemeente Helmond en de daadwerkelijke wachtwoordinstellingen in de applicatie. De bevindingen legt de beheerder vast door middel van print screens. Op deze print screen is de datum waarop de print screen is gemaakt zichtbaar.
2. De beheerder legt afwijkingen van de wachtwoordvereisten vast en legt deze ter beoordeling voor aan de proceseigenaar.
3. De DSPO controleert of de wachtwoordsterkte conform de kaders en deze tactische uitwerking is ingericht en beoordeelt of afwijkingen op basis van risicoafweging zijn goedgekeurd door de proceseigenaar.

6.3. Maandelijkse check in-, door- en uitstroom op netwerk en keyapplicaties

Deze controle is bedoeld om te waarborgen dat het in-, door- en uitstroomproces goed blijft werken. Omdat dit een relatief zware controle is, is deze alleen van toepassing op Active Directory en kritische applicaties.

1. De functioneel beheerders van de Active Directory of Servicedesk-medewerkers ontvangen maandelijks een lijst uit het personeelssysteem met alle doorstromers en uitstromers. Hierbij zijn de volgende gegevens benodigd: naam, afdeling, wijzigingsdatum (mogelijk een datum non-actief), en gegevens waaruit te herleiden valt welke autorisaties benodigd zijn voor de persoon.
2. De functioneel beheerders (of applicatiebeheerders) ontvangen maandelijks dezelfde lijst uit het personeelssysteem met alle doorstromers en uitstromers.

3. Op basis van deze lijst (en de eventueel aanwezige autorisatiematrix) checkt de Servicedesk-medewerker of beheerder of deze personen nog terecht beschikken over de autorisaties in het netwerk (Active Directory-autorisaties) of autorisaties in de key applicaties.
4. Indien een doorstromer of uitstromer onterecht nog beschikt over autorisaties, maakt de functioneel beheerder (of applicatiebeheerder) een wijziging via een service request aan in de service management-applicatie of Identity & Access Management-applicatie. Daarna wijzigt de functioneel beheerder de autorisaties in het AD of de key applicatie. Het is hierbij van belang dat achteraf zichtbaar blijft wanneer de autorisaties in de applicatie zijn gewijzigd en dat deze in lijn kunnen worden gebracht met de datum van het service request. Indien mogelijk is het wenselijk als deze informatie centraal wordt opgeslagen.
5. De functioneel beheerder onderzoekt de afwijking waardoor de wijziging niet eerder via regulier instroom-doorstroom-uitstroom-proces is opgepakt. De uitkomsten van dit onderzoek (ook als degene niet de oorzaak heeft kunnen achterhalen) legt de functioneel beheerder vast en deelt de beheerder met AOG en de proceseigenaar.

De DSPO controleert of de functioneel beheerders van de betreffende afdeling(en) bovenstaande controle uitvoeren. De DSPO analyseert de afwijkingen en zorgt dat eventuele verbeteringen in het autorisatiemanagementproces worden doorgevoerd.

6.4. Periodieke check autorisatiematrix

Proceseigenaren checken voor hun applicaties (op basis van input functioneel beheerders) periodiek of de autorisatiematrix in lijn is met de taken, functies en verantwoordelijkheden die horen bij hun medewerkers. De DSPO controleert of proceseigenaren deze periodieke check (laten) uitvoeren.

	Aanmaken gebruiker	Invoeren inkooporder	Goedkeuren inkooporder
Functioneel beheerder	V	X	X
Inkoopmedewerker A		V	
Inkoopmedewerker B		V	
Senior medewerker Inkoop	X	X	V

Hierbij wordt het volgende gecheckt:

- Zijn de rollen in de applicatie correct? (rolnaam juist, alle rollen staan in matrix)
- Zijn alle functies weergegeven die in de applicatie autorisaties horen te hebben?
    - Zijn alle functies weergegeven? (Volledigheid)
    - Zijn de namen van de functies juist weergegeven? (Juistheid)
- Staan de “vinkjes” en “kruisjes” op de juiste plaatsen? (Denk hierbij aan vertrouwelijkheid en aan functiescheiding).

Op basis van deze controle is dus geverifieerd of de matrix juist is. De functioneel beheerder legt de bevindingen hiervan zichtbaar vast. Dit is input voor de controle door de DSPO. Afwijkingen en benodigde wijzigingen worden geregistreerd als een beveiligingsincident. Hierbij wordt nagegaan of er onterecht gebruik is gemaakt van de uitgegeven autorisaties.

Frequentie control
De frequentie van deze controle is afhankelijk van het Basisbeveiligingsniveau (BBN) dat geldt voor het informatiecluster waarin de applicatie valt. Dit niveau moet worden vastgesteld vanuit de BIO. Voor BBN 2 en 3 geldt dat deze controle iedere 6 maanden uitgevoerd moet worden. Voor BBN 1 geldt dat deze controle iedere 12 maanden uitgevoerd moet worden.

