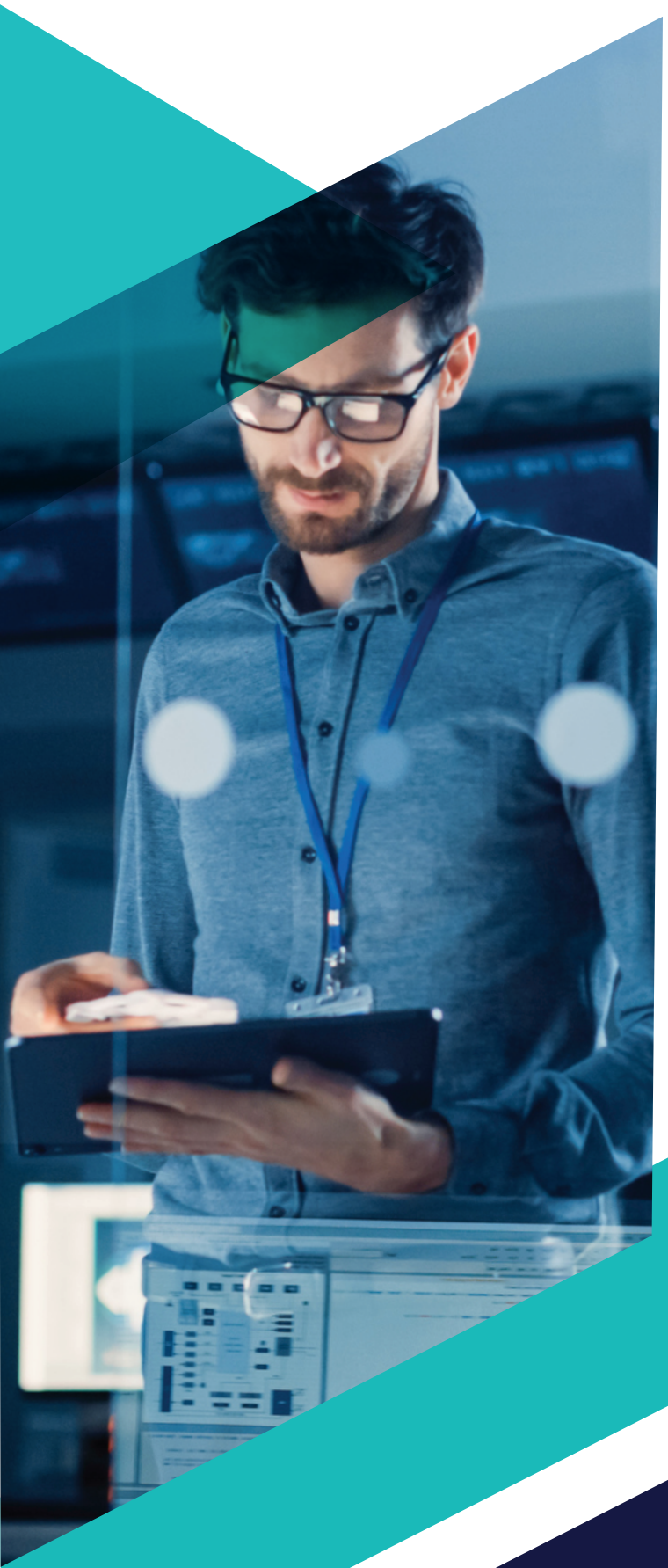


MODERNE CLOUD SECURITY

WHITEPAPER

Van een traditionele naar een moderne manier van beveiligen

INSPARK

INHOUDSOPGAVE

VEILIG IN DE CLOUD: EEN NIEUWE MINDSET

Traditionele security oplossingen bieden beveiliging door een IT-omgeving van de buitenwereld af te schermen, bijvoorbeeld met behulp van firewalls en VPN-tunnels. Een dergelijke beveiliging wordt dan ook vaak vergeleken met die van een kasteel: een bolwerk met één sterk bewaakte ingang, omringd door een diepe slotgracht. Maar de tijden waarin dit succesvol was, zijn nu voorbij, omdat deze aanpak niet meer voldoet in een cloud wereld. De cloud is namelijk 24 uur per dag, 7 dagen per week via het publieke internet te benaderen.

