

BIO-compliant account- en rechtenbeheer met de HelloID Governance module

Hoogheemraadschap Hollands Noorderkwartier is de waterbeheerder van Noord-Holland boven het Noordzeekanaal en inclusief Texel. Het hoogheemraadschap verzorgt de bescherming van het land tegen het water met veilige dijken, duinen en ruim tachtig sluizen. Daarnaast zorgt de organisatie voor schoon oppervlaktewater met vijftien rioolwaterzuiveringen, en met ruim 2200 gemalen beheert men het waterpeil in sloten en vaarten. Hierbij wordt gebruik gemaakt van verschillende IT-applicaties waarin ook privacygevoelige gegevens worden verwerkt. Mede daarom loopt binnen het hoogheemraadschap een uitgebreid project om de compliance met de Baseline Informatiebeveiliging Overheid (BIO) te borgen. Een belangrijk hulpmiddel daarbij is de Governance module van het HelloID Identity-as-a-Service platform.

Roel Assenmacher, Identity & Access Management Specialist bij het hoogheemraadschap: "Binnen het hoogheemraadschap beheren we met HelloID alle gebruikersaccounts in twee gescheiden IT-netwerken, ieder met een eigen Active Directory. Eén netwerk is ontkoppeld van internet en gebruiken we alleen voor de automatisering van technische beheersystemen zoals waterzuiveringssystemen en gemalen. Het andere netwerk wordt gebruikt voor de overige applicaties, zoals de reguliere kantoorautomatisering en verdere bedrijfstoepassingen. Gebruikers worden via Active Directory voorzien van onder andere basisrechten, mailaccounts en groepen. Ook verstrekken we de accounts voor TOPdesk, Studytube, de Unit4 tijdschijfapplicatie, Key2Belastingen en Key2Datadistributie. Die laatste twee applicaties gebruiken we binnen het hoogheemraadschap onder meer voor de heffing van de waterschapsbelasting. Voor deze applicaties verstrekken we niet alleen de accounts maar beheren we ook de verschillende toegangsrechten. Het overgrote deel van die rechten worden automatisch verstrekt met de HelloID Provisioning functionaliteit aan de hand van medewerkersgegevens zoals iemands functie of afdeling. Maar er zijn ook specifieke rechten die individueel worden toegewezen met behulp van de Service Automation module. Deze module wordt daarnaast gebruikt voor andere individuele licentie- en rechtenaanvragen."

In principe willen we binnen het hoogheemraadschap alle gebruikersaccounts en rechten beheren via HelloID, vertelt Roel: "Natuurlijk zullen er in de praktijk altijd uitzonderingen zijn maar het is wel een helder uitgangspunt in het kader van onze

Klant

Hoogheemraadschap Hollands Noorderkwartier

Uitdaging

Binnen het hoogheemraadschap loopt een organisatie breed project om de compliance met de Baseline Informatiebeveiliging Overheid (BIO) te borgen. Account- en rechtenbeheer is daarbij een belangrijk onderdeel en de vraag is hoe we dat beheer aantoonbaar compliant kunnen laten zijn.

Oplossing

Door accounts en rechten zoveel mogelijk te beheren via HelloID kun je op ieder moment aantonen dat je voldoet aan alle privacy- en beveiligingsrichtlijnen. De governance functionaliteit kan daarbij helpen die compliance te realiseren en daarna deze voortdurend te controleren en verder te verbeteren.

Producten

HelloID Provisioning - Service Automation - Governance. Koppelingen met HR systeem Youforce. Koppelingen met doelsystemen als Active Directory, TOPdesk, Studytube, de Unit4 tijdschijfapplicatie, Key2Belastingen en Key2Datadistributie. Koppeling met de Basisregistratie Kadaster (BRK) en de Unit4 Financiële applicatie worden onderzocht.

Resultaat

Dankzij de reconciliation functionaliteit van de HelloID Governance module kunnen we nu het rechtenbeheer binnen HelloID gaandeweg uitbreiden, verbeteren en optimaliseren. We werken er naartoe om zoveel mogelijk accounts en rechten te beheren via HelloID. Daarnaast zien we ook nuttige use cases voor de andere HelloID Governance functionaliteit zoals reconciliation en toxic rule beheer.

"De HelloID governance module is voor het hoogheemraadschap een belangrijk gereedschap voor onze BIO compliance. Met de governance tools ontdekken we inconsistenties tussen systemen, kunnen we business rules verder optimaliseren en voorkomen we onnodig gebruik van dure licenties"

Roel Assenmacher

Identity & Access Management Specialist bij Hoogheemraadschap Hollands Noorderkwartier

compliance met de Baseline Informatiebeveiliging Overheid (BIO). Binnen het hoogheemraadschap loopt daarvoor momenteel een organisatie breed project. Toegangsbeheer is een belangrijk element binnen de BIO en daarom willen we dat verstrekte accounts en rechten zoveel als mogelijk traceerbaar zijn binnen HelloID. We registreren en verwerken via systemen als Key2Belastingen, Key2Datadistributie en de Basisregistratie Kadaster (BRK) veel privacygevoelige gegevens en we willen op ieder moment kunnen aantonen wie daar toegang toe hebben en waarom. Daarom hebben we actief deelgenomen aan een pilot van de nieuwe Governance module van HelloID. We kunnen met de bestaande Provisioning en Service Automation modules nu al accounts en rechten verstrekken, registreren en beheren. Met de nieuwe governance functionaliteit willen we nu ook proactief inconsistenties tussen HelloID en de doelsystemen herkennen en oplossen. Daarnaast willen we hiermee ons raamwerk van business rules steeds verder uitwerken en als spin-off willen we voorkomen dat kostbare IT-licenties onnodig in gebruik blijven."

