HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

Ontwikkelingen op het gebied van identity and access management

L. (Lodewijk) Benjaminse en R. (Ruud) Buurma
januari 2020

OPENBAAR

Introductie

1

1. Introductie
2. Begrippen
3. Ontwikkelingen
4. Vooruitblik
5. Bronvermelding

Introductie
Ontwikkelingen en theorie

In deze publicatie gaan wij in op een aantal observaties en ontwikkelingen op het gebied van *identity and access management* die wij in de markt zien op basis van ons recente onderzoek en informatie van onze opdrachtgevers. Daarnaast behandelen wij in deze publicatie enkele theoretische aspecten van *identity and access management*.

Diverse wet- en regelgeving en normenkaders schrijven eisen voor aan *identity and access management*. Als een organisatie haar *identity and access management* niet op orde heeft, kan het (mede) leiden tot bevindingen van de accountant, negatieve berichtgeving in de pers, een opmerkingen in de ISAE-verklaring of zelfs boetes/dwangsommen van toezichthouders. Bij veel organisaties staat dit onderwerp hoog op de agenda, waar in veel gevallen nog hard aan wordt gewerkt.

Mocht intrinsieke motivatie bij een organisatie ontbreken, dan is er tegenwoordig steeds meer druk van buiten om *identity and access management* op orde te brengen.

Hieronder staan twee voorbeelden van boetes cq. dwangsommen die de Autoriteit Persoonsgegevens heeft opgelegd mede op grond van het gebrek aan "*passende technische en organisatorische maatregelen*" uit de AVG:

- De toezichthouder heeft een dwangsom van EUR 50.000 opgelegd[1] aan een zorgverzekeraar omdat gebleken is dat enkele medewerkers onnodig toegang hadden tot persoonsgegevens.
- Later heeft de Autoriteit Persoonsgegevens een bestuurlijke boete en een last onder dwangsom opgelegd[2] aan een ziekenhuis toen bleek dat zij onvoldoende maatregelen voor de beveiliging van patiëntgegevens hadden getroffen.

Een belangrijk deel van deze *"passende technische en organisatorische maatregelen"* vertalen zich grotendeels in beleid, procedures en naleving van *identity and access management*.

Introductie
BW, AVG, SOx, ISO 27001, ISO 27002, NEN 7510, PSD2, …

Het is voor organisaties van belang dat zij logische toegangsbeveiliging op orde hebben:

- In het kader van de jaarrekeningcontrole wordt door accountants veel waarde gehecht aan logische toegangsbeveiliging. Accountants moeten volgens artikel 393 lid 4 uit BW (Burgerlijk wetboek) boek 2 de *"betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking"* beoordelen. IT-auditors richten zich daarom onder andere op *identity and access management*.
- De AVG (Algemene verordening gegevensbescherming) stelt eisen aan de toegang die werknemers hebben tot persoonsgegevens. Een organisatie moet volgens artikel 32 lid 1 *"passende technische en organisatorische maatregelen"* nemen.
- Voor organisaties die genoteerd zijn aan de Amerikaanse beurzen, of toeleverancier zijn van een in de VS aan de beurs genoteerd bedrijf, is SOx (Sarbanes-Oxley Act) van toepassing die bedrijven verplicht aan te kunnen tonen dat ze de logische toegangsbeveiliging tot hun systemen onder controle hebben.
- Veel organisaties werken aan certificering (zoals bijvoorbeeld NEN 7510) om hun inzet ten aanzien van *identity and access management* onder de aandacht te brengen.
- In hoofdstuk Vertrouwelijkheid en integriteit van de Baseline informatiebeveiliging hoger onderwijs schrijft SURFnet over logische toegangsbeveiliging.
- In ISAE-verklaringen is het gebruikelijk beheersdoelstellingen op te nemen omtrent logische toegangsbeveiliging.
- Hoofdstuk *Access control* uit ISO 27002 gaat in op *identity and access management*.
- PSD2 (Payment Service Directive 2) eist dat SCA (Strong Customer Authentication) wordt toegepast op betalingen binnen de Europese Economische Ruimte (EER) voor transacties van meer dan EUR 30.