De security van deze omgevingen dient secure-by-design geïmplementeerd te worden, waarbij we zes lagen onderscheiden: identiteiten, endpoints (devices), applicaties, data, infrastructuur en web applicaties.

In deze whitepaper lees je hoe een dergelijke moderne en zeer noodzakelijke cloud security aanpak eruitziet. Deze informatie is gebaseerd op onze jarenlange ervaring en expertise, welke ook worden erkend door Microsoft.

DE ZES LAGEN VAN CLOUD SECURITY

De zes lagen waarop je je cloud omgeving dient te beveiligen:

1. IDENTITEIT

Maatregelen om zeker te weten dat je de juiste gebruiker voor je hebt, zonder dat de gebruiker hiervan hinder ondervindt. Zo zijn wachtwoorden tegenwoordig een zwakke vorm van beveiliging, dus passwordless is de toekomst.

2. ENDPOINTS &DEVICES

Moderne beveiliging van devices, omgevingen en workloads die verbinding maken met de cloud. Dit gebeurt met behulp van krachtige en intelligente Machine Learning modellen die op de achtergrond draaien en de gebruikers veilig houden, zelfs wanneer er sprake is van zeer recente en nog onbekende uitbraken (zogenaamde ‘zero-days’).

3. APPLICATIES

Scheiden van zakelijke en privé applicaties en beperking van applicatietoegang voor specifieke gebruikers op bepaalde locaties. Dit kan bijvoorbeeld door ervoor te zorgen dat bepaalde data niet in een privé dropbox geplaatst mogen worden en dat bedrijfsapplicaties die privacygevoelige informatie bevatten, niet geopend mogen worden in het buitenland.

DE ZES LAGEN VAN CLOUD SECURITY

4. DATA

Beveiliging die met de data zelf 'meereist', in plaats van beveiliging van de toegang tot de omgevingen waarmee de data bekeken en verstuurd worden. Een voorbeeld is de automatische classificatie van data op basis van specifieke kenmerken, zoals BSN-nummer of bankrekening gegevens. Op basis van deze classificatie kan dan automatische encryptie & Data Loss Prevention (DLP) toegepast worden, waardoor deze documenten niet zomaar door derden geopend of per mail verstuurd kunnen worden.

5. INFRASTRUCTUUR

Bijna elke organisatie heeft wel bedrijfsapplicaties die benaderd worden vanaf gehoste werkplekken. Deze bedrijfs applicaties worden vaak weer gehost in een data center, dat on-premises of in de cloud staat. Deze infrastructuur wordt steeds vaker ontsloten via het publieke internet en dient voorzien te worden van moderne endpoint beveiliging.
Een dergelijke infrastructuur moet "secure-by-design" ingericht worden, zodat servers niet langer via een extern bureaublad voortdurend openstaan voor de buitenwereld.

6. WEB APPLICATIES

Webapplicaties zijn vaak 24/7 verbonden met het internet. Hierdoor worden deze applicaties vaak gebruikt als 'point of entry' door aanvallers aangezien veel van deze webapplicaties kwetsbaarheden bevatten. Waar wij vanuit ons Infrastructure Protection Pack de infrastructuur laag beschermen en voorzien van monitoring, beschermen wij middels het Web Application Protection Pack de webapplicaties die ontsloten zijn richting het internet.

IN DRIE STAPPEN NAAR EEN SUCCESVOLLE CLOUD SECURITY STRATEGIE

Om jouw cloud omgeving optimaal te beschermen tegen de risico's van deze tijd, is het niet alleen noodzakelijk om de security aanpak van jouw organisatie af te stemmen op actuele veiligheidsdreigingen, maar ook om de nieuwste, meest moderne beveiligingsmogelijkheden daadwerkelijk in te zetten. Daarnaast moeten de processen voor het goed functioneren van die moderne security goed ingeregeld worden.

IN DE BASIS KENT EEN GEDEGEN CLOUD SECURITY AANPAK DRIE AANDACHTSGEBIEDEN:

1. Bescherming van de cloud omgeving en haar gebruikers,

2. Continue detectie van dreigingen binnen jouw cloud omgeving, en

3. Het snel & adequaat reageren op (potentiële) aanvallen en kwetsbaarheden.

Dit zijn de drie processtappen van moderne cloud security: Protect, Detect & Respond. Deze stappen zullen we in dit hoofdstuk bespreken.

