WHO STILL DARES TO SHARE?

Aandachtspunten bij gebruik van filesharing

Iedereen maakt vandaag de dag privé gebruik van diensten als Dropbox, OneDrive of Google Drive voor het opslaan en vooral ook delen van foto's en documenten. Deze tools zijn heel erg handig, intuïtief en werken ook goed op mobiele apparaten. Als werknemer is de verleiding groot om deze tools ook te gaan gebruiken voor zakelijke samenwerking. Hier kleven echter risico's aan. Hoe vind je als bedrijf een balans tussen in control blijven en voldoen aan compliance eisen en aan de andere kant om mee te gaan met medewerkerswensen en te komen tot een acceptabele en werkbare oplossing? Wat zijn de uitdagingen en aandachtspunten hierbij, in het bijzondere voor onderwijs- en onderzoeksinstellingen?

Onzorgvuldig gebruik van filesharingdiensten zorgt voor een aanzienlijk risico op het lekken van gegevens. Zeker met de nieuwe privacywetgeving AVG (Algemene Verordening Gegevensbescherming) is het lekken van vertrouwelijke persoonsgegevens zeer onwenselijk en kan aanzienlijke reputatieschade opleveren. Vaak wordt onderschat hoeveel data al als persoonsgegevens geclassificeerd moeten worden. Persoonsgegevens zijn alle informatie die direct dan wel indirect te herleiden is tot een natuurlijk persoon. In essentie is filesharing vaak net zo risicovol als het gebruik van reguliere e-mail, waarin alle mogelijke persoonsgegevens ook (in bijlagen) verstuurd worden. Aan de andere kant, kan een goed ingerichte en gebruikte filesharing ook veiliger zijn dan reguliere e-mail.

Er ligt dus nu een uitdaging, maar ook kans voor organisaties om dit passend te gaan inregelen. Enerzijds in technische zin, maar vooral ook: welke begrijpbare en werkbare spelregels spreek je met medewerkers af ten aanzien van het opslaan en delen van met name vertrouwelijke en geheime informatie? Kies je voor een onwerkbare oplossing, dan zijn de eindgebruikers vaak creatief genoeg om alternatieven te bedenken die meestal nog onwenselijker zijn. Bijvoorbeeld opslag op losse harde schijven of memory sticks, versturen van bestanden als bijlage naar privé e-mailadressen of het gebruik van een persoonlijke Dropbox of OneDrive.
In de academische wereld is samenwerken binnen de universiteit, met andere kennisinstellingen in Nederland, de EU dan wel wereldwijd en met commerciële bedrijven cruciaal om als kennisgenerator en als partner van het bedrijfsleven te kunnen optreden. Hierbij is het veilig en laagdrempelig kunnen delen van informatie en samenwerken met verschillende soorten partijen dus een must. Elke deelnemer heeft hierbij vaak zijn eigen systemen en beleidskaders.

Binnen de academische wereld bestaat, in tegenstelling tot bijvoorbeeld banken met een vergaande informatieclassificatie, een niet zo sterk gereguleerde omgeving. Hierbij zijn meestal geen maatregelen genomen als data loss prevention (DLP) en Enterprise Digital Rights Management (EDRM) tooling zoals in sterk gecontroleerde omgevingen. Het toezicht op de verspreiding van informatie is hierdoor lastiger.
Gebruik van filesharingdiensten wordt door een aantal aanbieders actief gepromoot binnen de onderwijswereld en daarbuiten. Zo promoot Microsoft het gebruik van OneDrive onder scholieren, studenten en academisch personeel door 'gratis' 1 TB opslag aan te bieden en heeft ook Dropbox promotiecampagnes (Dropbox Campus Cup) en speciale

aanbiedingen voor studenten. De verleiding is dus groot om van deze diensten gebruik te maken doordat het niks of weinig lijkt te kosten in vergelijking tot corporate opslagdiensten, zeker bij grotere hoeveelheden data. Maar boven kosten speelt het intuïtieve en bekende gebruikersgemak een doorslaggevende rol voor het gebruik.

