BLUE IDENTITY

BUSINESS WHITE PAPER

LESSONS LEARNED

EEN BEWEZEN METHODE OM CLOUD WORKLOADS TE BEVEILIGEN

Lessons learned na het beveiligen van een toonaangevend bedrijf.

www.blueidentity.nl

Over Ons

Blue Identity behoort tot de nieuwe generatie Microsoft Partners,
Als het gaat om IT automatisering lopen wij voorop in inzicht en transparantie voor onze klanten.

Wie zijn wij

Wij zijn Blue Identity, een Nederlandse organisatie welke zich richt op het optimaliseren van Security en Productiviteit binnen de Microsoft Cloud. Wij zijn opgericht in mei 2022 en hebben de ambitie om dé Microsoft adviseur te worden wanneer het gaat om een veilige en werkbare werkomgeving.

Wat doen wij

Ons business model bestaat uit het optimaliseren van de security laag van onze klanten. Wij kijken de omgeving van onze relaties na en meten deze tegen de huidige standaarden in de markt. Wij houden niet van maatwerk maar wel van eenvoud. Een omgeving moet zowel veilig als werkbaar zijn. Hiervoor smelten wij security en productiviteit samen.

Onze Missie

Blue Identity heeft als missie bedrijven te helpen het maximale uit hun Microsoft 365 omgeving te halen. Door het inzetten van van specifieke functionaliteiten geloven wij dat er meerwaarde uit de business gehaald kan worden. Dit doen wij door de ultieme balans te vinden tussen veiligheid en productiviteit

Onze Visie

Blue Identity ondersteunt haar klanten waar nodig op het gebied van de Microsoft Cloud. Zo zorgen we ervoor dat de medewerkers van onze klanten een prettige en veilige werkomgeving hebben. Wij garanderen dat deze altijd up-2-date, veilige en beschikbaar is.

Onze uitgangspunten

Eenvoud

Wij zorgen voor goede communicatie, begeleiding en adoptie binnen jullie organisatie. Met onze aanpak gaan wij voor het hoogst haalbare binnen de Microsoft cloud voor jullie onderneming.

Maatwerk met standaard

Wij gaan voor eenvoud en voorspelbaarheid. Wij hergebruiken opgedane kennis en vaardigheden. Zo kunnen wij effectiever aan de slag gaan en streven naar een 90/10 aanpak.

Samenwerken

Samen werken wij aan jullie toekomst binnen de Microsoft cloud en zijn wij jullie trusted adviser. Onze data staat op een plek.

Onze waarde

- Wij garanderen dat de omgeving van onze klanten veilig is
- Wij garanderen dat de omgeving van onze klanten up-2-date is
- Wij zorgen er met ons businessmodel voor dat jullie ontzorgt worden door de inbreng van onze expertise
- Met onze zorgeloze en veilige omgeving bieden wij waarde voor onze klanten

De feiten

Wij hebben meer dan
20
AFGENOMEN APK'S

Wij hebben meer dan
1500
ACTIEPUNTEN GEVONDEN

Wij hebben meer dan
200
CONTROLEPUNTEN

Security problemen met Cloud Infrastructuur

De reden achter de diverse aanvallen en hacks in de cloud zijn toe te wijzen aan een specifiek aantal categorien: Human error, runtime threats, Shadow IT en het gebrek van een juiste cloud security strategie

Human Errors

Vanwege de aard van cloudomgevingen worden de meeste inbreuken in de cloud veroorzaakt door menselijke fouten. In de cloud kan het ontbreken van een goed fundamenteel security element dit soort fouten erg kostbaar maken.
Deze fouten kunnen bijvoorbeeld zijn het niet of verkeerd configureren van Multi factor Authenticatie (MFA), of het openzetten van specifieke poorten op werkstations. Ook is het herkennen van phishing mails iets wat nog steeds niet goed gaat. Dit soort fouten transformeren cloud workloads in een voor de hand liggend doelwit welke op een eenvoudige manier te manipuleren zijn door kwaadwillenden.

