5 kritische vragen over de beveiliging van je cloud-data.

Durf jij ze te stellen?

Dataveiligheid raakt iedereen

Volg je het nieuws een beetje? Er gaat bijna geen dag voorbij of je hoort over cybercrime en datalekken. De veiligheidsrisico's van een online wereld, waarin alles 24/7 met elkaar in verbinding staat, horen bij de dagelijkse praktijk van het ondernemen.

En ze raken iedereen. Niet alleen bedrijven van MKB tot multinational, maar ook zorginstellingen en overheidsorganisaties worden slachtoffer van beveiligingsproblemen. Volgens onderzoek van McAfee is de wereldwijde economische schade van cybercrime inmiddels 600 miljard dollar per jaar.

Bestrijden is niet genoeg

Werk je met Azure en Office 365? Dan staat je data niet meer op je eigen servers, maar bij Microsoft in de cloud. Over technisch beheer hoef je je dus geen zorgen meer te maken, maar dat betekent niet dat je niet meer hoeft na te denken over beveiliging. Gebruikersgedrag en beheer zijn namelijk nog steeds de belangrijkste bronnen van onveiligheid. Wat moet je doen om dreigingen het hoofd te bieden? Als je daar nog over na moet denken als een cyberaanval, datalek of privacybreuk eenmaal gaande is, ben je te laat. De gevolgen kunnen je bedrijfsvoering compleet stilleggen of zelfs een faillissement betekenen voor je organisatie. Wacht daarom niet, maar kom nu in actie. Want hét geheim van goede cloud security is om voortdurend pro-actief naar je eigen omgevingen te kijken en verbeteringen aan te brengen.

5 kritische vragen

De eerste stap naar betere beveiliging van je Office 365- en Azure-omgeving zet je door de juiste vragen te stellen. En eerlijke antwoorden te geven. Alleen zo kom je erachter wat er moet gebeuren om jouw Microsoft cloud optimaal te beveiligen.

1 Weet je precies hoe veilig jouw Azure en Office 365 zijn?

Je kunt problemen niet oplossen als je ze niet kunt zien. Daarom begint security met het in beeld brengen van je situatie.

Dataclassificatie: beveiliging bij de bron

Nu je in de cloud werkt ligt de prioriteit niet bij het beveiligen van devices, maar bij het beveiligen van je applicatielaag en je databronnen. Het classificeren van data is daarbij de basis. Als dat onvolledig gebeurt, kun je nooit je identity management en je databeveiliging optimaal inrichten. Het is ook belangrijk dat je nagaat of door de hele organisatie heen data op dezelfde manier wordt geclassificeerd.

Admin-accounts in beeld

Een veel voorkomend beveiligingsrisico zijn bijvoorbeeld onbeheerde admin-accounts, die niet zijn opgeruimd toen een medewerker uit dienst ging of van functie wisselde. Wil je dit voorkomen, dan heb je up-to-date kennis nodig van alle admin-accounts. Dwing ook het gebruik van veilige, regelmatig wisselende wachtwoorden af en richt governance-processen zo in dat rechten worden ingetrokken als ze niet meer nodig zijn.

Een veilig mailsysteem

E-mail is het belangrijkste doelwit van hackers en phishing. Menselijk gedrag is daarbij het belangrijkste beveiligingslek. Door je e-mailsysteem regelmatig te testen weet je of phishing mails worden tegengehouden en hoe kwetsbaar je bent als er onverhoopt toch iemand op een onveilige link klikt.

Encryptie

Vertrouwelijke en privacygevoelige documenten kunnen bij het werken in de cloud ook op allerlei devices staan. Daarom is het belangrijk dat op concurrentiegevoelige documenten en persoonsgegevens encryptie wordt toegepast. Heb je 100% inzichtelijk waar je encryptie gebruikt en waarom?

Wie mag op welk device en met welke app welke data gebruiken?

Office 365 stelt je in staat om zeer nauwkeurig in te regelen welke identiteiten vanaf welke devices bij welke data mogen. Maar dan moet dat wel ingesteld zijn. Heb je inzicht in hoe deze functies zijn geconfigureerd?

Zijn je tools goed geconfigureerd?

Het configureren van Microsoft Data Loss Prevention is een klus die veel inzet en kennis vraagt. Door de voortdurende ontwikkelingen moet je je configuratie ook regelmatig updaten. Heb je de nodige kennis en capaciteit?

2 Weet je welke data je hebt en met wie je ze deelt?

Je cloud-omgeving bevat veel data. En dat wordt iedere dag meer, net als het aantal plaatsen waar deze data staat opgeslagen. Niet alleen op jouw corporate devices, maar ook op privé-apparaten van je werknemers en externen. Om al die data goed te kunnen beveiligen moet je weten welke data je hebt en wie erbij kan.

