CONTINUOUS SECURITY

WHITEPAPER

BROAD HORIZON

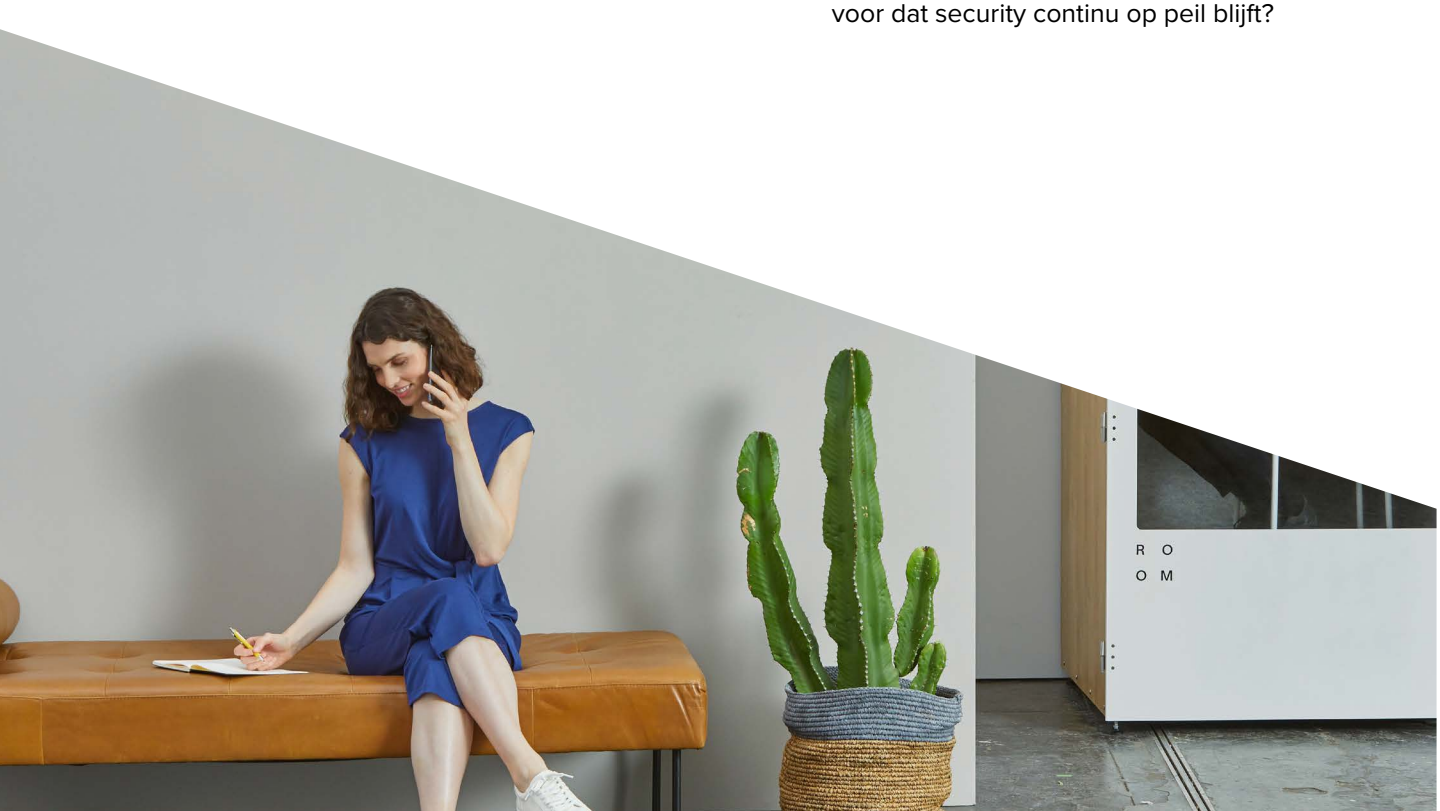
DE DECENTRALE REALITEIT

Cybercriminaliteit is aan de orde van de dag. Kwaadwillenden worden steeds sluwer in hun manieren om data te stelen of bedrijfsprocessen te ondermijnen. De aanvalsvormen worden met de dag geavanceerder en complexer. Soms zijn digitale aanvallen zelfs volledig geautomatiseerd – met speciale scanners struinen hackers het web af op zoek naar open poorten, verouderde systemen of wachtwoorden van medewerkers die gelekt zijn. Andere keren zijn de aanvallen juist heel specifiek gericht op een organisatie. De kwaadwillende(n) weten dan heel specifiek wie ze moeten benaderen, bijvoorbeeld een CEO, om gevoelige informatie buit te maken. Of ze richten zich op onwetende medewerkers en richten daar een ransomware-aanval naartoe.

