

ATTIC

FOR MICROSOFT 365

WERELDKLASSE CYBERSECURITY
VOOR OFFICE 365 EN AZURE
ACTIVE DIRECTORY



FIX JE DIGITALE VEILIGHEID

Attic is de eerste cybersecurity oplossing die geschikt is voor het MKB. Door proactief te handelen op onveilige configuraties in clouddiensten helpt Attic je veiliger online ondernemen.

Met Attic for Microsoft 365 maak je snel veiliger gebruik van Office 365 en Azure Active Directory.

Al jaren neemt de dreiging van cyberaanvallen op het Nederlandse MKB toe en ook kleinschalige ondernemers ontdekken dat ze niet langer veilig zijn voor cybercriminaliteit, zoals CEO-fraude en ransomware. Die groeiende kwetsbaarheid van bedrijven in alle soorten en maten komt onder andere door de steeds groter wordende afhankelijkheid van clouddiensten. Iedere onderneming gebruikt tegenwoordig wel een vorm van online dienstverlening om bedrijfsprocessen te versnellen en verbeteren.

Tegelijkertijd is het in al die jaren niet makkelijker geworden om jouw bedrijf tegen al die dreigingen te beveiligen – tot nu. Met Attic for Microsoft 365 onderneem je veiliger.



Met Attic for Microsoft 365 werk je veiliger online in Office 365

11
seconden

Er wordt wereldwijd elke 11 seconden een ransomware aanval uitgevoerd.

Volgens onderzoek van Cybersecurity Ventures

78
procent

78% van alle Microsoft 365-gebruikers heeft geen tweestapsverificatie

Aldus de cyberexperts van CoreView

50+
checks

Attic heeft meer dan 50 checks, waarvan veel met automatische fixes.

Voor uiteenlopende instellingen in Microsoft 365

1
critical alert

Admin heeft zojuist MFA uitgeschakeld. Onderneem direct actie.

Voorbeeld van hoe Attic alarmeert inclusief handelingsperspectief

ZO BEVEILIGT ATTIC JOUW BEDRIJF

Attic for Microsoft 365 helpt ondernemers om cybercriminelen te weren door cybersecurity te automatiseren in een gebruiksvriendelijke interface. De Attic-app wordt via een speciale, beveiligde verbinding gekoppeld aan jouw Microsoft 365-omgeving en controleert automatisch alle instellingen om vast te stellen waar er mogelijke kwetsbaarheden in het systeem zitten.

Je stelt Attic eenmalig in voor jouw systemen en vervolgens gaat de app op de achtergrond aan de slag.

Attic detecteert niet alleen problemen, maar levert vaak ook direct de oplossing. Wanneer er een zwakte in Microsoft 365 wordt gedetecteerd krijg je een melding van Attic, als er een fix beschikbaar is verhelp je het probleem met één druk op de knop. Ons systeem zorgt direct dat alles weer goed staat en jij veiliger verder kunt met het runnen van je bedrijf.

Met Attic zetten we bij Zolder BV zwaar in op de automatiseren van cybersecurity, zodat onze dienst goed schaalbaar én betaalbaar is. Dit maakt wereldklasse cybersecurity toegankelijk voor het mkb en dankzij onze app blijf je op de hoogte van jouw online veiligheid op kantoor, maar ook het schoolplein of de golfbaan.



HOE WERKT HET?

Wanneer je bent overtuigd dat je jouw Microsoft 365-omgeving simpel en snel met Attic wil beveiligen gaan we aan de slag om het systeem gereed te maken. Om onze dienst te kunnen leveren moeten we met Zolder BV geregistreerd worden als een zogeheten Cloud Solution Provider (CSP) voor jouw Microsoft 365-abonnement. Zo creëren we een koppeling met jouw bedrijf waardoor Attic de toegang krijgt om instellingen te controleren en waar nodig te wijzigen.

Deze CSP-koppeling regelen we simpel door vanuit Attic een verzoek te doen aan iemand met beheerrechten in jullie Microsoft 365-omgeving.

CHECKS & FIXES

De kracht van Attic zit in onze Checks & Fixes, een groeiende bibliotheek aan scripts die we ontwikkelen om continu jouw Microsoft 365-omgeving te controleren op kwetsbaarheden. Deze scripts voeren we, op de achtergrond, repeterend uit volgens een interval van bijvoorbeeld 15 minuut. Elk van deze scripts controleert een specifieke instelling in de Microsoft cloud (via de beschikbare API) en slaat alarm als deze instelling afwijkt van de optimale situatie.

Stel je voor de jij multi-factor authenticatie hebt ingesteld voor al jouw medewerkers en een gebruiker zet deze instelling uit. Dit maakt het makkelijker voor cybercriminelen om toegang te krijgen tot jullie systemen en Attic zal dan direct alarm slaan.

Zo'n alarm krijg je vervolgens binnen als een service ticket in de Attic-app, inclusief een push bericht om je hiervan op de hoogte te stellen. Ook kun je instellen dat één of meerdere e-mailadressen een melding ontvangen om zo snel mogelijk tot actie over te gaan.

In het voorbeeld van de multi-factor authenticatie die is gedeactiveerd is Attic in staat deze instelling programmatisch weer goed te zetten. In onze app kun je dus met één druk op de knop ook de Fix activeren en je systeem weer optimaal beveiligen.

