

NIS2

Van wetgeving naar veilig toegangsbeheer

Drie beste inzichten over:

- Wie onder de wet valt
- Zorgplicht, meldplicht en toezicht
- De rol van IAM bij NIS2

TOOLS4EVER



Inhoud

Inleiding	2
NIS2 en de Cyberbeveiligingswet	3
Welke organisaties vallen onder de Cyberbeveiligingswet?	5
Registratie en CSIRT	7
Zorgplicht	8
Meldplicht	9
Toezicht	11
Bestuursaansprakelijkheid	12
Hoe draagt IAM bij aan de NIS2 verplichtingen?	13
Over Tools4ever	15

Inleiding

In augustus 2026 is de Cyberbeveiligingswet (Cbw) in werking getreden. Deze wet implementeert binnen Nederland de EU-richtlijn 2022/2555, beter bekend als de NIS2-richtlijn (Network and Information Security). De wet vervangt de Wet beveiliging netwerk- en informatiesystemen (Wbni), die was gebaseerd op de eerdere NIS1-richtlijn.

De Europese richtlijn is vastgesteld om de cyberbeveiliging en digitale weerbaarheid van kritieke maatschappelijke of economisch belangrijke diensten in de EU-lidstaten te verbeteren. Kritieke diensten variëren van de energievoorziening en het betalingsverkeer tot de ICT-infrastructuur en de gezondheidszorg. Ten opzichte van NIS1 zijn er in NIS2 meer sectoren en organisaties opgenomen, en gelden nu uitgebreidere eisen voor risicobeheer, incidentmelding en toezicht. Ook is de aansprakelijkheid van bestuurders van organisaties beter vastgelegd.

In deze whitepaper geven we meer uitleg over de NIS2-richtlijn en de daaruit afgeleide wetgeving. We geven aan voor wie de wet van toepassing is, en aan welke eisen organisaties moeten voldoen. En omdat identity & access management een belangrijk hulpmiddel is om aan veel eisen te voldoen, zoomen we daar als IAM-specialist natuurlijk specifiek op in.



NIS2 en de Cyberbeveiligingswet

NIS2 verplicht organisaties die kritieke diensten leveren om dit centraal te registreren (registratieplicht), hun cyberrisico's actief te beheersen en daarvoor de noodzakelijke technische, operationele en organisatorische beveiligingsmaatregelen te treffen (zorgplicht). Ook is er een meldplicht voor significante incidenten. Het toezicht hierop is goed georganiseerd en de verantwoordelijkheden van bestuurders zijn nauwkeurig omschreven. De formele kaders voor bovenstaande zaken vind je in de volgende documenten:

- Uitgangspunt is de NIS2-richtlijn. Deze EU-richtlijn is in 2023 ingegaan en geeft de kaders voor de netwerk- en informatiebeveiliging rondom kritieke diensten, maar moest nog wel in iedere lidstaat worden omgezet in een nationale wet.
- In Nederland is daarvoor in 2026 de Cyberbeveiligingswet (Cbw) van kracht geworden. De inhoud van NIS2 vormt de basis, maar de wet legt vast hoe de NIS2-uitgangspunten in ons land precies worden gerealiseerd en gehandhaafd.
- Daarnaast is er het Cyberbeveiligingsbesluit (Cbb). Dit is de Algemene Maatregel van Bestuur (AMvB) die een verdere uitwerking geeft van de Cyberbeveiligingswet. Als de wet het bijvoorbeeld heeft over 'passende technische en organisatorische maatregelen', kunnen deze in het Cyberbesluit in detail zijn uitgewerkt.
- Ook zijn er ministeriële cyberbeveiligingsregelingen die de richtlijnen kunnen verfijnen voor een specifieke sector. Zo is er een Cyberbeveiligingsregeling voor de Zorg (CbrZ) waarin onder andere de criteria zijn vastgelegd om te bepalen wat een significant incident is.

