BackitUp Online Backup

Whitepaper – Securitatea Datelor

CUPRINS

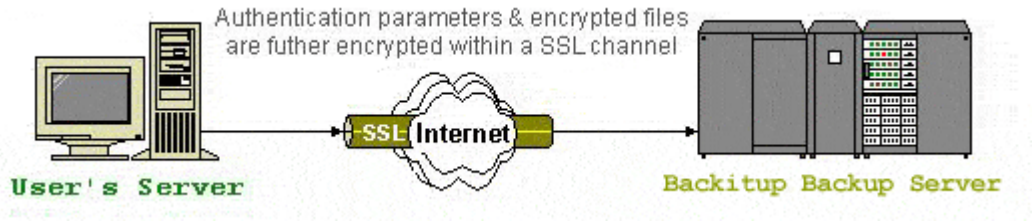
1 Introducere....3
2 BackitUp Offsite Backup Server – “Sigur, Robust şi Fiabil” 4
2.1 Comunicare Securizată prin 128-bit SSL....4
2.2 Datele salvate sunt criptate securizat 4
2.3 Cheile de criptare sunt bine protejate 4
2.4 Este folosit cel mai bun algoritm de criptare 5
2.5 Ar trebui 8.77 x 1017 ani pentru a sparge encripția de 128-bit....5
2.6 Acces limitat la date pe baza de adresa IP 5

1 Introducere

Acest document descrie măsurile de securitate disponibile în software-ul BackitUp din perspectiva utilizatorului. Documentul este menit să ajute partenerii Backitup să raspundă întrebărilor despre securitatea datelor clienților lor.

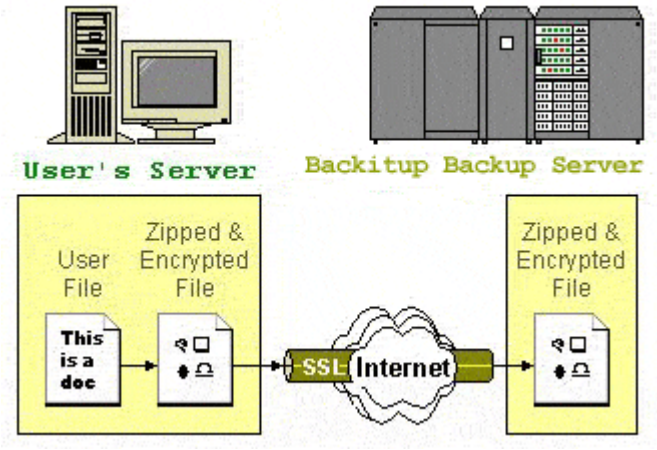
2 BackitUp Offsite Backup Server – “Sigur, Robust şi Fiabil”

2.1 Comunicare Securizată prin 128-bit SSL



Toate comunicările dintre serverul de backup BackitUp şi computerul tău sunt transportate printr-un canal de 128-bit SSL (Secure Socket Layer). Deşi toate fişierele la care se face backup trec printr-o rețea publică (internet), oricine ar asculta nu ar putea cunoaşte conținutul informatiei transmise.

2.2 Datele salvate sunt criptate securizat



Toate fişierele tale sunt prima dată arhivate şi encryptate cu cheia de criptare folosită de tine, înainte să fie trimise la serverul de backup BackitUp. Pentru toată lumea înafară de tine, toate fişierele stocate pe serverul de backup BackitUp nu sunt altceva decât nişte fişiere inutile cu conținut aleator.

2.3 Cheile de criptare sunt bine protejate

Cheia de criptare folosită pentru criptarea fişierelor tale rămâne doar pe calculatorul tău şi este ştiută doar de către tine. Nu este nicăieri şi niciodată transmisă pe internet sau rețea. Astfel, chiar şi administratorul de system nu poate să decripteze şi să vadă conținutul fişierelor stocate în serverul de backup fără permisiunea ta. Asta bineînțeles inseamnă că dacă ți-ai pierdut cheia de criptare, nu ai să poți niciodată să-ți recuperezi fişierele salvate.

Detalii Tehnice

Cheia de criptare pentru seturi de backup diferite sunt stocate în fişierul config.sys , care este encodat cu un altgoritm propriu al aplicației:

(Windows)	C:\Documents and Settings\administrator\.obm\config\config.sys
(Linux)	~/.obm/config/config.sys
(Mac OS X)	~/.obm/config/config.sys

Dacă aplicația client nu poate localiza fişierul config.sys (datorită ştergerii accidentale sau se autentifică pe o noua maşină cu acelaşi cont), are sa-l alerteze pe utilizator pentru a reintroduce cheia de criptare la setul de backup ca apoi să o țina şi în config.sys-ul local.

2.4 Este folosit cel mai bun algoritm de criptare

Algoritmul pe care îl folosim pentru criptarea fişierelor tale este 256-bit Twofish. Este un block cifrat proiectat de Laboratoarele Counterpane. A fost deasemenea unul din cinci Advanced Encryption Standard (AES) finalişti aleşi de National Institute of Standard and Technology (NIST). Este subiectul unor frecvente revizuiri publice dar nici un atac cunoscut asupra acestui algoritm nu a fost raportat.

2.5 Ar trebui 8.77 x 1017 ani pentru a sparge encripția de 128-bit

O cheie de mărimea 128-bit are 2^{128} sau în jur de 3.4 x 10^{38} posibile combinații. Chiar dacă ai avea cel mai bun super computer, ASCI White, SP Power3 375 MHz fabricat de IBM în Noiembrie 2000, ar trebui 8.77 x 10^{17} anii ca să testeze toate combinațiile, presupunând că aveți super computer-ul, ASCU White, SP Power3 375 Mhz cu 8192 de procesoare care totalizează o capabilitate de 12.3 teraflopi (trilioane de operații/secundă), disponibil ție. De asemenea el doar are nevoie de o operație a unui computer pentru a testa o combinație posibilă (care e deja mai rapidă decât ce poate el). Pentru a folosit atacul de tip “brut force” (verificarea tuturor combinațiilor) pe acest algoritm de encripție. Ar lua:

$$\frac{3.4 \times 1038}{12.3 \times 1012} \text{ secunde} \sim 2.76 \times 10^{25} \text{sec}$$

i.e. 876530835323573935 ani sau 8.77 x 10^{17} ani

pentru a încerca toate combinațiile cu succes. Nici chiar ASCI White nu poate procesa aşa de repede ce am descris aici. Poți să fi sigur că datele tale stocate la noi pe server sunt 100% sigure.

2.6 Acces limitat la date pe baza de adresa IP

Poți de asemenea să restricționezi accesul la fişierele tale salvate printr-un set de adrese IP pe care tu le defineşti. Dacă cineva încearcă să acceseze datele tale de la o adresă IP care nu este în lista definită de tine, accesul lui va fi oprit. Această metodă de securitate adițională asigură că fişierele salvate nu sunt deschise în orice locație, chiar daca userul şi parola sunt cunoscute.