TOOLS4EVER

Whitepaper V1.0 / 28 09 2022

BIO

en de rol van Identity Management

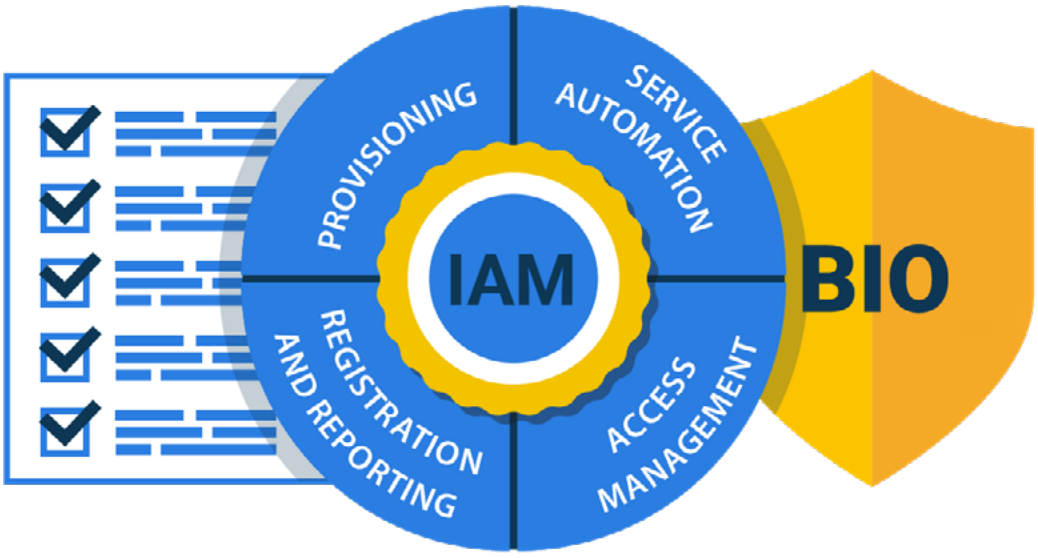
Inhoudsopgave

Inleiding

De Baseline Informatiebeveiliging Overheid (BIO) vormt sinds 2020 hét basisnormenkader voor informatiebeveiliging binnen de gehele overheid. De BIO vervangt eerdere normen (BIG, BIWA, IBI en BIR) die allemaal waren gericht op specifieke overheidslagen zoals gemeenten, waterschappen, provincies en het Rijk. BIO is gebaseerd op de internationale standaard voor informatiebeveiliging ISO 27001 en ISO 27002.

Het gebruik van één norm voor alle bestuurslagen die bovendien is gebaseerd op een internationaal geaccepteerde beveiligingsstandaard zorgt voor een veel effectievere informatiebeveiliging binnen de overheid. Naast alle overheidsorganisaties wordt de BIO ook geadviseerd voor organisaties waarmee de overheid publiek-privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is.

In deze whitepaper geven we eerst een overzicht van de BIO. Vervolgens tonen we welke rol Identity Management speelt bij het BIO compliant maken van overheidsinstellingen.



Van ISO 27001 en ISO 27002 naar BIO

BIO is gebaseerd op ISO 27001 en 27002. Beiden staan op de zogenaamde 'pas toe of leg uit'-lijst van de overheid.

ISO 27001 richt zich op informatiebeveiliging managementsystemen en beschrijft vooral hoe informatiebeveiliging procesmatig ingericht moet worden, zodat de vertrouwelijkheid, beschikbaarheid en integriteit van informatie is gegarandeerd. Zo eist de BIO een uitgebreide risico analyse naar mogelijke dreigingen en de impact ervan. Aan de hand hiervan wordt bepaald welke maatregelen nodig zijn en wel (rest)risico's acceptabel zijn. Informatiebeveiliging gaat dus niet om het blind afvinken van een standaard lijst met maatregelen, de grootste risico's moeten daadwerkelijk de hoogste prioriteit krijgen. Ook vereist de BIO dat een Plan-Do-Check-Act cyclus wordt doorlopen. Er moet voortdurend worden gemonitord of de bestaande beveiligingsmaatregelen nog steeds voldoen of inmiddels aangepast moeten worden.

