Lees dit als je je nooit meer druk wilt maken over onveilige wachtwoorden.

De 10 meestgestelde vragen over Identity & Access Management in de Microsoft cloud

Portiva.

De 10 meest-gestelde vragen

Security begint altijd met identiteit. Als je data beveiligt, ben je aan het nadenken over wie er welke acties op mag doen. Dat is volkomen nutteloos, als je niet weet wie degene is die jouw data benadert. Daarom maakt Microsoft van *Identity & Access Management* de kern van cloud security. Om je data en apps te beveiligen levert Microsoft dus een heel compleet en robuust identiteitsmanagement. Onder het motto *"Focus on identity"* bouwt Microsoft aan een infrastructuur die jou helpt om gemak, productiviteit en veiligheid met elkaar te combineren. En dat brengt ons meteen bij vraag 1:

1 Hoe verhoudt Microsoft A&I-management zich tot de concurrentie?

Natuurlijk zijn andere cloudproviders ook druk met identiteitsmanagement. De belangrijkste zijn natuurlijk Google Cloud Platform en Amazon Web Services.

Google Cloud Platform

Google werkt met een enkele identiteit. Dat is het bekende Gmail-adres dat bijna iedereen heeft. Je kunt dat soms gebruiken om bij andere cloud-apps in te loggen, maar het dient toch vooral om je te identificeren bij Google-services. Er is geen centraal management van deze logins en je kunt als beheerder dus geen data combineren. Je kennis over de veiligheid van je omgevingen blijft verdeeld over meerdere tools.

Amazon Web Services

Amazon biedt krachtig I&A-management. Dit is alleen helemaal toegesneden op de toegang tot AWS webservices en integreert nauwelijks met jouw eigen beveiligingsoplossingen. Dat betekent dat jouw gebruikers altijd met verschillende identiteiten zullen moeten blijven werken.

Totaaloplossing van Microsoft

Microsoft streeft ernaar een totale oplossing te bieden voor identiteitsmanagement. Dat betekent dat je binnen Azure je identiteiten centraal kunt managen, ook voor maatwerkoplossingen en apps van derden.

Dat geeft je mensen niet alleen gemak, het zorgt ook dat Azure heel goed kan zien of er vreemde dingen gebeuren op jouw omgevingen. Een login op een Azure-app vanuit Amsterdam, binnen een uur gevolgd door een e-mail login uit China? Dat kan nooit dezelfde persoon zijn. Grote kans dat hier hackers actief zijn. Azure zal in zo'n geval de beheerder waarschuwen. Of, als jij dat zo instelt, het account automatisch blokkeren.

Microsoft bouwt weliswaar aan zijn eigen *identitity provider*, maar doet dat op basis van open standaarden om te zorgen dat de software altijd goed kan samenwerken met software van andere partijen.

Nadenken over identiteit? Dan moet je het niet alleen over de cloud hebben, maar ook over Windows, servers, *on-premises* installaties, databases, bestandsservers etc. Jij bent jij en jouw rechten hangen aan jouw identiteit, of je nou in de cloud aan het werk bent of op je eigen laptop.

2 Hoe houden we onze data veilig als er steeds meer naar de cloud verhuist?

Cloud security begint ermee dat iedereen zijn *eigen* identiteit heeft. In heel veel bedrijven zie je dat er voor allerlei apps 'algemene' accounts zijn. Maar als 'secretariaat@mijnbedrijf.nl' bij de betalingsgegevens, de urenadministratie en de hotelboekingen kan, wie hebben er dan eigenlijk toegang tot die data? En verander je dan iedere keer het wachtwoord als er bij het secretariaat iemand uit dienst gaat?

Een migratie naar de cloud blijkt in de praktijk een goed moment om over dit soort dingen na te denken en ook het I&A-beleid voor andere applicaties strak te trekken. Als iedereen alle handelingen altijd met zijn eigen identiteit doet en als alle rechten direct gelinkt zijn aan een persoon, is alles traceerbaar, beheersbaar en configureerbaar. In de cloud, maar ook in je bestaande *on-premises* omgeving.

