Security Awareness

Houd controle over je gegevens

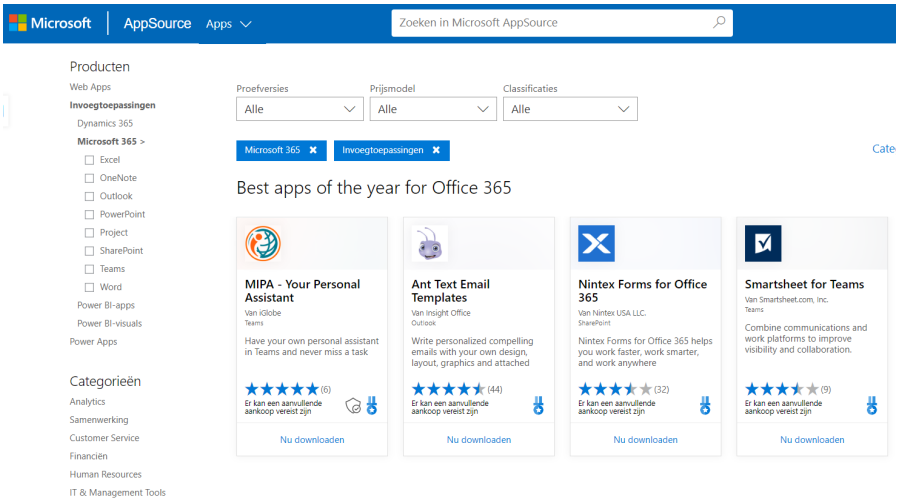
Je hebt vast wel eens een ‘sociale’ app geïnstalleerd op je werktelefoon. Handige hulpmiddeltjes die je leven een stuk aangenamer maken. WhatsApp, Facebook, Instagram, Spotify; wie kent de apps niet en wie heeft ze niet geïnstalleerd op zijn telefoon? Een hoop van deze apps toegang willen tot andere functionaliteiten. Deel je misschien niet teveel informatie met deze apps? Moet alles en iedereen maar toegang hebben tot je camera, adresboek of je locatiegegevens?

Nu veel bedrijven gebruik (gaan) maken van Microsoft 365[1] komt hier al snel hetzelfde om de hoek kijken. Het Microsoft 365-pakket kan je leven een stuk aangenamer maken. Het is mogelijk om applicaties te koppelen aan je Microsoft 365-account, maar ook hiervoor geldt: *houd controle over je gegevens*.

Onlangs heeft Microsoft een waarschuwing uitgegeven dat toestemming van apps die je gebruikt binnen Office365 misschien wel ongewenst gevoelige gegevens laat delen. Een extra signaal is dan ook op zijn plaats.

Ga verstandig om met toestemming geven!

Binnen Office365 is het mogelijk om applicaties van derden te installeren. Vaak mooie stukjes gereedschap die het werken met Office365 een stuk makkelijker maken en uitbreiding geven aan de functionaliteit.



(voorbeeld van applicaties die worden aangeboden voor Office365)