Begrippen

2

1. Introductie
2. Begrippen
3. Ontwikkelingen
4. Vooruitblik
5. Bronvermelding

Begrippen
Identificeren, authentiseren en autoriseren

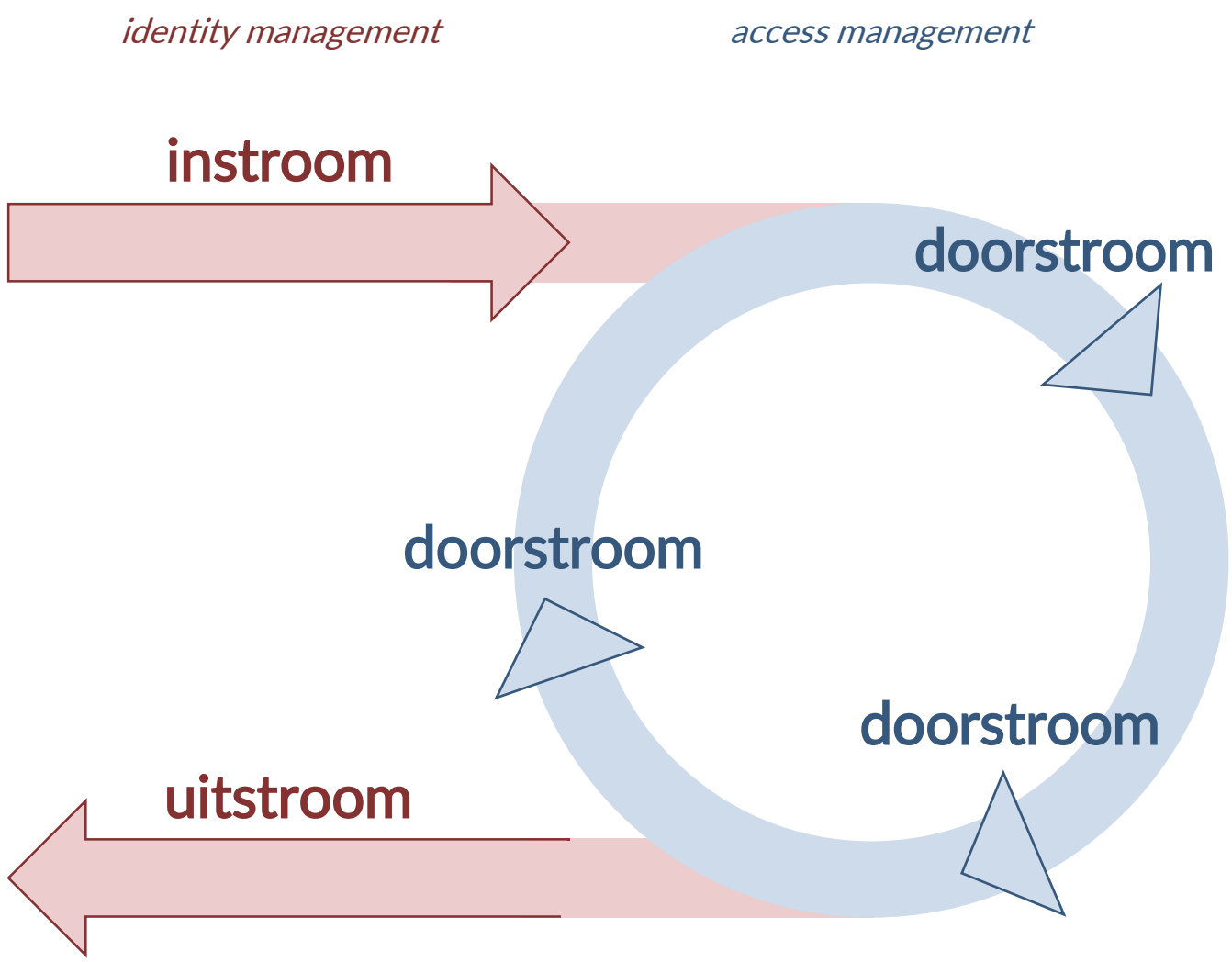
Onderstaande begrippen zijn nauw aan elkaar verbonden:

- *Identity management* is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen die een organisatie helpt om van gebruikers de identificatie en authenticatie te regelen, beheren en controleren.
- *Access management* is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat een organisatie helpt om geautoriseerd toegang tot het gebruik van systemen en gegevens te bieden, beheren en controleren.

Daarnaast is het van belang deze definities in het achterhoofd te houden:

- Het **subject** is de gebruiker, proces of een systeem die het object wil benadert.
- Het **object** zijn de gegevens (bijvoorbeeld een bestand of een record in een database) die door het subject worden benadert.
- Het **identificeren** is het vaststellen van de identiteit van een subject. De identiteit wordt gebruikt om de toegang van het subject tot een object te beheersen (autorisatie).
- Bij **authentiseren** wordt nagegaan of het object (een gebruiker, een computer of applicatie) daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit voldoet aan de verwachte echtheidskenmerken, bijvoorbeeld een in het systeem geregistreerd bewijs.
- Als laatste, **autoriseren** is het proces waarin een subject bevoegdheden krijgt op het benaderen van een object.

Begrippen
Cyclus



De cyclus voor *identity and access management* bestaat op hoofdlijnen uit de volgende stappen, veelal aangeduid met in-, door- en uitstroom.

instroom:

- Eerst zal **identificatie** van de gebruiker plaatsvinden. Een gebruiker kan in deze een natuurlijk persoon zijn, maar ook steeds vaker een robot of systeem dat zelf in kan loggen op een eigen account en activiteiten kan uitvoeren.
- Elke keer dat een gebruiker (subject) zich aanmeldt (bij een object), vindt **authenticatie** plaats, waarbij namens de organisatie wordt vastgesteld of de gebruiker daadwerkelijk is wie hij beweert te zijn.

doorstroom:

- Afhankelijk van de rol/functie die de werknemer gedurende zijn loopbaan in de organisatie vervult en de afdeling of project waar hij op dat moment actief is, zullen nieuwe **bevoegdheden** worden toegekend en oude worden ingetrokken.

uitstroom:

- Als de gebruiker de organisatie verlaat, zal de identiteit worden geblokkeerd en kan de gebruiker zich niet meer aanmelden.

Begrippen
Identificatie

Afhankelijk van de risico's cq. gewenste zekerheid omtrent **identificatie** kan dit op verschillende wijzen plaatsvinden, zoals bijvoorbeeld:

- alleen op basis van mailverkeer kan een persoon iets online kopen, soms zelfs als hij achteraf betaalt;
- een werkgever verlangt identificatie door middel van bijvoorbeeld een paspoort of identiteitskaart;
- soms wil de organisatie het mailadres bevestigd hebben, waarbij een code ter bevestiging naar dat mailadres wordt gestuurd;
- andere organisaties willen dat de persoon in kwestie fysiek zijn paspoort toont;
- iDIN van banken kan door (andere) organisaties worden gebruikt om de identiteit vast te stellen;
- sommige organisaties eisen dat men één cent overmaakt.

