nlcom
SLIM IN ICT

Cloud Security Packages

Bescherm uw Microsoft Cloud omgeving

Inhoud

Cloud Security Packages

Cloud Security Packages, voor wie is dat interessant?

Veiligheid en zekerheid in de breedste zin van het woord is voor elke onderneming belangrijk en vanzelfsprekend. Dit begint heel praktisch van een slot op de voordeur tot een brandwerende kluis voor de financiële administratie. Ook op gebied van ICT security is er een hoop af te spreken, in te stellen en vooral na te leven. Traditioneel vertaalt zich dit in onderwerpen als toegangspasjes, wachtwoordbeleid, rechtenstructuren op mappen en applicaties. Tegenwoordig zijn Clouddiensten als Exchange Online en SharePoint Online steeds normaler aan het worden, echter zien wij dat men de security van dergelijke Clouddiensten onderbelicht laat.

Houd je gegevens veilig opgeslagen.

Zorg ervoor dat alleen de juiste personen toegang hebben tot belangrijke gegevens met gegevensbescherming.

Verdedig jezelf tegen malware.

Bescherming tegen ransomware, spam, malware, virussen, phishing-pogingen, schadelijke koppelingen en andere bedreigingen.

Houd de touwtjes in handen.

Blokkeer toegang tot een bijlage zelfs nadat de e-mail je inbox heeft verlaten met cloudbijlagen.

Breng je eigen apparaten.

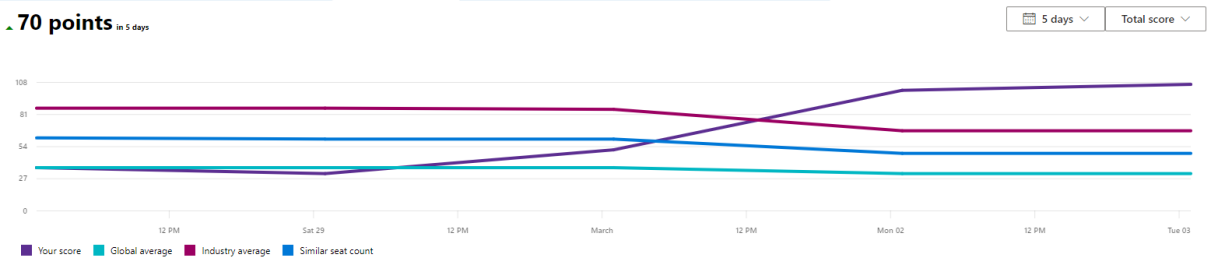
Bescherm je gegevens, zelfs wanneer die worden geopend op het persoonlijk apparaat van je medewerkers.

Met onze Cloud Security Packages willen we elke onderneming helpen de beveiliging van de Office365 en Microsoft365 te optimaliseren zoals dat vanzelfsprekend is voor de traditionele ICT-omgeving. Bij clouddiensten is beveiliging stukken belangrijker aangezien kwaadwillende, in theorie, alleen een internetverbinding nodig hebben om kwaad te kunnen doen. Met onze Cloud Security Packages activeren, configureren en monitoren we verschillende services die de veiligheid van de tenant waarborgen. Voor het implementeren van de meeste verbeterslagen op gebied van beveiliging geeft Microsoft punten, deze punten vormen samen de secure score van de tenant. Hoe hoger de secure score des te veiliger de tenant.

Secure score

De secure score is een meetlat waar Microsoft de beveiliging van de tenant in kwestie vergelijkt met het globale gemiddelde, het gemiddelde in dezelfde sector en het gemiddelde bij tenants met een vergelijkbaar aantal eindgebruikers.

In de volgende grafiek is te zien dat we vrijdag 28 maart een Cloud Security Package geïmplementeerd hebben. Deze implementatie heeft ertoe geleid dat de secure score van 30 naar 100 gestegen is. Een hoge secure score is geen doel op zich maar wel een goede indicatie of de tenant veilig is of niet. De groei van 30 naar 100 hebben we bij deze tenant behaald met de implementatie van zaken als MFA, Selfservice password reset en Mailbox Auditing. Hoe meer services juist zijn geïmplementeerd des te veiliger en des te hoger de score.