- Voor bepaalde digitale dienstverleners zoals DNS-dienstverleners, cloudaanbieders en vertrouwensdiensten, is er nog een aparte uitvoeringsverordening (EU) 2024/2690. Daarin vinden deze partijen extra technische en methodologische eisen rondom de te gebruiken beveiligingsmaatregelen.

Naast deze formele documenten, vind je op de website van het Nationaal Cyber Security Centrum (NCSC) veel aanvullende informatie en hulpmiddelen om organisaties te ondersteunen.



Samenhang met bestaande IB-normen

Veel organisaties voldoen al aan informatiebeveiligingsnormen zoals ISO 27001, NEN 7510 of de BIO. Een voor de hand liggende vraag is dan of je via die normen de digitale weerbaarheid eigenlijk al niet geregeld hebt. In de praktijk vormt compliance met zulke normen inderdaad een belangrijk hulpmiddel, want hiermee vul je met name veel praktische zaken binnen de NIS2/Cbw automatisch al in. Echter, de wet eist ook dat een aantal bestuurlijke en organisatorische zaken goed worden geïmplementeerd, en dan heb je méér nodig dan alleen zulke normen. Ze zijn dus een belangrijk hulpmiddel bij het voldoen aan de Cyberbeveiligingswet, maar ze vormen geen één-op-één invulling van de wet.





Welke organisaties vallen onder de Cyberbeveiligingswet?

Niet iedere organisatie valt onder de wet. In de praktijk zijn er nu ruim 8000 organisaties die als zogeheten ‘entiteit’ moeten voldoen aan de NIS2-verplichtingen. De meeste entiteiten zijn actief in kritieke sectoren, zoals energie, digitale infrastructuur, onderzoek en de overheid. De wet maakt daarbij onderscheid tussen essentiële entiteiten en belangrijke entiteiten. Aan beide typen entiteiten worden dezelfde eisen gesteld, maar het toezicht en de handhaving op essentiële entiteiten zijn veel uitgebreider. Om te bepalen wie onder de wet een entiteit is, en welk type entiteit, zijn er een aantal handvatten.

Rechtstreeks via de Wet weerbaarheid kritieke entiteiten (Wwke)

Tegelijk met de Cyberbeveiligingswet is de Wet weerbaarheid kritieke entiteiten (Wwke) van kracht geworden. De Wwke heeft een bredere scope en richt zich op de bescherming van ons land tegen uiteenlopende dreigingen. Dus naast cyberdreigingen ook sabotage, terrorisme, natuurrampen, spionage en hybride dreigingen. Verschillende ministeries hebben daarvoor een risicoanalyse uitgevoerd binnen de sectoren waarvoor zij verantwoordelijk zijn. Op basis daarvan zijn zo’n 500 organisaties aangewezen als kritieke entiteiten. Zo’n kritieke entiteit binnen de Wwke is vervolgens ook automatisch een essentiële entiteit onder de Cbw.

Grote en middelgrote organisatie in kritieke sectoren

Andere organisaties kunnen onder de Cyberbeveiligingswet vallen op basis van de sector waarin ze actief zijn, en hun omvang. Wat betreft de sectoren, onderscheidt de wet twee categorieën:

- Zeer kritieke sectoren (bijlage 1 Cbw): energie, vervoer, bankwezen, drinkwater, digitale infrastructuur, beheer van ICT-diensten, ruimtevaart, infrastructuur financiële diensten, gezondheidszorg, afvalwater, overheid
- Overige kritieke sectoren (bijlage 2 Cbw): digitale aanbieders, post- en koeriersdiensten, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek, vervaardiging

Binnen deze sectoren bepaalt vervolgens de omvang of en hoe men Cbw-plichtig is:

- Organisaties in zeer kritieke sectoren: grote organisaties vallen onder de wet als essentiële entiteiten, middelgrote organisaties als belangrijke entiteiten.
- Organisaties in overige kritieke sectoren: grote en middelgrote organisaties vallen onder de wet als belangrijke entiteiten.
- Kleine organisaties vallen in het algemeen niet onder de wet.