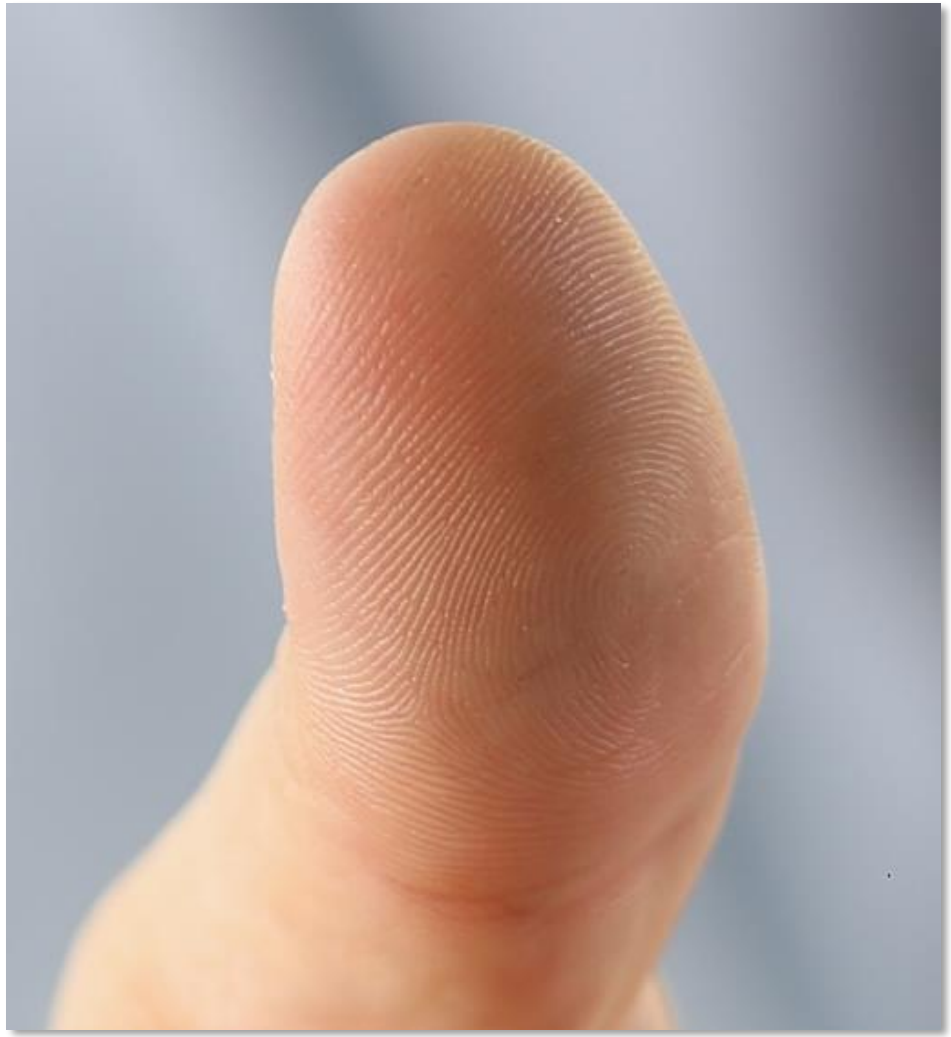
Hierbij wordt dus in sommige gevallen (mede) vertrouwd op identificatie die andere organisaties eerder hebben uitgevoerd. Zie ook verderop, waar wij beschrijven dat identificatie als dienst wordt aangeboden en dit bij organisaties uit handen wordt genomen.

Begrippen
Authenticatie

- Wanneer identificatie heeft plaatsgevonden is de gebruiker bekend bij de organisatie. Wie hij is, heeft de organisatie dan gekoppeld aan een identiteit (veelal een gebruikersnaam of een klantnummer). Als deze gebruiker zich later meldt (door in te loggen) bij de organisatie, zal derhalve niet de gehele identificatie opnieuw plaats hoeven te vinden.

- Bij **authenticatie** wordt nagegaan of een persoon daadwerkelijk degene is, wie hij beweert te zijn. Afhankelijk van de mate van zekerheid waarmee men dit wil controleren, worden meer of minder aspecten ingezet. Veelal past men in de eenvoudigste vorm enkel een wachtwoord toe. Wanneer er meer dan één (*multiple)* aspect (*factor*) wordt toegepast, spreekt men van *multiple factor authentication* (MFA).

