6 potentiële datarampen bij de beveiliging van Office 365

6 potentiële datarampen bij de beveiliging van Office 365

Zwakke plekken in de beveiliging van Office 365 – gegevensbescherming en gegevensinbreuken

Organisaties die nog niet zo lang met Office 365 werken, weten vaak niet op welke punten de beveiliging van O365 kwetsbaar is. Of ze zijn zich zelfs van geen enkel gevaar bewust. Van dat gevaar merken ze ook niets, totdat het misgaat – en dan zijn de gevolgen groot.

De meer ervaren organisaties weten van de gevaren, maar niet precies waar ze zitten en wat ze eraan kunnen doen. Dit heeft soms rampzalige gevolgen. Maar liefst 71,4% van de zakelijke Office 365 gebruikers krijgt elke maand te maken met ten minste één gecompromitteerd account, zo blijkt uit een onderzoek onder 27 miljoen gebruikers bij 600 bedrijven.

Vrijwel alle organisaties hebben hun basisbeveiliging op orde, ze beschikken bijvoorbeeld over antivirussoftware en firewalls. Maar tegen Office 365-gerelateerde beveiligingsproblemen ondernemen ze niets. Ze wanen zich veilig door de basismaatregelen die ze hebben genomen. Grotere organisaties kiezen vaak voor diepteverdediging om de algemene veiligheid en naleving te waarborgen en te voldoen aan regelgeving. Maar ook zij nemen geen specifieke maatregelen tegen de kwetsbaarheden van Office 365 op het gebied van veiligheid en naleving.

- En dat is Office 365-specialisten een doorn in het oog. Osterman Research vroeg IT-managers naar hun ervaringen met Office 365 en tekende de volgende zwakke plekken en kwetsbaarheden op:
- Monitoren en blokkeren van toegang via gecompromitteerde accounts – door 80% genoemd
- Audit, beheer en controle van geprivilegieerde toegang tot Office 365-applicaties – door 71% genoemd
- De mogelijkheid om het beveiligingsbeleid voor alle communicatiekanalen, binnen Office 365 én op andere platforms, centraal te beheren – door 57% genoemd

Weliswaar beschikt Office 365 zelf over een aantal beveiligingsfuncties en configuratieopties – en alle organisaties die O365 gebruiken, moeten deze ook zeker benutten. Maar veel kwetsbaarheden en problemen die door Osterman worden genoemd, worden met native of ingebouwde tools niet verholpen.

CoreView-oplossingen hebben gelukkig wel een antwoord op alle problemen die Osterman aankaart – ze gaan zelfs verder dan dat. CoreView beheert ruim 2 miljoen Office 365-licenties en weet precies waar de zwakke punten en problemen zitten, hoe dreigingen kunnen worden geneutraliseerd en hoe naleving

kan worden bereikt. In deze paper bespreken we zes zwakke plekken van Office 365 op het gebied van gegevensbescherming en gegevensinbreuken, en hoe de gevolgen daarvan kunnen worden beperkt.

1. ZWAKKE PLEK: GEVOELIGE BESTANDEN WORDEN EXTERN GEDEELD

Met de eigen beveiliging van Office 365 is het vrijwel onmogelijk om het delen van gevoelige, vertrouwelijke bestanden te onderscheppen. Een IT-afdeling kan alerts op basis van bestand of gebruiker instellen, waarmee de IT-afdeling of een groep gebruikers op de hoogte kan worden gesteld, maar die aanpak is verre van effectief. Een IT-afdeling ontvangt per dag al duizenden alerts: in die drukte vallen extra alerts nauwelijks op.

CoreView zorgt ervoor dat er meteen een werkstroom wordt opgestart zodra bijvoorbeeld een gebruiker van de verkoopafdeling een bestand deelt met een externe gebruiker (dankzij de unieke uitgebreide auditlog van CoreView kunnen gebruikers worden geïdentificeerd op basis van locatie of afdeling). Als onderdeel van deze workflow ontvangen de gebruiker die het bestand deelt, diens leidinggevende en de externe gebruiker allen een waarschuwing dat deze activiteit is geregistreerd en dat alle volgende activiteiten rondom het betreffende bestand worden gecontroleerd. In dit geval is de IT-afdeling niet eens betrokken. De verantwoordelijkheid wordt gedeeld door alle betrokken actoren, wat de veiligheid vergroot.