Stap 2 is het aanzetten van *multi-factor authentication (MFA)*. Door het gebruik van wachtwoorden *('something you know')* te combineren met bijvoorbeeld authenticatie met je mobiele telefoon *('something you have')* en/of een vingerafdruk *('something you are')*. Dit maakt het hacken van een identiteit extreem veel moeilijker.

De derde stap die je moet zetten is het maken van beleid: het simpelweg goed nadenken over wie waar aan mag zitten. Dit verschilt niet wezenlijk van wat je voor je *on-premises* omgeving al deed. Je kunt dat positief of negatief aanpakken. Ofwel je zet alles dicht en zet dan open wat mensen echt nodig hebben. Of je zet alles open en sluit dan de dingen af die je wilt beschermen.
Een trend die we zien bij het toewijzen van rechten is *just in time* rechtenmanagement. Moet je een site inrichten, een netwerkschijf bekijken of een klus doen die je normaal binnen je functie niet doet? Dan kan een beheerder je rechten geven voor een beperkte tijd. Dat kan een uur zijn, een week of een maand. Maar het betekent in ieder geval dat jouw extra rechten op een gegeven moment vanzelf weer verdwijnen, zonder dat iemand daar iets voor hoeft te doen. Dit voorkomt 'zwevende rechten': de rechten die ooit zijn toegekend en nooit meer opgeruimd. Het bouwt ook een extra controlestap in, omdat een beheerder de kans krijgt om te beoordelen of de rechten waar een gebruiker om vraagt ook echt passen bij het werk dat gedaan moet worden.

Awareness blijft daarbij een sleutelfactor: waarom doen we dit? Hoe werkt het? Geef je gebruikers opties en dwing ze niet in een keurslijf. Maak het ze makkelijk om een eigen, veilige manier van werken te ontwikkelen. Combineer online (video)training met trainingssessies en ondersteuning op de werkvloer.

Zet MFA aan: combineer 'something you know' met 'something you have' en/of 'something you are'

3 Hoe houden we in de gaten of onze gebruikers onveilig gedrag vertonen?

Veel organisaties gaan *security monitoring* pas serieus nemen als het een keer misgaat. We hoeven vast niet uit te leggen dat het beter is om monitoring eerder in te voeren. Namelijk meteen als je begint met werken in de cloud. Want zodra je begint te monitoren en data te verzamelen, begin je te leren en kennis op te doen. Zo weet je wat er van dag tot dag gebeurt met de identiteiten van jouw mensen en kun je effectief beleid bedenken.

Veel monitoring van gebruikersgedrag zit standaard in SharePoint en Teams, dus begin op dag 1 met het gebruiken van het Office 365 Security & Compliance Center om gebruikersgedrag binnen Office te monitoren.

Zet daarna de stap naar het monitoren van je hele omgeving via Azure. De security-tool Azure Sentinel geeft je een overkoepelende blik. Je kunt dus per identiteit, per systeem, per app of per tijdstip zien wat er gebeurd is om zo problemen op het spoor komen.

4 Wat is een effectief beleid voor het toelaten van externe gebruikers?

Wij houden van samenwerken. En dat is precies waar de cloud voor bedoeld is. We worden effectiever en gelukkiger als we zonder gedoe kunnen samenwerken met de mensen die we nodig hebben voor ons werk. En dat zijn allang niet meer alleen onze directe collega's. Om samen met externen, leveranciers en partners wereldwijd effectief te zijn, hebben we openheid en vertrouwen nodig. We adviseren dus om jouw mensen, waar dat kan, uit te laten nodigen wie ze willen uitnodigen.

Tegelijkertijd snappen we ook dat je grip op de zaak wilt houden door je eigen processen in te richten voor het uitnodigen van externen.