- Bij **authenticatie** moet de persoon aantonen dat hij daadwerkelijk is, wie hij beweert te zijn. Dit kan door middel van iets dat enkel die persoon 'heeft', 'weet' of 'is':
  - iets dat je 'hebt' kan onder andere jouw telefoon, paslezer of randomreader zijn;
  - iets dat je 'weet' is bijvoorbeeld een pincode of een wachtwoord die niet worden gedeeld met derden;
  - iets dat je 'bent' kan bijvoorbeeld jouw vingerafdruk, gedrag of een scan van zijn het gezicht zijn.



Begrippen
Autorisatie

Nadat een persoon is geauthentiseerd, wil hij veelal toegang tot gegevens en acties kunnen uitvoeren (**autorisatie**). Veelal wordt het *need to know* of *least privilege* principe toegepast, zodat personen enkel tot die gegevens toegang hebben en alleen die acties kunnen uitvoeren, mits dit voor zijn rol/functie binnen de organisatie noodzakelijk is.

Tot welke gegevens een persoon daadwerkelijk toegang krijgt, verschilt uiteraard:

- Dit zal in het geval van een medewerker, afhankelijk kunnen zijn van de plek (bijvoorbeeld afdeling of project) binnen de organisatie waar de medewerker actief is.
- Als het een klant van een boekenwinkel betreft, zal hij veelal tot zijn eigen bestellingen, adresgegevens, betalingen, … en persoonlijke kortingen toegang krijgen.
- Een klant van een zorgverzekeraar zal toegang kunnen krijgen tot zijn adresgegeven, bsn, polissen en verzekeringen met bijbehorende dekkingen, betalingen van premies, de gedeclareerde zorg en uitgekeerde vergoedingen.

Welke acties de gebruiker vervolgens in het systeem op die gegevens mag uitvoeren, hangt veelal af van zijn rol/functie binnen de organisatie:

- Een junior medewerker van de afdeling verkoop, zal misschien nog niet zelfstandig offertes mogen uitbrengen. Terwijl een medior medewerker dat wel zelf zelfstandig mag, als het totaal geoffreerde bedrag onder een bepaalde grens blijft.
- Een medewerker van de afdeling Audit zal waarschijnlijk alleen informatie mogen raadplegen binnen de systemen / processen die hij onderzoekt. Deze informatie mag hij niet muteren.

Welke acties de gebruiker in het systeem kan uitvoeren, kan op verschillende manieren worden ingericht:

- Aan de hand van de vier opties in de afkorting CRUD kan onderscheid tussen de acties worden gemaakt:
  - *create*: aanmaken/toevoegen;
  - *read*: raadplegen/inzien;
  - *update:* muteren/wijzigen;
  - *delete:* verwijderen/weggooien.
- Vaker zien we tegenwoordig het onderscheid tussen enkel ‘lezen’ en ‘schrijven’.
- Sommige systemen werken met schermen, functies of transacties waar een gebruiker toegang toe moet hebben om een bepaalde actie te kunnen uitvoeren.

Ontwikkelingen

3

1. Introductie
2. Begrippen
3. Ontwikkelingen
4. Vooruitblik
5. Bronvermelding

Ontwikkelingen

Ontwikkelingen in de markt en uitkomsten onderzoek

In de markt ziet HODARI de volgende ontwikkelingen op het gebied van *identity and access management.*

1. Traditionele gaat het RBAC-model (*roll based access control*) uit van een hiërarchische situatie waarbij een werknemer jarenlang onderdeel uitmaakt van dezelfde afdeling. Steeds meer organisaties hebben echter het agile werken omarmd, waardoor werknemers frequent van team wisselen en tegelijkertijd binnen verschillende teams een andere rollen kunnen vervullen. Hierdoor is er steeds meer behoefte om op flexibelere wijze (agile) bevoegdheden toe te kennen, bijvoorbeeld door middel van het ABAC-model (*attribute based access control*) waarbij aan de hand van attributen bevoegdheden worden toegekend. Door de bevoegdheden flexibel te koppelen aan attributen en deze attributen real time te laten beoordelen door het systeem, worden bevoegdheden gebaseerd op de actuele situatie van de werknemer en hoeven de bevoegdheden niet telkens handmatig te worden aangepast.

