Auteur: Pieter Muller IAM-/Security consultant, werkzaam bij Dux Group in Rotterdam. Hij staat altijd open voor een gesprek, je kunt hem benaderen via https://nl.linkedin.com/in/pieter-muller-61629563

Een bewuste manager is goud waard

Goud is waardevol, goud is mooi en veel mensen willen het hebben. Als je een medewerker binnen de organisatie aanspreekt en vraagt of goud waardevol is, is het antwoord al snel 'ja'. Dit komt omdat wij als mensen goud kunnen zien, het kunnen herkennen en zelfs kunnen opzoeken. Op het moment van schrijven is goud 58.800,64 euro per kilogram waard.

Als ik een kilo goud in bezit zou hebben, zou ik dit niet in mijn rugtas stoppen om vervolgens met het openbaar vervoer naar mijn werk te gaan. Ik zou dit goed beschermen en alleen toegankelijk maken voor de juiste personen. De Nederlandsche Bank heeft de goudvoorraad onlangs ook niet in rugtassen met het OV verplaatst naar het nieuwe DNB cashcentrum in Zeist.

Deze voorzichtigheid en voorzorgsmaatregelen zijn niet anders voor de toegang tot systemen en informatie.

Mijn ervaring is dat de toegang van identiteiten tot systemen en data niet vlekkeloos verloopt en dat voornamelijk het bewustzijn bij medewerkers en managers een groot pijnpunt is binnen organisaties wat betreft Identity- en Access Management. Tegenwoordig hebben we al vele manieren ontwikkeld om als organisatie een waarde te geven aan informatie, maar waarom vinden we het dan toch lastig om systeemtoegang tot deze informatie op de juiste manier te regelen?

Mijn ervaring

Als Young Professional kom je binnen bij een bedrijf en neem je een flinke scheut energie en prestatiedrang mee. Je wilt het goed doen bij een team, de klant goed bedienen en vooral je manager tevreden houden. Als een manager jou tijdens de start van je carrière onder druk zet om autorisatieverzoeken op een onjuiste manier te verwerken moet je van goeden huize komen om hier tegenin te gaan. *'Wil ik het juiste doen of wil ik een manager tevreden stellen?'*: deze gedachte heb ik wel eens gehad en ik kan me voorstellen dat ik niet de enige ben. Als de awareness niet bij de manager aanwezig is, kun je dit moeilijk vragen van de startende medewerker.

Binnen verschillende operationeel autorisatiebeheerteams ben ik verantwoordelijk geweest voor de koppeling van autorisaties aan de juiste medewerker. Een vraag die ik vaak voorbij heb horen komen is: *'Hoelang duurt het nog voordat H. van de Kool haar autorisaties in bezit heeft? Morgen begint zij met werken en ik heb dit gistermiddag doorgegeven aan HR.'* Ik denk dat veel autorisatiebeheerders zich hierin herkennen. Moet je jezelf eens voorstellen dat bovenstaande vraag van de leidinggevende wordt uitgesproken voor de toegang tot de goudkluis van de DNB… Het bewustzijn bij leidinggevenden en management over de toegang tot informatie en de benodigde activiteiten is vaak niet toereikend. Men wil zo snel mogelijk de medewerkers het werk laten uitvoeren in de systemen, maar op welke manier zij toegang krijgen, maakt vaak niet uit. Dit komt enerzijds door onwetendheid over autorisatiebeheer en anderzijds doordat de manager de medewerker zo snel mogelijk aan het werk wil zien gaan. Daarbij komt dat het functioneren van een beheerteam wordt beoordeeld op snelheid en aantallen (productiviteit) en niet op veiligheid (security). Dit komt niet overeen met het doel dat wij met Identity & Access Management nastreven:

De juiste medewerkers (identiteiten) op het juiste moment toegang geven tot de juiste informatie.

Wat mij verbaast, is dat veiligheid nog onvoldoende wordt opgenomen als kernwaarde bij het resultaat van een bedrijf of team. "Helaas hoor ik te vaak de welbekende zin vanuit security professionals 'eigenlijk moet een incident zich voordoen', want dan gaat het management de noodzaak van autorisatiebeheer als voorwaarde voor informatieveiligheid inzien."

Wanneer gaan we echt inzien dat de informatie van de organisatie, natuurlijke persoon of van een klant niet een testomgeving is, maar dat het data is die het verdient om beschermd te worden?

Awareness voor managers

We kunnen niet alleen vertrouwen op regels en techniek. Het bewustzijn van medewerkers met verantwoordelijkheid speelt een cruciale rol bij het succes van deze regels en techniek. Er zijn verschillende manieren bedacht om de awareness te verhogen en de meeste bedrijven voeren deze al uit. Denk hierbij aan online trainingen, posters en andere communicatiemiddelen. Mijn ervaring is dat de resultaten van deze middelen vaak tegenvallen, aangezien we gewoon doorklikken tot we honderd procent behaald hebben in het geval van e-learning. Zoals eerder geschreven willen mensen graag resultaten behalen en als dat met een work-around moet, doen we dat liever dan het veilige (en onbegrepen) proces volgen.