Heb je hulp nodig? Dan kan er bij ieder service ticket ook contact opgenomen worden met onze service desk. Zo helpt Attic je altijd verder wanneer je systeem beter beveiligd moet worden.



HOE SNEL IS ATTIC?

Om veiliger online te werken wil je zeker weten dat kwetsbaarheden zo snel mogelijk verholpen worden. De processen van Attic zijn volledig geautomatiseerd en repeterend – de tijd tussen mogelijk verdacht gedrag, de constatering hiervan en het verhelpen van problemen ligt hiermee aan de volgende factoren:

1. Check interval

Elke check in Attic is geconfigureerd met een interval, minimaal 15 minuten. Wanneer bijvoorbeeld tweestapsverificatie wordt uitgeschakeld dan slaat Attic binnen een kwartier alarm.

2. Toestemming van afnemer

Een fix die Attic voorstelt moet door een beheerder worden geaccordeerd alvorens Attic die uitvoert. Om dit proces te versnellen kan per fix op voorhand worden afgesproken dat deze altijd automatisch geaccordeerd wordt. Hierdoor zal een fix al binnen enkele minuten worden

uitgevoerd en het systeem weer beveiligd zijn.

3. (optie) Verwerkingstijd Sentinel

In Attic PRO wordt een koppeling gelegd met Microsoft Sentinel. Sentinel heeft, net als iedere SIEM, een interne verwerkingstijd van logbronnen naar alarmen. Onze ervaring is dat het maximaal 30 minuten duurt voordat een verdachte handeling tot een Sentinel alarm leidt.

PRO VOOR SENTINEL



Onderdeel van het Microsoft365 abonnement van jouw bedrijf is Microsoft Sentinel. Dat is de SIEM oplossing die elke Microsoft abonnee gratis kan inschakelen. Vervolgens is het mogelijk om een aantal logbronnen in de Microsoft cloud zonder meerkosten naar Sentinel te “streamen”. Voor andere logbronnen in de Microsoft cloud of daarbuiten, zoals firewalls, brengt Microsoft wel kosten in rekening.

Om Attic for Microsoft 365 PRO voor Sentinel in te schakelen is extra onboarding nodig, aangezien dit gekoppeld moet worden aan een Azure Subscription. Zo kan Microsoft, wanneer er extra logbronnen worden toegevoegd, deze kosten in rekening brengen. Attic zal deze logbronnen alleen na expliciet verzoek en toestemming activeren, zodat je niet voor onverwachte kosten komt te staan.

Na de onboarding worden in elk geval alle gratis logbronnen toegevoegd en de correlatieregels in Sentinel geactiveerd. Deze regels triggeren op bepaald verdacht gedrag en slaan vervolgens alarm. De afhandeling van die alarmen verloopt op dezelfde manier als hiervoor bij Checks & Fixes beschreven.

PERSOONSGEGEVENS

Als CSP en security monitoring dienst heeft Attic technisch gezien toegang tot data met persoonsgegevens van medewerkers in jullie Microsoft 365-omgeving, zonder deze toegang zou Attic niet naar behoren werken. Die toegang is onderhevig aan onze privacyverklaring en verwerkersovereenkomst waarin ook de specifieke verwerkingen zijn benoemd.

Attic kijkt niet naar persoonsgegevens om tot alarmen te komen. Wanneer een alarm gegenereerd wordt dat betrekking heeft op een bepaalde medewerker, zoals een admin, worden alleen de gegevens (e-mailadres, naam) van de betreffende gebruikers verzameld om gericht te adviseren in de afhandeling.

BEVEILIGING

Naast de bescherming van persoonsgegevens zoals beschreven in de verwerkersovereenkomst, zijn een aantal relevante beveiligingsmaatregelen van toepassing.

Changes

Attic brengt alleen wijzigingen aan met jullie expliciete toestemming. Hierin raden we aan dat je als organisatie zelf een interne wijzigingsprocedure instelt om te zorgen dat dit telkens goed verloopt. Wanneer een wijziging onverhoopt tot storingen leidt en teruggedraaid moet worden dan zal onze Servicedesk hier in overleg mee assisteren.

Secure Application Model

De CSP-koppeling tussen Attic en jullie Microsoft 365-omgeving wordt gelegd vanuit een afgezonderde

beheertenant van Zolder BV. Die koppeling is gebouwd conform het extra beveiligde Secure Application Model zoals Microsoft dit aan CSP's voorschrijft.



HET TEAM ACHTER ATTIC

De ontwikkeling van Attic wordt gedaan door de wereldklasse cyberexperts van Zolder, die samen meer dan 70 jaar ervaring in cybersecurity en ethical hacking hebben.

Het is de visie van Zolder dat iedereen toegang moet hebben tot betaalbare oplossingen om veilig online te ondernemen. Daarom gebruiken ze hun aanzienlijke kennis om ondernemers verder te helpen.



**De oprichters
van Zolder.**



WIL JE OOK JOUW DIGITALE VEILIGHEID FIXEN?

Ga naar onze website en start je abonnement. Al binnen één dag onderneem je veiliger online dankzij de geautomatiseerde aanpak van Attic.

www.atticsecurity.com

ATTIC
FOR MICROSOFT 365