Matto Fransen / m.j.fransen@rug.nl

Bestanden veilig uitwisselen

Matto Fransen is security manager bij het CIT. Met deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen.

Regelmatig komt het voor dat men een of meer bestanden met iemand wil uitwisselen. Gewoontegetrouw wordt dan het e-mailprogramma geopend en een nieuw bericht aangemaakt, waar de bestanden als attachment aan worden toegevoegd, zonder er bij stil te staan dat e-mail helemaal geen veilig medium is. E-mail is niet geschikt voor gevoelige informatie. De enige veilige manier om gevoelige informatie per e-mail te verzenden, is om de informatie eerst te versleutelen met een sterke encryptie-methode.

Bestanden met persoonsgegevens

Of het een goed idee is, een bepaald bestand per e-mail te versturen, hangt dus onder andere af van de inhoud van dat bestand. Is het een bestand dat geen gevoelige informatie bevat, dan is vanuit het perspectief van veiligheid niet veel bezwaar tegen het gebruik van e-mail.

Bestanden die op het werk gebruikt worden, bevatten echter vaak wel gevoelige informatie. Persoonsgegevens dienen zorgvuldig en vertrouwelijk behandeld te worden, daarom mogen bestanden met persoonsgegevens niet per onversleutelde e-mail worden verstuurd. Ook om andere redenen kan de informatie in een bestand vertrouwelijk zijn, bijvoorbeeld omdat deze gevoelige bedrijfsinformatie bevat.

Verschillende apparaten

Bestanden die per e-mail worden verstuurd, gaan zich vliegensvlug vermenigvuldigen. Zo kan al vlot een versie in een gecachte folder op uw lokale harde schijf staan, een versie in de box met verzonden mail van uw e-mailaccount, een versie in de inbox van de ontvanger en/of bijvoorbeeld een versie in een gecachte folder op de harde schijf van de ontvanger.

Tegenwoordig gebruiken veel mensen hun e-mail op verschillende apparaten, dus niet alleen de werkplek-pc, maar ook bijvoorbeeld een laptop, een tablet en een smartphone. Wanneer het mailtje op verschillende apparaten bekeken wordt, ontstaan daar ook weer kopieën in de lokale cache. Bij mobiele apparaten draait op de achtergrond soms ook nog synchronisatie naar de cloud-storage van bijvoorbeeld Apple, Google of Samsung. Daarnaast maakt de beheerder van het e-mailaccount backups.

Wie zich dit verschijnsel realiseert, zal zich ook afvragen of zelfs het per e-mail versturen van bestanden zonder gevoelige informatie wel de beste en meest efficiënte oplossing is.

Gedeelde opslag: Y:-schijf

Gelukkig bestaan voldoende alternatieven voor het uitwisselen van bestanden. De makkelijkste manier om binnen de universiteit bestanden uit te wisselen, is het gebruik van de Y:-schijf. Voorwaarde is wel, dat betrokkenen allen toegang tot dezelfde map hebben. Is dat het geval, dan is een bestand snel op Y: opgeslagen en door de andere partij snel te openen.

Maar wat gebeurt er daarna? Hoe lang moet zo'n bestand bewaard blijven, wie houdt dat in

Veilig e-mailen

E-mail is, voor internettermen, een zeer oud protocol. In de begintijd van het internet waren de verbinding minder betrouwbaar, en e-mail is op dit gebied een robuuste oplossing. Mailservers probeerden in die tijd soms wel een week lang om mail aan de ontvangende mailserver af te leveren. Echter, in de begintijd van het internet had informatieveiligheid minder de aandacht. De bedreigingen zijn sindsdien enorm toegenomen.

De twee belangrijkste aandachtspunten in e-mail zijn de authenticiteit van de verzender en de vertrouwelijkheid van de informatie-uitwisseling. Het is een fluitje van een cent om een gefingeerde afzender in een e-mailbericht te zetten. Alle informatie wordt open en onversleuteld uitgewisseld. Wereldwijd proberen aanbieders van e-maildiensten de informatie-uitwisseling beter te beschermen. Vaak verloopt het verkeer tussen de gebruiker en de mailserver al via versleutelde verbindingen. Ook bij de RUG is dit het geval.

Gebruikers hebben gelukkig wel zelf mogelijkheden om het e-mailgebruik veiliger te maken. Met behulp van moderne encryptietechnieken is het mogelijk om de authenticiteit van de afzender te waarborgen en de inhoud van de berichten tegen ongeautoriseerde inzage te beschermen. Wereldwijd zijn hier twee verschillende opties voor beschikbaar, S/MIME en OpenPGP.