---

[1] de oude naam van dit product is Office365

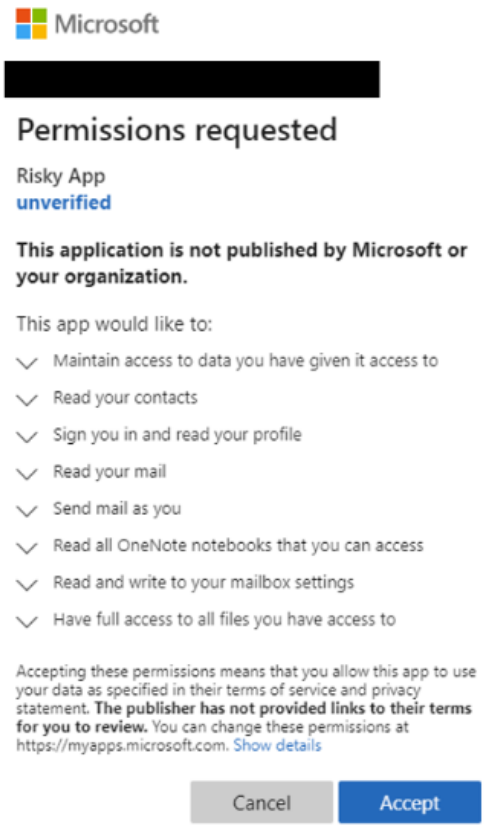
Deze applicaties hebben toestemming nodig om jouw gegevens te mogen gebruiken. Ze willen bijvoorbeeld (volledige) toegang tot je mailbox, je adresboek, je bestanden die je hebt opgeslagen in OneDrive of de notities die je hebt gemaakt in OneNote. Deze toestemming geeft je, al dan niet bewust, zelf.

Het risico van toestemming geven voor applicaties

Als je gebruikmaakt van Office365 dan heb je waarschijnlijk als eerste maatregel om je account en gegevens te beschermen Multifactor Authenticatie[2] (MFA) ingesteld. MFA wordt ook wel “sterke authenticatie” of “tweetraps verificatie” genoemd. Maak je hier nog geen gebruik van, stel dit dan als eerste in of laat je beheerder deze mogelijkheid activeren. Deze methode zorgt voor een extra bescherming die, helaas, bittere noodzaak is.

Als extra beschermingsmaatregel moet je verstandig omgaan met het geven van toestemmingen voor toegang tot je Office365-omgeving.

De mogelijkheid om Office365 verder uit te breiden met kent ook een risco. Cybercriminelen misbruiken deze mogelijkheid door malafide apps te ontwikkelen en jou te verleiden om deze te installeren. Bij de installatie van het pakket zijn de criminelen niet op zoek naar je naam en wachtwoord, maar naar je toestemming om gebruik te mogen maken van jouw gegevens.



Voorbeeld van “Risky App” die heel veel toestemming vraagt.

[2] Multi-Factor Authenticatie is een proces waarbij een gebruiker wordt gevraagd tijdens het aanmeldingsproces om een extra vorm van identificatie, zoals het invoeren van een code op hun telefoon of doormiddel van een vingerafdruk scan.

Microsoft schrijft hier zelf het volgende over: “Veel apps van derden die door zakelijke gebruikers kunnen worden geïnstalleerd, vragen om toestemming voor toegang tot gebruikersinformatie- en-gegevens en zich aan te melden namens de gebruiker in andere Cloud-apps. Wanneer gebruikers deze apps installeren, klikken ze vaak op accepteren zonder de details in de prompt te bekijken, met inbegrip van het verlenen van machtigingen aan de app. Het accepteren van app-machtigingen van derden is een potentieel beveiligingsrisico.”[3]

Een waarschuwing van Microsoft die je zeker niet in de wind moet slaan! Dus nogmaals:

Ga verstandig om met toestemming geven aan apps van derden!

Tips voor beheerders

Ben je beheerder van een Office365-omgeving? Dan heeft Microsoft diverse tips en trucs gedeeld om misbruik van malafide applicaties te voorkomen.

Deze, vaak Engelstalige, informatie is zeker de moeite waard om door te nemen. De tips maken je Office365-omgeving een stuk veiliger en risico’s op een digitale inbraak, ransomware en dataverlies een stuk kleiner.

Algemene informatie: https://www.microsoft.com/security/blog/2020/07/08/protecting-remote-workforce-application-attacks-consent-phishing/

Technische achtergronden: https://docs.microsoft.com/nl-nl/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide

OAuth-apps achtergrond: https://docs.microsoft.com/nl-nl/cloud-app-security/investigate-risky-oauth

Centraal beheren van toestemmingen voor apps: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-consent-requests

[3] https://docs.microsoft.com/nl-nl/cloud-app-security/investigate-risky-oauth