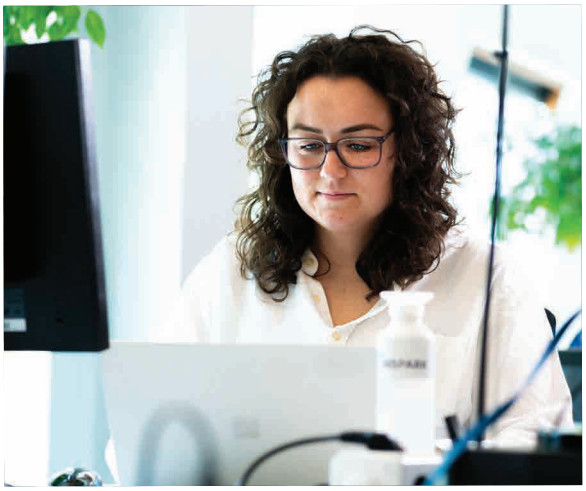
1. PROTECT

Zoals al eerder gezegd, is de traditionele IT beveiligingswijze in cloud-native omgevingen niet langer geschikt. Zodra je applicaties naar de cloud verplaatst en gebruik maakt van cloud diensten, werkt het 'kasteelmodel' niet meer. Cloud diensten als Microsoft 365 zijn door miljoenen gebruikers overal ter wereld te benaderen. De ontelbare kasteelpoorten staan als het ware dag en nacht open.

De grote zwakte van traditionele IT security: als je eenmaal binnen bent, heb je toegang tot alles. Het beveiligingsmodel dat wél werkt in een cloud omgeving, is het zogenaamde 'luchthavenmodel'. Zo heb je een openbare ontvangstruimte met daarbinnen afgeschermde, zwaarbewaakte zones en meerdere lagen van beveiliging (multi-layered security). Overal hangen beveiligingscamera's die met behulp van Artificial Intelligence op de achtergrond verdachte gedragingen detecteren en deze onmiddellijk melden aan de Airport Security (Advanced ThreatProtection).

Dit model geeft invulling aan het "Assume Breach" principe, waarbij de focus niet alleen ligt op het buitenhouden van potentiële indringers, maar waar ook detectie en opvolging van security incidenten centraal staan.

Net als bij de beveiliging van een on-premises infrastructuur draait het bij een cloud gebaseerde infrastructuur om de protectie van je (nu cloud-native) omgeving om te voorkomen dat onbevoegden toegang krijgen tot jouw applicaties en data. Een aantal voorbeelden van specifieke maatregelen bij het beveiligen van cloud omgevingen zijn:



WACHTWOORDBELEID

Wachtwoorden zijn vaak nog steeds dé sleutel tot alles. Dat brengt risico's met zich mee. Een groot deel van de datalekken wordt namelijk veroorzaakt door eenvoudig te kraken wachtwoorden. Sterker nog, als je voor veiligheid van een cloud omgeving volledig moet vertrouwen op een zwak wachtwoord als 'welkom' is het niet de vraag óf je gehackt wordt,maar enkel nog wanneer. En waarschijnlijk is dat dan al gebeurd. Wij adviseren organisaties niet om wachtwoorden regelmatig te wijzigen, maar juist om één uniek wachtwoord te selecteren en dit te combineren met Multi-Factor authenticatie (MFA) en Conditional Access.

CLOUD IDENTITY PROTECTION

Voeg je aan je wachtwoordbeleid ook nog eens de krachtige Cloud Identity Protection toe, dan kun je gebruikers eenvoudig op de hoogte stellen zodra hun wachtwoord voor komt in een groot datalek en bijvoorbeeld te koop wordt aangeboden op het dark web. Op deze wijze kun je automatisch een wachtwoord reset afdwingen, die de gebruiker zelf kan uitvoeren.

