HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

Uitkomsten van onderzoek identity and access management

R. (Ruud) Buurma
november 2019
Beesd

Aanleiding
Herkenning de markt: actueel vraagstuk

- "Identity and access management is een actueel onderwerp. Verder zijn we bezig om de periodieke reviews op toegang tot applicaties opnieuw vorm te geven."
- "Interessant onderwerp, en voor ons ook zeker erg actueel (al een tijdje ...)"
- "Wij zijn momenteel maximaal bezig met identity and access management, is op dit moment de hoogste prioriteit, gezien de aandachtspunten van de interne auditafdeling."
- "De complexiteit van onze organisatie, internationaal, cultuur, omvang, maakt dat het beheersen van het identity and access managementproces een taak is die oneindig is in zijn uitvoering."
- "Voor ons een onderwerp dat veel aandacht vraagt, temeer omdat onze studenten ook 'inhaken' op veel processen waarmee toegang wordt verleend tot onze applicaties."
- "Het is een hele toer om dit te organiseren voor onze (vaste en tijdelijke) medewerkers, dat lukt aardig zij het met veel inzet, maar het wordt gecompliceerder om ook onze klanten op een veilige wijze toegang te verlenen."
- Wij zijn blij het enigszins op orde te hebben daarom durven we het eigenlijk niet aan om nieuwe ontwikkelingen in te bouwen."

- Alle organisaties die wij benaderden zijn er (continu) mee bezig.
- De wijze waarop over een en ander gesproken wordt is vaak met een zekere 'vermoeidheid'.
- Ontwikkelingen worden wel enigszins gevolgd, maar veel tijd en energie wordt daar niet aan besteed. Vaker lijkt het een kwestie van alle zeilen bijzetten om de zaken op enig niveau te brengen of te houden.
- Opvallend ook dat in de meeste organisaties het eigendom bij één persoon ligt die er zich druk om maakt (en er wakker van ligt) terwijl de back-up (vanuit de top) soms te wensen laat.

Eisen ten aanzien van identity and access management
Voldoen aan wet- en regelgeving

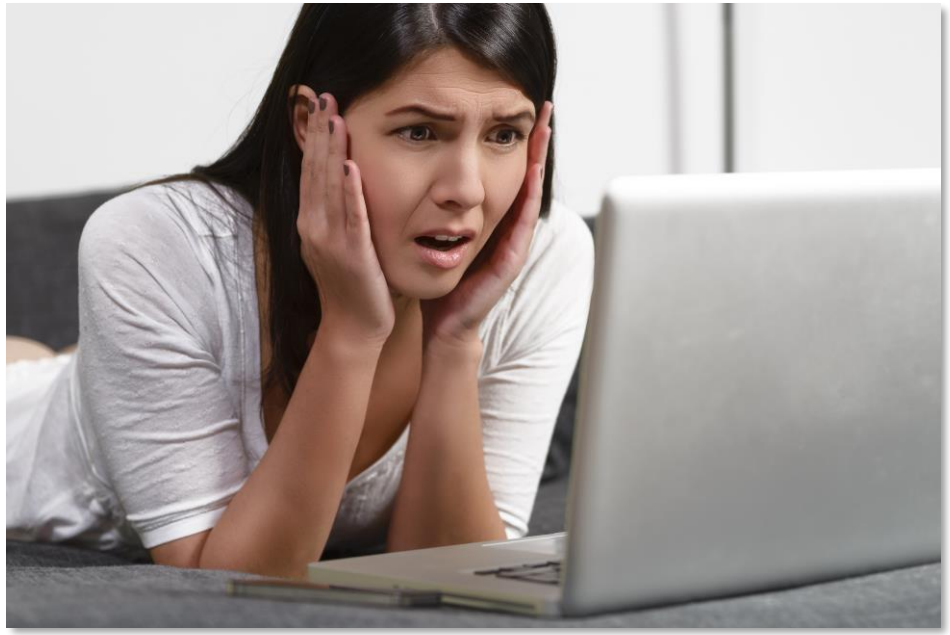
- In de ideale situatie hebben organisaties de intrinsieke motivatie om als organisatie **goed huisvaderschap** te tonen door je eigen gegevens te beschermen. Dit is een erg goede (beste) reden om logische toegangsbeveiliging in te zetten. Dit betreft bijvoorbeeld (persoons)gegevens en bedrijfsgeheimen.