Persoonsgegevens

Daarbij nemen persoonsgegevens een bijzondere plek in. Als deze uitlekken of verloren gaan schaadt dat je klantrelaties ernstig. Het kan, zeker na de invoering van de AVG, ook grote juridische gevolgen hebben. De AVG vraagt dat je een register bijhoudt van welke persoonsgegevens je hebt. Heb je dat allemaal geregeld en zijn je gegevens up-to-date?

Ongestructureerde data

Ongestructureerde data, zoals tekstberichten en grafisch materiaal, kan moeilijk te classificeren zijn. Weet jij wat je hebt aan ongestructureerde data, welke informatie die data bevat en wie erbij kan?

Oversharing

Office 365 maakt het makkelijk om samen te werken met externen. Maar het is daarbij ook makkelijk om te veel te delen, permissies te lang in stand te laten of per ongeluk te delen met de verkeerde mensen. Een goed ingericht security-systeem laat jou zien wie er van buiten toegang heeft tot welke data.

3 Veroorzaakt het gedrag van je mensen ongemerkt gevaren?

Herkennen jouw mensen phishing-mails en andere pogingen tot cybercrime als ze die tegenkomen? ABN Amro stuurde haar medewerkers een phishing-mail om dat te testen en ze schrokken van het resultaat. Heb jij de processen ingericht waarmee je regelmatig dit soort tests kunt uitvoeren?

Security-beleid: is het bekend en wordt het begrepen?

Je kunt nog zo hard werken aan het opstellen van een security-beleid, als dat beleid bij je mensen niet bekend is en/of niet begrepen wordt heeft het geen enkel effect. Maken voorlichting en training over security deel uit van je standaard onboarding en wordt materiaal regelmatig geüpdatet?

Voorkomen en genezen

Weten jouw medewerkers wat ze wat ze moeten doen om cybercrime en datalekken te voorkomen? Weten ze hoe te handelen bij een incident? Een adequate reactie van een goed opgeleide medewerker kan het verschil maken in een beveiligingscrisis. Maar je hebt nog liever medewerkers die het zover helemaal niet laten komen: voorkomen is beter dan genezen.

Trust, but verify

Natuurlijk wil je erop vertrouwen dat al je medewerkers zich keurig aan alle voorschriften houden. Maar de realiteit is vaak anders. Daarom heb je monitoring nodig op het gedrag van je gebruikers: welke data delen ze? Gebruiken ze veilige wachtwoorden? Die mogelijkheden zijn er allemaal in Office 365. De vraag is: zet je ze op dit moment optimaal in?

4 Welke apps en devices gebruiken je mensen, naast de officiële?

Het gebruik van externe devices en apps zorgt ervoor dat je in de cloud een heel ander soort security-beleid nodig hebt dan bij een on-premises infrastructuur. Om dit op te stellen is best wel diepgaande kennis van Office 365 nodig. Kennis die niet ieder bedrijf beschikbaar heeft.

Externe devices en apps

Heb je een sluitend security-beleid geconfigureerd voor externe devices en apps? Zijn deze devices kwetsbaar voor ransomware-aanvallen? Zitten er kwetsbaarheden je verificatieproces, die kunnen leiden tot ongeoorloofde toegang vanaf deze devices? Je hebt heel weinig controle over externe apps en devices, maar door goed naar beveiliging van je databronnen te kijken kun je er toch grip op krijgen.

Schaduw-IT

Hoeveel van jouw bedrijfsdata zwerft er over WhatsApp, Slack, Dropbox en in Facebook-groepen? Je medewerkers gebruiken privé al heel veel cloud apps en wisselen daar ook zakelijke gegevens mee uit. Gelukkig kun je met de tools van Microsoft duizenden apps automatisch detecteren. Gebruik je deze scan regelmatig?

100% grip

Ook gastgebruikers, zoals klanten en externen, loggen in met hun eigen devices en apps. En dan zijn er nog je andere systemen, met hun eigen oplossingen voor monitoring en beveiliging. Voor 100% grip op je cloud security is het belangrijk dat ook deze externe systemen in je beveiligingsbeleid worden geïntegreerd.

5 Kun je adequaat reageren als het misgaat?

We zeiden het al: voorkomen is beter dan genezen. Maar er zullen altijd incidenten zijn. Een goed ingerichte IT-organisatie heeft live inzicht op wat er gebeurt in de hele cloud-omgeving en heeft de kennis en de capaciteit om 24/7 te reageren op incidenten.