Het grootste probleem is niet zozeer dat deze aanvallen gebeuren - je kunt cybercriminaliteit namelijk niet voorkomen. Het grootste probleem is dat veel organisaties onvoldoende voorbereid zijn. De organisatie heeft bijvoorbeeld geen of onvoldoende securityprocessen, medewerkers zijn zich niet bewust van de gevaren en systemen kunnen verkeerde configuraties bevatten of outdated zijn. Hierdoor wordt het risico op een aanval voor organisaties groter.Vroeger was het meestal voldoende om een IT-omgeving van de buitenwereld af te schermen, bijvoorbeeld met behulp van firewalls en VPN-verbindingen. IT-omgevingen waren nog op een gecentraliseerde manier te beschermen. Maar die tijden zijn voorbij – het traditionele securitymodel werkt niet meer.

Niet alleen zijn cloudapplicaties 24/7 via het internet te benaderen; ze zijn er ook in grote aantallen binnen de organisatie. Doordat applicaties tegenwoordig overal kunnen staan, is het niet meer mogelijk om security op de traditionele manier aan te pakken: gecentraliseerd, beperkt tot een enkele omgeving.

Security beperkt zich namelijk niet tot een enkele laag van de organisatie. De crux zit hem in de verwevenheid van alle lagen en de kleine details die hierin vaak over het hoofd worden gezien. Door de decentralisatie van het applicatie- en datalandschap wordt het ook complexer om te bepalen bij welke laag je moet beginnen. En zorg je er dan voor dat security continu op peil blijft?



SECURITY MATURITY MODEL

"ONS SECURITY MATURITY MODEL IS GEBASEERD OP HET NIST-FRAMEWORK - EEN MECHANISME VOOR HET TOETSEN VAN JE SECURITYNIVEAU"

NIST-framework
https://www.nist.gov/cyberframework

In deze paper onderzoeken we de nieuwe manier van beveiligen. Een manier waar je security continu onder de loep moet nemen. Waar je inzichten vergaart uit mensen, processen en technologie en deze geregeld langs de meetlat legt. Hoe volwassen zijn wij als organisatie met onze security?

Bij Broad Horizon geloven we dat je security van je organisatie moet toetsen met een Security Maturity Model – een toetsingsmechanisme gebaseerd op het NIST-framework*. Om goed te bepalen waar jouw organisatie zich bevindt, is security vanuit de verschillende lagen van de organisatie te benaderen:

Mens:
Wat is het kennisniveau en het bewustzijn van medewerkers als het gaat om het herkennen van securityrisico's en ernaar acteren?

Processen:
Welke securityprocessen en controlemechanismen heeft de organisatie in kaart gebracht en geïntegreerd?

Technologie:
Welke technologieën en oplossingen gebruikt de organisatie en zijn deze ingericht met beveiliging in het achterhoofd?

Pas als je goed inzicht hebt in de diverse lagen van de organisatie, kun je tot een duidelijke score komen. In deze paper zoomen we met name in op de strategie en oplossingen die organisaties in kunnen zetten om tot een volgend securityniveau te komen. Zo creëer je focus op de onderdelen die het meest belangrijk zijn en kun je security op een efficiënte manier aanpakken. Het is slechts een greep uit de brede aandacht die security binnen organisaties zou moeten verdienen, maar desondanks een goed startpunt.

Tot slot sluiten we de paper af met de dienst die we hiervoor aan kunnen bieden: Continuous Security en de werkwijze die wij hanteren om organisatie te helpen naar een volgend securitylevel.

