Veilig e-mailen met Office 365 of Google Workspace

Voor het uitwisselen van persoonsgegevens heeft delen via het up- of downloaden naar een beveiligd platform altijd de voorkeur boven e-mailen. Mocht er toch geen andere optie zijn? Dan moet je zorgen dat je veilig mailt. In dit document beschrijven hoe we je veilig kunt e-mailen met Office 365 of Google Workspace en wat je daarvoor moet doen.

Zowel Microsoft als Google biedt de mogelijkheid om e-mails en attachments versleuteld te versturen binnen Office 365 en Google Workspace. De mail wordt door de verzender versleuteld en kan alleen door de ontvanger gelezen worden, ongeacht welk e-mailsysteem de ontvanger gebruikt. De software van de ontvanger moet wel in staat zijn om te ontsleutelen.

Office 365

E-mailberichten vanuit Office 365 kunnen op drie manieren worden versleuteld.
- Via de open standaard S/MIME
- Via Office 365 Mail Encryption (OME)
- Via Microsoft Purview Message Encryption

OME en Purview zijn alleen mogelijk met een Office 365 A3-licentie. Dit biedt extra functionaliteit in de admin-omgeving van Office 365, zoals het aangeven voor wie deze versleuteling aan staat, voor welke ontvangers, of zelfs voor wat voor inhoud.

Google Workspace

E-mails kunnen ook versleuteld worden via Google Workspace. Hiervoor wordt het S/MIME protocol gebruikt. De verzender kan dan bepalen welke mails worden versleuteld of dat ze altijd versleuteld moeten worden verzonden. Hoe het moet worden ingesteld in Google Workspace lees je op de supportpagina van Google.

S/MIME versleuteling

S/MIME versleuteling zorgt voor end-to-end versleuteling, waardoor een onderschepper de mail niet kan lezen. S/MIME versleuteling moet ondersteund worden door het emailprogramma van zowel de verzender als de ontvanger, maar ze hoeven niet hetzelfde programma te gebruiken. Microsoft Outlook, Apple Mail en Mozilla Thunderbird zijn voorbeelden van e-mailprogramma's die S/MIME ondersteunen.

Versleuteld e-mailen en firewalls

Het nadeel aan versleuteld e-mailen is dat een firewall ook niet aan malware-detectie kan doen, omdat het deze berichten ook niet kan ontsleutelen. Dit wordt ondervangen door de e-maildiensten zelf op malware te laten scannen. Het is daarom belangrijk om real-time anti-malware scanning op devices up-to-date te houden. Dit voorkomt ook dat op netwerken buiten school malware via een device kan worden binnengehaald. Je kunt het zelf uitrollen op de door school beheerde devices of leerlingen en personeel erop wijzen in het geval als er sprake is van Bring Your Own Device (BYOD).