Haal je het maximale uit je monitoring-tools?

Office 365 en Azure bieden veel monitoring-tools. Maar ook hier weer geldt dat het hebben van tools niet hetzelfde is als het effectief inzetten ervan. Adequaat reageren op incidenten doe je vanuit een Security Operations Center. Daar zitten jouw beveiligingsspecialisten, die 24 uur per dag, 7 dagen per week jouw monitoring tools in de gaten houden en bij kleine en grote incidenten adequaat reageren volgens vaste procedures. Alleen zo kun je volledig vertrouwen op de veiligheid van je *digital workplace*.

Heb je daarnaast nog tijd voor beleid, adoptie en innovatie?

Duizelt het je inmiddels? Het zijn veel vragen, en ze zijn allemaal belangrijk. En naast het inrichten van alle bestaande tools en het bestrijden van bekende dreigingen, moet je ook nog tijd maken om vooruit te kijken. Welke nieuwe tools komen eraan van de kant van Microsoft? Welke nieuwe beveiligingsrisico's zijn er? Hoe houden we onze mensen op de hoogte van de ontwikkelingen? Hoe maken we onze procedures efficiënter en effectiever?

Wat Microsoft al voor je doet.

Microsoft draagt zeer actief bij aan een veilige cloud-omgeving voor bedrijven en gebruikers wereldwijd. Alle cloudproviders hebben immers een gemeenschappelijk belang om de cloud veilig te houden. Daarnaast heeft Microsoft zich samen met andere grote techbedrijven gecommitteerd aan het Cybersecurity Tech Accord van 10 september 2018. Eén van de doelen daarvan is om een veilige cloud te realiseren voor iedereen en die verantwoordelijkheid samen met andere techbedrijven te dragen.

Jouw verantwoordelijkheden.

Het goede nieuws: jouw Office 365- en Azure-omgeving heeft de tooling die je nodig hebt om er de veiligst mogelijke digitale werkplek van te maken. Het minder goede nieuws: het is jouw verantwoordelijkheid om het ook daadwerkelijk voor elkaar te krijgen. Om de security tools die je hebt effectief in te zetten, moet je ze namelijk wel eerst aanzetten. Hieronder een aantal van deze security tools:

1. Beveilig je e-mailverkeer met *Advanced Threat Protection*
2. Gebruik *Cloud App Security* om de toegang tot Office 365 te beveiligen
3. Voorkom gegevensverlies met *Data Loss Prevention* en *Azure Information Protection*
4. Beveilig je on-premises omgeving met *Microsoft Security*
5. Monitor gebruikersgedrag met *Cloud App Security*
6. Beveilig bedrijfsdata door de hem te voorzien van *encryptie* en *specifieke gebruikersrechten.*
7. Stel een *Mobile Device Management*-beleid en *Mobile Application Management-beleid* op en beveilig daarmee devices en applicaties met behulp van *Intune*
8. Beveilig je cloudtoegang met *Azure Security Center*
9. Krijg grip op je admin accounts met *Privileged Identity Management*
10. Richt een *Security Operations Center* in om 24/7 te kunnen reageren op incidenten

Hulp nodig bij het aanzetten van jouw security tools in Azure en Office 365?

Neem contact op met onze security-experts

Helemaal op orde. Of zijn er open vragen?

Heb je al deze verantwoordelijkheden op orde en kun je dus volmondig 'ja' antwoorden op alle kritische vragen over jouw cloud security? Gefeliciteerd: je bent helemaal klaar om met een 100% beveiligde digital workplace de toekomst tegemoet te gaan.

Heb je vragen met 'nee' moeten beantwoorden of had je niet genoeg informatie om de antwoorden te vinden? Mis je mankracht en/of kennis om te voldoen aan de lange lijst verantwoordelijkheden die cloud security met zich meebrengt? Dan is het misschien een goed idee om eens verder te praten met een van de security-experts van Portiva.

Op portiva.nl kun je ook een webinar kijken over het beveiligen van data in Office 365 en de Azure Information Protection Datasheet downloaden.

Meer over cloud security

Over Portiva | Als productivity partner levert Portiva, met meer dan 60 professionals, consultancydiensten, end-to-end maatwerkontwikkeling en managed services oplossingen. Als high-end viervoudig Microsoft Gold Certified Partner richten wij ons op SharePoint, Office 365 en Azure. Wij hebben een strategische blik en pragmatische aanpak. Vanuit onze passie voor en kennis over technologie stemmen wij mensen, processen en technologie beter op elkaar af om organisaties meer te laten bereiken, effectiviteit te verhogen en onderlinge samenwerking en communicatie te optimaliseren.