Iemands omvang wordt daarbij bepaald op basis van onderstaande criteria:

Groot: ≥ 250 werknemers

Grote organisaties hebben 250 werkzame personen of meer, of ze hebben minimaal een jaaromzet van 50 miljoen euro én een balanstotaal van 43 miljoen euro.

Middel: 50 – 249 werknemers

Voldoe je niet aan de criteria voor een grote organisatie? Dan ben je middelgroot als je minimaal 50 medewerkers hebt, of een jaaromzet én een balanstotaal van allebei boven de 10 miljoen euro.

Klein: < 50 werknemers

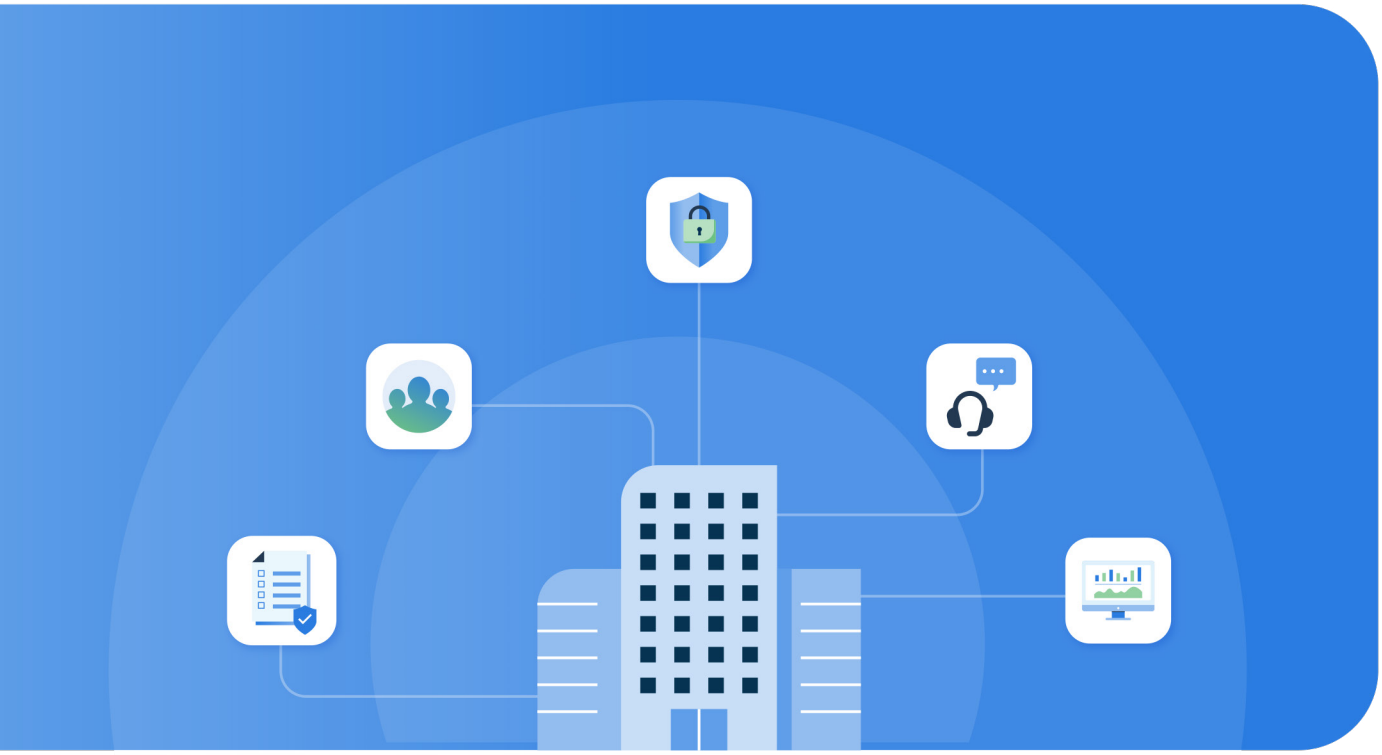
In alle andere gevallen ben je volgens de wet een kleine organisatie.