Vervolgens wordt de BIO concreet ingevuld aan de hand van ISO 27002. De ISO 27002-standaard vormt een set best practices met beveiligingsmaatregelen (zogenaamde 'controls'). De standaard geeft dus een nadere invulling van ISO 27001. ISO 27002 bestaat uit 114 beheersmaatregel en de BIO volgt dezelfde structuur. De controls zijn in de BIO letterlijk overgenomen. Waar nodig vult de BIO deze aan met specifieke overheidsmaatregelen met verfijnde of aanvullende eisen. Een voorbeeld van zo'n BIO maatregel die een ISO control specifieker invult:

- ISO 27002 beschrijft in control 9.4.2 over beveiligde inlogprocedures dat "Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure."

- De BIO voegt hier maatregel 9.4.2.1 aan toe met een concretere eis: "Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie."

BBN

Daarbij maakt de overheid onderscheid tussen drie zogenaamde basisbeveiligingsniveaus (BBN). BIO biedt een BBN-toets waarmee voor ieder bedrijfsproces binnen een organisatie het vereiste BBN niveau kan worden bepaald:

BBN1 is het minimale basis beveiligingsniveau dat men kan verwachten van de overheid. In BBN1 ontbreken complexe beveiligingseisen en BBN1 systemen kunnen bijvoorbeeld niet worden ingezet voor de verwerking van persoonsgegevens.

BBN2 is het beveiligingsniveau dat voor de meeste overheidsinformatie van toepassing is. Met BBN2 mag maximaal Departementaal Vertrouwelijk (DepV) en soortgelijke Privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau worden verwerkt. Ook persoonsgegevens, commercieel vertrouwelijke informatie en informatie in het kader van beleidsvorming vragen om BBN2. Bovendien moeten dreigingen van statelijke actoren en vergelijkbare dreigingen in ieder geval gedetecteerd kunnen worden.

BBN3 gaat duidelijk verder qua beveiliging want er zijn aanvullende maatregelen nodig om weerstand te kunnen bieden tegen statelijke actoren of criminele organisaties (of gelijksoortige actoren) of waar informatie wordt verwerkt die een classificatie heeft boven BBN2.

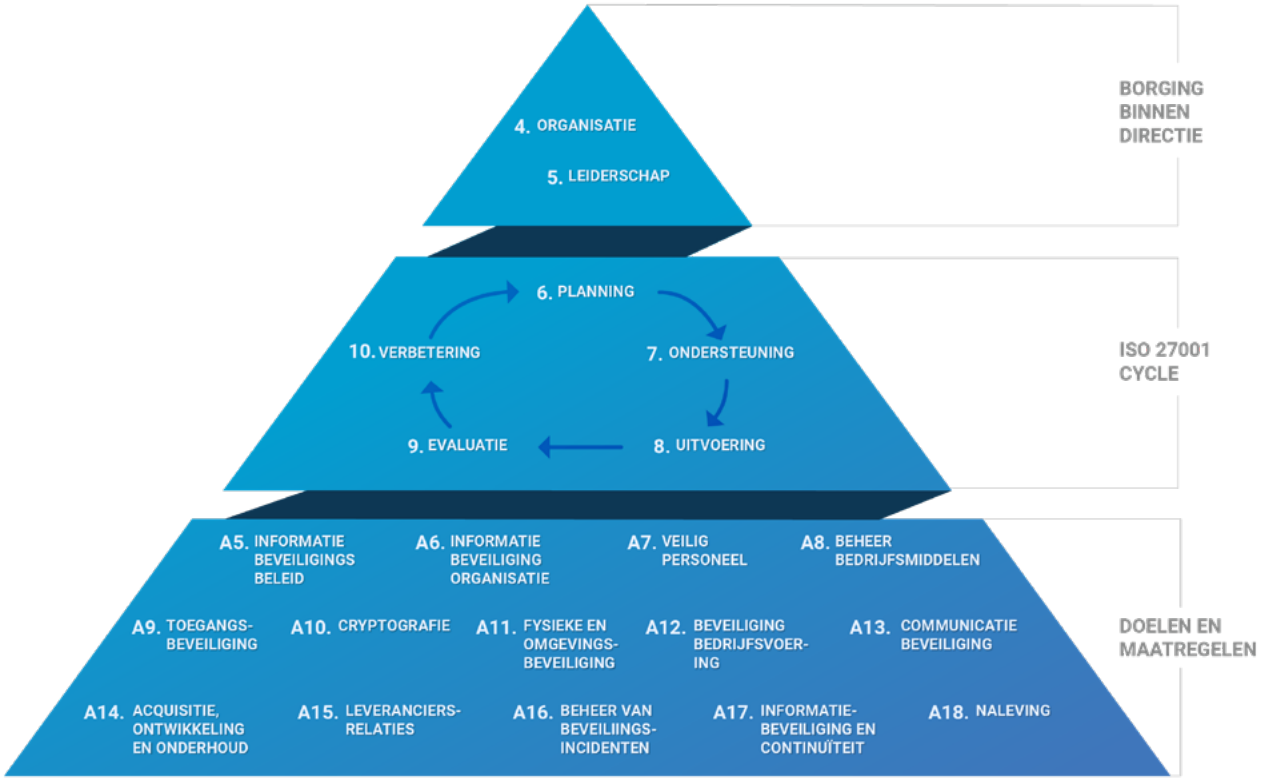
Vervolgens is in de BIO per control/maatregel beschreven of deze vereist is op BBN1 of BBN2. BBN1 processen hoeven alleen BBN1 maatregelen te implementeren, BBN2 processen moeten uiteraard zowel BBN1 als BBN2 maatregelen ondersteunen. Je vindt binnen de BIO geen aanvullende BBN3 maatregelen, want dat niveau vraagt maatwerk of men gebruikt NAVO en EU-normen.