Een specifieke zwakke plek en veiligheidsrisico is het delen van OneDrive met externe gebruikers, een probleem dat met CoreView eenvoudig kan worden aangepakt.

2. ZWAKKE PLEK: GEVOELIGE BESTANDEN WORDEN EXTERN GEDEELD

Voor bedrijven die zich bezighouden met productontwikkeling en research of die vooruitstrevende werkwijzen toepassen, is intellectueel eigendom ontzettend belangrijk. Concurrenten, en heel wat hackers, ook buitenlandse organisaties, zouden die kostbare informatie maar wat graag in handen krijgen.

CoreView voorkomt diefstal van intellectueel eigendom. En mocht diefstal toch nog voorkomen, dan helpt het de IT-afdeling om middels forensisch onderzoek van de diefstal uit te vinden wat er precies is gebeurd.

CoreView voorkomt diefstal van intellectueel eigendom. En mocht diefstal toch nog voorkomen, dan helpt het de IT-afdeling om middels forensisch onderzoek van de diefstal uit te vinden wat er precies is gebeurd.

Diefstal van intellectueel eigendom kan op twee manieren plaatsvinden: van buitenaf of van binnenuit. Voor CoreView zijn externe en interne dreigingen op dit vlak gelijk. Interne dreigingen worden op dezelfde manier geregistreerd als externe dreigingen, en op hetzelfde beveiligingsniveau behandeld.

Diefstal van intellectueel eigendom kan op twee manieren plaatsvinden: van buitenaf of van binnenuit. Voor CoreView zijn externe en interne dreigingen op dit vlak gelijk. Interne dreigingen worden op dezelfde manier geregistreerd als externe dreigingen, en op hetzelfde beveiligingsniveau behandeld.

Er is één specifiek CoreView-rapport dat een belangrijke rol speelt in de preventie van diefstal van intellectueel eigendom: het rapport over mislukte inlogpogingen. CoreView stelt een geografische kaart samen waarop te zien is vanaf welke locaties in de wereld wordt ingelogd. Laten we als voorbeeld een klant nemen die medewerkers heeft in Noord-Amerika en de EMEA-regio, maar niemand in Zuidoost-Azië. Inlogpogingen vanuit Zuidoost-Azië zijn voor deze klant dus duidelijk verdacht en moeten worden gesignaleerd. CoreView biedt ook langetermijnkaarten, die bijvoorbeeld mislukte inlogpogingen over een periode van 90 dagen weergeven.

"Ik hoor van beveiligingsprofessionals dat ze weten dat wordt geprobeerd in te loggen vanuit China, Indonesië, India, enzovoort," zegt Matt Smith, solution architect bij CoreView. "En dat klopt ook wel. Wat wij anders doen, is dat CoreView precies aangeeft welke accounts doelwit zijn, en niet alleen kijkt naar het netwerk, maar ook op applicatieniveau. Dankzij de unieke verrijkingsmogelijkheden van CoreView kunt u zien welke gebruikers, afdelingen of zelfs geprivilegieerde accounts doelwit van hackers zijn geweest. Plus welke maatregelen er waren genomen om die hackers te weren, zoals multifactor authenticatie of voorwaardelijke toegang. En wat uiteindelijk de reden is geweest dat de inlogpoging mislukte."

Met CoreView kan de IT-afdeling dit soort inbraakpogingen blokkeren door alleen inloggen vanaf goedgekeurde locaties toe te staan. Als een gebruikersaccount op deze manier wordt aangevallen, wordt dit door CoreView opgemerkt en onderzocht. Maar een Office 365-beheerder heeft met CoreView nog meer mogelijkheden. Zo kan hij contact opnemen met de gebruiker die doelwit was van de aanval, het werkstation vernieuwen, achterhalen welke andere apparaten door het doelwit worden gebruikt en welke licenties deze persoon op andere apparaten heeft.

Deze informatie en rapporten zijn planbaar. "Met deze rapporten creëren we dagelijkse, wekelijkse, maandelijkse en driemaandelijkse contactpunten die bijdragen aan een betere beveiliging. De dagelijkse contactpunten worden weergegeven op de CoreView beheerconsole. Een voorbeeld is malware op apparaten. De IT-afdeling kan een dagelijks rapport ontvangen over de eventuele aanwezigheid van malware op een apparaat. Naar aanleiding hiervan kunt u een aanvullend rapport opvragen dat laat zien welke bestanden de betreffende gebruiker heeft geopend sinds er malware op zijn account is gedetecteerd," legt Smith uit.