Scope

Gartner (1) definieert filesharing ofwel 'enterprise file synchronization and sharing' (EFSS)-diensten als: "a range of on-premises or cloud-based offerings that enables individuals to synchronize and share files (such as documents, photos and videos) among mobile devices and PCs. Sharing can happen among people (for example, partners and customers) within or outside the organization, as well as among applications. Smooth search, retrieval and access of files stored in multiple data repositories (e.g., file servers or content management platforms) from different client devices complement these offerings, as well as security, data protection and collaboration capabilities."
Grofweg zijn er volgens Gartner drie functionele gebieden te onderscheiden voor de inzet van EFSS (2). De eerste is de verhoging van de productiviteit van medewerkers door middel van de mogelijkheid om vanaf een willekeurig apparaat en vanaf elke locatie bestanden eenvoudig te kunnen benaderen en aan te passen. De tweede is de mogelijkheid om bestanden intern dan wel extern te kunnen delen. Hierbij zijn aspecten als versiebeheer en notificaties van wijzigingen belangrijk. Het laatste gebied zijn de mogelijkheden om bestaande interne opslagdiensten (waaronder FTP) te verplaatsen naar EFSS. Zodoende kan eenvoudig voorzien worden in passende redundantie en bijbehorende hoge beschikbaarheid en back-up met eenvoudige restore mogelijkheden. Aanvullend op bovenstaande punten neemt het gebruik van apps sterk toe en vereisen diverse apps integraties met één of keuze uit meerdere specifieke EFSS-diensten vereisen voor toegang tot data.
Afhankelijk van de specifieke organisatiebehoeftes zal de uiteindelijke keuze voor een EFSS-dienst dan ook verschillend zijn. Kosten per medewerker zullen ten alle tijden een cruciaal aspect blijven tijdens het selectietraject. Daarnaast dient er ook rekening gehouden te worden met de organisatievoorkeur ten aanzien van public, hybrid of private cloud dan wel alles on-premise. Recent worden er zelfs peer-to-peer blockchain-achtige oplossingen aangeboden met bijbehorende encryptie en compartimentering (3).

Uitdagingen en aandachtspunten

Hieronder een nadere uitwerking van een aantal uitdagingen en aandachtspunten bij de selectie en het gebruik van EFSS-diensten. Deze punten kunnen organisaties helpen om passende keuzes te maken bij de selectie en het gebruik van deze diensten.

Security versus functionaliteit

Waarschijnlijk zal al snel duidelijk worden dat het niet haalbaar is om aan alle securityeisen te voldoen in combinatie met de vereiste businessfunctionaliteiten. Men zal dus een balans moeten zoeken tussen de hoeveelheid controle en toezicht vanuit security en het toelaten om innovatie en wendbaarheid van de organisatie te ondersteunen. Geen richting geven aan EFSS-diensten en het oogluikend toestaan of gedogen van andere opslagmedia is nog risicovoller.

Synchronisatie

Voor gebruik van filesharingdiensten is het belangrijk om te kiezen voor diensten die gewijzigde bestanden enkel als delta synchroniseren in plaats van het hele bestand opnieuw te synchroniseren. Dit is niet alleen nuttig voor gebruikers met een trage internetverbinding (bijvoorbeeld bij gebruik van mobiel netwerk op platteland in het buitenland) maar voorkomt ook dat de zakelijk internetverbinding traag wordt door honderden gebruikers die gelijktijdig hun data synchroniseren. Een ander voordeel van delta synchronisatie is dat version history mogelijk is en dat bij ransomware infecties makkelijk terug gegaan kan worden naar een oudere versie. Verder is het belangrijk dat er bijvoorbeeld door een checksum te vergelijken van bestanden voor en na synchronisatie gevalideerd wordt dat de bestanden niet aangepast zijn.

Raoul Vernède is Security Officer bij Wageningen University & Research. Hij is bereikbaar via raoul.vernede@wur.nl.

Sterke authenticatie
Wachtwoorden als authenticatie bieden maar een zeer beperkte bescherming van gegevens. Sterke authenticatie door middel van een tweede factor is noodzakelijk voor de bescherming van vertrouwelijke data. Voor EFSS-diensten is twee factor authenticatie echter lastig in gebruik en bij diverse aanbieders zelfs afwezig. De tweede factor is meestal een mobiel apparaat dat zelf ook toegang heeft tot de via EFSS gedeelde bestanden, waardoor juiste initiële registratie noodzakelijk is om effectief te zijn.

Exit strategie
Denk al tijdens het selectietraject van een EFSS-dienst na over het moment dat men geen gebruik meer wil maken van de dienst. Bepaal een strategie voor het migreren van bedrijfsdata naar een andere dienst. De wetgeving m.b.t. privacy ontwikkelt zich constant en marktontwikkelingen gaan vaak nog sneller. De kans dat men na enige tijd een andere dienst wil of moet gebruiken is aanzienlijk.