6.5. Periodieke check juistheid personen

Bij de vorige controle is gecheckt of de autorisatiematrix in orde is. Bij deze controle wordt gecheckt of de juiste personen zijn gekoppeld aan de juiste taken/functies/verantwoordelijkheden. Proceseigenaren checken periodiek of de juiste mensen in de applicatie zitten. Hierbij wordt het volgende gecheckt:

- Is de medewerker nog in dienst en in dezelfde rol?
- Sluiten de autorisaties in de matrix aan bij de taken/functie/verantwoordelijkheden van de medewerker?

	Aanmaken gebruiker	Invoeren inkooporder	Goedkeuren inkooporder
Functioneel beheerder	V	X	X
Inkoopmedewerker A		V	
Inkoopmedewerker B		V	
Senior medewerker Inkoop	X	X	V

Naam	Taak/Functie/Verantwoordelijkheid
Hans Seerden	Functioneel beheerder
Vicky Coolen	Inkoopmedewerker A
Yasmina Beelen	Inkoopmedewerker A
Karen Janssen	Inkoopmedewerker A
Saïd el Ahmadi	Inkoopmedewerker B
Harold Pijnacker	Inkoopmedewerker B
Rebecca Hazelton	Senior medewerker Inkoop

Afwijkingen en benodigde wijzigingen worden geregistreerd als een beveiligingsincident. Hierbij wordt nagegaan of er onterecht gebruik is gemaakt van de uitgegeven autorisaties. De DSPO waarborgt dat functioneel beheerders de check periodiek uitvoeren.

Frequentie control
De frequentie van deze controle is afhankelijk van het Basisbeveiligingsniveau (BBN) dat geldt voor het informatiecluster waarin de applicatie valt. Voor BBN 2 en 3 geldt dat deze controle iedere 6 maanden uitgevoerd moet worden. Voor BBN 1 geldt dat deze controle iedere 12 maanden uitgevoerd moet worden.

6.6. Periodieke check autorisatiematrix met applicatie

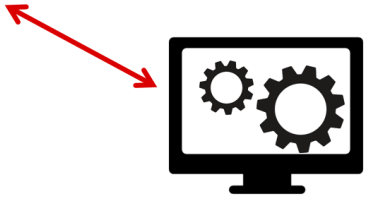
Bij de vorige controles is gecheckt of de autorisatiematrix nog correct is en of de namen gekoppeld zijn aan de juiste rol. De matrix is echter maar een papieren werkelijkheid. Het is ook van belang om te checken hoe deze rechten daadwerkelijk in de applicatie zijn ingericht. Daar is deze controle voor bedoeld.

De functioneel beheerders checken periodiek of de autorisatiematrix en namenlijst overeenkomen met werkelijk uitgegeven autorisaties in de applicatie:

1. Autorisaties in applicatie komen overeen;
2. Namen medewerkers komen overeen;
3. Autorisaties van medewerkers komen overeen;

	Aanmaken gebruiker	Invoeren inkooporder	Goedkeuren inkooporder
Functioneel beheerder	V	X	X
Inkoopmedewerker A		V	
Inkoopmedewerker B		V	
Senior medewerker Inkoop	X	X	V

Naam	Taak/Functie/Verantwoordelijkheid
Hans Seerden	Functioneel beheerder
Vicky Coolen	Inkoopmedewerker A
Yasmina Beelen	Inkoopmedewerker A
Karen Janssen	Inkoopmedewerker A
Saïd el Ahmadi	Inkoopmedewerker B
Harold Pijnacker	Inkoopmedewerker B
Rebecca Hazelton	Senior medewerker Inkoop



Afwijkingen en benodigde wijzigingen moeten worden geregistreerd. Voor wijzigingen is een akkoord benodigd van de proceseigenaar. Gaat de proceseigenaar niet akkoord, dan is de huidige situatie van kracht. Ook dit moet geregistreerd worden.
Afwijkingen worden daarnaast geregistreerd als een beveiligingsincident. Hierbij wordt nagegaan of er onterecht gebruik is gemaakt van de uitgegeven autorisaties. De DSPO waarborgt dat functioneel beheerders de check periodiek uitvoeren.

Frequentie control
De frequentie van deze controle is afhankelijk van het Basisbeveiligingsniveau (BBN) dat geldt voor het informatiecluster waarin de applicatie valt. Voor BBN 2 en 3 geldt dat deze controle iedere 6 maanden uitgevoerd moet worden. Voor BBN 1 geldt dat deze controle iedere 12 maanden uitgevoerd moet worden.

6.7. Rapportage door de DSPO

De DSPO beoordeelt of de controle door de functioneel beheerders, proceseigenaren en AOG heeft plaatsgevonden en rapporteert de bevindingen uit de periodieke controle aan het management. Voor IVA AD geldt dat de desbetreffende DSPO ook de technisch beheerders en applicatiebeheerders controleert. Zie bijlage 1 voor de controlechecklist.