Inconsistenties ontdekken met de reconciliation feature

"We gebruiken de reconciliation functionaliteit nu al intensief. Zoals ik vertelde willen we accounts en rechten zoveel mogelijk beheren via HelloID. In dat geval zijn vrijwel alle accounts en rechten én geregistreerd binnen HelloID én geactiveerd binnen de betreffende doelsystemen. Met de reconciliation tool kun je dan eenvoudig inconsistenties ontdekken tussen HelloID en de doelsystemen als gevolg van vergissingen of technische fouten. Die kunnen we dan snel herstellen, het rechtenbeheer compliant houden en verder optimaliseren.

Zover zijn we echter nog niet. Op dit moment wordt nog een deel van de accounts en rechten rechtstreeks handmatig aangemaakt binnen doelsystemen en dan zijn vergissingen sowieso altijd mogelijk. Dan treffen we bijvoorbeeld in AD groepen medewerkers aan die daar vanuit hun functie of afdeling niet thuishoren. Of we vinden shared mailboxen die zijn gekoppeld aan groepen, wat ongewenst is. Dankzij reconciliation kunnen we zulke mismatches nu eenvoudig ontdekken en analyseren. Soms blijkt er sprake van achterhaalde instellingen die we kunnen opruimen. Maar we vinden ook accounts en rechten die nog actief worden gebruikt. Met deze gegevens en de output van onze role mining sessies kunnen we onze rechtenstructuur binnen HelloID gaandeweg uitbreiden en verfijnen. Voor ons is reconciliation zo een cruciaal gereedschap om ons account- en rechtenbeheer steeds beter te organiseren en het op ieder moment inzichtelijk te hebben voor audits."

Doorwerken aan de governance

Roel vertelt ook enthousiast over mogelijk vervolgstappen: "Naast reconciliation werken we ook aan use cases met de andere governance features. Zo zien we duidelijke toepassingen voor de recertification functie. We gebruiken de Service Automation module voor het individueel verstrekken van accounts en toegangsrechten. Dat doen we bijvoorbeeld bij rechten die we niet automatisch aan iedereen met een bepaalde functie of op een bepaalde afdeling willen geven. Ook verstrekken we soms individuele rechten ten behoeve van een bepaald project. Dat kunnen ook privacygevoelige applicaties betreffen zoals de Basisregistratie Kadaster en in dat geval willen we zo'n toegangsrecht regelmatig - bijvoorbeeld iedere drie of zes maanden - opnieuw laten beoordelen door de verantwoordelijke manager. Dankzij recertification kunnen we dat hele herbeoordelingsproces nu eenvoudig inplannen, laten uitvoeren en daarmee garanderen dat rechten weer tijdig worden ingetrokken. Naast onze compliance kan het ook helpen de kosten te beheersen want de uitgifte van dure licenties als Visio en MS Project kunnen we zo regelmatig opnieuw laten beoordelen.

Op vergelijkbare manier zien we ook een duidelijke case voor het toxic rule beheer binnen de Governance module. Binnen de Provisioning module ontvangen mensen rechten aan de hand van bijvoorbeeld hun functie of afdeling. Soms worden mensen in het HR-systeem gekoppeld aan meerdere functies of afdelingen en het effect hiervan kan zijn dat ze binnen HelloID meerdere en soms ook strijdige rechten ontvangen. Dat is ongewenst want je wilt bijvoorbeeld niet dat iemand binnen de belastingapplicatie toegang krijgt tot zowel de heffing- als de inningfunctionaliteit. Dankzij het toxic rule beheer binnen HelloID kunnen we dit soort strijdige rechten voortaan herkennen en voorkomen. Zo willen we met toxic rule beheer een extra vangnet inbouwen om uitgifte van strijdige toegangsrechten te voorkomen. Zo bekijken we binnen het hoogheemraadschap actief hoe we met de HelloID Governance module ons account- en rechtenbeheer steeds beter compliant en kostenefficiënt te maken!"

Voordelen

- Probleemloze uitrol
- Automatische provisioning en beheer van accounts en toegangsrechten
- Eenvoudig inconsistenties detecteren tussen HelloID en doelsystemen
- Governance functies tbv compliance en kostenbeheersing
- Compliant met wet- en regelgeving en goed auditeerbaar
- Cloud-based en toekomstgerichte oplossing