MULTI-FACTOR AUTHENTICATIE (MFA) & PASSWORDLESS INLOGGEN

Om ervoor te zorgen dat alleen de juiste personen toegang tot je cloud omgeving krijgen, kun je niet vertrouwen op inloggegevens alleen. Gebruikersnamen en wachtwoorden kunnen, al dan niet bewust, lekken of gedeeld worden met anderen. Dat maakt het gebruik van alleen wachtwoorden een zwakke wijze van beveiliging. Daarom is het belangrijk om naar ándere zaken te kijken: bijvoorbeeld of iemand gebruik maakt van een vertrouwd apparaat dat gemanaged wordt door je organisatie in combinatie met een vertrouwd IP-adres. Daarnaast doe je er verstandig aan om gebruikers zich te laten identificeren via een per sms of authenticator app verzonden toegangscode of via persoonskenmerken zoals een vingerafdruk of gezichtsscan (facial recognition). Met het laatste wordt het passwordless inloggen een feit, iets wat tegenwoordig steeds vaker voorkomt én bijdraagt aan de algehele versnelling van werkprocessen.

BEHEERDERTOEGANG-ON-DEMAND

Admin accounts met uitgebreide rechten op de gehele IT-omgeving brengen een groot risico met zich mee: wanneer deze rechten in de verkeerde handen vallen, is de impact enorm. Met Privileged Identity Management (PIM) wordt dit risico aanzienlijk verkleind, bijvoorbeeld door Just-In-Time (JIT) toegang te verlenen. Daarnaast kan meervoudige verificatie worden afgedwongen of goedkeuring voor slechts een specifiek tijdsbestek worden verleend. Hiermee krijgen gebruikers dus enkel nog toegang tot de applicaties en data die ze op dát moment nodig hebben.

CONTINUE E-MAIL SCANNING

32% van alle inbreuken vindt plaats via phishing. E-mail is de nummer 1 methode om binnen te komen en malware te verspreiden. Zo kan een bijgevoegd Word-document bijvoorbeeld macro's bevatten, die bij het openen automatisch malware downloaden. Of er worden nagenoeg niet van echt te onderscheiden e-mails verstuurd met ogenschijnlijke interessante inhoud zoals links naar bonusplannen, of gepersonaliseerde berichten van een door een echte collega gedeeld document met daarin een valse OneDrive link die je inloggegevens opslaat. Office 365 A TP beschermt je tegen dergelijke aanvallen door bijlages vóórdat ze afgeleverd worden bij je gebruikers, eerst te openen in een afgeschermde omgeving en de effecten van deze bijlages te onderzoeken. Daarnaast worden ook links in e-mails gecheckt. Dit gebeurt op continue basis. Daardoor worden ook links die pas na een aantal dagen "op scherp" gezet worden, afgevangen.

INFRASTRUCTUURTOEGANG-ON-DEMAND

Hoewel organisaties steeds vaker inzetten op PaaS- en SaaS-platformen, zijn (virtuele) servers meestal nog steeds het kloppend hart van veel organisaties. Deze servers worden meer en meer verplaatst naar de cloud, waardoor ze kwetsbaar zijn voor brute-force RDP- aanvallen. Dergelijke aanvallen nemen in duizelingwekkend tempo toe en maken gebruik van kwetsbaarheden in Windows. Door beheerderidentiteiten met MFA te beschermen en just-in-time toegang in te richten voor Virtuele Machines, zorg je ervoor dat de twee meest gebruikte ingangspunten voor hackers in 99% van de gevallen afgedicht zijn en enkel opengezet worden op de momenten dat dat echt nodig is. Verder helpen Azure Policy, Desired State Configuration (DSC) & Azure Security Center Adaptive Application Control om een baseline van je workloads vast te stellen. Op basis van deze baseline kan worden afgedwongen dat wijzigingen eerst goedgekeurd moeten worden via een apart proces.
Zo verhinder je dat wijzigingen, die niet voorzien zijn door je organisatie, automatisch doorgevoerd worden op je omgeving. In het geval van een veiligheidslek kunnen hackers dus geen infrastructurele aanpassingen doen. De kans op (nieuwe) kwetsbaarheden wordt zo aanzienlijk kleiner.