Omdat Microsoft daar geen standaard-oplossing voor heeft, werken wij zelf aan zo'n oplossing. Codenaam: PEAM (Portiva External Access Manager. Maar als je een suggestie hebt voor iets pakkenders, laat het ons vooral weten). Deze tool geeft je de mogelijkheid om iedere keer als iemand een externe uitnodigt een workflow te triggeren die bijvoorbeeld notificaties stuurt, extra data logt of rechten aanpast.

5 Wat is een effectief beleid voor het toelaten van externe gebruikers?

In de media is er veel aandacht voor cybersecurity en vaak gaat het dan over 'veilige wachtwoorden'. We willen niet de doemprofeet uithangen, maar er bestaat helaas niet zoiets als een veilig wachtwoord. Hackers hebben tegenwoordig zulke geavanceerde technieken en zoveel rekenkracht tot hun beschikking, dat ieder wachtwoord te kraken is.

Tegelijkertijd maken we ons dus niet zo druk meer om wachtwoorden, maar zetten wel altijd *multi-factor authentication (MFA)* aan. Door je, naast je wachtwoord, te identificeren met iets anders laat je op meerdere manieren zien dat je bent wie je beweert te zijn. Dit is voor een cybercrimineel erg moeilijk te imiteren.

Natuurlijk is het raadzaam om niet voor alle webwinkels, sociale media én voor je werk-account hetzelfde wachtwoord te gebruiken. Dat maakt het hackers wel erg makkelijk. Maar we moeten niet te ingewikkeld doen over wachtwoorden. Het afdwingen van ingewikkelde wachtwoorden en dan ook nog eens eisen dat gebruikers die iedere zes weken veranderen maakt het nodeloos moeilijk voor hen. Het is veel beter om gebruikers één keer een wachtwoord van minimaal 8 karakters te laten kiezen en dat te combineren met MFA.

6 Hoe voorkom ik dat collega's elkaars account gebruiken om buiten Beheer om rechten te regelen?

De basis van cloud security is dat je weet wie welke rechten heeft. Dat werkt alleen als je iedereen kunt identificeren. Zodra mensen elkaars accounts gaan gebruiken loopt dat in het honderd.

Met het aanzetten van MFA houd je dit effectief tegen. Maar alleen tegenhouden is niet het antwoord. Vraag je eens af: *waarom* delen mensen eigenlijk accounts en wachtwoorden met elkaar? Waarom zijn gebruikers op zoek naar manieren om het systeem te omzeilen? Dit gebeurt bijna nooit uit kwaadwilligheid, maar vrijwel altijd omdat de 'officiële weg' te veel gedoe is. Als je medewerkers bepaalde rechten nodig hebben om hun werk te doen, dan moeten ze die makkelijk kunnen krijgen. Regel je dit niet goed, dan gaan ze op zoek naar sluipweggetjes.

Privileged Identity Management kan daarbij enorm helpen. Met deze voorziening binnen Azure Active Directory kun je mensen tijdelijke rechten geven om een klus te doen. Of je kunt gebruikers toestaan om hun rechten te delen met anderen, zodat ze hun account niet hoeven te delen. Dat heet *delegated access*. Gebruikers die hun rechten delen moeten zich dan wel realiseren dat ze ook verantwoordelijkheid dragen voor wat er met die rechten gebeurt.

Dit is dus weer typisch zo'n uitdaging waar er niet één makkelijke oplossing is. Combineer techniek, awareness en training en luister naar de wensen van je teams. Zo kom je tot een oplossing die werkt.

7 Hoe beheer ik rechten op niet-Microsoft accounts

Zoals we al zeiden wil Microsoft een totaaloplossing bieden voor identity management. Azure Active Directory kan gebruikt worden om toegang te beheren tot honderden niet-Microsoft apps. Maar binnen de Microsoft-cloud kun je ook de corporate Twitter-, Facebook- en LinkedIn-accounts koppelen. Als je dat gedaan hebt, kun je binnen je Microsoft-omgeving bepalen wie er bij die accounts mag. Zo kun je traceren wie wat gedaan heeft, makkelijk nieuwe medewerkers onboarden en, niet onbelangrijk, alle rechten in één keer intrekken als iemand uit dienst gaat.

