Digitaal archief

Tekst en beeld Wim A.B.

Werken met digitale documenten vraagt evenveel aandacht voor opslaan en beheren als het werken met papieren varianten. In dit artikel wordt aandacht besteed aan onderwerpen die betrekking hebben op de manier waarop digitale documenten voor korte en lange termijn worden bewaard. Er worden enkele diensten besproken die dit opslaan ondersteunen. De menselijke factor in gebruik van digitaal werken is, en blijft, de grootste risicofactor waar het gaat om de veiligheid van verwerken en opslaan.

Van papier naar digitaal

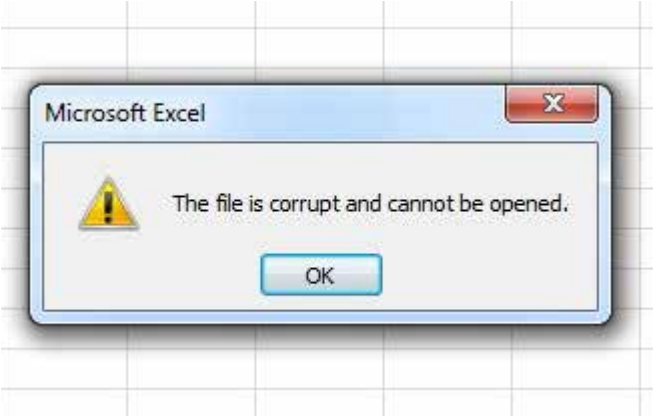
Sinds 1980 is de Nederlandse samenleving veranderd. Wie toen in de spits een foto nam van reizigers op een treinstation zag wachtende mensen met een krant of boek. Zij vullen de tijd van het wachten in met lezen. Wie vandaag op het station dezelfde foto neemt ziet nog steeds mensen lezen, maar dan op een smartphone, tablet of e-reader. Het lezen is gebleven maar de middelen zijn veranderd. De invloed die digitalisering op onze samenleving heeft is ongeëvenaard. Niet alleen de middelen zijn veranderd maar ook de beschikbaarheid van informatie, in welke vorm dan ook, is toegenomen en complex geworden. Om bij het treinstation te blijven; wie wil weten hoeveel vertraging een trein heeft kijkt naar de digitale vertrekborden of raadpleegt zijn NS-app op de smartphone. Ook de hoofdconducteur heeft zijn kniptang ingeruild voor een digitale tablet met scanner.

Het voorbeeld laat zien dat de veranderingen vanzelfsprekend doorgaan. Dit artikel gaat daarom uit van de gedachte dat niet een terugblik naar de ‘veilige’ en ‘overzichtelijke’ oude wereld de oplossing is voor een bespreking maar dat een vooruitblik naar een ‘overzichtelijke’ en ‘slimme’ wereld de manier is om digitalisering te bespreken. Het gebruiken en bewaren van informatie is van alle tijden. De hoeveelheid informatie waarover mensen kunnen beschikken is gigantisch. Het is meer de vraag hoe slim mensen deze informatie beschikbaar maken.
We kennen de uitspraak “papier zal nooit verdwijnen”. Het is zelfs een feit dat er in het digitale tijdperk meer papier wordt gebruikt dan ooit tevoren. Maar er was een tijd zonder papier. Informatie was beschikbaar in verhalen en liederen. Wie vooruit kijkt zou dan ook mogen verwachten dat de opslag van informatie in de toekomst nog anders wordt vorm gegeven dan nu het geval is. Wat blijft, we willen dingen bewaren onafhankelijk van de bedenkers en schrijvers. Opslaan is dus van alle tijden.

Wat is eigenlijk digitale veiligheid

Feiten en fictie liggen dicht bij elkaar. Waar je mee vertrouwd bent geraakt voelt goed en daarmee voelt het veilig. Die veiligheid hangt samen met de voorspelbaarheid van de dingen die je weet. De papieren archieven zijn een zeker gevoel. Je kunt het vastpakken. Men is vertrouwd geraakt met conserveren van papier en perkament. In archieven liggen soms brieven en oorkondes van honderden jaren oud. Veilig achter glas, in het donker en in een brandvrije ruimte. We weten welke bedreigingen er zijn waardoor papier kan vergaan. Dat is met een digitaal bestand wel anders.