STRATEGIE

Er zijn veel verschillende strategieën om security aan te pakken. In de basis gaat het om drie zaken: beveiligen, signaleren en ingrijpen.

1. BEVEILIGEN

Een traditionele securitystrategie werkt niet meer, omdat veel organisaties gebruikmaken van cloudapplicaties die 24/7 beschikbaar zijn. Die applicaties kun je niet op de traditionele, centrale manier beschermen. Het beveiligingsmodel dat wél werkt in een cloud-omgeving, is een zogenaamde gelaagde omgeving, ook wel gelaagde security of multi-layered security genoemd. Bij een gelaagde securitystrategie houd je in alle facetten van een omgeving in de gaten. Je beveiligt op het vlak van identiteit (wie heeft toegangsrechten tot welke cloudapplicaties?), apparaten, applicaties en data.

2. SIGNALEREN

Hoe goed je de toegang tot je cloudomgeving ook beveiligt, je kunt nooit voorkomen dat hackers toch proberen in te breken. Maar als het gebeurt, dan wil je die aanvallen snel detecteren.

Het komt echter ook voor dat de bedreiging al in je bedrijfsnetwerk aanwezig is. Bijvoorbeeld omdat hackers beveiligingsmaatregelen omzeilen, of omdat er sprake is van een lek. Daarom wil je naast het detecteren van aanvallen ook de omgeving continu monitoren. Hoe langer het duurt om een lek op te sporen, des te groter is de impact. Het uitgangspunt is: ga ervan uit dat je gehackt wordt en anticipeer daarop.

2. INGRIJPEN

Zodra je een dreiging detecteert moet je actie ondernemen. Binnen de organisatie moet je hier duidelijke afspraken over maken die passen bij het privacy- en securitybeleid. Een deel van deze afspraken is van technische aard, maar dit geldt zeker niet voor alle scenario's. Denk 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. Het snel opvolgen van een gedetecteerde bedreiging, bijvoorbeeld het isoleren van een gebruiker, is essentieel in dit geval. Daarom moet dit zowel technisch- als qua compliance geregeld zijn. Security stopt namelijk niet als iedereen naar huis gaat, maar kan 24/7 plaatsvinden.

OPLOSSINGEN

Om een strategie te handhaven zijn er veel verschillende oplossingen. De oplossingen zijn te plaatsen in drie kaders: users & devices, application & data en infrastructure & connectivity.

1. USERS & DEVICES

Het zijn vaak medewerkers die zich onvoldoende bewust zijn van de mogelijke securityrisico's op de werkvloer. Door onwetendheid klikken zij op phishingmails, worden zij slachtoffer van social engineering of gebruiken zij zwakke wachtwoorden. Of zij gebruiken apparaten die onvoldoende beveiligd zijn, bijvoorbeeld als een laptop een verouderd besturingssysteem draait, geen virusscanner heeft of een smartphone die jailbroken is. In dit hoofdstuk een aantal oplossingen die om de risico's van de mens tot een minimum beperken.

1.1 Beveiligen

Beheerderstoegang-on-demand

De beheerdersaccount van een applicatie of omgeving is het meest interessante account voor hacker. Wanneer deze namelijk in verkeerde handen valt, is de impact enorm. Met Privileged Identity Management (PIM), een service binnen Microsoft Azure, valt hier iets tegen te doen. Deze service kan bijvoorbeeld door Just-In-Time (JIT) toegang verlenen en Multi-Factor Authentication afdwingen. Dat betekent dat een beheerder alleen toegang krijgt voor een specifiek tijdsbestek en altijd meerdere apparaten nodig heeft om in te loggen. Hiermee krijgen beheerders dus enkel nog toegang tot de applicaties en data die ze op dát moment nodig hebben.

