GDPR compliance, binnen én buiten de cloud

De komst van de General Data Protection Regulation (GDPR) op 25 mei 2018 roept bij menig ICT-manager, CEO en security officer vraagtekens op. Hoe gaat u aan de strenge Europese privacyregels voldoen? Met Azure Information Protection (AIP) beveiligt u al uw documenten slim en met de mogelijkheid om deze te traceren.

Informatiebeveiliging in orde gebracht met Azure Information Protection

Al langere tijd staat informatiebeveiliging vanwege toenemende hack- en lekgevaar bij leidinggevenden hoog op de agenda. Met de introductie van de GDPR nemen zorgen toe rond deugdelijke afscherming van wat niet voor de ogen van derden is bestemd. De GDPR vraagt van bedrijven dat informatie niet alleen afdoende wordt beschermd tegen buitenstaanders, maar ook tegen onbevoegde medewerkers van de eigen organisatie. Handhaving op zulke vereisten vraagt om functionaliteit als labeling en tracking, zowel binnen als buiten uw netwerk. Gebruikmaken van antivirus, firewall en/of BitLocker is dus niet voldoende. Een meerderheid van Nederlandse bedrijven weet op dit moment niet zeker of het eigen informatiebeleid aan de GDPR voldoet, zo blijkt uit recent Citrix onderzoek.

Documenten altijd en overal beschermd

Azure Information Protection, onderdeel van Microsoft Enterprise Mobility + Security (EMS), helpt bedrijven de data in kaart te brengen die aan GDPR-regels moet gaan voldoen en 'volgens het boekje' de GDPR-richtlijnen na te leven. Zoals de Azure-naam al prijsgeeft, draait deze tooling in de cloud. Hoewel het wel een voorwaarde is om gebruik te maken van een identiteit van Azure Active Directory, kunnen de data die u wilt beveiligen zich ook op lokale computers en/of fileservers bevinden. Het dus zeker geen 'cloud-only' manier om aan de GDPR te voldoen.

AIP werkt met templates die bepalen welke gebruikers of groepen recht krijgen op een document. Labeling zorgt ervoor dat een document niet bewerkt of gemaild mag worden. Of alleen bekeken mag worden door managers van een bepaalde afdeling. Deze classificatie kan niet zomaar aangepast worden. AIP versleutelt bestanden voor de gebruiker onzichtbaar volgens veilige 128 of 256 bits AES-algoritmen en laat organisaties meer dan 40 policies op documenten instellen, waaronder ook het (geautomatiseerd) intrekken van documenten buiten de firewall.

Alle controle in eigen handen

Via een portal kunnen beheerders zien waar (gevoelige) documenten staan en wie deze heeft geopend. Mocht een onbevoegde een beschermd document proberen te openen, dan toont een melding waarom de toegang niet wordt verleend. Externen als inhuurkrachten of partners zijn onderdeel van de in te stellen policies. Zij kunnen met documenten aan de slag waarvoor u en gerechtigde medewerkers groen licht geven. Ook als deze zich op een mobiel device als een Android-toestel of iPhone bevinden en ook als het bestanden zijn buiten de Microsoft (Office) familie. AIP ondersteunt namelijk ook pakketten als CAD, Illustrator en Photoshop.

De werking van Azure Information Protection in een notendop