In Deel 2 van de BIO (het Kader BIO) vind je de genoemde BBN-toets. Ook worden hier de niveaus zijn verder beschreven aan de hand van de eisen die worden gesteld op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid:

BBN	Beschikbaarheid	Integriteit	Vertrouwelijkheid
1	Laag	Laag	Laag
2	Midden	Midden	Midden
3	Midden	Midden	Hoog

Controls en overheidsmaatregelen

Het Kader BIO omvat naast de BBN toets en beschrijving vooral ook een overzicht van alle controls en maatregelen. Deze zijn ingedeeld in 14 verschillende categorieën (hoofdstuk 5 t/m 18):



5. Informatiebeveiligings-beleid	Als aanvulling op het algemene organisatiebeleid moet ook een specifiek informatiebeveiligingsbeleid worden opgesteld en regelmatig geëvalueerd.
6. Organisatie van informatiebeveiliging	Er is niet alleen een informatiebeveiligingsbeleid nódig, het moet ook worden geïmplementeerd en beheerd. Welke rollen zijn nodig met welke verantwoordelijkheden en bevoegdheden? Rolscheiding is daarbij een belangrijk aandachtspunt en ook is er vandaag de dag veel aandacht nodig voor online werken en het gebruik van (eigen) mobiele apparaten.
7. Veilig personeel	Uiteraard moeten medewerkers voldoende zijn opgeleid en zich bewust zijn van het belang van informatiebeveiliging. Dat betreft het hele 'dienstverband', van de juiste werving van medewerkers tot en met de benodigde beveiligingsmaatregelen als mensen de organisatie weer verlaten.
8. Beheer van bedrijfsmiddelen	Bedrijfsmiddelen om informatie te verwerken (zoals software en computersystemen) moeten goed geregistreerd en beheerd worden. Wie mag de systemen gebruiken en worden bedrijfsmiddelen en gebruiksrechten na beëindiging van de werkzaamheden weer teruggegeven? Alle informatie moet goed worden geclassificeerd en voldoende veilig opgeslagen.
9. Toegangsbeveiliging	Er zijn maatregelen nodig om te zorgen dat medewerkers alleen toegang krijgen tot netwerken, systemen en gegevens die ze nodig hebben voor hun eigen werkzaamheden.
10. Cryptografie	Gegevens moeten voldoende versleuteld worden om zowel de vertrouwelijkheid als de integriteit van gegevens te kunnen garanderen.
11. Fysieke beveiliging en beveiliging van de omgeving	Organisaties moeten voorkomen dat onbevoegden toegang krijgen tot computers en gegevensdragers op kantoorlocaties. Dat betekent ook dat bij bijvoorbeeld stroomuitval of een calamiteit de informatiebeveiliging intact moet blijven. En bij afvoer van apparatuur moeten de gegevens verwijderd zijn.
12. Beveiliging bedrijfsvoering	Er moeten duidelijke afspraken en procedures zijn om informatiesystemen veilig te gebruiken en de systemen te beschermen tegen malware. Ook zijn er duidelijke back-up en monitoring maatregelen nodig.
13. Communicatiebeveiliging	Zowel de interne netwerkfaciliteiten als de externe netwerkcommunicatie moeten beveiligd zijn tegen onbevoegde toegang en misbruik.
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	Organisaties moeten bij inkoop, ontwikkeling en beheer van IT systemen rekening houden met de beveiliging van de systemen en data. Daarbij gaat het niet alleen om operationele systemen. Ook bijvoorbeeld ontwikkel-, demo- en testsystemen moeten voldoende beveiligd zijn.

