Microsoft Office 365

Microsoft Office 365

De Corona-crisis raakt ons allemaal. In ons privéleven, maar ook zakelijk. In plaats van op kantoor, ontmoeten we elkaar digitaal vanuit onze huiskamers, keukens, werkkamers, enzovoorts. We videobellen met verjaardagen, om in contact te blijven, voor de wekelijkse teamvergaderingen en zelfs bij raadsvergaderingen. Het werken op afstand blijkt niet alleen heel handig, het is in deze tijd een noodzakelijke voorwaarde om de democratie te laten functioneren.

Met Microsoft 365 geeft medewerkers en partners de mogelijkheid om op afstand te werken en contact te houden. Lees bijvoorbeeld het klantverhaal van de gemeente Beek hoe zij Microsoft Teams in combinatie met iBabs gebruiken voor de digitale raadsvergaderingen en digitale besluitvorming doen via Microsoft Forms. Of het klantverhaal van de Provincie Limburg die met de intrede van Corona haar medewerkers faciliteert in het digitaal samenwerken en vergaderen met behulp van Microsoft Teams.

Centric is bezig om de mogelijkheden van Office 365 verder te integreren in haar applicaties. Zo kun je documenten vanuit Centric-applicaties al jaren bewerken in de Office-applicaties. Ook de Office-applicaties die onderdeel zijn van Office 365. In het komende jaar breiden wij dit uit met de mogelijkheid om vanuit SaaS-applicaties documenten ook te lezen én te bewerken met de Office Online apps van Microsoft 365. Zo werken medewerkers volledig in SaaS met alle applicaties die zij thuis ook gebruiken. In 2021 gaan wij onderzoeken welke verdere integratiemogelijkheden er vanuit onze applicaties met Office 365 zijn, deze gaan wij dan in de daaropvolgende jaren implementeren.

Het thuiswerken heeft ook minder fijne kanten. Naast moeizamere sociale contacten, misbruiken criminelen de maatregelen rondom corona om malware te plaatsen of via phishing gegevens buit te maken. In de afgelopen jaren zijn helaas ook gemeenten het slachtoffer geworden van hacks en ransomware. Een ingrijpende gebeurtenis die een organisatie zelfs weken kan platleggen. Nu mensen veel thuiswerken, komt er een aanvalsvector bij. Want hebben mensen thuis de beveiliging net zo goed op orde als dat je dat op kantoor hebt? Reden genoeg tot hoofdpijn bij de afdeling ICT.

Vanzelfsprekend ondersteunt Microsoft 365 Multi-Factor Authentication zodat ongeautoriseerde personen geen toegang krijgen tot het account van de medewerker en de data in Microsoft 365, ook als ze het wachtwoord van een medewerker weten te kraken. Daarnaast is er de applicatie Intune, waarmee je de beveiligingsinstellingen voor mobiele apparaten en werkplekken centraal beheert. Hiermee zorg je dat zowel de apparaten die jouw organisatie uitgeeft, als de privé-apparaten zijn beschermd. (Intune is afhankelijk van het afgenomen Microsoft 365-abonnement.)

Om incidenten te voorkomen en eventuele schade te beperken, heb je een robuuste oplossing nodig die helpt om informatie te beschermen. Microsoft 365 biedt Data Loss Prevention en Advanced eDiscovery zodat je geautomatiseerd datalekken voorkomt én audits kan uitvoeren over alle documenten en communicatie. Slaat iemand bijvoorbeeld een Excel-document met persoonsgegevens op? Dan herkent het systeem dit en zorgt het systeem dat dit document niet gedeeld kan worden met externen.

En mocht een machine geïnfecteerd worden met ransomware, dan kan Microsoft 365 met OneDrive dit herkennen, de infectie opruimen én de versleutelde bestanden automatisch herstellen. Zo voorkom je dat belangrijke informatie verloren gaat en kunnen medewerkers vrijwel meteen doorwerken.