2. Veel organisaties zoeken hun heil in tooling om zo (volledig geautomatiseerde) *provisioning* door te voeren. Als een organisatie haar administratie van personen, accounts en bevoegdheden niet op orde heeft, zal dergelijke tooling niet de oplossing gaan bieden. Daarnaast is deze tooling vaak nog niet gericht op het agile werken en ondersteunen ze in beperkte mate het flexibelere ABAC-model en zien wij dat organisaties zelf hiervoor tooling gaan ontwikkelen.

- HODARI heeft een onderzoek gedaan naar de ervaringen van *identity and access management* bij organisaties in Nederland. De uitkomsten van dat onderzoek zijn gepresenteerd tijdens een event dat op 19 november 2019 plaatsvond.
- Ons onderzoek is gedaan onder een zeer grote (internationale) organisaties waar in totaal (circa 90.000) medewerkers werkzaam zijn.
- Het onderzoek bevestigt de beelden van de ontwikkelingen, op het gebied van *identity and access management*. Daarnaast werden een aantal opvallende details vastgesteld.
- Op deze en de volgende slides geven wij een samenvatting van de uitkomsten van dat onderzoek weer.

Ontwikkelingen
Markt

3. Banken verlangen al enkele jaren van hun klanten dat zij inloggen met behulp van *multi factor authentication*. Dit kende verschillende vormen zoals lijsten met TAN-codes, SMS berichten, identifiers, tokens en steeds vaker worden apps ingezet. Dergelijke *multi factor authentication* worden nu ook door andere organisaties ingezet, niet alleen voor hun klanten maar ook voor eigen werknemers. Voor klanten is het in sommige gevallen nog optioneel, maar steeds vaker wordt dit afgedwongen.

4. Er is meer en meer druk om *identity and access management* op orde te brengen na een negatieve stroom van berichten in de media (veelal over datalekken), boetes cq. dwangsommen[1] [2] die worden opgelegd door toezichthouders.

Ontwikkelingen
Markt

5. Er ontstaan steeds meer platforms die diensten op het gebied van identificatie, authenticatie en autorisatie aanbieden als tussenpersoon/dienst. Dergelijke platforms acteren tussen de personen en een organisatie, waarbij de initiële identificatie door het platform wordt uitgevoerd. Bijkomend voordeel hiervan kan zijn, dat niet elke organisatie waar die persoon zaken mee doet de persoonsgegevens van die persoon (ten behoeve van identificatie) hoeft te bewaren; dit ligt immers centraal bij dat platform. Voorbeelden van dergelijke platforms zijn eHerkenning, iDIN en DigiD.
   - De organisatie die een dienst/product levert aan de persoon, vertrouwt daarbij op de **identificatie** die het platform heeft uitgevoerd.
   - Elke keer dat een persoon zich bij een organisatie aanmeldt, wordt de **authenticatie** op de achtergrond door het platform uitgevoerd.
   - In aanvulling daarop kan het platform ook worden gebruikt om de persoon wel of geen toegang (**autorisatie**) tot bepaalde diensten/producten te geven. Denk hierbij bijvoorbeeld aan de vraag of een persoon jonger/ouder is dan 18 jaar. De organisatie die iets aan die persoon wil verkopen, hoeft helemaal niet de exacte geboortedatum van die persoon te weten, dat weet het platform immers: enkel het antwoord ‘jonger’ of ‘ouder’ moet voor de organisatie voldoende zijn om te besluiten dergelijke dienst/product wel of niet aan deze persoon aan te bieden.