15. Leveranciersrelaties	Organisaties zijn afhankelijk van leveranciers voor hun IT systemen. Dat geldt zowel voor systemen en software die on-premises worden geleverd, als leveranciers die gevoelige cloud data beheren. Er zijn duidelijke afspraken met leveranciers nodig om de informatiebeveiliging te garanderen.
16. Beheer van beveiligingsincidenten	Ondanks alle beveiligingsmaatregelen kan er toch een incident plaatsvinden. Hiervoor moeten goede procedures met duidelijke verantwoordelijkheden aanwezig zijn, inclusief afspraken over de verdere rapportage en oplossing.
17. Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	Bij incidenten met de IT voorzieningen moet er specifiek op worden gelet dat de continuïteit van de informatiebeveiliging altijd gegarandeerd blijft.
18. Naleving	Als organisatie moet je voortdurend kunnen aantonen dat je voldoet aan alle geldende wet- en regelgeving.

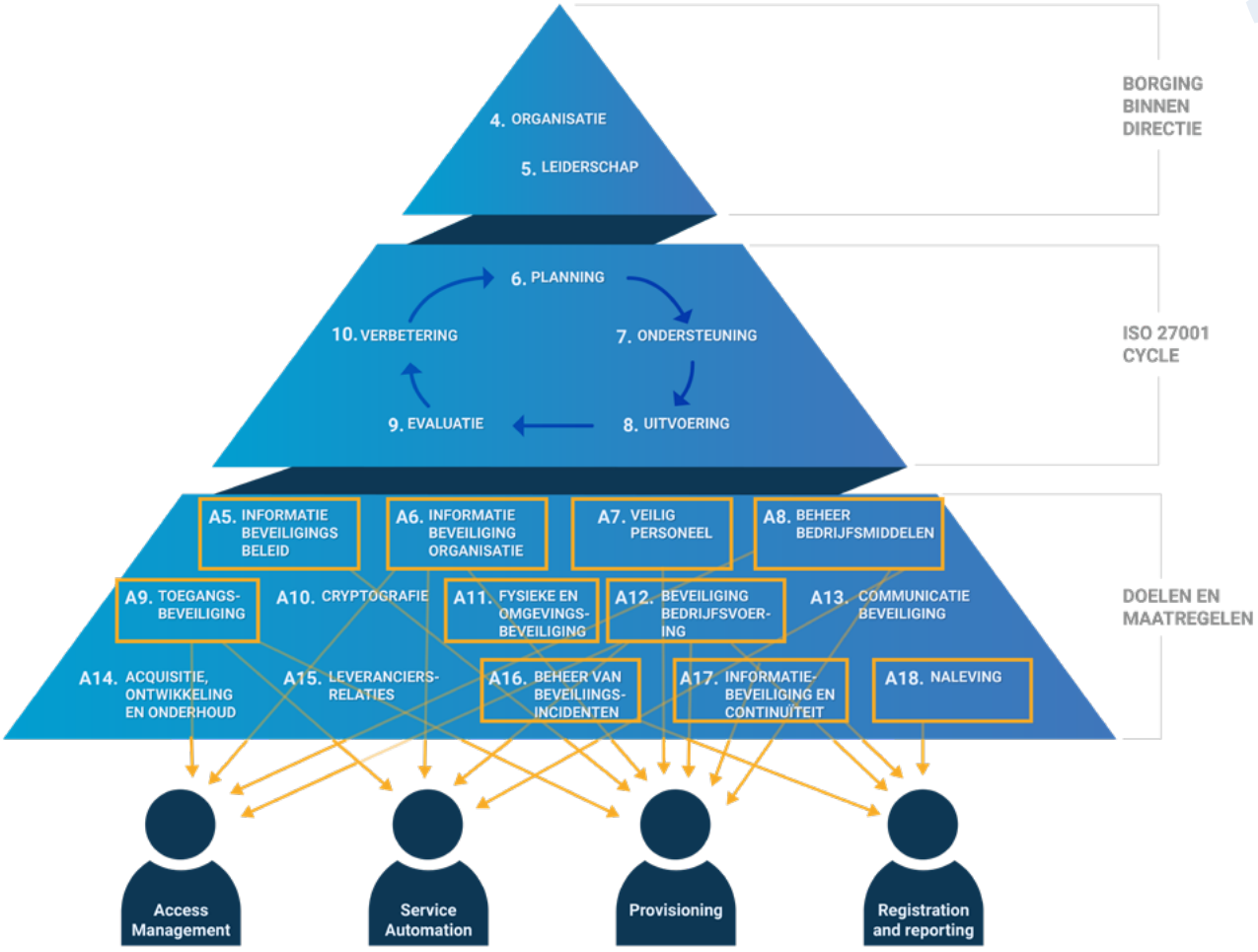
Zoals aangegeven beschrijft ISO 27002 meer dan honderd controls en de BIO heeft een aanzienlijk deel van de controls verder uitgewerkt met aanvullende maatregelen. Sommige maatregelen zijn elementair voor een betrouwbare en professionele informatievoorziening binnen de overheid. Anderen komen direct voort uit bestaande wet- en regelgeving waar overheidsinstellingen sowieso aan moeten voldoen. Daarnaast zijn er maatregelen die cruciaal zijn om de beveiliging in een procesketen of netwerk binnen overheidsorganisaties te garanderen. Als binnen een overheidssysteem zo'n maatregel niet wordt geïmplementeerd vormt dat direct een risico voor alle andere partijen in de keten. Ook voor zogenaamde generieke diensten is dat belangrijk.

Concreet biedt de BIO dus in de onderstaande categorieën een overzicht van 114 ISO 27002 controls (in blauwe tekst in de BIO) en de aanvullende overheidsmaatregelen (herkenbaar aan groen).

De BIO omvat ook nog een addendum met eisen die specifiek verplicht zijn voor een bepaalde overheidslaag.