"Dankzij de unieke-blahcverrijkingsmoge-lijkheden van CoreView kunt u zien welke gebruikers, afdelingen of zelfs geprivilegieerde accounts doelwit van hackers zijn geweest. verrijkingsmogelijkheden van CoreView kunt u zien welke gebruikers, afdelingen of zelfs geprivilegieerde accounts doelwit van hackers zijn geweest.

Plus welke maatregelen er waren genomen om die hackers te weren, zoals multifactor authenticatie of voorwaardelijke toegang.

En wat uiteindelijk de reden is geweest dat de inlogpoging mislukte."

Voor een optimale bescherming tegen diefstal van intellectueel eigendom heeft de IT-afdeling rapporten nodig over onjuist toegewezen accounts, zodat een correct configuratiebeheer mogelijk is. En rapporten over mobiele apparaten die in strijd zijn met het MDM-beleid, of over afdelingsmanagers waarvoor geen 'legal hold' is ingeschakeld. "Zo gebruiken we onze database voor zowel forensische als blokkeringsdoeleinden, om u te laten zien wat er precies aan de hand is én om het aantal signalen dat bij O365-beheerders binnenkomt, te beperken tot een behapbaar volume," zegt Smith. "En constateert CoreView dat met een besmet apparaat uit ons rapport is ingelogd, dan kunt u hiervoor een auditrapport opvragen met informatie over de betreffende gebruiker en alles wat sinds de detectie van de malware door deze gebruiker is geopend."

3. ZWAKKE PLEK: VOORKOMEN VAN GEGEVENSLEKKEN EN SLECHTE DATAKWALITEIT (DLP)

Gegevenslekken zijn vergelijkbaar en overlappen op sommige punten zelfs met diefstal van intellectueel eigendom. Het verschil is dat bij gegevenslekken de gegevens niet van buitenaf, door een externe partij, worden gestolen, maar worden gelekt door iemand binnen de organisatie. Dit kan zijn met kwaadaardige bedoelingen of per ongeluk, door onachtzaamheid, een slechte configuratie of een ontoereikende beveiliging. Denk bijvoorbeeld aan een ontslagen werknemer die vertrouwelijke of zelfs schadelijke gegevens online plaatst.

Zeker voor Office 365 is dit een essentieel probleem: uit onderzoek blijkt dat 58,4% van de gevoelige informatie in de cloud is opgeslagen in Office-documenten. Wat ook een rol speelt, zijn fouten van systeembeheerders. "Er is een aanzienlijke toename van het aantal fouten als gevolg van het door systeembeheerders plaatsen van gevoelige gegevens in publieke, voor iedereen toegankelijke cloudomgevingen," concludeert het Verizon Data Breach Investigations Report 2019.

DLP-regels gelden niet voor gebruikers die voor hun werk toegang hebben tot gegevens, zoals spreadsheets voor klantaccounts. Gelukkig registreert CoreView deze toegang, zodat deze informatie kan worden geraadpleegd bij kritische gebeurtenissen, zoals wettelijke verzoeken en HR-gebeurtenissen, bijvoorbeeld als een werknemer het bedrijf verlaat.

CoreView weet waar gevoelige gegevens zich bevinden, wie ze kan inzien en wat deze personen ermee doen. "Als ik praat over beveiliging, laat ik als eerste de landingspagina in het CoreView-dashboard zien, waarbij ik uitleg hoe we beveiligingsgerelateerde gegevens verzamelen. De echte kracht van het platform zit hem niet in de mooie grafieken en tabellen, maar in de unieke manier waarop we beveiligingsgegevens verzamelen, zoals niemand anders dat kan," zegt Smith. "We

DLP-regels gelden niet voor gebruikers die voor hun werk toegang hebben tot gegevens, zoals spreadsheets voor klantaccounts. Gelukkig registreert CoreView deze toegang, zodat deze informatie kan worden geraadpleegd bij kritische gebeurtenissen, zoals wettelijke verzoeken en HR-gebeurtenissen, bijvoorbeeld als een werknemer het bedrijf verlaat.