Over de resultaten van iedere periodieke controle wordt zowel aan de CISO als aan de relevante proceseigenaren gerapporteerd. Deze rapportage dient van de volgende onderdelen te zijn voorzien:

- Wie heeft de controle uitgevoerd?
  - De volledige naam, functie en voorzien van een (herleidbare) handtekening/paraaf;
- Resultaten van de controle, die kan bestaan uit:
  - Autorisatie overzichten (voor controles zie H 6, voorzien van een productiedatum);
  - Een controledatum;
  - De conclusie van de controle;
- Aanbevelingen

Tot slot is er in bijlage 1 een overzicht opgenomen met alle verwijzingen naar specifieke controls en maatregelen vanuit de BIO die betrekking hebben op logische toegangsbeveiliging.

7. Bijlage 1: Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

6.1.2	Scheiding van taken
9.1.1	Beleid voor toegangsbeveiliging
9.1.2	Toegang tot netwerken en netwerkdiensten (zie beleid mobiele apparatuur)
9.2.1	Registratie en afmelden van gebruikers
9.2.1.1	Sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties
9.2.1.2	Gebruik van groepsaccounts is niet toegestaan zonder motivatie en vastlegging.
9.2.2	Gebruikers toegang verlenen
9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris
9.2.2.2	Risicoafweging voor functiescheiding en toegangsrechten
9.2.2.3	Mandaatregister met bevoegdheden voor het verlenen van toegangsrechten
9.2.3	Beheren van speciale toegangsrechten
9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers
9.2.5	Beoordeling van toegangsrechten van gebruikers
9.2.5.1 1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.(tenzij in dit document anders bepaald)
9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident
9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld
9.2.6	Toegangsrechten intrekken of aanpassen
9.3.1	Geheime authenticatie-informatie gebruiken
9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden middels wachtwoordkluis
9.4.1	Beperking toegang tot informatie
9.4.1.1	Maatregelen fysiek en/of logisch isoleren van informatie met specifiek belang
9.4.1.2	Gebruikers kunnen alleen die informatie inzien/verwerken die ze nodig hebben
9.4.2	Beveiligde inlogprocedures
9.4.2.1	Toegang vanuit onvertrouwde zone naar vertrouwde zone gebeurd op tweefactor authenticatie
9.4.2.2	Risicoafweging voor externe leveranciers voor toegang tot netwerk
9.4.3	Systeem voor wachtwoordbeheer (Helmonds beleid afgestemd op best practices)
9.4.4	Speciale systeemhulpmiddelen gebruiken
9.4.5	Toegangsbeveiliging op programmabroncode
11.2.9	‘Clear desk’- en ‘clear screen’-beleid
11.2.9.1	Een onbeheerde werkplek in een ongecontroleerde omgeving is altijd vergrendeld
11.2.9.2	Automatische schermbeveiliging na 15 minuten inactiviteit
11.2.9.3	Sessies met een remote desktop worden na 15 minuten inactiviteit vergrendeld
11.2.9.4	Systemen die chipcardtoken gebruiken worden bij verwijderen van de token automatisch vergrendeld

8. Woordenlijst

Active Directory	Active Directory is een Microsoft-product dat bestaat uit verschillende services voor het beheer permissies en toegang. Het staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een volledig bedrijf te beheren.
Admin	Een gebruiker met verhoogde rechten op een applicatie of systeem.
Bring Your Own Device (BYOD)	(Externe) medewerkers die hun privé-apparatuur gebruiken voor zakelijke verwerkingen.
Data protection impact assessment (DPIA)	Instrument / onderzoek om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en om daarna maatregelen te kunnen nemen om de risico's te verkleinen.
Electronic Identities And Trust Services (eIDAS)	Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen.
IDS - Intrusion Detection System	Geautomatiseerd systeem dat hackpogingen en voorkomens van ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert.
IPS – Intrusion Prevention System	Geautomatiseerd systeem dat hackpogingen en voorkomens van ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert en blokkeert.
Multifactor authenticatie	Multi-Factor Authenticatie (MFA) een methode voor authenticatie waarbij de gebruiker twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen.
Remote Desktop Protocol	Remote desktop is een functionaliteit die ervoor zorgt dat één of meer mensen via een pc, de "client", toegang kunnen krijgen tot een andere computer, de "remote". Het remote desktop-protocol (RDP) is een meerkanaalsprotocol dat gebruikt wordt om verbinding te kunnen maken tussen de partijen.
Single Sign On	Single sign-on -software (afgekort SSO) stelt eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk. Eenmalig inloggen is de Nederlandse term.
Software-as-a-Service (SaaS)	Software die als een online dienst wordt aangeboden.