Uitzonderingen

Belangrijk is dat hier allerlei nuanceringen en uitzonderingen mogelijk zijn. Zo zijn er digitale dienstverleners - zoals bijvoorbeeld DNS-dienstverleners of aanbieders van elektronische communicatiediensten - waarbij de omvang niet altijd relevant is. Hetzelfde geldt voor overheidsorganisaties, terwijl er ook overheidsorganisaties expliciet zijn uitgesloten, zoals politie en defensie. Het is bovendien relevant dat niet alle subsectoren binnen de kritieke sectoren automatisch onder de wet vallen, en omgekeerd kan een minister in specifieke gevallen ook organisaties buiten de genoemde sectoren toevoegen. Juist daarom stelt de NCSC ook een nuttige zelfevaluatie beschikbaar, waarmee je via een toegankelijke vragenlijst direct een goede indicatie krijgt.

Als je niet onder de Cyberbeveiligingswet valt?

Als je niet Cbw-plichtig bent, betekent dat overigens niet per se dat je niets hoeft te doen. Levert jouw organisatie bijvoorbeeld een product of dienst aan een klant of partner die wél onder de wet valt? Dan heeft jouw klant of partner ongetwijfeld vragen over jouw digitale risicobeheer. Entiteiten moeten bij hun cyberbeveiligingsmaatregelen ook rekening houden met risico's in hun toeleveringsketen. Daarom zullen ze in de praktijk beveiligingseisen stellen aan leveranciers, ook als die zelf niet rechtstreeks onder de wet vallen.



Registratie en CSIRT

Valt jouw organisatie onder de Cyberbeveiligingswet (Cbw)? Dan moet je je registreren in het nationaal entiteitenregister van het NCSC. Dat kan online via het MijnNCSC portaal. Registratie is verplicht en als je jouw organisatie niet of onjuist registreert, kan dit leiden tot sancties.

Registratie is overigens niet alleen een verplichting, je kunt daarna ook gebruikmaken van de dienstverlening van een Computer Security Incident Response Team (CSIRT). Dat is een team specialisten dat helpt bij het voorkomen, onderzoeken en oplossen van digitale beveiligingsincidenten. Voor de meeste sectoren fungeert het NCSC als CSIRT, maar er zijn aparte CSIRTs voor onder andere de gezondheidszorg (Z-CERT) en de waterschappen (CERT-WM).

Complexe en internationale bedrijfsmodellen

Bestaat een organisatie uit meerdere onderdelen of is een bedrijf internationaal actief? Bij zulke complexere bedrijfsmodellen is het belangrijk om zorgvuldig vast te stellen welke onderdelen onder de Cyberbeveiligingswet vallen en in welke EU-lidstaat of lidstaten verplichtingen gelden. Welke regels van toepassing zijn, kan onder meer afhangen van het soort entiteit en de diensten die zij verricht. Daardoor kan een organisatie in bepaalde gevallen onder de wetgeving van één lidstaat vallen, terwijl in andere situaties in meerdere lidstaten verplichtingen kunnen gelden. Het NCSC heeft hiervoor de ‘Handreiking complexe bedrijfsmodellen’ ontwikkeld.