2. DETECT

Hoe goed je de toegang tot je cloud omgeving ook beveiligt, je kunt nooit voorkomen dat hackers toch proberen in te breken. In dat geval is het essentieel dat je aanvallen zo snel mogelijk detecteert. Het komt echter ook vaak voor dat de bedreiging al in je bedrijfsnetwerk aanwezig is, doordat hackers je beveiligingsmaatregelen hebben weten te omzeilen, of doordat bijvoorbeeld (oud)medewerkers of freelancers - bewust of onbewust - een lek hebben gecreëerd. Het is dan ook essentieel niet alleen aanvallen te detecteren, maar ook je eigen IT-omgeving continu te monitoren. De tijd die het gemiddeld duurt voordat een security breach gedetecteerd wordt, bedraagt namelijk bijna 200 dagen.
En hoe langer het duurt om een lek op te sporen, des te groter is de impact. In een gedegen cloud security strategie mag detectie, op basis van het “assume breach” principe, daarom niet ontbreken. Voorbeelden van maatregelen op dit gebied zijn:

BESCHERMING VAN DE IDENTITEIT VAN GEBRUIKERS

Ga er maar vanuit dat ruim de helft van je gebruikers hetzelfde of een soortgelijk wachtwoord op meerdere plekken gebruikt. Wanneer een dergelijk wachtwoord betrokken is bij een datalek, volgt een domino-effect, waarbij de gestolen inloggegevens gebruikt worden om systeem na systeem binnen te dringen. Microsoft Azure AD Identity Protection is een voorbeeld van software waarmee verdachte incidenten met betrekking tot de identiteit van gebruikers worden gedetecteerd, waarna je hierop de juiste actie kunt ondernemen.

MONITORING OP AFWIJKEND GEDRAG

Zorg voor realtime inzicht in afwijkende handelingen van de gebruikers in je cloud omgeving. Denk hierbij bijvoorbeeld aan een medewerker die normaliter in Amsterdam werkt en ineens inlogt vanuit Azië, of een medewerker die midden in de nacht inlogt en de volledige klantendatabase kopieert. Het kan een medewerker zijn die vanaf zijn vakantieadres inlogt of een medewerker die een back-up maakt, maar als dit niet het geval is, wil je hiervan direct op de hoogte zijn.

MALWARE EFFECTEN MONITOREN

Er zijn miljoenen verschillende virussen en malware varianten. Beveiligingsonderzoekers hebben steeds meer moeite om ze allemaal bij te houden en het kat-en-muisspel tussen de aanvallers en de verdedigers wordt steeds complexer. Iedere malware of virus infectie heeft gelukkig wel één ding gemeen: ze voeren allemaal wijzigingen op een omgeving door, waardoor de gebruiker vaak niet meer (productief) kan werken. Detectieproducten als Microsoft Defender ATP draaien op de achtergrond mee en houden de effecten van geopende applicaties, documenten en downloads in de gaten. Mocht bijvoorbeeld een ogenschijnlijk onschuldige applicatie (nog onbekend, want net uitgebracht door een aanvaller, zogenaamde unknown malware) in één keer heel veel bestanden versleutelen, dan heb je te maken met ransomware. Op Machine Learning gebaseerde detectietechnologie zorgt er dan voor dat deze applicatie als een virus gekenmerkt wordt. De aanval mislukt, de applicatie wordt geblokkeerd en de overige werkplekken zijn veilig. Door de kracht van de Intelligent Security Graph gebeurt dit in één keer op wereldwijde schaal. Zo heb je dus ook voordeel van de leringen die getrokken worden uit de eerste infectie (patient zero), ook al vindt die niet plaats binnen je eigen organisatie en zo profiteer je maximaal van de schaalgrootte van de cloud.

3. RESPOND

Zodra een dreiging is gedetecteerd, moet daarop natuurlijk ook meteen actie ondernomen worden. Hiervoor moeten duidelijke afspraken gemaakt worden, opbasis van het privacy en security beleid van je organisatie. Een deel van deze afspraken is van technische aard, maar dit geldt zeker niet voor alle scenario's. Denk bijvoorbeeld aan de wettelijke plicht om een datalek te melden bij de Autoriteit Persoonsgegevens (AP) of het inlichten van de HR-afdeling bij verdachte gedragingen van medewerkers. Snelle opvolging van een gedetecteerde bedreiging, bijvoorbeeld het isoleren van een gebruiker of workload, is essentieel. Daarom moet dit 24/7 geregeld zijn.