Het is belangrijk om niet alleen te steunen op het informatiebeveiligingsbewustzijn van de manager, dit kan ook op een formele manier benaderd worden. Zij hebben tenslotte al genoeg aan hun hoofd met de dagelijkse werkzaamheden. Het is belangrijk dat een gestructureerde aanpak wordt gehanteerd om het bewustzijn van medewerkers te vergroten en de veiligheid van informatie te waarborgen.

Door middel van het leggen van formele verantwoordelijkheid bij managers kan informatieveiligheid betrokken wor-

Autorisatiebeheer KPI's

Het is belangrijk op te merken dat de drempelwaarden voor het beoordelen van KPI's zoals hieronder genoemd, afhankelijk zijn van de specifieke context en doelen van de organisatie.

- Percentage onjuiste toegangsverzoeken dat wordt geweigerd of gecorrigeerd per risiconiveau of gevoeligheidsniveau van de informatiebronnen ☛ Dit geeft inzicht in de effectiviteit van het weigeren of corrigeren van onjuiste toegangsverzoeken op basis van het potentiële risico.
- Aantal beveiligingsincidenten gerelateerd aan ongeautoriseerde toegang per beveiligingsmaatregel ☛ Dit meet het aantal incidenten dat wordt veroorzaakt door ongeautoriseerde toegang, zoals pogingen tot inbraak, misbruik van gebruikersreferenties of ongeautoriseerde toegang tot gevoelige gegevens. Het wordt uitgesplitst per beveiligingsmaatregel, zoals sterke authenticatie, toegangscontroles, logging en monitoring, om de effectiviteit van specifieke maatregelen te evalueren bij het voorkomen van ongeautoriseerde toegang.
- Gemiddelde tijd (in dagen) die nodig is om toegangsrechten in te trekken of te wijzigen bij personeelsverloop, uitgedrukt als een percentage van de totale doorlooptijd van het proces ☛ Dit meet de efficiëntie van het proces voor het beheren van toegangsrechten wanneer medewerkers het bedrijf verlaten of van functie veranderen. Het geeft inzicht in hoe snel toegangsrechten worden aangepast om ongeautoriseerde toegang te voorkomen en de beveiliging te waarborgen.

Nog een aantal losse KPI's zonder toelichting:

- Percentage van de identiteiten met de juiste en actuele toegangsrechten
- Aantal herstelacties na interne audits of beveiligingscontroles
- Percentage van de identiteiten met te veel toegangsrechten (overprivilege)
- Percentage van de identiteiten met afwijkende of ongebruikelijke toegangsactiviteiten
- Het aantal unieke referenties (zoals gebruikersnamen en wachtwoorden) in verhouding tot het aantal toegangspunten
- De gemiddelde tijd die nodig is om een nieuwe gebruiker volledige toegang te geven tot alle benodigde bronnen

den in de resultaten die teams behalen. Op deze manier worden leidinggevenden op een gestructureerde en formele manier bewust gemaakt van het belang van informatiebeveiliging en worden de risico's op incidenten geminimaliseerd. Hier zijn KPI's (zie kader) voor op te stellen zodat de score op informatieveiligheid betrokken wordt in de resultaten en ook tastbaar wordt. Op deze manier kunnen we in plaats van bewustzijn creëren, bewustzijn opleggen bij leidinggevenden. Zinnen als 'kunnen jullie de autorisaties even snel toevoegen' hoop ik daardoor minder te horen op de werkvloer.

Ondertussen schaar ik mezelf niet meer tot de Young Professionals en heb ik mezelf laatst ook betrapt op hetzelfde gedrag: even snel autorisatiekoppelingen laten doorvoeren door autorisatiebeheer om resultaat te laten zien aan de opdrachtgever. Doe ik gewoon hetzelfde! Meer dan menselijk natuurlijk, maar het benadrukt wel de resultaatgerichte werkomgeving in Nederland. Gelukkig heb ik dit nog op tijd teruggetrokken, want ik wil zelf het resultaat niet alleen beoordelen op snelheid en aantallen, maar ook op juistheid en veiligheid.

Het nieuwe goud

Deel dit met je manager en laten we de verantwoordelijkheid voor de bescherming van het nieuwe goud samen pakken. Samen kunnen we ervoor zorgen dat de berg van informatie niet alleen groter wordt, maar ook veiliger. Laten we toegangsbeheer niet langer zien als een kostenpost, maar als een waardevol resultaat dat het management met trots kan presenteren. Laten we samen de weg banen naar een toekomst waarin de waarde van informatie wordt gekoesterd en waarin veiligheid een van de essentiële (formele) pijlers is waarop we bouwen.