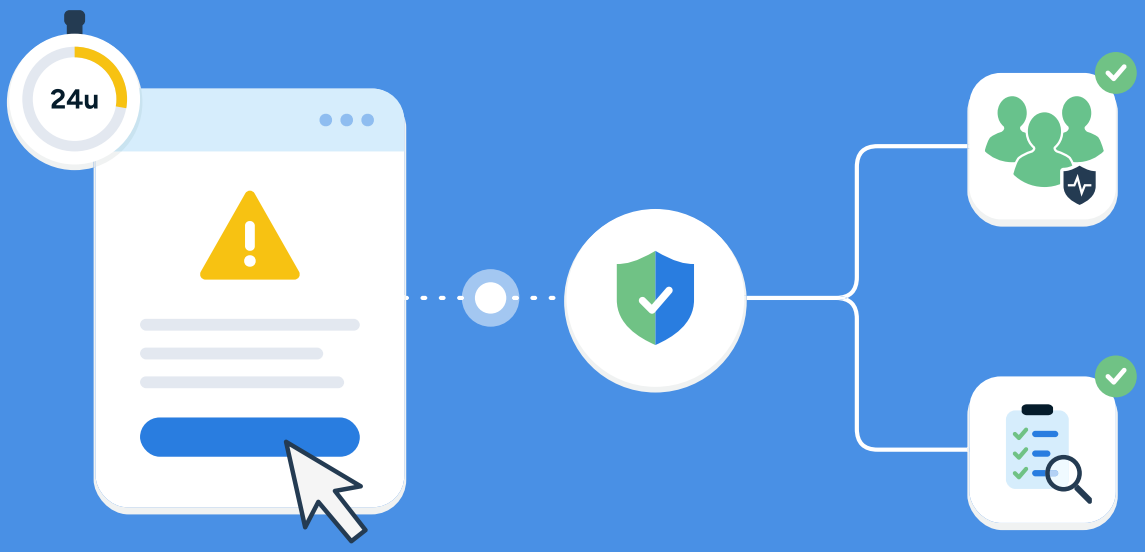


Zorgplicht

Organisaties die onder de wet vallen, hebben een zorgplicht. Dat houdt in dat ze passende technische, operationele en organisatorische maatregelen moeten nemen om cyberrisico's te beheersen, incidenten te voorkomen en de gevolgen van onverhoopte incidenten te beperken. De zorgplicht is met name vastgelegd in artikel 21 van de Cyberbeveiligingswet, met daarin 10 maatregelen, die het NCSC op haar website als volgt samenvat:

1. Maak een risicoanalyse
2. Richt incidentrespons in
3. Bereid je voor op uitval
4. Maak je toeleveringsketen veilig
5. Zorg dat cyberhygiëne op orde is
6. Beveilig netwerk- en informatiesystemen
7. Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer
8. Gebruik passkeys voor authenticatie
9. Stel cryptografiebeleid op
10. Beoordeel de effectiviteit van maatregelen

De zorgmaatregelen zijn omschreven in de wet, vaak verder uitgewerkt in het cyberbeveiligingsbesluit en soms ook verfijnd in sectorspecifieke aanvullingen. Het NCSC geeft op haar website een toelichting en adviezen bij de verschillende maatregelen. In een enkel geval is het NCSC zelfs concreter dan wat is vastgelegd in de wettekst. Een voorbeeld is maatregel 8 over passkeys, waarop we in de paragraaf over IAM nog terugkomen.



Meldplicht

De meldplicht betekent dat organisaties significante incidenten moeten melden bij het NCSC via het mijnNCSC portaal. Met zo'n melding worden ook automatisch de sectorale CSIRT en de toezichthouder op de hoogte gebracht. Met significant wordt bedoeld dat de dienstverlening ernstig wordt verstoord, financiële schade wordt veroorzaakt of dat bij andere organisaties grote schade kan ontstaan. Per sector zijn criteria vastgesteld die bepalen wanneer een incident significant is. Een geregistreerde entiteit kan overigens ook kleinere en bijna-incidenten vrijwillig melden. Zo'n melding gaat dan alleen naar de relevante CSIRT en niet naar de toezichthouder.

Stappenplan en termijnen

Zo'n melding doorloopt normaliter 3 stappen:

1

Uiterlijk 24 uur na ontdekking

Vroegtijdige waarschuwing

Hierbij geef je aan of het incident vermoedelijk kwaadwillig is en of er gevolgen zijn buiten Nederland. Ook verstrek je de relevante contactgegevens.