Beide opties werken met encryptie op basis van publieke en geheime sleutelparen. Het belangrijkste verschil is het beheer van de sleutels. De makkelijkste optie is hierbij het gebruik van S/MIME, hier wordt het sleutelbeheer voor u geregeld. U downloadt en installeert dit op de werkplek waar vanaf u e-mail wilt verzenden. Op My University is hiervoor een handleiding aanwezig, zoek op 'Beveilig uw data', de linkjes staan bij 'E-mail versleutelen'.

Nadat een en ander is geïnstalleerd, kunt u voortaan uitgaande e-mailberichten voorzien van een digitale handttekening, dit is een klein bestandje dat mee gestuurd wordt, waarmee de ontvanger kan verifiëren dat het bericht écht van u afkomstig is en dat na het verzenden de inhoud ongewijzigd is.

Wanneer u S/MIME wilt gebruiken voor het versleutelen van de inhoud van het e-mailbericht en eventuele attachments, dan dient de ontvanger ook S/MIME te hebben geïnstalleerd en dient uw e-mailprogramma over de publieke sleutel van de ontvanger te beschikken. <

de gaten en wie gaat het na verloop van tijd wissen? Bij het gebruik van gedeelde opslag is het van belang van te voren bij dit soort vragen stil te staan en bijvoorbeeld een mappenstructuur te kiezen die hier ondersteunend aan is.

Unishare

Binnen de RUG wordt Unishare aangeboden. Dit is een bestandssynchronisatiedienst die ook geschikt is voor het delen van bestanden met anderen, zowel binnen als buiten de universiteit. De programmatuur en data staan op servers van de universiteit en voor het transport van de data van en naar de server wordt gebruik gemaakt van versleutelde verbindingen die door middel van een gesigneerd certificaat zijn geauthentiseerd.

Deze dienst werkt op een manier die vergelijkbaar is met Dropbox. De gebruiker wijst één of meer mappen op zijn werkstation aan, om die te laten synchroniseren met Unishare. Wijzigingen in zo'n map, zoals het toevoegen van nieuwe bestanden of het aanpassen van een bestand, worden daarbij in Unishare in de gesynchroniseerde map overgenomen. De gebruiker kan per map anderen machtigen en toegang geven tot de bestanden.

De werking is eenvoudig. Een handleiding is beschikbaar via My University, zoek op Unishare. Daar is ook de link naar de inlogpagina te vinden. De gebruiker kan voor maximaal 100GB data opslaan in Unishare.

Unishare is een goede manier om veilig mappen met bestanden met anderen te delen, voor een enkel bestand is het minder geschikt. Net als bij de Y:-schijf, is het van belang vooraf na te denken over een goede (sub-)mappenstructuur, die ondersteunend is aan het tijdig weer opruimen van de bestanden.

Surfdrive

Surfdrive is een met Unishare vergelijkbare dienst, waarbij Unishare beheerd wordt door de RUG en Surfdrive door Surf. De functionaliteit is vrijwel gelijk, met dit verschil dat u alleen kunt delen met andere leden van de Surf community.

Ook Surfdrive biedt 100GB opslag per gebruiker.

Surffilesender

Surffilesender is gemaakt voor het ad hoc delen van een enkel bestand, met als bijzonderheid dat dit ook geschikt is voor zeer grote bestanden, tot wel 500 Gb. De programmatuur en data staan in Nederland. De bestanden wordt automatisch na 21 dagen van de server gewist. Surffilesender werkt volledig via de webbrowser, de gebruiker hoeft niets op zijn werkstation te installeren.

Het inloggen op Surffilesender gaat via Surfconext. Voor het transport van de data van en naar de server wordt gebruik gemaakt van versleutelde verbindingen die door middel van een gesigneerd certificaat zijn geauthentiseerd. Bestanden tot 250 Mb kunnen voorafgaand aan het uploaden worden versleuteld, waarbij de gebruiker de sleutel via bijvoorbeeld SMS aan de ontvanger doorgeeft.

De ontvanger hoeft geen deel uit te maken van de Surf community. Om een bestand te verzenden, logt u via Surfconext in op Surffilesender. Op My University staat een verwijzing naar de veelgestelde vragen-pagina en naar de inlogpagina, zoek op Filesender. <