EEN AANTAL TIPS OM SNEL IN TE KUNNEN GRIJPEN:

ACTIE OP BASIS VAN DATACLASSIFICATIE

Als een gebruiker/endpoint toch geïnfecteerd of gehackt wordt, is dat natuurlijk heel vervelend. Maar het wordt nog vervelender als er op de werkplek van deze gebruiker documenten met persoonsgegevens aanwezig zijn. Indien je gebruik maakt van de dataclassificatie-mogelijkheden van Microsoft, dan wordt het voor een security analist heel eenvoudig om vast te stellen of deze werkplek zulke gevoelige documenten bevat en zelfs of deze geraadpleegd zijn. Afhankelijk van de resultaten kan het nodig zijn om andere wegen te bewandelen in de afhandeling van dit security incident.

ISOLEREN VAN DE HACK

Voor een security analist wordt het, zodra je gebruik maakt van Microsoft Defender ATP, heel eenvoudig om een aanval te stoppen: de specifieke applicatie, URL of zelfs de hele werkplek kan namelijk meteen geïsoleerd worden. Maak je gebruik van een modern operating systeem (zoals de laatste versie van Windows 10), dan kun je binnen 20 seconden een werkplek isoleren en de gebruiker voorzien van een melding waarom dit gedaan is. Het vrijgeven van de werkplek is net zo eenvoudig. Je kunt er zelfs voor kiezen om communicatie via e-mail wel actief te houden.

VOORBEREIDING IS HET HALVE WERK

Zorg ervoor dat je processen met betrekking tot hoe je moet handelen in het geval van een veiligheidslek, hebt uitgewerkt. Een ISO27001 certificering helpt je hierbij. Dit heeft weinig met technologie te maken, maar de certificering wijst je op functionaliteiten die helpen bij het vaststellen of je een breach wel of niet moet melden bij de Autoriteit Persoonsgegevens. Denk hierbij aan audit logging binnen je Microsoft 365 omgeving. Door deze gratis feature te activeren, kun je simpel herleiden welke data geraadpleegd zijn en door wie. Daarnaast wordt het met Microsoft Cloud App Security heel eenvoudig om snel in te grijpen zodra er een e-mail forwarder wordt ingesteld op een mailbox van een gehackte gebruiker. Zo voorkom je een potentieel continu openstaand datalek.

MISVATTING:

MIJN CLOUD PROVIDER VERZORGT DE BEVEILIGING VAN MIJN CLOUD OMGEVING

Een veelvoorkomende misvatting is dat het afnemen van een Microsoft E5-licentie op zichzelf voldoende is voor een volledige cloud beveiliging. Cloud security is juist een gedeelde verantwoordelijkheid van cloud provider en gebruiker. Hoewel de licentie toegang verschaft tot de security features waarmee je je cloud kunt beveiligen, is de juiste configuratie en het correcte gebruik hiervan jouw eigen verantwoordelijkheid. Vergelijk het met de beveiliging van je huis: goede sloten zijn natuurlijk aanwezig, maar je moet wel zelf de deur op slot doen en je afvragen of je geen alarmsysteem met een koppeling naar een alarmcentrale nodig hebt, zodra er wordt ingebroken via de achterdeur of het raam.

ZELF DOEN OF UITBESTEDEN?

Misschien wel net zo belangrijk als een gedegen strategie voor cloud security op zich, is de vraag of je organisatie er wel klaar voor is om de eigen cloud omgeving te beveiligen.
Ga je een eigen security afdeling optuigen of besteed je dit uit? Bedenk dat je als organisatie altijd zélf verantwoordelijk blijft. De verantwoordelijkheid blind bij een externe partij neerleggen kan dus niet. Als je wilt weten of je zelf in staat bent om je security te organiseren en te waarborgen, vraag je dan het volgende af:

BESCHIKKEN WE OVER DE JUISTE KENNIS?

