vijfhart
IT-OPLEIDINGEN

CYBERSECURITY & MICROSOFT: OOK VOOR JOUW BEDRIJF ENORM BELANGRIJK!

Inhoud

Waarom dit whitepaper? 2

Microsoft: Van totaalontzorger tot doe-het-zelf markt 2

Jouw bedrijfsgegevens: de pot met goud voor de cybercriminelen 2

Identiteitsbeheer 3

De aanval tijdig herkennen 3

Ook jouw bedrijf loopt risico 3

Microsoft role-based security cursussen 4

Basiscursus 4

Microsoft Security, Compliance and Identity Fundamentals (SC-900) 4

Technische cursus – Azure 4

Microsoft Azure Security Technologies (AZ-500) 4

Technische cursus – Microsoft 365 5

Microsoft 365 Security Administration (MS-500) 5

Security specifieke cursussen 5

Microsoft Cybersecurity Architect (SC-100) 5

Microsoft Security Operations Analyst (SC-200) 5

Microsoft Identity and Access Administrator (SC-300) 5

Microsoft Information Protection Administrator (SC-400) 5

Conclusie 6

Waarom dit whitepaper?

In dit whitepaper willen we jou wijzen op de relevante securitycursussen van Microsoft. Waarom deze cursussen zo relevant zijn worden in dit whitepaper nader uiteengezet. Tegenwoordig kun je geen nieuwssite bezoeken of er is wel een artikel over cybersecurity te lezen. Een drietal opvallende berichten:

1. Pathé, een grote internationale bioscoopketen maakte in 2019 na het ontvangen van nepmails (phising) 19 miljoen euro over aan oplichters; het verantwoordelijke Nederlandse management werd ontslagen[1].
2. De Universiteit Maastricht werd getroffen door een ransomware aanval. Dit type aanval maakt bedrijfsgegevens onleesbaar, waarna het bedrijf moet betalen om de gegevens te ontsluiten. In dit geval bedroeg de schade 'maar' twee ton[2].
3. Meer recent is Mediamarkt door een soortgelijke aanval getroffen. Hoe dit precies is afgelopen is buiten de pers gehouden.

Microsoft: Van totaalontzorger tot doe-het-zelf markt

De kop van deze paragraaf is overdreven maar bevat wel een kern van waarheid. Tot en met de applicatie aan toe (zoals bij Microsoft 365, bijvoorbeeld MS Teams of SharePoint Online), is Microsoft geheel verantwoordelijk.

Echter, daarna (denk aan alle in MS Teams en SharePoint Online opgeslagen gegevens, en de toegang er toe) ben jij zelf verantwoordelijk. Uiteraard biedt Microsoft de nodige cloudgebaseerde diensten aan om jou dit werk mogelijk te maken. Zaak is wel dat jouw eigen bedrijf er mee aan de slag gaat.

Deze benadering is bij andere cloudproviders overigens niet anders. Dit wordt ook wel **gedeelde verantwoordelijkheid** genoemd. Kortom, jouw bedrijf zal zelf actief aan de slag moeten om te zorgen dat al jullie bedrijfsgegevens voldoende beschermd worden en blijven. En dat op tijd wordt ingegrepen wanneer er een aanval plaats vindt.

Jouw bedrijfsgegevens: de pot met goud voor cybercriminelen

Cybercriminelen hebben vele manieren om zich toegang tot jouw IT-omgeving te verschaffen. Ongeacht de gebruikte methodiek hebben ze altijd hetzelfde doel: jouw bedrijfsgegevens. Daarmee kunnen ze veel geld verdienen.

Juist in deze tijd is het voor bedrijven een grote uitdaging om hun bedrijfsgegevens te bewaken. Denk hier o.a. aan het inzichtelijk maken van de gegevenssoorten, de locaties en de beperkingen ervan.

Hoe krijg je inzicht op jouw bedrijfsinformatie en de locaties waar het staat? Hoe zorg je ervoor dat het alleen daar is waar het mag en dat het niet (al dan niet per ongeluk) op ongeoorloofde plekken komt, zoals bijvoorbeeld, de concurrentie? En, welke gegevens moeten heel lang bewaard worden en welke maar heel even? Hoe zie je erop toe dat dit

[1] *Zie: https://fd.nl/ondernemen/1277850/hoe-de-top-van-pathe-voor-19-mln-om-de-tuin-werd-geleid*
[2] *Zie: Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald (nos.nl)*

allemaal ook daadwerkelijk gebeurt? Zeker in deze tijd, waar de data zich overal kan bevinden, dus ook buiten de muren van jouw bedrijf, is dit een enorme uitdaging. Microsoft biedt hier een aantal cloudgebaseerde oplossingen voor. Alleen zul je er zelf mee aan de slag moeten gaan.