Wanneer u en ik op onze computer een tekstdocument maken verschijnt dit op een beeldscherm. We zien de letters, en afhankelijk van het programma of de applicatie ziet het eruit of we op een papier schrijven. Maar nog steeds maken veel mensen een uitdraai op een printer om even na te lezen of het eruit ziet zoals gewenst. We willen het vast kunnen houden, met een pen verbeteringen aanbrengen, onderstrepen etc. etc. Maar wanneer we het opslaan, stopt voor velen van ons de kennis wat we eigenlijk bewaren. Dat is prima als we maar weten dat het terug te vinden is en opnieuw gelezen of gebruikt kan worden. Daar begint het onbekende en daarmee onze zoektocht naar veiligheid. Het grootste gevaar van een digitaal document is dat de codes waaruit een document is opgebouwd ‘in de war raken’ en verdwijnen. Het document wordt onbruikbaar. Vergelijk dit met het vergaan van papier waardoor de tekst onleesbaar wordt. Een beeld van de oude tijd geplot op onze hedendaagse digitale werkelijkheid.
Dit is het eerste belangrijke onderdeel van digitale veiligheid: de codes waaruit documenten zijn opgebouwd moeten leesbaar blijven in de toekomst.



Een tweede onderdeel van veiligheid is het programma waarmee de tekst is geschreven. Soms ontvangt u een bestand wat u niet kunt lezen. We gaan ervan uit dat het bestand de goede codes heeft maar het programma waarmee u werkt is niet geschikt om de codes om te zetten in leesbare tekst. Sommigen die al lang van een computer gebruik maken herkennen dit omdat de teksten die gemaakt zijn met WordPerfect (één van de meest bekende tekstverwerkers uit het begin van deze eeuw) door huidige tekstverwerkers, bijvoorbeeld MS Word, eerst moeten worden 'vertaald' voordat ze weer leesbaar worden. Met teksten lukt dat vaak nog wel. Wie met rekenschema's of dataverzamelingen werkt heeft veel meer problemen. Deze programma's zijn vaker veranderd en gebruiken heel andere coderingen. Je kunt dan de bestanden prima bewaren maar zonder het juiste programma is de informatie onleesbaar geworden.

Een heel apart verhaal van dit tweede onderdeel is wanneer u wisselt van besturingssysteem op uw computer. Wie de software van Apple gebruikt weet dat teksten niet automatisch gelezen kunnen worden op een computer met Windows en omgekeerd. Natuurlijk zijn er aanpassingen mogelijk maar vaak is de tekst heel anders dan oorspronkelijk was bedoeld.

Een derde onderdeel van digitale veiligheid is het bewust veranderen van de codes van bestanden. Dit gebeurt door besmetting met computervirussen of hackers die onze computers binnendringen. De reden of bedoeling van dit vandalisme valt buiten de scope van dit artikel maar de bestanden zijn wel onbereikbaar geworden of verdwenen.
Voor dit laatste onderdeel is veel aandacht in de media. De eerste twee worden nauwelijks benoemd maar zorgen juist voor veel problemen in de toekomst. Bij digitaal archiveren zijn alle drie onderdelen van even groot belang.