2

Uiterlijk 72 uur na ontdekking

Melding

Je geeft een update ten opzichte van je eerdere waarschuwing, en geeft een eerste beoordeling van de ernst en de gevolgen.

3

Uiterlijk 1 maand na de melding

Eindverslag

Hierin beschrijf je het incident, de oorzaak en de genomen maatregelen.

Als het incident inmiddels is afgehandeld, is de genoemde rapportage ook direct de eindrapportage. Duurt een incident langer, dan verstuur je na een maand een voortgangsverslag, en een eindverslag binnen 1 maand na de afhandeling. Ook kan je CSIRT of de toezichthouder tussendoor om updates vragen. Dat heet een tussentijds verslag.

Bovenstaande termijnen zijn overigens de maximale termijnen, het uitgangspunt is dat incidenten zo snel mogelijk moeten worden gemeld. En er zijn uitzonderingen. Levert een organisatie bijvoorbeeld zogeheten vertrouwensdiensten, dan zijn de wettelijke termijnen korter.

Ondersteuning door CSIRT

Je CSIRT reageert binnen 24 uur op je eerste waarschuwing en kan je ondersteunen bij de verdere afhandeling van het incident. Ook kan men adviseren hoe je het incident bij de opsporingsdiensten kunt melden als je vermoedt dat er sprake is van strafbare feiten. Is er impact in andere landen, dan informeert het centrale contactpunt binnen het NCSC de andere lidstaten en het EU-agentschap voor cybersecurity (Enisa). De CSIRT gebruikt de melding ook voor de cijfermatige rapportages.





Toezicht

De Cyberbeveiligingswet regelt ook het toezicht op entiteiten. Dit wordt verzorgd door bestaande toezichthouders binnen de verschillende ministeries, zoals de Rijksinspectie Digitale Infrastructuur (RDI). Via een 'Doorverwijsboom Cyberbeveiligingswet' kun je eenvoudig nagaan welke toezichthouder verantwoordelijk is binnen jouw sector.

Het toezicht betreft uiteraard de organisatie als geheel, maar ook individuele bestuurders kunnen zo nodig worden onderzocht. We noemden al dat bij het toezicht er verschil is tussen belangrijke en essentiële entiteiten:

Essentiële entiteiten

Proactief toezicht

Dit betekent dat er toezicht wordt gehouden op het naleven van de verplichtingen, ongeacht of er incidenten hebben plaatsgevonden.

Belangrijke entiteiten

Alleen reactief toezicht

Zo kan de regelgever besluiten een onderzoek in te stellen na bijvoorbeeld een cyberincident of meldingen van externe auditors of andere organisaties.

Daarnaast kunnen de sancties voor essentiële entiteiten hoger zijn dan voor belangrijke entiteiten.



Bestuursaansprakelijkheid

Belangrijk is dat bestuursleden van entiteiten direct verantwoordelijk zijn voor de naleving. Ze moeten de onder de zorgplicht horende risicobeheersmaatregelen expliciet goedkeuren, toezicht houden op de implementatie van de wet, en verantwoordelijkheid nemen voor de naleving ervan. Om daarop voorbereid te zijn, eist de wet dat bestuurders onder andere in staat zijn om:

1. Risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren.
2. Risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen.
3. De gevolgen van de risico's en risicobeheersmaatregelen voor de diensten die door de entiteit worden verleend te kunnen beoordelen.

Ieder bestuurslid moet deze competenties en vaardigheden kunnen aantonen met een certificaat, waaruit de deelname blijkt aan een training die de genoemde onderwerpen behandelt. Ook moeten de bestuurders deze kennis actueel houden.



Hoe draagt IAM bij aan de NIS2 verplichtingen?

De Cyberbeveiligingswet legt eisen vast om de weerbaarheid tegen cyberincidenten te verbeteren en de continuïteit van de bedrijfsvoering te waarborgen. Identity & access management (IAM) is daarin uiteraard één aspect, maar dit aspect wordt wel steeds belangrijker. Niet voor niets hanteren veel cyberspecialisten tegenwoordig het uitgangspunt 'Identity is the primary security perimeter' en worden veel cyberincidenten veroorzaakt door kwetsbaarheden in de toegangsbeveiliging. Een IAM-oplossing helpt dan ook op meerdere manieren om invulling te geven aan de NIS2/Cbw-verplichtingen.