Strikt wachtwoordbeleid

Wachtwoorden zijn vaak nog steeds dé sleutel voor toegang, maar daardoor ook risicovol. Een groot deel van datalekken is namelijk te danken aan zwakke wachtwoorden die eenvoudig te kraken zijn. Het komt nog geregeld voor dat cloudomgevingen 'beschermd' zijn met zwakke wachtwoorden zoals 'welkom' of 'Amsterdam', maar dan is het eigenlijk wachten tot je gehackt wordt. Misschien is het zelfs al gebeurt. Daarom adviseren wij om een goed wachtwoordbeleid te hanteren. Dat doe je niet door regelmatig verplicht wachtwoorden te laten wijzigen, maar door een combinatie van Multi-Factor Authenticatie (MFA) en Conditional

"COMBINEER EEN WACHTWOORDBELEID MET MFA"

Access. Met MFA hebben medewerkers altijd een tweede apparaat nodig (bijvoorbeeld een smartphone) om in te loggen. Het voordeel hiervan is dat medewerkers prima één wachtwoord kunnen hanteren, een soort meesterwachtwoord. Al moet die natuurlijk wel sterk zijn en moeilijk te kraken.

Cloud Identity Protection

Een hele krachtige om toe te voegen aan je wachtwoordbeleid is Cloud Identity Protection – een tool die gebruikers eenvoudig op de hoogte stelt als hun wachtwoord voorkomt in een groot datalek of te koop staat op het dark

web. Het is niet moeilijk voor een kwaadwillende om toegang te krijgen tot deze lijsten met wachtwoorden. Vaak kiezen gebruikers bovendien dezelfde wachtwoorden voor diverse diensten, maar net een klein beetje veranderd. Cloud Identity Protection maakt het mogelijk een wachtwoord reset af te dwingen. Een gebruiker kan dit zelf doen via een self-serviceportaal.

Passwordless inloggen

Over het algemeen kun je niet vertrouwen op alleen de inloggegevens van een gebruiker om toegang te krijgen. Die inloggegevens kunnen namelijk ook in handen zijn van een hacker of (al dan niet onbewust) gedeeld zijn met anderen. Hoe weet je dan zeker dat de persoon die inlogt echt diegene is? Dat maakt wachtwoorden een zwakke schakel in de beveiliging van systemen.

Daarom is het belangrijk om naar andere zaken te kijken: gebruikt iemand een vertrouwd apparaat die via Microsoft Intune wordt gemanaged, in combinatie met het vertrouwde IP-adres van bijvoorbeeld een kantoorlocatie?

Een extra validatiecheck is ook om gebruikers te laten valideren via SMS of een authenticatorapp.

“JE KUNT BETER NIET VERTROUWEN OP ALLEEN DE INLOGGEGEVENS.”

Die apps bevatten tegenwoordig steeds meer opties om ook in te loggen met vingerafdruk of gezichtsscan (facial recognition) – opties waarmee passwordless inloggen een feit wordt.

1.2 Signaleren

Identiteitsbescherming

Je kunt ervan uitgaan dat je medewerkers vaak dezelfde wachtwoorden gebruiken op meerdere plekken. Wanneer dit wachtwoord betrokken is bij een datalek volgt vaak een domino-effect: de gestolen inloggegevens worden gebruikt om systeem na systeem binnen te dringen.

Met Microsoft Azure Active Directory Identity Protection kun je dit soort verdachte activiteiten tijdig traceren. De identiteit van de gebruiker wordt bekend, waardoor je snel een juiste actie kunt ondernemen. Bijvoorbeeld de gebruiker isoleren van de systemen waar deze toegang voor heeft.

Malware monitoring

Er zijn miljoenen virussen en malwarevarianten. Het is voor beveiligingsonderzoeker lastiger om ze allemaal bij te houden omdat het kat-en-muisspel tussen aanvaller en verdediger steeds complexer wordt.

Gelukkig hebben infecties één ding gemeen: ze maken in de basis gebruik van dezelfde aanpassingen om een stukje malware te maken. Een detectiedienst zoals Microsoft Defender ATP draait op de achtergrond mee en houdt de effecten op applicaties, documenten en downloads in de gaten.