Vertrouwen in een digitale wereld

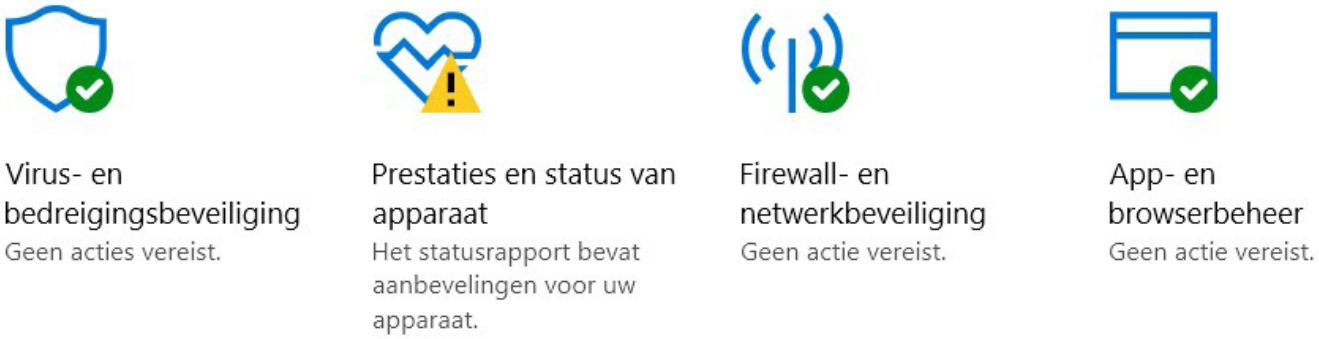
Opslaan is een vanzelfsprekend woord geworden. De beleving of iets veilig is opgeslagen gaat gelijk op met een gevoel en mening over veiligheid. Een tekst wordt opgeslagen op een computer, vaak op de harde schijf in een computer. Voor de mensen die al lang met een computer werken was er een tijd dat zij hun bestanden bewaarden op een diskette. Vandaag imiteren gebruikers van computers dit diskette gedrag door 'data sticks' te gebruiken, beter bekend als USB sticks. In ieder geval werden bestanden opgeslagen op een tastbaar medium dat je kunt meenemen naar een andere plaats. Het geeft een vertrouwd gevoel. Maar is dit wel zo vertrouwd, zo veilig als wij denken? Bestanden op draagbare media (diskettes, harde schijven in laptops, data sticks, externe harde schijven) zijn kwetsbaar voor magnetische straling en kun je verliezen of kunnen gestolen worden.

Het werken in 'the cloud' heeft voor velen een omgekeerd gevoel van veiligheid. De bestanden gaan via internet naar een server ('internetcomputer') op een onbekende plek in de wereld. Waar die staat, wie er op kan kijken of wat er mee gebeurt: u kunt het niet 'zien'. En juist in het zien en voelen zit een sterk gevoel van veiligheid. Maar is dit wel zo onveilig? Opslaan op een harde schijf gaat via dezelfde route en wanneer de server in hetzelfde gebouw staat gebruikt u ook netwerkkabels. Juist bij het werken in *the cloud* gelden strenge regels en zijn veel veiligheidsmaatregelen getroffen om bestanden te sturen en te ontvangen.

Veilig werken, bescherming

Om heel veel redenen zijn er mensen en instanties die kwaadwillende bestanden en virussen rondsturen over en via het internet. Deze vormen voor de digitale archieven een groot gevaar. Dit begint op het moment van productie. Voor welke organisatie u ook werkt, de bescherming van de bron (uw computer) is in eerste instantie uw grootste en eerste zorg. De volgende aandachtspunten gelden hiervoor:

- Gebruik een computer die voorzien is van een actueel besturingssysteem (bijvoorbeeld Windows 10) en waarop alle relevante veiligheidsupdates van het besturingssysteem zijn geïnstalleerd.
- Maak duidelijke afspraken met uzelf welke informatie van het internet op uw computer mag staan. Wie bankzaken doet met zijn computer ziet in de opdrachtregel van de browser een groen slotje staan. Dit betekent dat er een veilige verbinding met uw bank is. Staat dit slotje er niet, bedenk dan of u die pagina wel wil bezoeken. U wilt er in ieder geval geen bestanden van downloaden.
- Open alleen e-mail van mensen en instanties die u kent of vertrouwt. Bedrijven waarschuwen u ook regelmatig dat in naam van een bekend bedrijf valse e-mails in omloop zijn.
- Gebruik actuele en bekende virus beschermingssoftware.
- Gebruik alleen Wifi en andere internetverbindingen van vertrouwde netwerken. Het is fijn dat ieder



winkelcentrum Wifi aanbiedt maar wanneer u daarmee verbinding maakt weet u dan wat er met de bestanden op uw tablet of smartphone gebeurt?
- Gebruik bij voorkeur geen data-sticks (USB-sticks), zeker niet van anderen. De mogelijke werking en besmetting van zo'n stick kan niet door iedere beschermingssoftware worden gevonden. Dit geldt ook voor cd's en dvd's van anderen. De aanpak voor overzetten van grote hoeveelheden bestanden vindt u verderop in dit artikel.