Provisioning van gebruikersaccounts en -rechten

Groepsaccounts zijn tegenwoordig not done, evenals het ongecontroleerd aanmaken van nieuwe accounts en toegangsrechten. In plaats daarvan heb je eenduidige beleidsregels nodig, zodat op ieder moment duidelijk is wie toegang heeft tot welke data en applicaties. Ook moeten toegangsrechten altijd aansluiten bij iemands taken en verantwoordelijkheden.

Binnen HelloID borgen we dit met behulp van geautomatiseerde provisioning en Role (of Attribute) Based Access Control. Daarbij gebruikt het IAM-platform actuele gegevens, bijvoorbeeld uit het HR-systeem, om medewerkers automatisch te voorzien van de juiste accounts en rechten. Als iemands rol in de organisatie verandert, past je IAM-omgeving automatisch de toegangsrechten aan. En als iemands dienstverband of overeenkomst wordt beëindigd, worden de accounts tijdig geblokkeerd om misbruik te voorkomen.

Deze automatische provisioning vormt de basis om invulling te geven aan maatregelen 6 en 7 van de zorgplicht: het beveiligt je netwerk- en informatiesystemen, en versterkt de beveiliging op het gebied van personeel, toegang en assetbeheer. Bovendien is het gebruik van een autorisatiematrix of rollenmodel ook een belangrijk hulpmiddel bij de melding en analyse van eventuele incidenten. Ook helpt een goed georganiseerde provisioningketen bij het beantwoorden van vragen van de toezichthouder.

Beheer van de uitzonderingen

Goede informatiebeveiliging leunt dus allereerst op duidelijke beleidsregels. Tegelijk zijn er soms individuele uitzonderingen nodig, en ook zulke verzoeken moeten goed worden afgehandeld. Daarom moet een IAM-platform ook de verdere serviceprocessen stroomlijnen. HelloID maakt het bijvoorbeeld mogelijk dat individuele gebruikersverzoeken worden ingediend via een helpdesk, via een manager of rechtstreeks door gebruikers via een self-serviceportaal. Het platform zorgt, na goedkeuring door de relevante managers, dat de wijzigingen automatisch veilig worden doorgevoerd in de aangesloten doelsystemen. Ook kunnen rechten desgewenst voor een bepaalde periode worden verstrekt. Sowieso is op ieder moment traceerbaar welke medewerkers beschikken over welke rechten, wie deze heeft verstrekt en met wiens toestemming.

Dit vormt een belangrijke aanvulling op de invulling van de hiervoor genoemde maatregelen 6 en 7 van de zorgplicht: naast automatische provisioning worden immers nu ook de individuele uitzonderingen zodanig beheerd dat we grip houden op alle wijzigingen en deze altijd kunnen traceren. Daarnaast is de IAM-oplossing een belangrijk hulpmiddel om op een beheersbare manier tijdelijk individuele rechten te verstrekken als workaround bij de afhandeling van incidenten en het in stand houden van de dienstverlening (maatregelen 2 en 3 van de zorgplicht).

Logging en reporting

Registratie en rapportage zijn daarbij essentieel. Zo zal een moderne IAM-oplossing het authenticatieproces automatisch monitoren, en via rapportages is altijd inzichtelijk wie, welke applicaties heeft geraadpleegd, op welk moment en vanaf welke locatie. Zo kunnen mogelijke dreigingen sneller worden herkend.

Daarnaast kun je met een platform als HelloID ook alle beheeracties loggen, zoals het aanmaken, inschakelen, updaten en verwijderen van accounts. Hetzelfde geldt voor het toekennen en intrekken van permissies. Zijn rechten individueel toegekend (buiten de business rules), dan registreert het platform wie de aanvraag deed, welke functionaris het verzoek heeft goedgekeurd en welke wijzigingen in achterliggende systemen zijn doorgevoerd.