Heb je de kennis in huis om de beschikbare technologieën op een juiste manier in te zetten en zo je security beleid na te leven? Het gaat hierbij niet alleen om de kennis zelf, maar ook om de capaciteit om dit op dagelijkse basis uit te kunnen voeren. Je hebt security experts nodig die de ontwikkelingen op het gebied van beveiliging nauwkeurig bijhouden, maar die ook alle ontwikkelingen van de cloud omgeving zelf kunnen bijbenen. Deze ontwikkelingen volgen elkaar in een razend tempo op. En niet bijblijven is simpelweg geen optie.

HEBBEN WE DE CAPACITEIT OM ALLE SECURITY MELDINGEN EN AANBEVELINGEN TE VERWERKEN?

Het detecteren van bedreigingen kan grotendeels worden geautomatiseerd. Denk hierbij bijvoorbeeld aan het filteren van false positives, waarbij de ontdekte bedreiging toch vals alarm blijkt. Uiteindelijk blijven er echter altijd reële alerts, bedreigingen en rapportages over, waarvoor handmatige acties noodzakelijk zijn. Je moet over voldoende capaciteit in de vorm van security experts beschikken om deze meldingen te analyseren, te ordenen en te beoordelen op urgentie. Dit kunnen duizenden meldingen per maand zijn. Het kost veel tijd om die te onderzoeken als je niet over de juiste kennis en ervaring beschikt.

KAN ONZE IT-AFDELING ZICHZELF KRITISCH BEOORDELEN?

Vertrouw je erop dat alle medewerkers een (potentieel) datalek ook daadwerkelijk melden? Of bestaat de mogelijkheid dat zij het lek zelf ongemerkt dichten, omdat ze denken hiervan op deze manier geen gevolgen te ondervinden? In dit laatste geval kunnen de consequenties voor je organisatie desastreus zijn. Een separate security afdeling die toeziet op het naleven van je security beleid is dus een goed idee en wordt zelfs steeds vaker verplicht gesteld.

KUNNEN WE 24 UUR PER DAG MONITOREN ÉN REAGEREN BIJ DREIGING?

Het werken in de cloud gaat 24 uur per dag, 7 dagen per week en over de hele wereld door. Ook hackers houden zich niet aan kantooruren of landsgrenzen. Je organisatie moet dus eveneens zo ingericht zijn dat 24/7 monitoring én opvolging van beveiligingsincidenten mogelijk is. Beschik je over de kennis en middelen om zelf een Security Operations Center (SOC) op te zetten en te beheren?

CLOUD SECURITY CENTER

Het Cloud Security Center van InSpark, bekroond met de Microsoft Global Security & Compliance Partner of the Year 2019 Award, garandeert dat jouw cloud omgeving altijd voorzien is van de meest recente en moderne Microsoft security features voor maximale bescherming. Daarnaast monitoren onze security experts jouw cloud omgeving 24 uur per dag, 7 dagen per week op mogelijke incidenten. En we zorgen natuurlijk dag en nacht voor directe opvolging wanneer dat nodig is.

WAAROM CLOUD SECURITY CENTER?