Doordat dit platform ‘toch al’ over gegevens van de betreffende persoon beschikt, kan zo ook worden voorkomen dat de organisatie de adresgegevens van die persoon te weten komt. Enkel voor de verkoop van een product heeft de organisatie de adresgegevens van die persoon immers niet nodig. Aan de partij die de bezorging verzorgt, kunnen dan separaat – buiten de organisatie om – de adresgegevens door het platform worden verstrekt. Op deze wijze wordt de verspreiding van persoonsgegevens beperkt.

Ontwikkelingen
Uitkomsten onderzoek

Naast eerder genoemde ontwikkelingen, is het volgende gebleken uit ons onderzoek:

- Nagenoeg alle organisaties melden nooit klaar te zullen zijn met *identity and access management* maar beschouwen dit als een continu en arbeidsintensief proces.
- Investeringen in een goedlopend proces voor *identity and access management* wordt door veel organisaties als een noodzakelijk kwaad gezien. Intrinsieke motivatie om met *identity and access management* bezig te zijn, is vaak afwezig dat zet veel druk op diegenen die verantwoordelijk zijn gesteld. Veel organisaties geven aan dat wet- en regelgeving, vaak in combinatie met (bevindingen uit) audits, aanleiding geven om aandacht te besteden aan *identity and access management*.
- Een toenemende complexiteit ligt in het feit dat ook klanten, studenten, patiënten, toeleveranciers, ... steeds vaker toegang hebben tot systemen.
- Een geautomatiseerde vorm van *provisioning* wordt nog zeer beperkt toegepast.
- Ondanks dat de combinatie van een gebruikersnaam en wachtwoord nog de gebruikelijkste vorm is voor authenticatie, is *two factor authentication* aan een opmars bezig, zeker daar waar op afstand of met gevoelige persoonsgegevens wordt gewerkt.
- Veel organisaties worstelen met het probleem van een statisch proces *identity and access management*, in een tijd dat de dynamiek steeds groter wordt, (agile) maakt dat niet altijd de meest efficiënte en effectieve oplossing kan worden gemaakt.
- Bij uitvoeren van periodieke reviews wordt nog veel handmatig werk verricht. Geautomatiseerde *provisioning* en het automatisch uitvoeren van periodieke reviews is nog zeer beperkt.

Ontwikkelingen

4

1. Introductie
2. Begrippen
3. Ontwikkelingen
4. Vooruitblik
5. Bronvermelding

Vooruitblik
Herkenbare situaties

HODARI helpt organisaties bij het verbeteren van *identity and access management*. Wij treffen regelmatig de volgende situaties aan:

- een organisatie kan een toezichthouder of accountant niet overtuigen dat zij aantoonbaar *in control* is over haar *identity and access management*;
- een organisatie heeft niet inzichtelijk welke bevoegdheden aan een account van een gebruiker moeten worden gekoppeld (instroom);
- een organisatie heeft geen volledig inzicht in de gebruikers die toegang hebben tot systemen en gegevens;
- het account van een gebruiker wordt niet (tijdig) geblokkeerd wanneer hij de organisatie verlaat (uitstroom);
- een organisatie past bevoegdheden die aan een account zijn gekoppeld niet (tijdig) aan wanneer die persoon een andere rol/functie binnen de organisatie krijgt (doorstroom);
- doordat data (bij HR en IT) niet juist of volledig zijn, stranden initiatieven om tooling voor *provisioning* in te voeren;
- de verantwoordelijkheden ten aanzien van *identity and access management* van de afdeling HR, de information security officer, de afdeling IT en leidinggevenden zijn niet helder;
- een organisatie past niet op alle wachtwoorden hetzelfde beleid toe, waardoor wachtwoorden van sommige accounts nooit worden gewijzigd;
- een medewerker heeft toegang tot persoonsgegevens zonder dat dit vanuit zijn functie/rol is toegestaan;
- de procedure om toegang te krijgen tot gegevens is niet beschreven waardoor bijvoorbeeld ad hoc bevoegdheden worden toegekend.