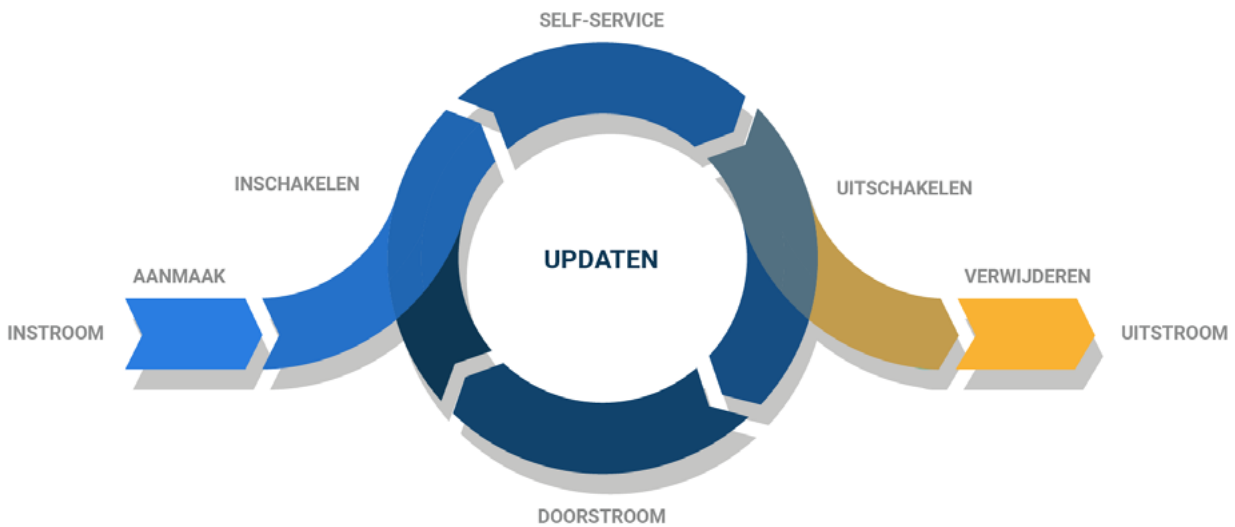
Identity Management en BIO

De BIO vult dus de ISO controls aan met maatregelen die een overheidsorganisatie moet implementeren om informatie goed te beveiligen. Het beheer van eindgebruikers en hun rechten worden daarbij steeds belangrijker. Medewerkers, partners en klanten mogen alleen toegang krijgen tot applicaties en data op een 'need to know' basis. Ook is het noodzakelijk dat alle IT activiteiten zijn te traceren tot het niveau van individuele gebruikers. Het maakt Identity Management een belangrijk gereedschap bij de realisatie van een 'BIO proof' informatiebeveiliging. In dit hoofdstuk mappen we de verschillende categorieën met BIO controls en maatregelen op de mogelijkheden binnen een state-of-the-art Identity Management oplossing. Dit illustreren we aan de hand van onze eigen HelloID cloudbased Identity & Access Management (IAM) platform.



Provisioning van gebruiksaccounts en -rechten

Groepsaccounts zijn in het algemeen binnen de overheid niet toegestaan, evenals het 'copy user' principe voor nieuw binnenkomende medewerkers. Toegangsrechten moeten vandaag de dag eenduidig zijn gekoppeld aan individuele gebruikersaccounts. Er moet op ieder moment duidelijk zijn wie er toegang heeft tot data en applicaties en wie bepaalde handelingen uitvoert. En natuurlijk moeten de accountgegevens en toegangsrechten altijd up-to-date zijn. Dus steeds in lijn met iemands huidige rol en positie binnen de organisatie. Professioneel en geautomatiseerd gebruikersaccountmanagement is daarvoor cruciaal.



Binnen HelloID borgen we dit door middel van geautomatiseerde provisioning. Hiermee zijn iemands digitale identiteit en toegangsrechten altijd in lijn met de informatie zoals geregistreerd in het HR systeem. Dankzij een rechtstreeks koppeling tussen dat HR systeem en HelloID ontvangt de nieuwe medewerker bij onboarding direct een gebruikersaccount met daaraan gekoppeld de faciliteiten en rechten die passen bij diens rol. Ook tijdens het verdere dienstverband houden we dit automatisch actueel. Verandert iemands rol, dan past HelloID ook direct de toegangsrechten aan. En verlaat iemand de organisatie, dan zorgt HelloID dat automatisch het account wordt geblokkeerd en de vertrekkende medewerker geen toegang meer heeft. Stapeling van rechten en accounts die per ongeluk toegankelijk blijven zijn niet langer mogelijk.

Automation: standaardisatie met ruimte voor uitzonderingen

Goede informatiebeveiliging leunt op duidelijke beleidsregels, heldere processen en weinig ruimte voor individueel en ongecontroleerd maatwerk. Om dat te borgen willen we identity management processen zoveel als mogelijk standaardiseren en automatiseren. Daarbij moet het mogelijk zijn concepten als Role Based access te ondersteunen en processen te implementeren met een duidelijke scheiding van rollen. Tegelijkertijd zijn er altijd uitzonderingen en moet iedere organisatie een eigen balans zoeken tussen gebruiksvriendelijkheid en bedrijfsveiligheid. Automatisch te veel rechten verstrekken, leidt tot ongewenste beveiligingsrisico's. Maar medewerkers steeds onnodig laten wachten op hun toegangsrechten belemmert hun werk.