Met CoreView is de IT-afdeling op de hoogte van elke transactie binnen het Microsoft-platform, en van de configuratiegegevens. Dat betekent dat de IT-afdeling weet wanneer een document is aangemaakt, wanneer het is gekopieerd naar Office 365, wanneer het is geopend en wanneer het is gewijzigd.

maken via elke beschikbare API verbinding met Office 365. Zo is er een Graph API, bekend voor de meeste IT-professionals die met Office 365 werken. We gebruiken ook de auditlogmeldingen van Microsoft, waardoor we dezelfde gegevens kunnen verzamelen en analyseren als Splunk en het nieuwe Microsoft Azure Sentinel."

CoreView duikt in de API's van alle applicaties. Exchange heeft bijvoorbeeld Exchange-webservices. Skype heeft activity logs en SharePoint en Teams hebben ook hun eigen API's. En tot slot ontvangt CoreView gegevens uit Azure Active Directory (Azure AD). Al deze gegevens worden extern opgeslagen in een Microsoft Azure-abonnement. "De gegevens verlaten op geen enkel moment het Microsoft-platform. U verplaatst ze niet over het internet of naar desktopcomputers en verstuurt ze niet naar Amazon Web Services. Alles blijft binnen Azure. Omdat zowel Office 365 als CoreView op Azure draait, blijven de gegevens binnen de datacenters van Microsoft.

U kunt gegevens opslaan zo lang u wilt en ze verrijken op het moment dat ze binnenkomen. Omdat u gegevens uit al deze verschillende bronnen ontvangt, kunt u via het auditlog een diepgaand beeld krijgen. Zo weet u bijvoorbeeld niet alleen dat het een bepaalde gebruiker was die een bestand op OneDrive heeft geopend, maar heeft u inzicht in het volledige pad dat hij naar dat bestand heeft afgelegd. U weet hoe hij het heeft geopend, met welk mobiel apparaat, en welk MDM-beleid er op zijn mobiele apparaat van toepassing was. En u weet precies wie de betreffende gebruiker is: afdeling, land, bedrijf, evenals adminrollen in de tenant. Plus wanneer en vanaf welk IP-adres hij het bestand heeft geopend," vertelt Smith.

Met CoreView is de IT-afdeling op de hoogte van elke transactie binnen het Microsoft-platform, en van de configuratiegegevens. Dat betekent dat de IT-afdeling weet wanneer een document is aangemaakt, wanneer het is gekopieerd naar Office 365, wanneer het is geopend en wanneer het is gewijzigd. CoreView slaat al die informatie extern op in een onveranderbare database, waarin gegevens niet kunnen worden gewijzigd. In principe is dit de volledige blockchain-informatie voor elke transactie in Office 365.

4. ZWAKKE PLEK: GEGEVENSINBREUKEN ZIJN NIET TE VOORKOMEN

De beste uitleg van hoe groot de schade van gegevensinbreuken kunnen zijn, is te vinden in het rapport 'Cost of a Data Breach' van Ponemon en IBM. Wat kost een verloren bestand? Volgens het rapport 128 euro. Een gegevensinbreuk kost een bedrijf gemiddeld 3,3 miljoen euro. Het duurt gemiddeld 191 dagen voordat een gegevensinbreuk wordt ontdekt.

De beste verdediging is om gegevensinbreuken niet te herstellen maar te voorkomen. Het vinden en vasthouden van betrouwbaar IT-talent is een cruciaal onderdeel van een goede beveiliging. "Uit een IT-onderzoek blijkt dat meer dan 50% van de gegevensinbreuken plaatsvindt doordat dingen niet goed zijn geconfigureerd. De fouten zijn te herleiden tot die twee arme IT-medewerkers in de kelder die al het werk moeten doen. Het alternatief is om wereldwijde beheerdersrechten te geven aan 167 mensen en maar te hopen dat ze niet op de verkeerde knop drukken," zegt Smith.

Om inbreuken te voorkomen, neemt CoreView als basis de signalen van Microsoft, om deze vervolgens aanzienlijk te verrijken. Zo biedt CoreView een wereldkaart met inlogpogingen, waarop niet alleen zichtbaar is vanaf welk IP-adres hackers een vergeefse aanval hebben gelanceerd, maar ook op welke accounts ze het voorzien hadden. Ook laat het zien of multifactor authenticatie deel uitmaakte van de configuratie en of bij een specifieke aanval voorwaardelijke toegangsmaatregelen effectief zijn geweest. En tot slot geeft het een gedetailleerd overzicht van het eindresultaat van de inlogpoging.

