Whitepaper – Segurança de Dados

Version 5.2.6
Outubro / 2008

Índice

1 Apresentação

Este documento descreve as características de segurança adotados pela iCOM para Backup de dados via o software próprio iCOMSAFE. Com linguagem clara e utilizando a perspectiva do usuário o documento serve como referência aos usuários e parceiros iCOM.

2. Servidor de Backup Remoto ICOM
Seguro, Robusto e Confiável

2.1 Segurança em 128/256-bit através de comunicação SSL

Toda a comunicação entre os servidores de Backup iCOM e o seu computador é realizadas através de um canal seguro de 128/256-bit que utiliza a tecnologia SSL (Secure Socket Layer). Esta tecnologia é amplamente utilizada por bancos e instituições financeiras para proteger as informações que trafegam nas redes. A utilização desta tecnologia mascara o fluxo\transporte de dados entre as duas extremidades (seu computador e o servidor iCOM).

2.2 Todos os Dados são Criptografados e Compactados

Todos os dados são compactados e criptografados antes de serem enviados via Internet. A criptografia é realizada no seu computador através da chave única, que somente você possui.
Desta forma mesmo que os dados fossem capturados por software furtivo, estes não fariam sentido algum pois estariam criptografados, impossibilitando a leitura.
A iCOM não armazenada chave de criptografia de seus clientes. Mantendo assim o elevado nível de segurança das informações armazenadas em nossos servidores.

2.3 Chave de Criptografia Única

A chave de criptografia única é criada e utilizada para criptografar seus arquivos, e é conhecida e armazenada somente por você. Esta chave não é transmitida via Internet.
Isto significa que se ocorrer perda da chave de criptografia será necessário efetuar o backup inicial novamente e criar uma nova chave.

2.4 Melhor Algoritmo de Criptografia

Atualmente os algoritmos de criptografia utilizados nos softwares iCOMSAFE e iCOMSAFE DATABASES são: 128 AES\ 256 AES, DES e TwoFish. Os algoritmos são blocos de cifras desenhados pela internacionalmente reconhecida empresa de segurança virtual: Counterpane Labs Inc. (http://bt.counterpane.com/) .
O algoritmo AES (Five Advanced Encryption standard), é do mesmo padrão utilizado pelo **NIST** (Instituto Nacional Norte Americano de Padrões e Tecnologia) http://www.nist.gov/ .
Os algoritmos são freqüentemente submetidos a revisões públicas, mas até o momento nenhum ataque bem sucedido à este código foi reportado.

2.5 Necessários 8.77 x 10^{17} anos para quebrar o código de criptografia 128/256-Bit.

A tamanho da chave de 128/256-Bit tem 2^{128} ou aproximadamente 3.4 x 10^{38} possíveis combinações. Mesmo se você tivesse hoje, o melhor supercomputador do mundo, o ASCI White SP Power3 375 MHZ fabricado pela IBM in Novembro 2000(com 8192 processadores, o qual possibilita uma capacidade de processamento de 12.3 Teraflops - trilhões de operações por segundo), levaria 8.77 x 10^{17} anos para testar todas as combinações possíveis.

Teste de combinações possíveis:

3.4 x 1038
---------- segundos ~ 2.76 x 10^{25}sec
12.3 x 1012
Ex.:. 876530835323573935 anos ou 8.77 x 10^{17} anos

Você pode ter 100% de certeza que seus dados estarão muito bem salvaguardados em nossos servidores seguros.

2.6 Acesso restrito à IPs não autorizados

Você poderá também restringir o acesso aos seus arquivos de backup através da solicitação de configuração de IP autorizados ou Range de IPs. Desta forma somente IP's autorizados terão acesso aos seus dados, e as demais tentativas de acesso serão negadas pelos servidores iCOM.
Este item de segurança adicional garante que seus arquivos de backup não poderão ser abertos de qualquer lugar, mesmo que a tentativa seja realizada por pessoa autorizada no sistema e que possua nome de usuário e senha válida.

Equipe de Segurança
iCOM