- Vaker treffen wij situaties aan waar organisaties worden **gedwongen door wet- en regelgeving** en eisen vanuit toezichthouders en klanten:
  - In het kader van de jaarrekeningcontrole wordt door accountants veel waarde gehecht aan logische toegangsbeveiliging.
  - De AVG (Algemene verordening gegevensbescherming) stelt eisen aan de toegang die werknemers hebben tot persoonsgegevens.
  - De meldplicht datalekken heeft (als onderdeel van de WbP) een boost gegeven aan aandacht voor identity and access management. Hoe organisaties met datalekken moeten omgaan, staat nu in de AVG verwoord.
  - Voor organisaties die genoteerd zijn aan de Amerikaanse beurzen, of toeleverancier zijn van een in de VS beursgenoteerd bedrijf, is Sarbanes-Oxley (SOx) van toepassing.
  - Veel organisaties werken aan certificering om hun informatiebeveiliging aan te tonen: bijvoorbeeld ISO 27001 besteedt veel aandacht aan identity and access management.
  - In ISAE-verklaringen is het gebruikelijk beheersdoelstellingen op te nemen omtrent logische toegangsbeveiliging.

Observaties en ontwikkelingen in de markt

Knelpunten in de praktijk

- een organisatie kan een toezichthouder of accountant niet overtuigen dat zij aantoonbaar *in control* is;
- een organisatie heeft niet inzichtelijk welke bevoegdheden aan een account van een gebruiker moeten worden gekoppeld zodat hij zijn werkzaamheden kan uitvoeren;
- een organisatie heeft geen volledig inzicht in de gebruikers die toegang hebben tot systemen en gegevens;
- een organisatie past bevoegdheden die aan een account zijn gekoppeld niet (tijdig) aan wanneer die persoon een andere rol/functie binnen de organisatie krijgt;
- doordat data (bij HR en IT) niet juist of volledig zijn en onderling nauwelijks informatie uitwisselen, stranden initiatieven om tooling voor provisioning in te voeren;
- de onderlinge verantwoordelijkheden ten aanzien van *identity and access management* tussen de afdeling HR, de information security officer, de afdeling IT en leidinggevenden zijn niet duidelijk belegd;
- 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 (bijvoorbeeld voor een externe of beheerder);
- functiescheiding wordt doorbroken doordat een gebruiker te veel bevoegdheden heeft;
- bevoegdheden houden snel wijzigende organisatie (agile projecten) niet bij.



Observaties en ontwikkelingen in de markt
Gevolgen

- 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.
- uit onderzoek van de Gartner Group blijkt dat het gemiddeld 12 dagen duurt voordat een nieuwe medewerker een account en de juiste bevoegdheden heeft.

Praktijk
Trends en ontwikkelingen

- Na het RBAC-model (*role based access control*) is er meer behoefte aan opties 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 (bijvoorbeeld het team waar je deel van uit maakt) bevoegdheden worden toegekend.

- Organisaties zoeken hun heil in tooling om zo (volledig geautomatiseerde) provisioning door te voeren. Als een organisatie haar basis (bijvoorbeeld op het gebied van HR, accounts en bevoegdheden) niet op orde heeft, zal dergelijke tooling niet de oplossing gaan bieden.

- Platforms, zoals DigiD en IDIN, die diensten op het gebied van 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.

- Autorisaties die gemonitord worden vanuit gedrag, bijvoorbeeld dat een systeem herkent dat je met een nieuw/ongebruikelijk device inlogt, vanaf een andere locatie, andere activiteiten uitvoert dan gebruikelijk.....

- Op het eerste gezicht lijkt biometrics een onfeilbare manier te bieden voor systemen om individuele mensen met bijna zekerheid te herkennen met behulp van hun unieke biometrische gegevens.

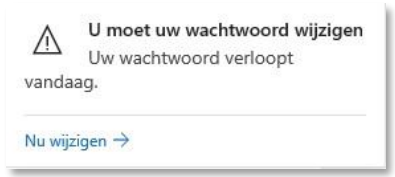
Praktijk
Trends en ontwikkelingen

- Vroeger dwongen instellingen af dat eindgebruikers hun wachtwoord moesten wijzigen. Er is echter meer en meer aandacht voor de nadelen van het frequent wijzigen van wachtwoorden. Sinds enige tijd raadt Microsoft aan het wachtwoord te wijzigen, zonder dit ogenschijnlijk verplicht te stellen.
  - *"Soms doet het meer kwaad dan goed om te vereisen dat gebruikers hun wachtwoorden regelmatig wijzigen."*
  - *"[...] uit onderzoek blijkt dat [het wijzigingen van wachtwoord] meer kwaad doet dan goed."*
- Mogelijk dat de opkomst van two factor authentication daar een rol bij speelt.

Wachtwoorden van eindgebruikers:

- Voor beheeraccounts beveelt Microsoft wel aan het wachtwoord periodiek te wijzigen.