01 Je kiest zelf wat je beveiligt middels vier protection packs voor Microsoft 365 en Azure.

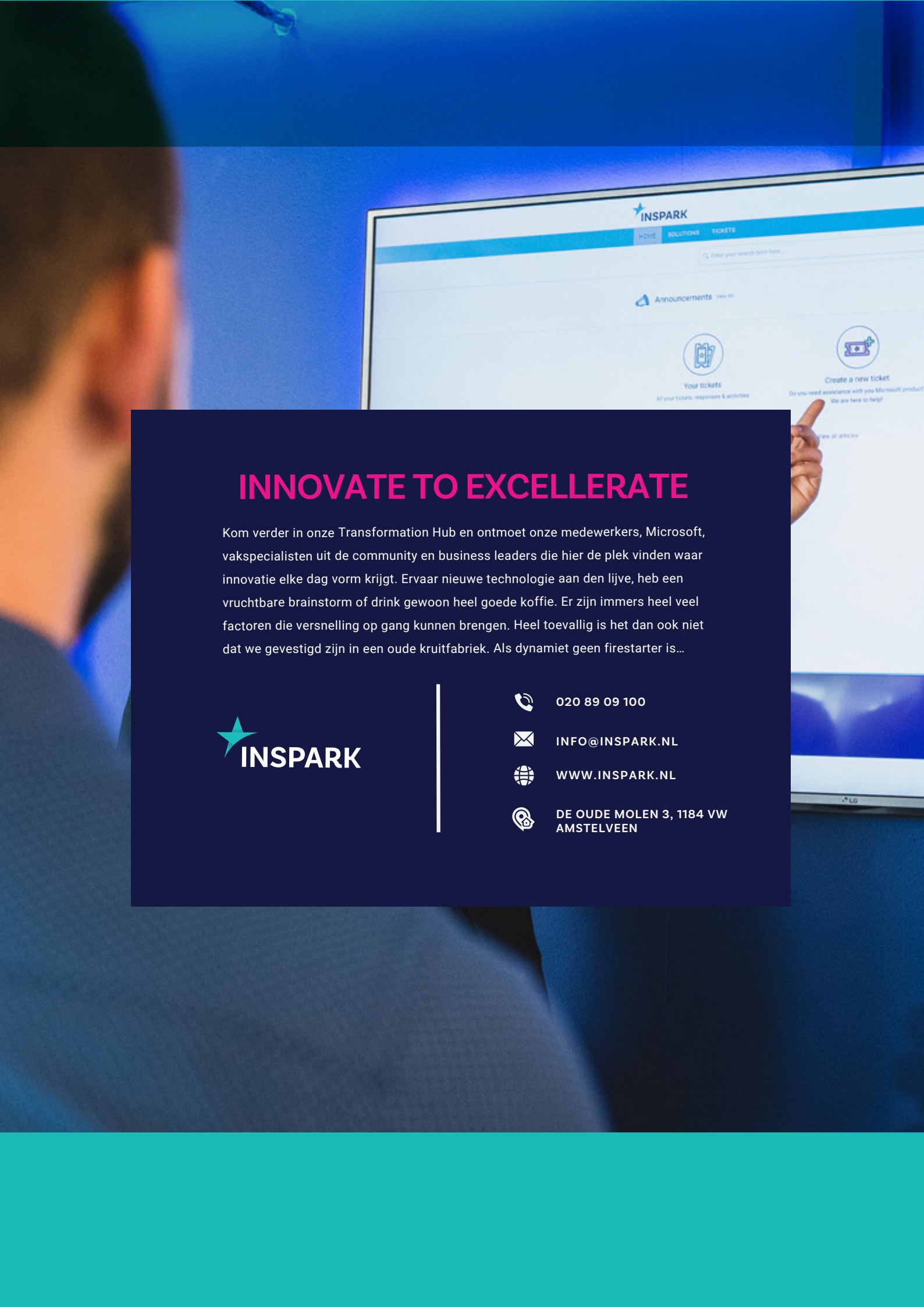
02 Je bent altijd voorzien van de laatste security features. Je profiteert maximaal van AI-driven security diensten van Microsoft.

03 Jouw omgeving wordt 24/7 gemonitord en bedreigingen worden meteen opgevolgd via ons SOC.

04 Je wordt proactief geïnformeerd én beschermd bij grote aanvallen.

05 De beveiliging is afgestemd op jouw security en privacy beleid en geborgd in een Incident Response Plan.

06 Je betaalt een transparant all-in bedrag per gebruiker/workload per maand.



INNOVATE TO EXCELLERATE

Kom verder in onze Transformation Hub en ontmoet onze medewerkers, Microsoft, vakspecialisten uit de community en business leaders die hier de plek vinden waar innovatie elke dag vorm krijgt. Ervaar nieuwe technologie aan den lijve, heb een vruchtbare brainstorm of drink gewoon heel goede koffie. Er zijn immers heel veel factoren die versnelling op gang kunnen brengen. Heel toevallig is het dan ook niet dat we gevestigd zijn in een oude kruitfabriek. Als dynamiet geen firestarter is…

INSPARK

020 89 09 100

INFO@INSPARK.NL

WWW.INSPARK.NL

DE OUDE MOLEN 3, 1184 VW AMSTELVEEN