Hiermee ondersteun je bij de analyse van onverhoopte incidenten en lever je data voor rapportages als onderdeel van de meldplicht.

Governance

Aanvullende governance-features maken het mogelijk het actuele rechtenbeheer te evalueren en verder te verbeteren en te optimaliseren. Met role mining kun je bijvoorbeeld de account- en rechtenprovisioning steeds verder optimaliseren, en een feature als reconciliation voorkomt interne inconsistenties tussen applicaties, en vervuiling in je IT-systemen. Ook helpen governance tools te voorkomen dat conflicterende rechten worden verstrekt, en dat individuele rechten nodeloos lang actief blijven.

Met deze governance tools geef je invulling aan maatregel 10 van je zorgplicht, waarin is voorgeschreven dat je periodiek de effectiviteit van maatregelen moet beoordelen en zo nodig aanpassen. Daarnaast zijn tools als reconciliation een krachtig hulpmiddel bij het analyseren van incidenten.

Access Management

Voor de authenticatie van gebruikers en aanvullende mechanismen als Single Sign-On wordt vaak geen gebruikgemaakt van het IAM-platform, maar van een aparte identity provider zoals Microsoft Entra ID. Het is belangrijk na te gaan of de gebruikte identity provider de eisen vanuit de cyberwetgeving volgt.

Rondom authenticatie gaat het NCSC-advies verder dan de wettekst. De wet stelt 'wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.' Het NCSC adviseert bij zorgmaatregel 8, op basis van de actuele inzichten, waar mogelijk gebruik te maken van passkeys. Als NIS2-plichtige organisatie is het goed om na te gaan of de gebruikte identity provider dit ondersteunt.



Over Tools4ever

Tools4ever is een Nederlands softwarebedrijf. We ontwikkelen innovatieve en gestandaardiseerde Identity as a Service (IDaaS)-oplossingen. De hedendaagse IDaaS-oplossingen zijn complex, daarom hebben wij onszelf toegelegd op het ontwikkelen en leveren van IDaaS-oplossingen die eenvoudig te implementeren en beheren zijn. Van 2013 tot en met 2020 hebben we maximaal geïnvesteerd om deze doelstelling te realiseren.

HelloID is van scratch opgebouwd waarbij gebruikgemaakt wordt van de modernste softwaretechnieken. De eerste release van HelloID is begin 2020 met veel enthousiasme ontvangen. HelloID is een mooi product waar onze gebruikers blij van worden. We voelen ons verplicht om voor een eerlijke vergoeding, excellente service te verlenen, en te blijven investeren in verdere ontwikkeling van HelloID.



Meer weten?

Ben je geïnteresseerd in hoe je concreet aan de slag kunt met NIS2 en de Cyberbeveiligingswet?

Dan is het webinar NIS2 een prima startpunt.

Hierin vertellen we onder meer over de Cyberbeveiligingswet en belangrijke elementen zoals de zorgplicht en meldplicht. Ook zoomen we uitgebreider in op de rol van identity & access management bij het borgen van de vele NIS2-verplichtingen.

Aanvullend kun je met behulp van de HelloID-NIS2 checklist eenvoudig beoordelen bij welke specifieke NIS2-verplichtingen de HelloID-functionaliteit je organisatie kan ondersteunen. En wil je direct je huidige HelloID-implementatie evalueren en verbetermogelijkheden inventariseren? Neem dan rechtstreeks contact op met je accountmanager om samen een HelloID Health Check in te plannen.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Tools4ever BV

Adres	Amalialaan 126C 3743 KJ Baarn Nederland
Algemeen	+31 (0) 35 54 83 255
Support	+31 (0) 35 54 83 280
Informatie	info@tools4ever.com
Verkoop	sales@tools4ever.com
Support	tools4ever.nl/support