Shadow IT

Shadow IT zijn applicaties die gebruikt worden op zakelijke devices zonder medeweten van de IT-afdeling. Dit is vaak een ander groot probleem in een cloud omgeving en zorgt vaak voor diverse uitdagingen. Dit soort applicaties zijn vaak een dreiging omdat de applicaties niet goed beveiligd zijn. Ook zien wij dat er regelmatig wachtwoorden en configuraties in worden opgeslagen waardoor deze vrij eenvoudig te compromitteren zijn. Ook zien we steeds vaker dat Shadow IT een groter probleem wordt naarmate bedrijven overstappen op Dev/Ops werken in zelf sturende teams. Hierdoor kan een team vaak zelf bepalen waarmee ze werken, hoe ze werken, wanneer ze werken en waar ze werken. IT security staat vaak voor een uitdaging om hier grip op te krijgen.

Runtime Threats

In de public cloud zoals Microsoft 365 is een deel van de onderliggende infrastructuur al beveiligd door de Cloud service provider (in het geval van Microsoft 365 is dat Microsoft). Echter is alles wat besturingsysteem applicatie en gevens betreft de verantwoordelijkheid van de gebruiker of de afnemer. Dit kan ervoor zorgen dat bijvoorbeeld bij onbewuste acties de omgeving niet volledig en goed beschermd is. Dit kan ervoor zorgen dat kwaadwillenden het besturingsysteem en de applicaties kunnen aanvallen om toegang te krijgen. Aanvallers gebruiken zero-day exploits om voet aan de grond te krijgen waarna ze vervolgens malefiede software kunnen installeren wat kan leiden tot een ransomware aanval en een versleuteling van alle data en bestanden. De cloud biedt meer dan alleen rekenkracht. Het is ook een opslagfaciliteit geworden voor intellectueel eigendom en vertrouwelijke documenten, waardoor cloud-workloads een steeds aantrekkelijker doelwit worden voor aanvallers. Dit is een trend die het CrowdStrike Services-team heeft waargenomen bij talloze inbreuken die het dit jaar heeft onderzocht en die hun oorsprong vonden in cloud-workloads, waar veel kwaadwillenden zich specifiek op lijken te richten.

Gebrek aan een cloud security strategie

Terwijl steeds meer workloads naar de cloud worden verplaatst. Blijven beheerders dit soort workloads beveiligen op dezelfde manier als dat ze servers in een privé- of on-premises datacenter beheerden. Helaas zijn traditionele datacenter-beveiligingsmodellen niet geschikt voor de cloud.
Wij zien steeds vaker de onderstaande gewoonten:

- Het gebruik van statische wachtwoorden voor authenticatie en autorisatie, in plaats van MFA (multifactor authenticatie) en IAM (identiteits- en toegangsbeheer).
- Organisaties houden legacy IT in stand in plaats van tijdelijke workloads en te vertrouwen op DevOps om de verantwoordelijkheid voor de beveiliging op zich te nemen,
- Er wordt vertrouwd op standaard configuraties welke generiek beschikbaar zijn gesteld maar niet specifiek voor de betreffende omgeving zijn gemaakt.
- Wanneer er wel een correcte inrichting is gedaan worden er toch uitzonderingen gemaakt zonder dit security risico te accepteren of te beoordelen

Zelfs als klanten cloud beveiliging producten bezitten, slagen ze er vaak niet in om hun cloudworkloads te beveiligen. Alle grote bedrijven die vorig jaar een inbreuk hebben meegemaakt, hadden zelfs een cloud beveiligings oplossing.
Deze vraagstukken laten zien dat een goede cloudstrategie ook adoptie moet omvatten om draagvlak binnen de organisatie te krijgen. Het opleiden van teams, zoals het opslaan van geheimen, het roteren van sleutels en het toepassen van goede IT life cycle management tijdens softwareontwikkeling is essentieel, maar ontbreekt vaak.