5. ZWAKKE PLEK: HET IS NIET TE ACHTERHALEN WAAROM EEN GEGEVENSINBREUK HEEFT PLAATSGEVONDEN

Eerlijk is eerlijk. Hoeveel obstakels we ook opwerpen, soms komen inbreuken toch voor. En de meeste IT-organisaties ontdekken zo'n inbreuk pas maanden of zelfs meer dan een jaar later. Hoe kunt u dan nog achterhalen hoe en wanneer de inbreuk precies heeft plaatsgevonden?

Het antwoord is forensisch onderzoek op basis van loggegevens die over de lange termijn worden opgeslagen en bewaard, zodat u een goede beveiligingscontrole kunt uitvoeren. Zo achterhaalt u wat er is gebeurd, zodat u lopende schade kunt beperken. En door de bron op te sporen, voorkomt u dat het nog eens gebeurt.

En dat is precies waar het bij de controlemogelijkheden van CoreView om draait. "Als ik niet weet wat er aan de hand is, hoe kan ik dan ooit het probleem onderzoeken? Eén van de belangrijkste pijlers van beveiliging is 'ken uzelf'," aldus Smith van CoreView. "Microsoft bewaart applicatiegegevens 30 dagen en maakte onlangs bekend deze termijn te zullen verlengen tot één jaar, maar alleen voor E5-licenties. Hoe kan ik effectief handelen als ik niet eens kan zeggen wie er een jaar geleden heeft ingelogd?" Het antwoord: de IT-afdeling moet voor de hele duur van het gebruik van het O365-platform een administratie over inlogpogingen bijhouden.

Als er zich een gegevensinbreuk voordoet, of een infectie met malware, dan is het belangrijk dat u daar alles over te weten komt. En dat is waar basisbeveiligingsprogramma's tekortschieten. "Kijken we naar de forensische kant, dan kan antivirussoftware u vertellen dat de pc van een specifieke gebruiker op maandag een virus had. Er is echter geen antivirusplatform ter wereld dat precies laat zien wat die gebruiker allemaal heeft gedaan sinds hij dat virus heeft opgelopen," zegt Smith.

Een gegevensinbreuk kost een bedrijf gemiddeld 3,3 miljoen euro. Het duurt gemiddeld 191 dagen voordat een gegevensinbreuk wordt ontdekt.

Een beheerder met CoreView kan via 'bestandstoegang' alle bestanden zien die na de gegevensinbreuk of de malwareaanval zijn geopend, evenals de namen van die bestanden en de paden ernaartoe.

CoreView daarentegen komt meteen tot de kern van de zaak. Een beheerder met CoreView kan via 'bestandstoegang' alle bestanden zien die na de gegevensinbreuk of de malwareaanval zijn geopend, evenals de namen van die bestanden en de paden ernaartoe. "CoreView kan deze rapporten ook opslaan. De volgende stap is om te achterhalen waar de malware zich naartoe heeft verspreid. U kunt bijvoorbeeld precies zien welke mogelijk besmette bestanden binnen het OneDrive-platform door mensen zijn geopend. Deze mensen kunnen besmet zijn met malware, omdat het door hen geopende bestand in aanraking is geweest met één specifieke gebruiker die al met malware besmet was. Tot slot kan een admin nog kijken naar OneDrive-rapporten en vervolgens naar externe uitnodigingen," vertelt Smith.

6. ZWAKKE PLEK: GEHACKTE E-MAIL

E-mail is de meest voorkomende manier waarop hackers in uw systemen inbreken. Gebrekkig beveiligde postvakken en een slechte omgang met e-mail vormen misschien wel de grootste bedreiging voor uw beveiliging. Postvakken worden kwetsbaar door onveilige, zwakke wachtwoorden die nooit worden gewijzigd, en het ontbreken van multifactor authenticatie (MFA).

Het monitoren van gedrag van werknemers, zoals de manier waarop mensen omgaan met hun e-mail, kan risicogedrag blootleggen en bedrijfskritische gegevens proactief beschermen. Door risicovol gedrag, zoals het automatisch doorsturen naar externe e-mailadressen, te voorkomen en door toegangsrechten tot e-mail van anderen te beperken, kan de verspreiding van malware en het lekken van gegevens via e-mails worden voorkomen. Verder werkt een beter bewustzijn van ongebruikelijke e-mailactiviteit preventief tegen gerichte spam of menselijke misleidingstactieken die deel uitmaken van de huidige cyberdreigingen.