8 Hoe maak ik het makkelijk voor mijn gebruikers (en voor mijn helpdesk)?

Identity & Access Management is altijd een balanceer-act tussen mensen ruimte geven om hun werk te doen, het technisch afdwingen van veiligheidseisen en het kweken van verantwoordelijkheidsgevoel en bewustzijn.

Als je het te ingewikkeld maakt en te veel beperkingen oplegt, wordt je helpdesk continu overspoeld met vragen en wachtwoord-resets. Uiteindelijk gaan mensen dan ook op zoek naar manieren om je beveiliging te omzeilen. Wat wil je dus afdwingen? Een minimum wachtwoordlengte van 200 karakters? Geen probleem! Alleen kan niemand dat onthouden. Self-service password reset blokkeren? Waar is dat goed voor? Het leidt alleen tot een stortvloed van telefoontjes na de zomervakantie.

Zelfstandigheid kweek je met goede adoptie en awareness. En dat begint altijd met opleiden en uitleggen. Leg je medewerkers uit waarom bepaalde dingen moeten of niet mogen. En help ze dan met de praktische uitvoering.

Identity & Access Management is altijd een balanceer-act tussen mensen ruimte geven om hun werk te doen, het technisch afdwingen van veiligheidseisen en het kweken van verantwoordelijkheidsgevoel en bewustzijn.

9 Kunnen we met een pilot beginnen? Om te kijken of het voor ons werkt?

Het korte antwoord? Ja, natuurlijk! Welkom in de cloud, waar het opzetten van een *proof of concept* een fluitje van een cent is. Je kunt dus heel makkelijk met een klein groepje gebruikers of met één afdeling een pilotproject draaien.

Maar daar zijn ook risico's aan verbonden. We zien soms dat zo'n pilotproject vreselijk escaleert, omdat security een onderwerp is waar veel mensen zo hun eigen mening over hebben. Er is dus een kans dat zo'n klein, maar verregaand project tot eindeloze discussies leidt en dat daardoor het overkoepelende security-project vertraging oploopt.

Vaak is het handiger om wel de hele organisatie mee te nemen, maar dan in kleine stapjes. Begin bijvoorbeeld met het aanzetten van MFA voor een kleine groep gebruikers. Gaat dat goed? Dan kun je het invoeren voor de hele organisatie. Kom daarbij nog niet aan de rest van het security-beleid. Laat mensen eerst aan MFA wennen. Daarna kun je in kleine stapjes je wachtwoordbeleid gaan verbeteren.

Onthoud vooral dat security niet iets is wat je even doet en wat dan 'af' is. Je krijgt het nooit in één keer perfect, dus blijf je ermee bezig. Iedere keer maak je dingen weer een stukje beter, maar dan wel voor alle gebruikers.

Wij kiezen dus het liefst voor een *agile* aanpak. We nemen de tijd om niet alleen de techniek, maar ook bedrijfsvoering, beheer en implementatie mee te nemen in de veranderingen.

Onthoud vooral dat security niet iets is wat je even doet en wat dan 'af' is . Je krijgt het nooit in één keer perfect. Wij kiezen het liefst voor een agile aanpak.

10 Wat is de beste manier om nieuwe medewerkers in te werken in de cloud?

Als er een nieuwe medewerker binnenkomt wil iedereen dat die zo snel mogelijk aan het werk kan. Maar bij de praktische invulling daarvan komen veel vragen langs. Welk materiaal stellen we beschikbaar? Hoeveel tijd moeten we inruimen voor onboarding? Regelen we dit centraal of laten we de teams het doen? Automatisch, remote of met persoonlijke aandacht? Allemaal vragen met antwoorden die per organisatie verschillen, maar een paar punten gelden altijd:

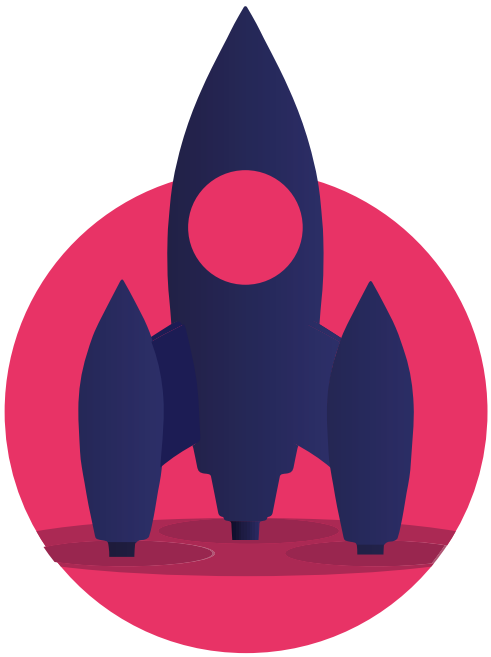
- Richt zo veel mogelijk van tevoren in. Zorg dat bestanden automatisch gesynchroniseerd worden, vraag bij een eerste inlog automatisch om een nieuw wachtwoord en zorg dat overal de 'juiste vinkjes' aan staan. Dat scheelt veel tijd en irritatie en is dus een investering die zich terugbetaalt bij iedere nieuwe medewerker die binnenkomt.

- Help managers zo veel mogelijk bij de dingen die je niet automatisch kunt laten gebeuren. Laat ze rechten toewijzen op basis van groepen en regels, in plaats van aan een individu. Dit is sneller, overzichtelijker en veel veiliger.

- Denk aan je informatievoorziening. Je kunt een nieuwe medewerker automatisch een postvak geven en toegang tot de gedeelde schijf. Maar hoe weet diegene dat die schijf bestaat en hoe hij zijn mail moet openen? Deze standaardvragen kun je beantwoorden met content, zodat medewerker en manager daar zo min mogelijk tijd mee kwijt zijn.

- Richt alles in met een standaardproces (in de volksmond een 'wasstraat') waar iedere nieuwe medewerker doorheen moet. Ze weet je zeker dat je niets vergeet.

Het Microsoft A&I-management zorgt dat de nieuwe identiteit meteen overal wordt meegenomen in logging en rapportages. Maar ook regels voor het spamfilter worden meteen toegepast op de nieuwe inbox. Werk je overal met encrypted harddisks? Dan wordt die instelling automatisch overgenomen op de nieuw aangemelde laptop.



Stappen zetten. Niet morgen, maar vandaag...

En dat is misschien wel de belangrijkste winst die cloud-technologie heeft gebracht. Door de nieuwe manier van betalen voor software en rekenkracht, per maand per gebruiker in plaats van met grote investeringen vooraf, kunnen ook kleinere bedrijven nu gebruik maken van enterprise-level technologie en beveiliging. En juist bij die bedrijven is er veel winst te halen uit het optimaal inrichten en waar mogelijk automatiseren van identiteitsmanagement.

Er is dus geen excuus meer. Begin vandaag met stappen zetten naar betere security. Verder praten over identity & access management in Azure? Bel of mail ons en we vertellen je er alles over. We verheugen ons er nu al op!

Verder praten? We kunnen niet wachten!

Neem contact op met Thomas Schrader
Teamlead Security
tschrader@portiva.nl
0648592570

Over Portiva | Als productivity partner levert Portiva consultancydiensten, end-to-end maatwerk ontwikkeling en managed services oplossingen. Als high-end Microsoft Gold Certified Partner richten wij ons op SharePoint, Office 365, Security en Azure. Wij hebben een strategische blik en pragmatische aanpak. Vanuit onze passie voor en kennis over technologie stemmen wij mensen, processen en technologie beter op elkaar af om organisaties meer te laten bereiken, effectiviteit te verhogen en onderlinge samenwerking en communicatie te optimaliseren.