Veilig bewaren

Wie de notulen van de kerkenraadsvergadering heeft gemaakt wil die ook graag echt veilig opslaan. Opslaan op een manier zodat ze bewaard worden voor iedereen die het recht heeft deze te lezen. Belangrijk is dat u de verantwoordelijkheid niet kunt overdragen aan anderen. Wanneer u de notulen naar anderen verzendt, bijvoorbeeld per e-mail, moeten er afspraken zijn hoe de ontvanger met de bestanden omgaat. De wet op de privacy (vastgelegd in de AVG regels, zie verderop) vraagt van u hier rekening mee te houden.

Digitaal veilig bewaren betekent dat de code ook voor langere tijd leesbaar moet blijven. Digitale opslagmedia zijn net als papier gevoelig voor veroudering. Door veroudering raakt de code langzamerhand in de war en wordt onleesbaar. De enige remedie hiertegen is bestanden op meerdere opslagmedia te bewaren en regelmatig opnieuw op te slaan. Hier wordt de meerwaarde van vooral clouddiensten zichtbaar. Bij gerenommeerde cloudopslag rouleren de data over meerdere servers en zorgt de aanbieder van de diensten (de provider) ervoor dat opslagmedia worden vervangen wanneer die onbetrouwbaar dreigen te worden. Grote ondernemingen hebben vaak eigen IT diensten om dit te regelen. In de kerkelijke wereld is dit niet gebruikelijk waardoor de stap naar een cloudoplossing heel verstandig is.

Veilig opslaan is ook regelen dat alleen de mensen die daar recht op hebben bij de bestanden kunnen komen. Hier zijn drie wegen in te onderscheiden:

1. De bron; het apparaat waarop u werkt moet met wachtwoord zijn beveiligd zodat alleen u bij de bestanden kunt komen. Wanneer u wegloopt en uw computer onbeheerd achterblijft, log dan uit. Voor Windows gaat dit eenvoudig door de toetscombinatie [Windowstoets + L] in te drukken.
   Bij heel gevoelige documenten kunt u de documenten zelf ook van een wachtwoord voorzien.

2. Het transport; bijvoorbeeld naar een externe schijf via netwerkkabels of Wifi. Wifi-signalen kunnen gemakkelijk worden onderschept. Bekabeld werken heeft de voorkeur maar dan moet de verbinding zo rechtstreeks mogelijk verlopen als mogelijk is.

3. De opslag; bijvoorbeeld een externe schijf (dit kan dus ook een serverschijf in een gebouw zijn) of cloudopslag. Ook hier gaat het erom dat er belemmeringen zijn om de bestanden te kunnen openen. Dit kan een wachtwoord zijn voor een hele schijf, een wachtwoord voor een groep schijven of een cloudopslag. Bij Office 365 kunt u opslaan in een zogenaamde OneDrive opslag. Hierin kan worden aangegeven wie wat mag lezen. We noemen dit het rechtenbeheer. Overigens lijkt dit heel erg op het rechtenbeheer in een papieren archief. Ook daar mag niet iedereen zomaar elke kast open maken.

Wie de notulen van de kerkenraadsvergadering heeft gemaakt wil die graag verspreiden naar de kerkenraadsleden, en niet naar iedereen in Nederland

Denkt u er nog even aan hoe u bestanden opslaat. Kies een formaat wat ook voor langere tijd door ieder programma te lezen is. Zo kunt u voor tekstbestanden een zogenaamd open source formaat kiezen. Wilt u dat iets alleen maar leesbaar is maar niet veranderbaar, sla het dan op in een zogenaamd PDF formaat. Dit formaat is behoorlijk definitief in de lay-out en kan tot in lengte der dagen door verschillende programma's gelezen worden, inclusief tabellen en beeldmateriaal. Ook in de PDF formaten zijn weer meer mogelijkheden en veiligheidsgraden. Dit blijft in dit artikel buiten beschouwing.