Packages & services

Packages

Cloud Security Package 1	*Cloud Security Package 2*	*Cloud Security Package 3*
• Mailbox auditing • E-mail authenticatie (SPF/DKIM/DMARC) • Multi Factor Authentication • MailTips • NLcom security best practices	• **Cloud Security Package 1** • Anti-spam en anti-malware • Advance Threat Protection* *Benodigd: Office 365 Advance Threat Protection P1	• **Cloud Security Package 1** • **Cloud Security Package 2** • Configuratie Attack Simulator* • Configuratie Data Loss Prevention* • Configuratie unified labels* • Inschakelen alerting policies* *Benodigd: Microsoft 365 Business

Services

Mailbox auditing

Met mailbox auditing worden alle bewerkingen rondom een e-mailbericht binnen de omgeving bijgehouden. Daarmee is in te zien wanneer een item wordt verplaatst, verwijderd of gewijzigd en door wie. Naast e-mailberichten kan dit o.a. ook met betrekking tot groepen, documenten en rechten.

E-mail authenticatie (SPF/DKIM/DMARC)

De standaarden SPF, DKIM en DMARC worden gebruikt om de integriteit (echtsheidskenmerken, e-mailauthenticatie) van e-mail te borgen, zodat ontvangers kunnen controleren of e-mails ook daadwerkelijk afkomstig zijn van de veronderstelde afzender. Dit betekent dat phishingmails van aanvallers beter kunnen worden herkend, en dat de kans op misbruik afneemt.

Multi Factor Authentication

Deze optie maakt het mogelijk om in te loggen met een wachtwoord in combinatie met een code die via een telefoon app, e-mail, sms of Yubi-key wordt ontvangen. De beste MFA is gebaseerd op tenminste twee van de volgende kenmerken:

- Iets dat je weet (gebruikersnaam/ wachtwoord)
- Iets dat je hebt (device van een gebruiker of een token)
- Iets wie je bent (vingerafdruk/irisscan/gezichtsherkenning)

Lees voor meer informatie **onze blog over MFA.**

MailTips

MailTips zijn informatieve berichten die aan gebruikers worden getoond terwijl ze een bericht opstellen. Terwijl een nieuw bericht is geopend en wordt opgesteld, analyseert Exchange het bericht (inclusief ontvangers). Als er een mogelijk probleem wordt gedetecteerd, wordt de gebruiker op de hoogte gebracht met een MailTip voordat het bericht wordt verzonden. Met behulp van de informatie in de MailTip kan de gebruiker het bericht aanpassen om ongewenste situaties of niet-bezorgingsrapporten (ook bekend als NDR's of bounce-berichten) te voorkomen.

Security best practices

Door de jaren heen hebben we meerdere best practices omarmd. Indien er nieuwe best practices gedefinieerd worden of bestaande best practices doorontwikkeld worden voeren we dit door op elke Microsoft tenant met een Cloud Security Package.

Anti-spam en anti-malware

Bescherming tegen spam en malwarebestrijding. Microsoft heeft ingebouwde inkomende en uitgaande malwarefiltering om uw organisatie te beschermen tegen schadelijke software en ingebouwde spamfiltering om uw organisatie te beschermen tegen het ontvangen en verzenden van spam (bijvoorbeeld in het geval van gecompromitteerde accounts).

Advanced Threat Protection

Bescherm je organisatie tegen geavanceerde bedreigingen zoals phishing en zero-day-malware, laat het Microsoft vervolgens onderzoeken en aanvallen automatisch herstellen. Bruikbare inzichten helpen potentiële bedreigingen zoals phishing en malware te identificeren, te prioriteren en via aanbevelingen op te lossen, en je organisatie proactief te beschermen tegen aanvallen.

Configuratie Attack Simulator

Het is van essentieel belang om gebruikers te trainen in het herkennen en melden van aanvallen. De Attack Simulator helpt gebruikers via simulaties om zich bewust te worden van aanvallen. Gebruikers worden ook gewaarschuwd voordat ze op onbekende koppelingen klikken en krijgen hulp bij het melden van verdachte inhoud. De Attack Simulator is het kleine broertje van onze eigen NSAT.