Wachtwoorden van beheeraccounts:



Ons onderzoek
Overeenkomsten tussen de onderzochte organisaties

- Nagenoeg alle organisaties melden nooit klaar te zullen zijn met identity and access management maar beschouwen dit als een continu en arbeidsintensief proces.
- De role based access benadering is nog steeds de belangrijkste basis van waaruit IAM wordt aangevlogen, ook al vindt nagenoeg iedereen dit model minder houdbaar vanwege de dynamiek in de organisatie. De HR administratie is meestal leidend.
- Alle organisaties geven aan dat wet- en regelgeving, vaak in combinatie met (minder positieve) audits, de aanleiding vormen om aandacht te besteden aan identity and access management.
- Een toenemende zorg bij alle organisaties is het feit dat ook klanten, studenten, toeleveranciers, etc. toegang hebben tot systemen.
- Investeringen in een goedlopend identity and access managementproces wordt bij alle organisaties nog als een noodzakelijk kwaad gezien.
- Geautomatiseerde vorm van provisioning is nog beperkt.
- Er is weinig tijd of ambitie om nieuwe ontwikkelingen in te bouwen in het IAM-proces.
- Single-sign-on is in alle gevallen een wens om meer vat te krijgen op toegang, vaak zijn (oude) applicaties echter niet geschikt om dat te optimaliseren.
- Two factor authentication is aan een opmars bezig, zeker daar waar op afstand wordt gewerkt.
- Voor de meeste organisaties is het moeilijk om snel en effectief inzicht te krijgen in de tekortkomingen, vaak komen daar nog veel handmatige bewerkingen bij kijken.
- De combinatie van een gebruikersnaam en wachtwoord is nog de meest gebruikelijke vorm van aanmelden.

- Ons onderzoek is gedaan onder een aantal zeer grote (internationale) organisaties totaal aantal (circa 90.000) medewerkers die hierbij betrokken zijn.

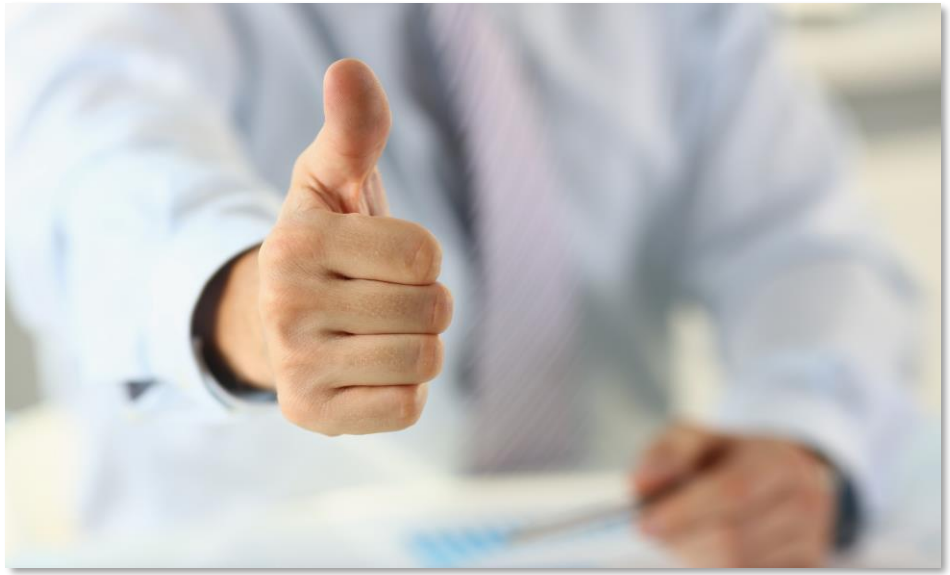
Aanleiding
Gedwongen door wet- en regelgeving en certificering

- NEN 7510 (9.4.1.) stelt: "Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging"
- NEN 7510 (12.4.1) en NEN 7513 (5.1) geven aan dat logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld
- ISO 27002 (9.1.1.) Er dienen passende regels voor toegangsbeveiliging, -rechten en -beperkingen voor specifieke gebruikersrollen ten aanzien van hun bedrijfsmiddelen vastgesteld te worden ....
- ISO 27002 (9.2.1.) Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
- Toetsingskader DNB (pagina 11) ... Daarnaast let DNB erop dat toegang tot gegevens en informatiesystemen door middel van toegangsrechten is beheerst....
- NOREA-guide privacy control (pagina 17) ... Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken. Dit verkleint de kans op ongeautoriseerde toegang tot en onjuiste verwerking van persoonsgegevens, of inbreuk in verband met persoonsgegevens door interne medewerkers, derden of hackers.
- In de AVG zijn op verschillende plekken bepalingen over passende technische en organisatorische maatregelen opgenomen.

