www.boxcryptor.com	**BoxCryptor**	
	Client-side vercijfering van data gestockeerd in bestaande file sync & share systemen (Dropbox, Google Drive, …)	
	System Requirements: Windows, Mac OS X, Chrome (beta), iOS, Android, Windows Phone, windows RT, Blackberry	
	Ontwikkeld door:	Secomba GmbH
Betalend, gratis basisversie	**Contactpersoon:**	Kristof.Verslype@smals.be

Functionaliteiten

File sync & share (FSS) systemen zoals Dropbox, Box en OneDrive hebben bij gebruik in principe toegang tot je potentieel gevoelige gegevens. Server-side encryptie verandert hier niets aan gezien de dienstverleners zelf de bijhorende sleutels beheren. BoxCryptor wil deze kwestie verhelpen.

Er wordt gebruik gemaakt van een lokaal geïnstalleerde BoxCryptor client die instaat voor 1) de (client-side) encryptie voordat gegevens naar een FSS dienst verstuurd worden en voor 2) de (client-side) decryptie voor toegang tot de gegevens. Daarbij wordt gebruik gemaakt van bestaande FSS systemen. BoxCryptor biedt dus zelf geen opslagruimte aan.

Wat BoxCryptor wel doet is het beheer van de sleutels die voor de vercijfering gebruikt worden[1]. Elke gebruiker heeft zijn eigen paswoord-beschermd sleutelpaar, waarmee per-folder AES sleutels beschermd worden. Verlies van uw paswoord impliceert dus verlies van toegang tot uw vercijferde gegevens.

Bedrijven kunnen weliswaar met de Unlimited Business licentie d.m.v. de *Master Key* toegang krijgen tot de vercijferde gegevens van hun medewerkers. Deze Master Key maakt ook een paswoord reset voor accounts van medewerkers mogelijk. Bedrijven hebben daarnaast de mogelijkheid om policies in te stellen zoals minimumlengte van de paswoorden. Sinds kort wordt LDAP/AD ondersteund voor enterprise use.

Delen van gegevens met andere gebruikers is mogelijk maar daarbij moeten allen een BoxCryptor account hebben en gebruikmaken van een zelfde FSS dienst.

BoxCryptor ondersteunt momenteel 16 diensten en het WebDAV protocol, wat het ook bruikbaar maakt in combinatie met minder bekende of zelfs custom-made oplossingen, die niet per se FSS of cloud hoeven te zijn. Daarnaast kan het ook gebruikt worden voor vercijfering van puur lokale gegevens.

1. Voor meer info over het sleutelbeheer zie slides 101-117 van de infosessie “Gevoelige Overheidsdata en de Cloud” (http://www.smalsresearch.be/publications/document/?docid=107)

Conclusies en Aanbevelingen

Wanneer bij de zoektocht naar een veilig FSS systeem een on-premise oplossing financieel of technisch niet haalbaar is, kan geopteerd worden voor BoxCryptor als deel van de totaaloplossing. Hou er rekening mee dat het wat omslachtig is en dat het slechts één aspect van de security oplost: het zorgt er enkel voor dat de cloud provider geen toegang meer heeft tot uw gegevens. Een hacker die het paswoord kent van zowel uw FSS account als uw BoxCryptor account (vaak dezelfde!) heeft bijvoorbeeld nog steeds toegang tot uw gegevens.

Testen en Resultaten

BoxCryptor 2 werd getest. Deze versie is niet compatibel met *BoxCryptor Classic* wat de eerste versie was en in een eerdere Quick Review besproken werd.

