

Hoe is de data beveiligd?

Om op een verantwoorde wijze over het publieke Internet gegevens te versturen, is het nodig om deze gegevens te versleutelen, door het toepassen van encryptie technieken. SmartBackup heeft gekozen voor een manier van versleuten(encrypten) welke het onmogelijk maakt data te onderscheppen en te ontcijferen. Alleen de bezitter van de toegangcodes die gebruikt zijn voor het beveiligen van de data heeft toegang tot deze data.

Wat is Encryptie?

Wanneer er gekeken wordt naar de voordelen van een off-site backup methode via het Internet, is het logisch dat gebruikers zich afvragen of hun data op een veilige manier getransporteerd en opgeslagen wordt. Als veiligheid van transport en opslag voor de gebruiker noodzakelijk is, kunnen een aantal vormen van encryptie toegepast worden, die er voor zorgen dat data alleen toegankelijk gemaakt wordt met de juiste toegangcodes. Encryptie zorgt er voor dat een gebruiker een toegangscade of wachtwoord moet ingeven, zonder deze code is data voor iedereen onleesbaar. Er zijn honderden mogelijke vormen van encryptie, maar er zijn maar enkele veelgebruikte encryptiemethodes die goed gestandaardiseerd zijn. Bij SmartBackup zijn de volgende encryptie methoden beschikbaar: TwoFish, Triple DES en Advanced Encryption Standard (AES).

Het SmartBackup proces

Binnen het SmartBackup proces wordt er meerdere malen encryptie toegepast om er voor te zorgen dat de data goed beveiligd is:

Communicatie

Omdat de informatie over het Internet getransporteerd wordt, is het aan te bevelen om de communicatie tussen de cliëntsoftware en de server te versleutelen. Als onderdeel van de initiële communicatieprocedure zorgt de SmartBackup cliënt er voor dat er een encryptie-methode wordt afgesproken met de server, voordat er enige data naar de server wordt verstuurd. Dit verzekert de gebruiker ervan dat er op een veilige manier met de server wordt gecommuniceerd en dat de verkeersstroom gedurende de gehele transactie compleet versleuteld wordt.

Opslag op de server

Wanneer de versleutelde data succesvol is ontvangen door de SmartBackup server, wordt deze onmiddellijk versleuteld op de disk opgeslagen en worden de filenamen nog verder versleuteld om het nog ingewikkelder te maken om specifieke userdata te identificeren. De data wordt versleuteld opgeslagen om ongeautoriseerde toegang te voorkomen in geval een derde zich op enigerlei wijze toegang weet te verschaffen tot de fysieke disken.

Opslag op de cliënt-pc

Belangrijke informatie, zoals het wachtwoord van de gebruiker moet worden opgeslagen op de client-pc om er voor te zorgen dat het login-process op de SmartBackup server juist verloopt. Dit wachtwoord en andere belangrijke informatie wordt in versleutelde vorm opgeslagen door de SmartBackup cliënt en kan alleen door de cliënt weer worden uitgelezen.

Authenticatie van de gebruiker

Gebruikersauthenticatie wordt onmiddellijk uitgevoerd nadat de versleutelde verbinding tussen de SmartBackup cliënt en de SmartBackup servers is opgezet. De cliënt verstuurt de usernaam en wachtwoord naar de server om te worden gevalideerd in de userdatabase van de server. Deze authenticatie-methode zorgt voor een veilige en robuuste manier van het gebruikersbeheer.

Samenvattend

Met de hedendaagse encryptie mogelijkheden en de makkelijke toegankelijkheid van het Internet kunnen bedrijven van allerlei grootte (dus ook MKB-bedrijven) beschikken over de mogelijkheid van een niveau van dataprotectie dat tot voor kort alleen te bekostigen was voor grotere bedrijven. Off-site data opslag zorgt voor een veilige wijze van het bewaren van data tegen eventuele catastrofes. Door op juiste wijze beveiligingsmaatregelen, zoals encryptie toe te passen zorgt SmartBackup er voor dat de data op een veilige manier bewaard blijft tijdens transport en opslag op de SmartBackup-server.

Verschillende manieren van encrypten

De volgende encryptie methoden zijn mogelijk:

DES

DES is gebaseerd op een secret key systeem waarbij de zender en ontvanger een enkele key gebruiken om data te encrypten en te decrypten. De verzender gebruikt de key om de data te encrypten volgens een complex rekenkundig algoritme en alleen gebruikers met de juiste key kunnen deze data weer decrypten.

De key heeft een lengte van 64bits, 56 worden gebruikt als key en de laatste 8 worden gebruikt voor het controleren op fouten. Het DES algoritme zal voor de data encryptie niet meer ruimte gebruiken dan de originele data. De gebruiker selecteert vervolgens 1 of meerdere van de 72 biljard transformatie functies, door het selecteren van een 56-bit key. De theorie achter de DES-security is dat er naast het proberen van alle 72 biljard combinaties geen mogelijkheid is, om het algoritme te "kraken".

Triple DES

Om de veiligheid van DES te verhogen, gebruiken sommige organisaties de Triple DES - security, oftewel 3 DES- bewerkingen met 2 keys om data te beschermen. Deze methode verbruikt echter meer rekenkracht, waardoor de performance van een systeem lager uit kan vallen