Identiteitsbeheer

Het beschermen van de inloggegevens is topprioriteit, meervoudige authenticatie in combinatie met andere controles, is een must. Door gelekte inloggegevens kan een hacker snel en eenvoudig toegang krijgen tot uw bedrijfsomgeving en -informatie, ongeacht de locatie.

Ook hier biedt Microsoft meerdere cloudgebaseerde oplossingen voor. Maar ook hier moet jouw bedrijf er zelf mee aan de slag gaan.

De aanval tijdig herkennen

Cyberaanvallen maken veelal gebruik van bekende technieken. Deze zijn o.a. door toegangscontrole op systemen en data vroegtijdig op te sporen. Dit kan de aanval voorkomen en mogelijke schade beperken.

Vergeet echter de achterkant niet, de zogenaamde achterdeurtjes. Deze moeten ook dicht zitten, dit kan door alle systemen, van servers tot en met de werkplek (inclusief de smart phones en tablets!) continu te bewaken en op zwakheden te controleren. Uiteraard heeft jouw organisatie meerdere beveiligingsoplossingen in gebruik, zowel hardware- als softwarematig. Denk bijvoorbeeld aan firewalls, intrusiondetectionsystemen, antivirus- en antimalware oplossingen. Deze oplossingen bevinden zich zowel in jouw organisatie, als er buiten in de verschillende clouds. Door al deze verschillende puntoplossingen op meerdere locaties, is het een enorme uitdaging om een totaaloverzicht te verkrijgen. Alleen dan weet je wat er echt speelt. Misschien is een inbraak gaande en kun je doeltreffend optreden.

Ook hier biedt Microsoft meerdere cloudgebaseerde oplossingen voor. Maar het is geen vrijbrief om er zelf niks mee te doen. Jouw bedrijf zal er zelf mee aan de slag moeten gaan.

Ook jouw bedrijf loopt risico

Het zijn niet alleen de grote bedrijven die risico lopen. Volgens het *Expertise Centrum Cyber Weerbaarheid* (**ECCW**) ziet een groot gedeelte van de bestuurders van het MKB niet in dat cybercrime een groot risico voor hun bedrijf is[3].

Niet alleen jouw eigen bedrijf, maar ook de bedrijven waarmee jij samengewerkt lopen risico, bijvoorbeeld doordat de productie of informatievoorziening van een bedrijf in de keten wegvalt.

[3] Zie: Slechts 30% van de bestuurders uit het MKB zien cybercrime als een groot risico voor de organisatie (eccw.nl)

Voor jouw bedrijf is het belangrijk om zoveel mogelijk te doen om dit soort aanvallen te voorkomen, tijdig te ontdekken en maatregelen te treffen. Overkomt jouw bedrijf iets, dan heb je de middelen en kennis klaar staan om het snel en doeltreffend op te lossen.

Microsoft role-based security cursussen

Kennis van de risico's en de oplossingen waarmee de eerdergenoemde gevaren kunnen worden voorkomen, helpen jouw bedrijf weerbaarder te worden in het gevecht tegen cybercrime.

Er zijn veel verschillende tools beschikbaar om dit soort aanvallen te ontdekken en te pareren. Zo heeft Microsoft meerdere complete, geïntegreerde securityoplossingen voor hun clouddiensten, alleen met hun eigen doel. Denk hierbij aan bescherming van inloggevens, bescherming van bedrijfsdata en bescherming van de systemen, van de cloud naar uw eigen servers tot en met de werkplekken aan toe. Ook biedt Microsoft een systeem dat een totaaloverzicht geeft van de actuele beveiligingstoestand van jouw gehele IT-landschap.

Er is daarvoor wel kennis nodig om de verschillende oplossingen doeltreffend in te regelen, te bewaken en te gebruiken. En, wanneer er een aanval plaats vindt, goed te reageren.

Onderstaande cursussen geven die kennis waarmee je jouw organisatie weerbaarder kunt maken tegen cybercrime.

Basiscursus

Dit is een cursus die door iedereen gevolgd kan worden. Voor iedere collega die in aanraking komt met Microsoft 365 en/of Azure is deze basiscursus interessant. Kortom, zowel voor eindgebruikers als voor de meer technisch onderlegde collega's.