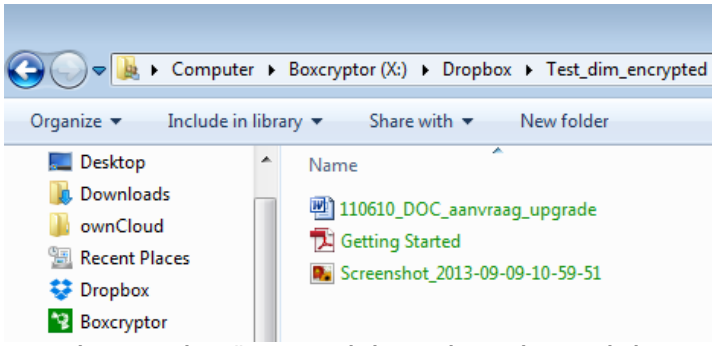
De testen werden uitgevoerd m.b.v. twee gratis accounts, wat onder meer als beperking heeft dat slechts twee toestellen en één FSS-account gelinkt kunnen worden aan een BoxCryptor account en dat de inhoud van de bestanden wel geëncrypteerd wordt, maar niet de bestandsnaam. Verder werd gebruik gemaakt van twee gratis Dropbox accounts en twee accounts op een on-premise installatie van ownCloud 7 Community Edition.

BoxCryptor Client voor Windows versie 2.0.431.403 werd voor één gebruiker geconfigureerd op een Windows 7 PC, in combinatie met Dropbox en ownCloud. Op een iOS tablet werd de BoxCryptor app versie 2.3.401 (444) geconfigureerd voor een andere gebruiker, eveneens in combinatie met Dropbox en ownCloud.

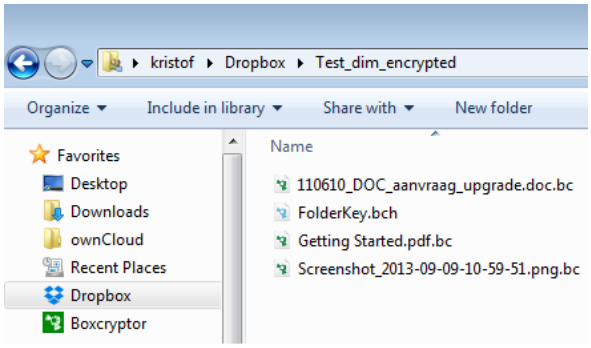
Op PC of MAC zorgen FSS clients typisch voor synchronisatie tussen de gegevens in de cloud en een lokale map. BoxCryptor herkent deze lokale mappen. In een door BoxCryptor gecreëerde network drive mapping (standaard X:\) krijgt de gebruiker toegang tot zowel de vercijferde als de onvercijferde gegevens in deze lokale mappen. Vercijferde gegevens worden in het groen weergegeven en zijn niet leesbaar buiten de network drive mapping. Ook op mobiele toestellen is er ondersteuning voor meerdere FSS accounts op hetzelfde moment, maar hier wordt gebruik gemaakt van directe toegang i.p.v. synchronisatie.

Een gebruiker heeft bijgevolg twee accounts nodig: één voor de FSS dienst en één voor BoxCryptor. Gezien een BoxCryptor client enkel voor de vercijfering zorgt en niet voor synchronisatie zijn op PC en MAC zowel de FSS synchronisatieclient als de BoxCryptor encryptieclient vereist. Op mobiele toestellen volstaat de BoxCryptor app, maar deze biedt enkel directe toegang en geen synchronisatie.

Hoewel het encypteren en decrypteren vlot lijkt te werken, is het delen van bestanden met anderen toch wat omslachtig. Niet alleen in de FSS dienst moet aangegeven worden dat de vercijferde gegevens gedeeld moeten worden, maar ook in de BoxCryptor client. Zowel de delende als de ontvangende gebruiker moeten dus zowel BoxCryptor als dezelfde FSS dienst gebruiken.



Figuur 1. Drie geëncrypteerde bestanden gezien vanuit de BoxCryptor network drive mapping



Figuur 2 Dezelfde drie geëncrypteerde bestanden, gezien vanuit de lokale Dropbox folder. Er is nog een vierde bestand aangemaakt door BoxCryptor.

Gebruiksvoorwaarden

Naast de gratis account die enkel de basisfunctionaliteit bevat, zijn er twee betalende licenties: *Unlimited Personal* (36€ per jaar per gebruiker) en *Unlimited Business* (72€ per jaar per gebruiker). Daarnaast zijn er mogelijks licentiekosten verbonden aan het gebruik van de FSS-dienst.