HelloID biedt die gewenste combinatie van standaardisatie en uitzonderingen:

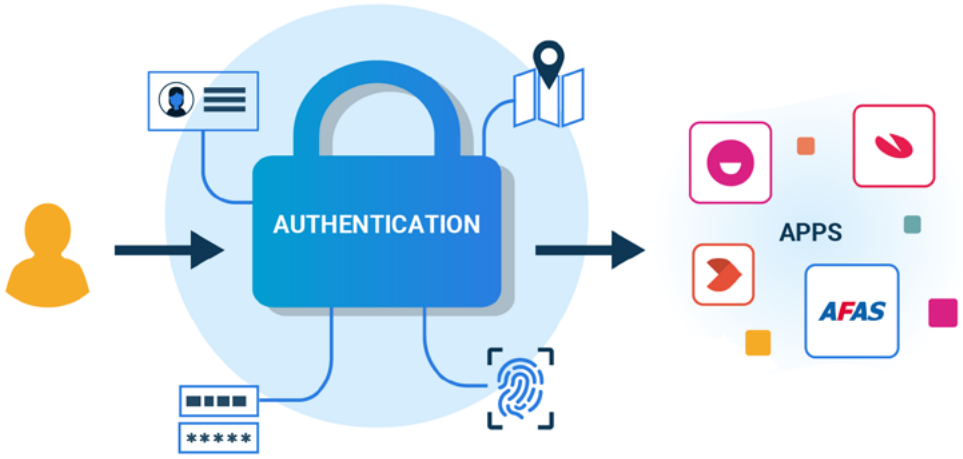
- *Standaard kun je binnen HelloID rechten toekennen met behulp van de zogenaamde Attribute Based Access Control (ABAC) functionaliteit. De organisatiestructuur met rollen en bijbehorende werkzaamheden vertalen we in HelloID naar configureerbare business rules die automatisch bepalen welke toegangsrechten een medewerker krijgt. Vanaf de automatisch onboarding bij indiensttreding tot en met de vertrekprocedure bij vertrek.*

- *Het merendeel van de rechten wordt dus volledig geautomatiseerd uitgegeven, maar zo'n standaard rollenmatrix is nooit volledig dekkend en daarom voorziet HelloID ook in uitzonderingen. Voor specifiekere en moeilijker automatisch uitdeelbare rechten kun je self-service processen ontwerpen. Gebruikers kunnen hiermee zelf online toegang vragen tot applicaties of datashares waarbij automatisch de juiste goedkeuringsstappen worden gevolgd. Na goedkeuring zorgt het geautomatiseerde proces voor de verdere activering zonder risicovolle uitzonderingen of vergissingen.*

Geautomatiseerde configuratieregels zorgen dat de dienstencatalogus automatisch up-to-date blijft. Een nieuwe share wordt bijvoorbeeld direct zichtbaar in de catalogus. Op ieder moment kan het systeem een overzicht geven van welke medewerkers actief zijn en welke licenties, applicaties, shares, et cetera zij in gebruik hebben.

Access management

Een state-of-the-art toegangsmanagement zorgt dat medewerkers - en zo nodig ook partners en klanten - eenvoudig en uniform toegang krijgen tot applicaties en data. Zoals hiervoor uitgelegd is het uitgangspunt daarbij dat iedere gebruiker is voorzien van één persoonlijk gebruikersaccount. Met een concept als Single Sign-On zorg je vervolgens dat mensen maar één keer hoeven in te loggen. Juist zo'n combinatie van gebruiksvriendelijke én veilige toegang-soplossingen voorkom je dat medewerkers onveilige work-arounds verzinnen.



HelloID ondersteunt alle gangbare Single Sign-On protocollen om gebruikers per applicatie te authentiseren. Voor toegang tot applicaties zonder ingebouwde SSO faciliteiten, biedt HelloID andere methodes om de toegang te verzorgen. Voor de primaire authenticatie kunnen we HelloID integreren met Active Directory en andere zogenaamde Identity Providers zoals Azure, Google, Salesforce, SAML en OpenID. Ook ondersteunt het platform extra beveiligingsopties zoals Two Factor Authentication (2FA). HelloID herkent contextuele factoren zoals de inloglocatie en het tijdstip en kan afhankelijk daarvan de gebruiker vragen om een extra authenticatie. Naast soft of hard tokens en sms biedt HelloID ook verschillende one time passwords (OTP's) als tweede factor.