Veilig verspreiden

Wie de notulen van de kerkenraadsvergadering heeft gemaakt wil die graag verspreiden naar de kerkenraadsleden, en niet naar iedereen in Nederland. Dit vraagt vooral discipline. Maak hierover afspraken zoals:
- Wij gebruiken een e-mailadres van de kerkenraad om

de notulen door de scriba/secretaris te laten verzenden aan de kerkenraadsleden. Deze e-mail mag nooit naar anderen worden doorgestuurd.
- Kerkenraadsleden wissen hun bestanden wanneer hun ambtstermijn is afgelopen.
- De scriba/secretaris bewaart op een afgesproken plaats alle bestanden en draagt zorg voor een veilige opslag (zie boven).
- Een nog betere oplossing is: wij delen de bestanden met kerkenraadsleden vanaf een gemeenschappelijke opslag in de cloud. Kerkenraadsleden mogen die bestanden opslaan en printen maar moeten die na de vergadering weer wissen of inleveren voor vernietiging.
- Een veilige variant is om kerkenraadsleden en kerkelijke werkers een e-mailadres van hun kerk te geven. De kosten zijn hiervoor zijn laag omdat het om non-profit gebruik gaat. Dit maakt het gemakkelijker voor een beheerder om het 'transport' virusvrij en veilig te houden.

Veilige aanbieders

Omdat kerken vaak geen eigen IT dienst hebben (overigens soms wel heel bekwame gemeenteleden) is men aangewezen op oplossingen van partijen buiten de eigen organisatie. Op afstand zijn de twee grote aanbieders in Nederland hiervoor favoriet:

- Microsoft Office 365. Een combinatie van opslag in de cloud en de daarbij zichzelf updatende tekstverwerker, spreadsheet en e-mailbeheer. Microsoft geeft aanzienlijke kortingen aan non-profit gebruikers. Zie de website https://www.techsoup.nl/about-pngoprogramme_nl. Wilt u meer weten wat hier mogelijk is kijk dan eens op https://support.office.com/ .
- Google voor non-profit organisaties. Zie https://www.google.com/intl/nl/nonprofits/ . Dit is een aanbod wat identiek is aan de omgeving die iedereen gebruikt met Gmail en Google Drive maar dan met de garanties van een zakelijk account. Die heeft vooral betrekking op de belofte dat de gegevens beter worden beschermd dan bij particulier gebruik. Ook zijn er meer aanvullende programma's beschikbaar.

Verder worden er oplossingen aangeboden door zakelijke aanbieders die soms gebruik maken van een Office 365 aanbod, soms ook in eigen beheer de bestanden opslaan. Bij deze aanbieders moeten de afspraken over toegang, bewaartermijnen, verhuisbaarheid en snelheid heel nadrukkelijk worden vastgelegd in een afspraken overeenkomst, het Service Level Agreement genaamd.

Samenhang met GDPR / AVG

Wie gegevens opslaat van personen moet al langere tijd verantwoording afleggen wat er wordt opgeslagen en hoe dit wordt opgeslagen. Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming ingegaan, beter bekend als AVG. Internationaal wordt dit aangeduid als GDPR, General Data Protection Regulation. Dit heeft nadrukkelijk betrekking op het digitaal archiveren van gegevens. Voor een papieren archief gelden andere regels. Wie meer wil weten over de AVG kan dit nalezen op de website van de autoriteit persoonsgegevens.

Digitalisering blijft mensenwerk

Hoe behulpzaam techniek ook kan zijn, het blijft mensenwerk. Wie zorgvuldig met bestanden wil omgaan moet zich bewust zijn van de afspraken en werkwijze in zijn eigen kerk of werkgroep. De 'digitale etiquette' is een kwaliteitsnorm voor verstandig omgaan met informatie. Digitaal werken gaat snel en versluiert hoeveel zorg en aandacht aan veiligheid wordt besteed. Bovendien is veilig werken vaak synoniem aan gebruik van wachtwoorden en min of meer omslachtig opslaan en bewaren van zaken. We moeten ons die houding vooral eigen maken en het als vanzelfsprekend beschouwen oog te hebben voor veilig werken.