Delen van data
Een standaard functionaliteit is het kunnen delen van documenten en mappen met externe personen. Dit gebeurt met behulp van zakelijke of persoonlijke dan wel sociale e-mailadressen waarbij er beperkte zekerheid is dat de eigenaar van het e-mailadres ook daadwerkelijk de beoogde ontvanger is. Verder is de authenticatie enkel op basis van wachtwoorden waarbij men als eigenaar van de informatie geen wachtwoordbeleid of twee factor authenticatie kan afdwingen bij de ontvanger waardoor de kans op een security incident groter wordt.
In geval van het lekken van vertrouwelijke persoonsgegevens is het maar de vraag of de Autoriteit Persoonsgegevens het delen van persoonsgegevens enkel op basis van een e-mailadres en bijbehorend wachtwoord als voldoende passende beveiliging zal beoordelen. Een mogelijke toekomstige oplossingsrichting zou kunnen zijn om bepaalde domeinen van organisaties waarmee men contractuele afspraken heeft en die men vertrouwt, te kunnen white-listen om zo met deze externe medewerkers van die organisatie te kunnen samenwerken. Voordeel hierbij is ook dat indien een medewerker van zo'n samenwerkingspartner vertrekt het account wordt dichtgezet en deze persoon dan geen toegang meer heeft tot de gedeelde data. Dit in tegenstelling tot filesharing accounts die gekoppeld zijn aan privé e-mailadressen.

Toegang data
Filesharingdiensten zijn persoonsgebonden en niet team of afdeling gebonden. Toegang tot bedrijfsdata bij een normaal einde dienstverband dan wel bij een (security)incident vereist daarom toegang of minimaal het op afstand kunnen verwijderen (remote wipen) van data. Zijn hiervoor eenvoudige en transparante tools voor aanwezig in de geselecteerde EFSS-dienst? Bepaal de bewaartermijn van de EFSS-data na contractbeëindiging van een medewerker, anders bestaat het risico dat data en bijbehorende back-up verwijderd zijn op het moment dat de vertrokken medewerker toch nog niet gedeelde documenten had.

Logging
Makkelijk toegankelijke en gedetailleerde logging over een langere periode is cruciaal om onder andere in geval van een mogelijk datalek te kunnen aantonen dat de data niet is gelekt. Denk bijvoorbeeld aan de situatie dat een wachtwoord gecompromitteerd is. Verder kan logging ook inzicht geven in het gebruikersgedrag, wat bijsturen mogelijk maakt op ongewenst gedrag. Rechtstreekse koppeling naar een eigen SIEM om correlaties te ontdekken, kan wenselijk zijn.

Verspreiding data
Doordat gebruikers sync-clients en apps installeren op eigen niet zakelijk beheerde apparaten (BYOD) zoals laptops, tablets als ook smartphones en data synchroniseren, zal zakelijke data gefragmenteerd worden over meerdere en vooral ook beperkt beheerde locaties. Diefstal of verlies van privé apparaten zonder passende beveiliging zoals dataencryptie dan wel het ongewild peer-to-peer delen van te veel datamappen kan tot datalekken leiden. Bij sommige diensten is het mogelijk als beheerder op afstand gesynchroniseerde bestanden te verwijderen (in geval van verlies/diefstal dan wel einde dienstverband) op het moment dat het apparaat weer op het internet komt. Het niet toestaan van sync-clients haalt veel handige en door de gebruikers gewenste functionaliteit weg en is in veel gevallen bijna geen optie. Als alternatief zouden de bestanden dan enkel via een webbrowser te benaderen en te bewerken zijn. Of men moet ervoor kiezen BYOD geheel onder beheer te nemen door middel van EMM (Enterprise Mobility Management) met bijbehorende aanzienlijke kosten.

Fysieke locatie data
Voor diverse organisaties is het onwenselijk en onacceptabel indien bedrijfsinformatie buiten het eigen land dan wel de EU (of Europese Economische Ruimte) opgeslagen wordt. Dit ondanks het vernieuwde Privacy Shield als opvolger van Safe Harbour. Sommige aanbieders bieden daarom Europese datacentra aan. Het blijft echter vaak de vraag (4) in hoeverre de data in transit dan wel de metadata en indexering van de bestanden buiten de EU komt en zo makkelijk af te tappen is. Navraag bij de EFFS-aanbieder kan hier mogelijk deels inzicht in geven op basis van certificeringen, transparency reports en government data requests principles.

Samenwerking
Voor interne dan wel externe collaboratie binnen projecten bieden organisaties vaak ook specifieke samenwerkingsomgevingen aan (denk hierbij bijvoorbeeld aan Microsoft SharePoint teamsites). De functionaliteit hiervan is meestal uitgebreider en omvat vaak zaken als actielijsten en agendabeheer. Doordat er echter overlap met EFSS-diensten bestaat is het belangrijk om als organisatie te bepalen in welke situaties van welke hulpmiddelen gebruik gemaakt kan worden en wanneer niet. Veel organisaties redeneren van binnen naar buiten toe als het gaat om de keuze en inrichting van externe samenwerkingshulpmiddelen. Hierdoor moet bij samenwerking onderling besloten worden welke dienst gebruik gaat worden. In samenwerkingsverbanden (bijvoorbeeld EU-onderzoeksprojecten) met diverse of veel partners is dit bijna onmogelijk. Vaak wordt er daarom door gebruikers als een soort connectiviteitslaag gebruik gemaakt van een cloud gebaseerde breed verspreide EFFS-dienst (meestal Dropbox of Google Drive).