Cloud based Identity Management met hoge beschikbaarheid

Ook steeds meer overheidsorganisaties migreren hun bestaande IT dienstverlening naar de cloud en ook voor Identity en Access Management zoekt men dus een cloud-based oplossing. De beschikbaarheid, betrouw-baarheid en veiligheid is daarbij cruciaal. Als centrale schakel binnen de dienstverlening moet de 'identity management' keten altijd functioneren en mag de toegangsbeveiliging nooit worden 'kortgesloten'.

HelloID verzorgt Identity & Access Management vanuit de cloud met als voordeel lagere investeringen, een snelle installatie en configuratie terwijl Tools4ever het technische beheer verzorgt, inclusief automatische updates. De oplossing wordt gerealiseerd met behulp van maximaal beveiligde Microsoft Azure- en Google Cloudomgevingen, die bovendien iedere zes maanden grondig wordt gecontroleerd door Deloitte Risk Services. Compliance aan de strenge securi-ty-eisen is dan ook gewaarborgd. De dienstverlening heeft bovendien een zeer hoge beschikbaarheid dankzij de ingebouwde redundantie.

Reporting

Binnen de BIO is registratie en rapportage essentieel. Als organisatie moet je kunnen aantonen dat de verschillende processen conform de relevante wet- en regelgeving worden uitgevoerd. Ook moet je bij een beveiligingsincident zoals een datalek kunnen traceren welke gebruikers binnen het netwerk welke handelingen hebben uitgevoerd.

Als cloud based oplossing moet HelloID voldoen aan steeds strengere wet- en regelgeving op het gebied van audits en beveiliging. Alle toegangspogingen, geautomatiseerde en handmatige processen, en het gebruik van ons platform worden daarom geregistreerd en inzichtelijk gemaakt. Zo wordt het authenticatieproces automatisch gemonitord en is via rapportages altijd inzichtelijk wie welke applicaties heeft geraadpleegd, op welk moment en vanaf welke locatie. Dit geeft niet alleen een gedetailleerd beeld van het doorlopen authenticatietraject, maar toont bijvoorbeeld ook inlogpogingen vanaf verdachte IP-adressen. Mogelijke dreigingen kunnen tijdig worden herkend om tegenmaatregelen te nemen.

Extra onderscheidend is dat binnen HelloID de volledige identity lifecycle per systeem én per gebruiker auditable is. Alle uitgevoerde acties worden gelogd, zoals het creëren, inschakelen, updaten, verplaatsen, disablen en verwijderen van accounts. Hetzelfde geldt voor het toekennen en intrekken van permissies. Zijn rechten ad hoc toegekend (buiten de reguliere rollenmatrix) dan is via HelloID precies te zien wie dit heeft aangevraagd, welke persoon het verzoek heeft goedgekeurd en tot welke exacte wijzigingen in achterliggende systemen dit heeft geleid. Daarmee is het HelloID proces volledig transparant, toetsbaar en aanpasbaar.

Meer weten?

Identity Management vormt vandaag de dag een centrale rol binnen je IT beveiliging. Medewerkers, partners en klanten mogen alleen nog met een eigen account toegang krijgen tot applicaties en data. Rechten moeten altijd worden verstrekt op een ‘need to know’ basis. We moeten bovendien alle IT activiteiten tot het niveau van individuele gebruikers kunnen traceren. Het maakt je Identity Management platform een belangrijk element bij het inrichten van je BIO compliant informatiebeveiligingssysteem.

Meer weten over de rol die Identity Management kan spelen bij de BIO compliancy binnen je organisatie? En hoe kun je je IT omgeving veilig houden zonder in te leveren op gebruiksvriendelijkheid? We vertellen je hier graag meer over. Bijvoorbeeld aan de hand van onze reference list BIO – HelloID. In deze lijst behandelen we alle BIO controls en maatregelen met per maatregel een toelichting of – en zo ja, hoe – HelloID Identity Management hieraan een bijdrage kan leveren.

TOOLS4EVER

Adres	Amalialaan 126c 3743 KJ Baarn Nederland
Telefoon	+31 (0) 35 54 832 55
Website	Tools4ever.nl
Mail	info@tools4ever.com
Sales	sales@tools4ever.com
Support	tools4ever.nl/support