- De AVG (Algemene verordening gegevensbescherming) stelt eisen aan de toegang die werknemers hebben tot persoonsgegevens. Een organisatie moet immers volgens artikel 32 lid 1 *"passende technische en organisatorische maatregelen"* nemen.
- In ISAE-verklaringen is het gebruikelijk beheersdoelstellingen op te nemen omtrent logische toegangsbeveiliging. Met name in hoofdstuk *Access control* uit ISO 27002 wordt ingegaan op *identity and access management*.
- In het kader van de jaarrekeningcontrole wordt door accountants veel waarde gehecht aan logische toegangsbeveiliging. Accountants moeten immers volgens artikel 393 lid 4 uit Burgerlijk wetboek boek 2 de *"betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking"* beoordelen. IT-auditors richten zich daarbij onder andere op *identity and access management*.

Uitkomsten onderzoek
Positieve uitkomsten

- Gemiddeld wordt een cijfer 3 (uit 5) gegeven voor wat betreft de gepercipieerde kwaliteit.
- Onder druk van wet- en regelgeving en certificering is er meer aandacht voor identity and access management.
- Two factor authentication is aan een opmars bezig.
- Dat geldt ook voor single sign on.
- In iedere organisatie is het dossier belegd bij een verantwoordelijke.
- Er is een begin gemaakt in het verhogen van de awareness bij medewerkers m.b.t. identity and access management.
- Veel organisaties zijn zich ervan bewust dat een goed werkend IAM proces (financiële, reputatie, imago) schade kan voorkomen, risico's zijn dus beter in beeld gekomen.
- Alle organisaties kennen een lijst van noodzakelijke activiteiten die ondernomen moet worden om IAM op orde te krijgen/houden.



Uitkomsten onderzoek
Negatieve werkelijkheid

- Intrinsieke motivatie om met identity and access management bezig te zijn is vaak afwezig (aan de top) dat zet veel druk op diegenn die verantwoordelijk zijn gesteld.
- Vanwege voorgaande is het beschikbaar stellen van middelen vaak (te) beperkt.
- Awareness bij personeel is te verbeteren door daar structureel en frequent aandacht aan te geven.
- Het in-, door- en uitstroom proces is meestal bij HR belegd, zij zijn niet altijd alert op de link die naar identity and access management dient te worden gelegd met name voor wat betreft tijdigheid.
- Nieuwe ontwikkelingen worden niet- of nauwelijks ingebouwd vaak wordt er voortgeborduurd op bestaande processen en werkwijzen.
- Het feit dat externen (klanten, leerlingen, studenten, ...) eveneens toegang hebben tot bepaalde systemen maakt het beheer gecompliceerder; vaak wordt identity and access management op separate plaatsen binnen de organisatie opgepakt waardoor een effectieve, beheersbare toegangsverlening voor zowel gebruikers binnen als buiten de organisatie niet altijd wordt gevonden.
- Elke organisatie worstelt met het probleem van een statisch identity and access managementproces, in een tijd dat de dynamiek steeds groter wordt, (agile, lean, ...) maakt dat niet altijd de meest efficiënte en effectieve oplossing kan worden gemaakt.
- Het geautomatiseerd verlenen van autorisaties en het monitoren van de benodigde kwaliteit is nog beperkt, er komt nog veel handmatig werk bij kijken.
- Tooling wordt soms gezien als de holy grail als het gaat om het oplossen van knelpunten, maar is dat niet.

Handreikingen
Praktische tips

- Zorg voor een goed werkend in-, door- en uitstroomproces.
- Zorg dat de single point of truth kwalitatief op orde is.
- Onderzoek welke aanpassingen nodig zijn om single sign on in te voeren.
- Besteed frequent en gestructureerd aandacht aan de bewustwording bij medewerkers.
- Zorg voor draagvlak door het eigenaarschap van het identity and access management dossier op het hoogste niveau belegd te krijgen.
- Vraag om commitment en het beschikbaar stellen van de daarbij behorende middelen.
- Zorg dat identity and access management een wezenlijk onderdeel van het informatiebeveiligingsbeleid is.
- DNB, Autoriteit Persoonsgegevens (AVG), ISO, NEN, ... zijn belangrijke bronnen voor identity and access management.
- Imago en reputatie kunnen flinke averij oplopen als een organisatie uit de bocht vliegt (denk aan Haga Ziekenhuis).
- Ook financiële schade ligt op de loer, bijvoorbeeld als vanwege het ontbreken van functiescheiding geld wordt weggesluisd.
- Een (externe) audit kan de noodzaak om het dossier hoog op de agenda te krijgen helpen.

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