Configuratie Data Loss Prevention

Om te voldoen aan zakelijke normen en branchevoorschriften, moeten organisaties gevoelige informatie beschermen en onbedoelde openbaarmaking ervan voorkomen. Gevoelige informatie kan financiële gegevens of persoonlijk identificeerbare informatie (PII) omvatten, zoals creditcardnummers, Burgerservicenummers of medische dossiers. Met een Data Loss Prevention (DLP) -beleid in het Security & Compliance Center kun je gevoelige informatie identificeren, bewaken en automatisch beschermen.

Configuratie vertrouwelijkheid labels

Vertrouwelijkheid labels worden gebruikt om e-mailberichten, documenten, sites, en meer te classificeren. Wanneer een label wordt toegepast (automatisch of door de gebruiker), is de inhoud of site beveiligd op basis van de instellingen die u kiest. U kunt bijvoorbeeld labels maken waarmee bestanden worden versleuteld, inhoudsmarkering wordt toegevoegd en de gebruikerstoegang tot bepaalde sites wordt beheerd.

Inschakelen alerting policies

Gebruik een waarschuwingsbeleid om activiteiten van gebruikers en beheerders, malwarebedreigingen of incidenten die leiden tot gegevensverlies in uw organisatie bij te houden. Nadat de activiteit waarover we een melding willen ontvangen is gedefinieerd, verfijnen we het beleid door voorwaarden toe te voegen, en te besluiten wanneer de waarschuwing moet worden geactiveerd. Deze meldingen komen in ons servicedeskticketsysteem waarna we het voor u beoordelen en oplossen.

Waarom is security en Advanced Threat Protection zo belangrijk?

Reden 1: Beveiliging tegen onveilige bijlages

Office 365 Advanced Threat Protection scant alle bijlages die in een e-mailbox binnenkomen of ze veilig zijn. Een bijlage wordt automatisch geopend en getest in een virtuele omgeving op kwalijke bedoelingen. Als het een onveilige bijlage blijkt te zijn wordt deze automatisch verwijderd. Een veilige bijlage kan worden geopend zoals de gebruiker gewend is.

Reden 2: Alleen e-mails met veilige links

Iedereen weet dat je nooit op links van onbekende afzenders moet klikken. Maar als je dat toch per ongeluk doet of een bekende afzender is zelf gehackt wil je goed beveiligd zijn.
Office 365 Advanced Threat Protection controleert alle links in zowel e-mails als Office-documenten. Als er op een link in een binnenkomende email wordt geklikt, controleert Office 365 Advanced Threat Protection de link voordat deze wordt geopend.

Als de link veilig is, kan deze gewoon worden geopend. Als de link schadelijk is, krijgt de gebruiker een waarschuwing om niet naar de website te gaan of een melding dat de website is geblokkeerd. Een soortgelijk proces vindt ook plaats bij links in Office-documenten. Office 365 Advanced Threat Protection biedt ook uitgebreide rapportages waarmee je onder andere kunt bijhouden welke gebruikers wanneer op een link hebben geklikt.

Reden 3: Je bent spoof proof

Je hebt vast wel gehoord van situaties waarbij cybercriminelen spoofing hebben gebruikt om te hacken, waarbij ze zich voordoen alsof ze iemand uit de organisatie zijn. Office 365 Advanced Threat Protection controleert email berichten op spoofing met speciale spoof intelligence. De ingebouwde spoofbeveiliging zorgt ervoor dat de legitieme e-mails worden verzonden, terwijl je organisatie wordt beschermd tegen kwaadaardige bedoelingen. De verschillende spooffilters kun je zelf definiëren.

Reden 4: Bescherming tegen phishing aanvallen

Office 365 Advanced Threat Protection beschermt je organisatie ook tegen phishing-aanvallen. Met de antiphishing-functies kan je IT-beveiligingsteam alle inkomende berichten controleren op aanwijzingen dat het een phishing-poging kan zijn.

Hoe? Wanneer de e-mail in je inbox binnenkomt, wordt het bericht geëvalueerd of het een kwaadwillende e-mail is. Als dat het geval is, voert Office 365 Advanced Threat Protection een actie uit, op basis van de vooraf gedefinieerde configuratie. Deze anti-phishingbeleid configuratie kan worden ingesteld voor een specifieke groep mensen in de organisatie of voor een volledig domein.