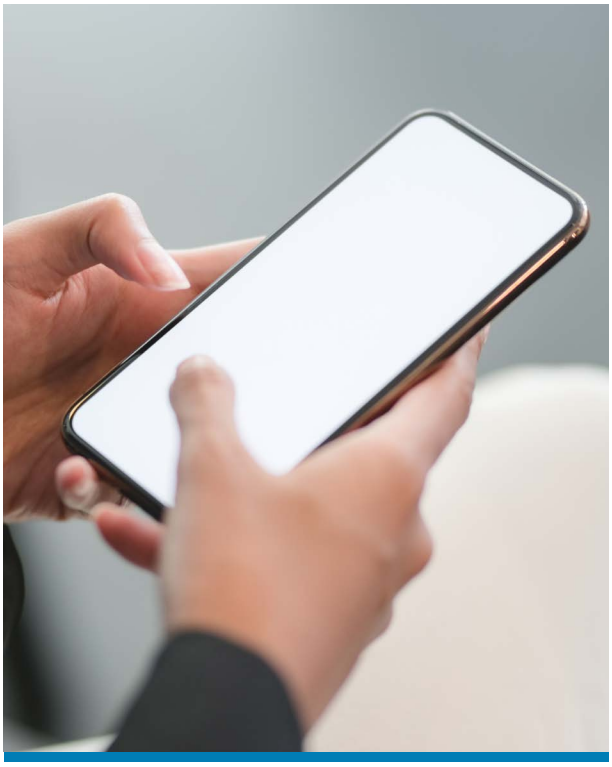
De dienst houdt in de gaten of onschuldig uitziende applicaties (aangepast door een aanvaller) verdachte acties uitvoeren. Denk aan in één keer heel veel bestanden versleutelen – wat duidt op ransomware. Machine learning (AI) detectietechnologie in de dienst merkt het virus op, waarna ATP in werking treedt en ervoor zorgt dat de aanval vroegtijdig mislukt.

1.3 Ingrijpen

Isoleren van een hack

Microsoft Defender ATP is ook zeer geschikt om aanvallen te stoppen. Een specifieke applicatie, URL of zelfs een complete digitale werkplek kun je met ATP isoleren. Maak je gebruik 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.

“MAAK JE GEBRUIK VAN WINDOWS 10, DAN KUN JE BINNEN 20 SECONDEN EEN WERKPLEK ISOLEREN EN DE GEBRUIK VOORZIEN VAN EEN MELDING.



3. APPS & DATA

Het aantal (cloud)applicaties binnen organisaties groeit enorm. Niet alleen de zakelijke applicaties die goedgekeurd zijn door de IT-afdeling, maar ook het applicaties dat een medewerker privé op de werkvloer gebruikt of zakelijke applicaties buiten het zicht van de IT-afdeling. Door het aantal applicaties groeit ook de hoeveelheid data binnen de organisatie – en dat is voor kwaadwillenden interessant. Waar in traditionele IT-omgevingen data vaak op een centrale plek werd opgeslagen, is dat binnen moderne omgevingen vaak gecentraliseerd, waardoor je al snel het overzicht verliest.

2.1 Beveiligen

Continue e-mailscanning

E-mail blijft een effectieve methode om malware te verspreiden. Een bijgevoegd Word-document kan bijvoorbeeld macro's bevatten, die bij het openen van het bestand automatisch malware downloaden en installeren. Maar denk ook aan niet van echt onderscheiden e-mails, die ogenschijnlijke interessante inhoud zoals links naar bonusplannen bevatten of andere gepersonaliseerde berichten waarin linkjes staan. Met Office 365 ATP word je beschermd tegen dergelijker aanvallen. Deze applicaties opent bijlagen namelijk eerst in een afgeschermde omgeving: een zogenoemde sandbox. Daarnaast checkt Office 365 ATP ook de links op continue basis in e-mail. De software checkt of het een valide link is en geeft meldingen als dat niet het geval is.