Wij verminderen het risico:

Blue Identity richt zich op het minimaliseren van het risico. Wij zorgen ervoor dat de omgeving preventief goed is geconfigureerd

Verminder het risico op exposure

TOEPASSEN VAN SEGMENTATIE

32%

Door het toepassen van Netwerk, applicatie en toegang segementatie wordt het risico met 32% verminderd

TOEPASSEN VAN ENCRYPTIE

71%

Door het gebruik van encryptie op data en devices wordt het risico op malware en ransomeware met 71% verminderd

INRICHTEN VAN PROCESSEN

27%

Door het toepassen van shift left of het opzetten van de juiste processen wordt de foutmarge op een risico verminderd met 27%

MULTI FACTOR AUTHENTICATIE

79%

Door het inschakkelen van MFA wordt het risico op een hack met 79% verminderd

PRO ACTIEF MONITOREN

82%

Bij het toepassen van de juiste montioring is het mogelijk om tot 82% van de cyberrisico's op tijd te ontdekken en te mitigeren.

BLUE IDENTITY

Microsoft 365 APK

De Microsoft 365 APK is een security audit voor het Microsoft 365 platform. In deze audit kijken wij naar workloads en features welke jullie gecontroleerd willen hebben. Wij gebruiken onze eigen APK richtlijnen welke opgesteld zijn door onze specialisten uit het veld. Wij gebruiken dan ook een combinatie van veld expertise, markt expertise, Microsoft Best Practices en specifieke onderwerpen welke in Cybersecurity verzekeringen aangestipt worden

Onze 12 punten controle

- Algemene Microsoft 365 settings
- Administratieve rollen en rechten
- Fundamentele Security settings
- Fundamentele Compliance settings
- Logging en Analytics
- Authenticatie methoden
- Conditional Access
- Licentie toekenning
- Externe delen en toegang
- Aangesloten applicaties
- Fundamentele governance settings
- Microsoft 365 Teams Governance

"Blue Identity kijkt naar de waarde van security voor de onderneming. Het gaat niet alleen om een strikte beveiliging!"

ERWIN DERKSEN

Microsoft 365 APK

Intake

Nadat je contact met ons hebt opgenomen gaan we de afspraak en verwachting scherp stellen en bepalen we de scope in een gezamenlijke meeting

Contract

Wanneer de scope duidelijk is stellen we een NDA op en brengen wij een offerte uit van de kosten.

Uitvoeren APK

Wanneer de opdracht is verstrekt en toegang is geregeld gaan we aan de slag met de 0-meting

Rapportage en inzicht

Na de 0-meting wordt een rapport opgeleverd waarbij inzicht wordt gegeven in de status van jullie omgeving

Actiepunten en prioriteiten

De in het rapport vermelde actiepunten worden gezamenlijk in een meeting geprioriteerd.

Support

Wanneer gewenst levert Blue Identity support bij het mitigeren van de actiepunten. Samen stellen we een roadmap op en controleren wij jullie omgeving elk kwartaal.

BLUE IDENTITY

Microsoft 365 APK

Ben je nieuwsgierig geworden naar onze APK. Maar zie je het nog niet zitten om gebruik te maken van onze diensten. Dan zijn de volgende pagina's zeker voor jou geschikt. In deze pagina's plaatsen wij een aantal controles welke ook in onze APK zijn opgenomen.

Let op! Wij zijn niet verantwoordlijk voor het verkeerd uitvoeren van scripts, code of uitvoeren van changes tijden welke de productie verstoren!

Overzicht gratis controle punten

- Is Multi factor authenticatie op de juiste manier ingeschakeld?
- Is Modern authenticatie ingeschakeld?
- Is Legacy authenticatie geblokkeerd?

BLUE IDENTITY

Is Multifactor authenticatie op de juiste manieren ingeschakeld?

Er zijn verschillende manier om MFA toe te passen binnen een Microsoft 365 omgeving. Waarbij vroeger MFA afgedwongen werd per user gebruikt men tegenwoordig conditional access. Door gebruik te maken van conditional access wordt MFA nog steeds toegepast op de gebruiker maar de user verplicht om aan voorwaarden te voldoen voordat de gebruiker toegang krijgt tot de data waar deze naartoe moet.