Encryptie
Sommige aanbieders van EFSS-diensten bieden naast encryptie van de verbindingen ook encryptie van eigenlijke data aan. Dit beschermt echter niet tegen vordering van data door wettelijke instanties (in het buitenland). Een extra laag van encryptie van de brondata waarbij de cryptografische sleutels binnen het eigen bedrijf worden opgeslagen en beheerd heeft als nadeel dat zaken als zoeken op basis van indexering niet meer werken. Lokaal gesynchroniseerde data is standaard niet versleuteld en is zo potentieel een bron voor een datalek bij verlies of diefstal.

Gebruikersgedrag
Doordat veel medewerkers privé al consumenten filesharingdiensten gebruiken, zullen zij terughoudend zijn om mogelijke, net iets minder handige, zakelijke EFSS-diensten te gaan gebruiken. Gebruikersgemak en -bewustwording is cruciaal om medewerkers te verleiden naast heldere en werkbare gebruiksvoorwaarden en beleidskaders. Maar al te vaak zullen er anders privéfoto's en bestanden opgeslagen gaan worden als back-up voor thuis. Gebruikersfouten, zoals het abusievelijk delen van een hele map in plaats van een enkel bestand, zijn natuurlijk ook aandachtspunten. Daarnaast moeten de gebruikskaders van andere losse opslagmedia zoals USB-memorysticks dan wel losse harde schijven helder zijn voor de gebruikers.

Identiteiten en authenticatie
Integratie van EFSS-diensten met de eigen directory services (zoals AD) is eigenlijk een must om accounts makkelijk te kunnen beheren en het wachtwoordbeleid te kunnen afdwingen. Het gaat hierbij dus om provisioning van accounts en authenticatie met behulp van bijvoorbeeld het SAML v2 protocol. In geval van claim based authenticatie kan men ook gebruikmaken van de eigen IDP (identity provider zoals ADFS of SecureAuth) met eigen toegangsregels, inclusief het afdwingen van twee factor authenticatie. Door federatieve afstemming en afspraken tussen organisaties wordt het delen van data makkelijker. Binnen de Nederlandse onderwijs- en onderzoeksinstellingen biedt SURF een gezamenlijke EFFS-dienst SURFdrive aan waarbij alle medewerkers van de aangesloten instellingen federatief kunnen inloggen (5).

Digital rights management
Inzet van een EDRM-systeem (Enterprise Digital Rights Management) om te voorkomen dat specifieke documenten gedeeld worden, is in specifieke gevallen noodzakelijk. Implementatie en gebruik van EDRM-systemen is echter complex en werkbaarheid voor medewerkers is een cruciaal aandachtspunt. Eventueel zou ook besloten kunnen worden om via geo-fencing (op basis van IP-gegevens) de toegang vanuit bepaalde landen tot EFFS-dienst te beperken. De bescherming hiervan is echter beperkt omdat dit door gebruik van VPN-verbindingen omzeilt kan worden.

Conclusie

Inzet van EFFS-diensten is complex en omvat veel aspecten variërend van security, privacy tot gebruikersgemak waarmee rekening gehouden zal moet worden. Geen keuzes maken als organisatie is erger dan richting geven, ook al zijn het soms suboptimale oplossingen. Ongecontroleerd gebruik of niet gebruikmaken van de functionele mogelijkheden van EFFS-diensten is een gemiste kans. Dus ja, voor onderwijs en onderzoek geldt zeker: dare to share! Intensieve en veilige samenwerking met partners en in productieketens en netwerken is cruciaal. Neem indien mogelijk, als sector of keten, hierin het initiatief en vorm federaties waarbinnen informatie veilig gedeeld kan worden.

Referenties

(1) Magic Quadrant for Enterprise File Synchronization and Sharing door Monica Basso, Karen A. Hobert, Jeffrey Mann – 2016 – Gartner
(2) The Top 10 Best Practices for Choosing and Deploying an Enterprise File Sync and Sharing Solution door Charles Smulders, Monica Basso, Karen A. Hobert – 2016 – Gartner
(3) Zie https://storro.com/
(4) How to Mitigate the Risks of Public Cloud EFSS and Storage door Raj Bala, Monica Basso – 2016 – Gartner