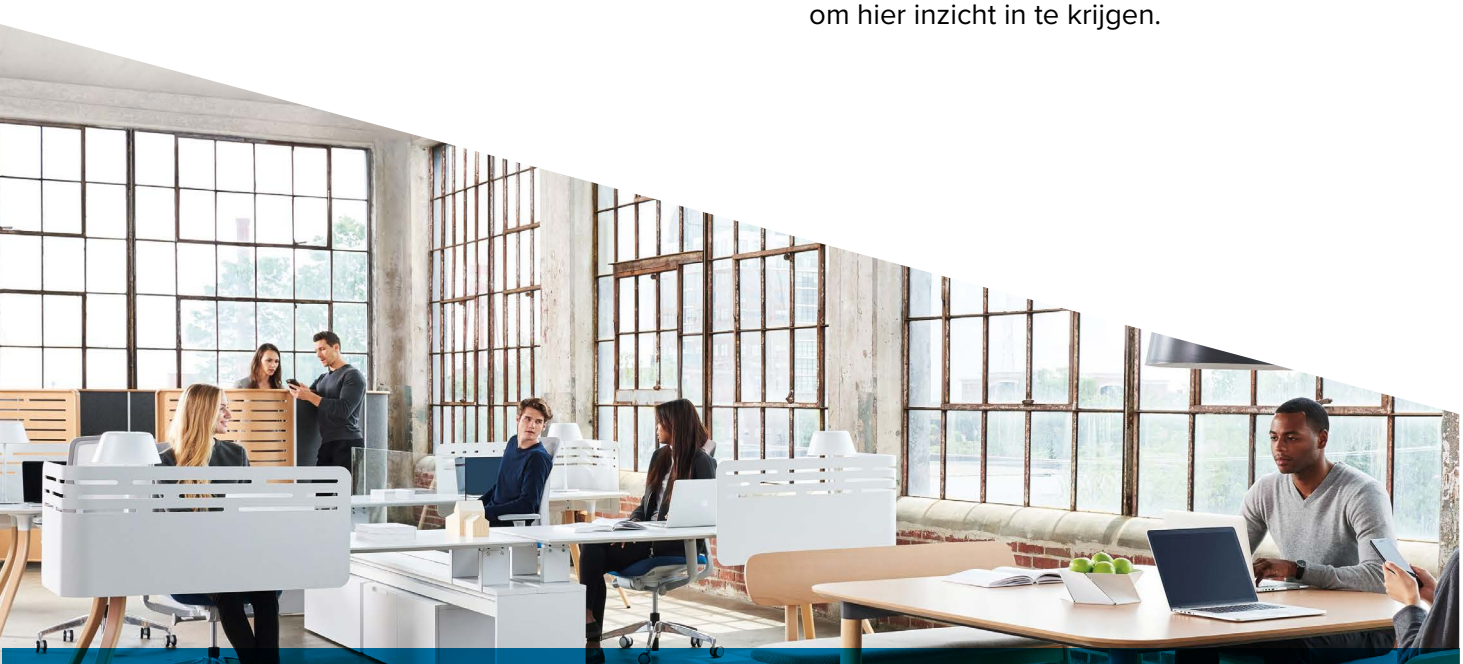
2.2 Ingrijpen

Actie op basis van dataclassificatie

Het is vervelend als een gebruiker of een apparaat van de gebruiker gehackt wordt. Maar het is nog vervelender als de werkplek van deze gebruiker belangrijke documenten of persoonsgegevens bevat en een hacker daar toegang tot krijgt. Met de dataclassificatie-mogelijkheden van Microsoft, wordt het voor een securityanalist heel eenvoudig om vast te stellen of deze werkplek zulke belangrijke gegevens bevat en of ze geraadpleegd zijn. De securityanalist kan bijvoorbeeld de toegang tot data beperken, denk aan het niet kopiëren of slepen van bestanden. Als dat wel gebeurt, zijn er alerts in te stellen. Afhankelijk van de resultaten kan het nodig zijn om andere wegen te bewandelen in de afhandeling van dit security incident.

Voorbereiding is het halve werk

Een van de belangrijkste zaken om op orde te krijgen zijn dat je processen uitwerkt over hoe je moet handelen in het geval van een securitylek. Een certificering, zoals de ISO 27001 certificering die toetst op de omgang van informatiebeveiligingsprocessen in een organisatie, helpt hierbij. Zo'n certificering heeft in eerste instantie weinig met technologie te maken, maar de certificering wijst je wel op de stappen en maatregelen die je moet ondernemen bij een datalek – en in welke mate het nodig is om deze te melden bij de Autoriteit Persoonsgegevens. De meeste IT-serviceproviders hebben een compliance-afdeling die kan helpen om hier inzicht in te krijgen.