De controle

In deze controle kijken we of MFA is uitgeschakeld in het oude MFA portaal van Azure en of deze wordt afgedwongen middels conditional access

1. Ga naar het legacy Multifactor portaal
2. Controleer of de Multi factor auth status op disabled staat.
3. Staat niet alles op disabled pas de status van deze accounts dan aan naar disabled
4. Ga naar Portal.azure.com -> Security -> Conditional Access
5. Controleer of er een policy tussen staat die MFA toepast op alle user accounts in de tenant.
6. Staat er geen regel tussen die dit toepast klik dan op "new policy from template"
7. Selecteer de template categorie "identities"
8. Selecteer de template "Require Multifactor Authentication for all users"
9. Geef de policy een naam
10. Pas de Policy state aan naar On en klik op Next
11. Klik vervolgens op Create policy om de policy aan te maken en toe te passen.

BLUE IDENTITY

Is Modern authenticatie ingeschakkeld?

Door het blokkeren van Legacy authenticatie en protocollen voorkom je dat cyber criminelen gebruik kunnen maken van zwakten in jouw omgeving. Een aantal voorbeelden van Legacy authenticatie zijn; basic authenticatie (simpel username en password), ActiveSync, Secure Pop3, Secure IMAP, Remote Powershell. Voordat je verder gaat met het blokkeren van legacy authenticatie is het van belang dat je eerst een controle doet of dit nog ergens in de systemen gebruikt wordt.

Let op! Wij zijn niet verantwoordlijk voor het verkeerd uitvoeren van scripts, code of uitvoeren van changes tijden welke de productie verstoren!

In deze controle kijken we wat de huidige configuratie is met betrekking tot legacy authenticatie. Voorheen kon deze aanpassing enkel via Powershell, tegenwoordig kan dit ook via de Microsoft 365 Admin Portal.

1. Ga naar het Microsoft 365 admin center
2. Klik op settings
3. Ga naar Org settings
4. Klik op Modern Authentication
5. Staat het vinkje "enable moden authentication" aan of uit?
6. Staat het vinkje uit? Controleer dan eerst goed of de genoemde protocollen nog gebruikt worden voordat je dit aan zet.

BLUE IDENTITY

Is legacy authenticatie geblokkeerd?

Door het blokkeren van Legacy authenticatie en protocollen voorkom je dat cyber criminelen gebruik kunnen maken van zwakten in jouw omgeving. Een aantal voorbeelden van Legacy authenticatie zijn; basic authenticatie (simpel username en password), ActiveSync, Secure Pop3, Secure IMAP, Remote Powershell. Voordat je verder gaat met het blokkeren van legacy authenticatie is het van belang dat je eerst een controle doet of dit nog ergens in de systemen gebruikt wordt.

Let op! Wij zijn niet verantwoordlijk voor het verkeerd uitvoeren van scripts, code of uitvoeren van changes tijden welke de productie verstoren!

De controle

In deze controle kijken we wat de huidige configuratie is met betrekking tot legacy authenticatie. Voorheen kon deze aanpassing enkel via Powershell, tegenwoordig kan dit ook via de Microsoft 365 Admin Portal.

1. Ga naar het Microsoft 365 admin center
2. Klik op settings
3. Ga naar Org settings
4. Klik op Modern Authentication
5. Staat het vinkje "enable moden authentication" aan of uit?
6. Staat het vinkje uit? Controleer dan eerst goed of de genoemde protocollen nog gebruikt worden voordat je dit aan zet.
7. Ga naar Portal.azure.com -> Security -> Conditional Access
8. Controleer of er een policy tussen staat die legacy authenticatie blokkeerd.
9. Selecteer de template categorie "identities"
10. Selecteer de template "Block legacy authentication"
11. Geef de policy een naam
12. Pas de Policy state aan naar On en klik op Next
13. Klik vervolgens op Create policy om de policy aan te maken en toe te passen.

BLUE IDENTITY

Summary

Is het gelukt om de bovenstaande controle's uit te voeren? Zo ja dan is jouw organisatie een stuk veiliger geworden. Je voorkomt nu dat kwaadwillenden zeer eenvoudig jouw omgeving kunnen binnendringen.

De controle die hierboven is gedaan betreffen een 3 tal checks die in onze 12 punten APK terugkomen. In deze APK gaan wij nog een stuk dieper in op specifieke onderwerpen. Maar je bent nu al goed op weg.

Heb je vragen of wil je meer informatie ontvangen stuur ons dan een email:

Mail@blue-identity.com

BLUE IDENTITY