Microsoft Security, Compliance and Identity Fundamentals (SC-900)

Met deze eendaagse Microsoft Security, Compliance & Identity (SC-900) basiscursus krijg je inzicht in beveiligings-, compliance- en identiteitsconcepten en cloud gerelateerde Microsoft-oplossingen. De volgende onderwerpen komen aan bod: beveiliging, compliance en identiteitsconcepten. Zie hier voor meer informatie over deze cursus.

Technische cursus – Azure

Deze cursus is voor technische collega's die dagelijks met Azure werken. Denk aan Azurebeheerders, DevOps engineers en Azure developers.

Microsoft Azure Security Technologies (AZ-500)

Dit is de vierdaagse Azure beveligingscursus die elke Azurebeheerder moet volgen. Als Azurebeheerder leer je hoe jij op een veilige en verantwoordelijke wijze Azure uitrolt, configureert en beheert. Zie hier voor meer informatie over deze cursus.

Technische cursus – Microsoft 365

Deze cursus is voor technische collega's die dagelijks met Microsoft 365 werken. Denk aan Microsoft 365 beheerders, werkplekbeheerders en databeveiligers.

Microsoft 365 Security Administration (MS-500)

Dit is de vierdaagse Microsoft 365 beveligingscursus die elke Microsoft 365 beheerder moet volgen. Als Microsoft 365 beheerder leer je hoe jij op een veilige en verantwoordelijke wijze Microsoft 365 uitrolt, configureert en beheert. Zie hier voor meer informatie over deze cursus.

Security specifieke cursussen

Microsoft biedt cursussen aan die een hele sterke focus hebben op security en dan op basis van meerdere complete, geïntegreerde securityoplossingen voor clouddiensten. Deze cursussen zijn praktijk gericht waardoor ze goed inzetbaar zijn in jouw omgeving.

Microsoft Cybersecurity Architect (SC-100)

Ben jij een beveiligingsspecialist en werkzaam in een IT-omgeving waar vele Microsoft-producten en clouddiensten gebruikt worden? Dan is deze vierdaagse cursus voor jou. Je leert o.a. om cyberbeveiligingsstrategieën te ontwerpen en te evalueren op de volgende gebieden: Zero Trust, Governance Risk Compliance (GRC), beveiligingsoperaties (SecOps).

Je leert ook hoe je oplossingen ontwerpt en bouwt met behulp van Zero Trust-principes en hoe je beveiligingsvereisten specificeert voor cloudinfrastructuur in verschillende servicemodellen (SaaS, PaaS en IaaS). Zie hier voor meer informatie over deze cursus.

Microsoft Security Operations Analyst (SC-200)

Leer in deze vierdaagse cursus hoe jij cyberbedreigingen kunt onderzoeken, erop kunt reageren en ze kunt opsporen met behulp van Microsoft Azure Sentinel, Azure Defender en Microsoft 365 Defender. Zie hier voor meer informatie over deze cursus.

Microsoft Identity and Access Administrator (SC-300)

Deze vierdaagse cursus biedt jou de kennis en vaardigheden die nodig zijn om identiteits-beheeroplossingen te implementeren op basis van Microsoft Azure Active Directory (Azure AD) en de daarmee verbonden identiteitstechnologieën. Zie hier voor meer informatie over deze cursus.

Microsoft Information Protection Administrator (SC-400)

Leer in deze driedaagse cursus hoe jij de bedrijfsgegegevens kunt beschermen in jouw Microsoft 365-omgeving. Deze cursus richt zich op data governance en informatie-beveiliging binnen jouw bedrijf. Deze cursus behandelt o.a. de implementatie van beleid ter voorkoming van gegevensverlies, typen gevoelige informatie, gevoeligheidslabels, beleid voor gegevensbewaring en Office 365-berichtversleuteling. Zie hier voor meer informatie over deze cursus.

Conclusie

Er zijn vele uitdagingen ten aanzien van cyber-security. Gelukkig zijn er ook manieren om inzicht en grip te verkrijgen op de risico's voor ieder bedrijf.
Goed opgeleide IT-medewerkers zijn hierbij noodzakelijk om het beveiligingsbeleid, uitgezet door het management, te vertalen naar de juiste inzet van de vele Microsoft-beveiligingsoplossingen. De eerdergenoemde cursussen zijn hiervoor dan ook cruciaal.
Uiteraard moeten de eindgebruikers hier niet vergeten worden. Een goede en degelijke bewustwording is dan ook belangrijk, dit in combinatie met een regelmatige herhaling van de boodschap.
Alleen dan is en blijft de cirkel gesloten en uw bedrijfsinformatie daar waar het hoort. Uit de handen van cybercriminelen.

Dankwoord

Dit whitepaper is mede tot stand gekomen dankzij de waardevolle input van onze docent Henk Buddingh.