3. INFRA & CONNECTIVITY

Iedere applicatie in ‘de cloud’ krijgt uiteindelijk een plek op een server in een datacenter. Maar of dat nou een datacenter is van Microsoft, Google of Amazon of van een lokale hostingprovider– je hebt altijd te maken met iemand’s computer waar je verbinding meemaakt. Als deze verbindingen niet beveiligd zijn dan kunnen ze gekaapt worden. In dit hoofdstuk een aantal oplossingen die een aanvullende beschermingslaag om infrastructuurniveau brengen zonder dat ze het dagdagelijkse gebruik van het internet van een medewerker niet hinderen.

3.1 Beveiligen

Infra-on-demand

Binnen veel organisaties zijn (virtuele) servers nog altijd het kloppend hart, ondanks de vele PaaS- en SaaS-diensten die organisaties afnemen. Wanneer deze virtuele servers naar de cloud migreren, zijn ze kwetsbaar voor geavanceerde aanvallen. Dat komt omdat zulke aanvallen gebruikmaken van kwetsbaarheden in het besturingssysteem van deze servers, die vaak op Windows is gebaseerd. Het is daarom aan te raden om beheerdersaccounts met MFA en Just-In-Time toegang in te regelen op het niveau van virtuele servers/virtuele machines. Hiermee zorg je ervoor dat de twee meest gebruikte toegangspoorten voor het grootste gedeelte gedicht zijn. Ze gaan alleen open op het moment dat toegang nodig is, en alleen met uitgebreide authenticatie.

Permissie voor wijzigingen

Diensten als Azure Policy, DSC en Security Center helpen om een baseline van de workloads vast te stellen. Binnen deze baseline kun je afdwingen dat wijzigingen eerst goedgekeurd worden via een proces. Het is een belangrijke manier om te voorkomen dat je omgeving gehinderd wordt door wijzigingen die niet voorzien zijn. Het maakt het voor hackers een stuk lastiger om op basis van een veiligheidslek infrastructurele aanpassingen te doen, waardoor de kans op (nieuwe) kwetsbaarheden aanzienlijk kleiner wordt.

“JE KUNT BETER NIET VERTROUWEN OP ALLEEN DE INLOGGEGEVENS”

3.2 Signaleren

Monitoring op afwijkend gedrag

Het is belangrijk om inzicht te krijgen in afwijkend gedrag van medewerkers. Stel dat je medewerker normaal gesproken inlogt vanuit Amsterdam, maar plots vanuit Azië inlogt, dan is het noodzakelijk om dit te onderzoeken. Het kan een medewerker zijn die vanaf zijn/haar vakantieadres inlogt of een medewerker die een back-up maakt, maar als dit niet het geval is, wil je hiervan direct op de hoogte worden gebracht en actie kunnen ondernemen. Met diverse monitoringtools binnen de Microsoft 365 stack is dit te realiseren zoals de Security Operating Center op basis van Sentinel. Hiermee zijn vooraf de belangrijkste parameters in te stellen waarmee je afwijkend gedrag kunt monitoren.

Broad Horizon - Being Ahead

Als organisatie wil je vooroplopen, vernieuwen en continu kunnen verbeteren. Doordat de wereld om ons heen constant verandert, moet jouw organisatie wendbaarder zijn dan ooit. Broad Horizon helpt hierbij door op basis van slimme data-inzichten, uitgebreide industriekennis en een volledig dienstenportfolio, bestaande en toekomstige vraagstukken van organisaties op te lossen. Wij zorgen ervoor dat onze klanten altijd een stap vooroplopen.
https://www.broadhorizon.nl

“ ENVIRONMENTS CAN CHANGE AT ANY MOMENT. BUT IF YOU ANTICIPATE, THESE CHANGES WILL OPEN UP UNEXPECTED POSSIBILITIES”

Dave Canterbury
Pathfinder

Keienbergweg 100, 1101 GH Amsterdam – +31 88 008 3500

BROAD HORIZON