Belangrijke regels voor e-mailbeveiliging draaien om toegangsrechten. CoreView signaleert gebruikersaccounts met afwijkende rechten, zoals toegangsrechten voor meer dan vijf postvakken van andere gebruikers, toegang tot postvakken van andere afdelingen, uitgeschakelde accounts die toegang hebben tot andere postvakken, enzovoort. Het gaat hierbij niet om gedeelde postvakken of postvakken van een ruimte of team, maar om postvakaccounts van individuele gebruikers. Gebruikers die dit soort uitgebreide toegangsrechten hebben tot postvakken van andere gebruikers, moeten worden onderzocht om er zeker van te zijn dat deze rechten worden gebruikt voor aanvaardbare bedrijfsdoeleinden.

Spam en malware zijn bekende bedreigingen voor uw e-mailbeveiliging. CoreView ontdekt wanneer malware vanuit uw organisatie via e-mail wordt verzonden, en kan de verspreiding tot in het kleinste detail traceren.

Zeven manieren om te weten dat uw Office 365-beveiliging op orde is

1. U kunt binnen enkele seconden een logboek maken voor elke beheerhandeling binnen Office 365 sinds de ingebruikname van het platform. (Een bankmedewerker heeft tenslotte ook een transactieregister waarin elke storting en opname is terug te vinden. Waarom zouden we dit voor O365 dan niet hebben?)

2. Als een werknemer de organisatie verlaat, voert de IT-afdeling altijd een auditrapport uit voor elk bestand dat de werknemer in de afgelopen x dagen heeft geopend.

3. Als er op een apparaat van een werknemer malware of gelekte gebruikersgegevens worden aangetroffen, controleert de IT-afdeling altijd alle handelingen die door die gebruiker in O365 zijn verricht sinds de ontdekking van de malware, waarbij ook wordt gecontroleerd op Trojaanse paarden/ransomware/configuratiewijzigingen.

4. De IT-afdeling weet niet alleen waar aanvallen in O365 vandaan komen, maar ook op wie ze gericht zijn, hoe de doelwitten geconfigureerd zijn en welke acties zijn ondernomen tegen geslaagde aanvallen.

5. De IT-afdeling hanteert een volledig operationeel toegangsmodel op basis van minste rechten voor Office 365. En de IT-afdeling kan precies beschrijven welke functies actoren kunnen uitvoeren, en wat de reikwijdte daarbij is.

6. De IT-afdeling kan het gewenste configuratiebeheer (rapporteren/waarschuwen/oplossen) binnen Office 365 uitvoeren op account- of apparaatniveau.

7. De IT-afdeling weet hoe de beveiligingsmentaliteit van zijn O365-configuratie zich verhoudt tot die van vergelijkbare organisaties en hoe zijn beveiligingsscore zich in de loop van de tijd heeft ontwikkeld.

Ontdek hoe CoreView uw omgeving beschermt en meer

Aan de slag met CoreView – gratis

Onze nieuwe CoreDiscovery-oplossing helpt beheerders inzicht te krijgen in hun O365-tenant en ondersteunt bij beheer, beveiliging en de bevordering van acceptatie van O365-apps. Lees meer op de CoreDiscovery productpagina: https://www.coreview.com/corediscovery/.

Vraag uw gratis software aan op de CoreDiscovery aanmeldpagina: https://www.coreview.com/core-discovery-sign-up/.

Meer weten over hoe CoreView u kan behoeden voor onnodige uitgaven voor licenties, onbenutte

applicaties of een onjuiste omgang met beveiliging en configuraties? Onze gratis CoreView Office 365 Health Check brengt al uw Office 365-problemen in kaart. Vraag een Office 365 Health Check aan en wij stellen voor u een uitgebreid 20 pagina's tellend rapport samen waarmee u al uw problemen met Office 365 oplost.

Nog niet toe aan een uitgebreid rapport op maat? U kunt wel alvast eens een Health Check-voorbeeldrapport bekijken.

Zelf zien hoe CoreView Office 365 problemen oplost en de beveiliging verbetert? Vraag een demo aan.

Vraag een Office 365 Health Check aan en wij stellen voor u een uitgebreid 20 pagina's tellend rapport samen waarmee u al uw problemen met Office 365 oplost.