De voorbeelden die wij hier links beschrijven, kunnen nadelige gevolgen hebben voor organisaties:

- boetes van de Autoriteit Persoonsgegevens vanwege het niet naleven van de AVG;
- bevindingen in de management letter van de accountant;
- opmerkingen van toezichthouders zoals DNB en ECB;
- reputatieschade als gevolg van het lekken van (persoons)gegevens;
- betalingen worden door de verkeerde personen geautoriseerd waardoor geld onterecht de organisatie verlaat;
- ouders behouden toegang tot informatie (bijvoorbeeld medische dossiers of schoolresultaten) van hun (inmiddels) meerderjarige kind;
- medewerkers houden toegang tot systemen en gegevens nadat ze uit dienst zijn getreden.

Vooruitblik
Resultaat

Om gericht resultaten te boeken, helpt HODARI organisaties regelmatig het volgende in te richten.

Snelle resultaten behalen op korte termijn:
- complexiteit van wachtwoorden door middel van wachtwoordinstelling afdwingen;
- accounts laten blokkeren nadat deze langere tijd niet zijn gebruikt;
- een eenduidig proces voor in-, door-, en uitstroom van medewerkers.

Doorvoeren van verbeteringen op middellange termijn:
- vaststellen visie, beleid en procedures ten aanzien van *identity and access management*;
- opstellen van een control framework en het periodiek toetsen van deze controls;
- gewenste functiescheiding in bedrijfsprocessen vastleggen in autorisatiematrix;
- meer inzicht door rapportages over de naleving van beleid, procedures en controls;
- één leidende administratie voor accounts en bevoegdheden;
- uitvoeren van periodieke controles ten aanzien van accounts en bevoegdheden;
- introductie van *two factor authentication.*

Borgen van verbeteringen op lange termijn:
- geautomatiseerd toekennen en intrekken van bevoegdheden aan de hand van bijvoorbeeld HR-administratie;
- doorvoeren van *single sign on*;
- introduceren van tooling voor *identity and access management.*

Randvoorwaarden voor het doorvoeren van verbeteringen en het permanent borgen van de resultaten zijn strategie en beleid. Hieruit moet blijken dat het management achter *identity and access management* staat:
- beleid moet beschrijven hoe *identity and access management* aansluit op de strategie van de organisatie;
- raamwerken voor specifieke sectoren, zoals bijvoorbeeld NEN 7510 in de zorg, ENSIA voor gemeenten, CobiT zoals dit door DNB wordt gehanteerd, het normenkader en toetsingskader van SURF voor onderwijsinstellingen geven heldere handvatten;
- de juiste *tone at the top* en mandaat vanuit het management van de organisatie is van groot belang.

Bronvermelding

5

1. Introductie
2. Begrippen
3. Ontwikkelingen
4. Vooruitblik
5. Bronvermelding

Bronvermelding

1. "*Financieel jaarverslag 2018*", Coöperatie Menzis, 29 maart 2019, https://www.zorgictzorgen.nl/wp-content/uploads/2019/04/Jaarrekening-2018-Cooperatie-Menzis-UA.pdf
2. "*Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom*", Autoriteit Persoonsgegevens, 18 juni 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf

HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

HODARI levert diensten op het gebied van privacy, compliance, information security en governance. Wij brengen IT op orde door risico's in informatiebeveiliging te beperken en wij helpen organisaties aantoonbaar in control te komen. Wij bieden kwalitatief hoogwaardige oplossingen waarbij de meest complexe vraagstukken tot in detail zijn opgelost. Wij hebben ruime ervaring opgedaan binnen verschillende sectoren, zoals de financiële sector, energiesector, (rijks)overheid, advocatuur, IT-dienstverleners en retail. Regelmatig handelen wij binnen projecten naar aanleiding van fusies en overnames, reorganisaties, bevindingen van accountants of opmerkingen van toezichthouders.

HODARI B.V.

071-2032385
hodari.nl

L. (Lodewijk) Benjaminse
lodewijk.benjaminse@hodari.nl
06-53736105