

Newsletter

Até onde vão as ‘firewalls’ da sua empresa

Nos últimos anos, as empresas por todo o mundo tomaram consciência dos riscos emergentes associados aos computadores e falhas de redes, bem como à perda de informação crucial.

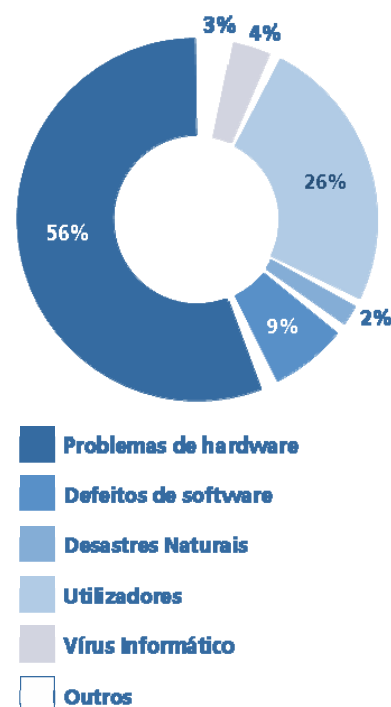
Todos os dias as redes informáticas das organizações são violadas por “hackers”, tentando encontrar falhas nos seus sistemas de segurança, causando graves danos.

São poucas as empresas a ter políticas correctas de “backup”

De acordo com as estatísticas “Ontrack” da Kroll, 93% de toda a informação/documentos é criada electronicamente, incluindo e-mails, cálculos, acordos, contratos e projectos de construção. Só 70% desta informação estará disponível em formato electrónico. A estatística mais preocupante é que só 26% desta informação de carácter profissional é guardada correctamente e que apenas 22,5% das empresas adoptaram políticas correctas de “backup”.

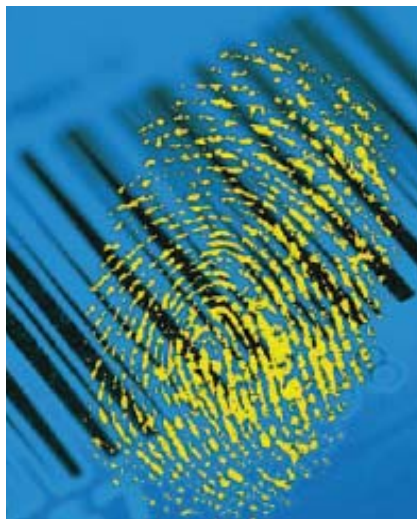
De longe que a maioria da perda de informação resulta de quebras no hardware. Com uns adicionais 26% atribuídos à má utilização dos profissionais envolvidos. Poderá surpreender, mas só aproximadamente 4% das perdas de informação se devem a vírus informáticos.

Causas da perda de dados



Quem está em risco?

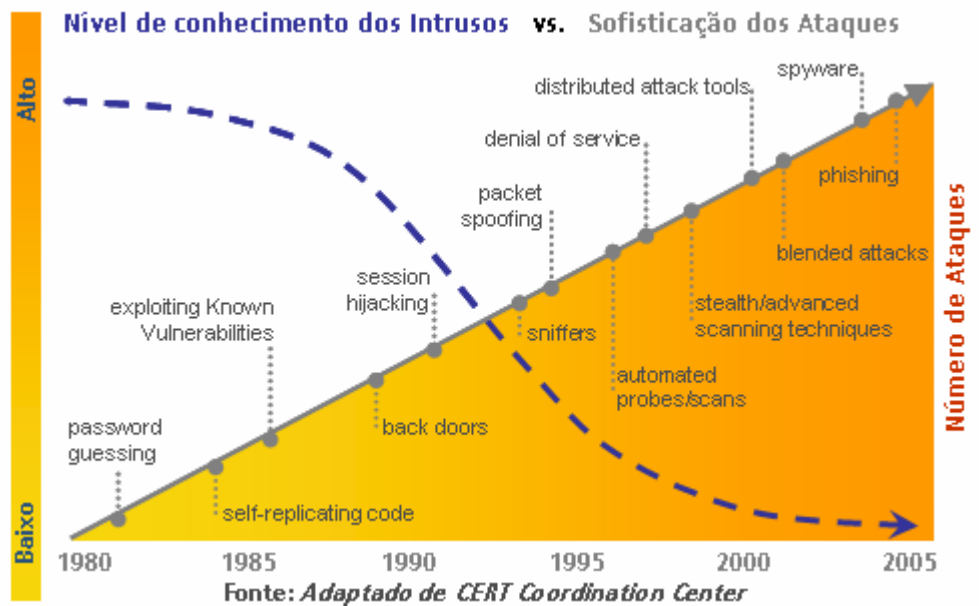
Virtualmente todas as empresas têm o risco de uma avaria séria nos sistemas de Informáticos. A título de exemplo, as companhias podem não ter condições para enviar a factura aos clientes ou para operar fábricas - os indesejados custos financeiros são inevitáveis. Consumidores que depositaram dados pessoais confidenciais, clientes, administradores, directores e accionistas são alguns dos interessados ou



afectados em situações relacionadas com os sistemas de informação.

A ciber-exposição (vírus, hackers, etc), a privacidade e segurança da informação, a propriedade intelectual e a disputa pelos direitos de patentes, a pirataria e contrafacção, a perda de capital intelectual para concorrentes, as cláusulas contratuais cada vez mais exigentes, quer nos prazos, quer nos aspectos relativos à qualidade (técnica, produtos,

serviços), quer na apresentação de garantias/cauções ou seguros de responsabilidade civil, a transferência ou a acumulação de responsabilidades após processos de fusões, aquisições ou parcerias regionais/mundiais, a integração de diferentes tecnologias (de versões e fornecedores/marcas diferentes), a deficiência de software ou hardware, os erros humanos e o blackout dos sistemas, são apenas alguns dos vectores que as empresas precisam ter em conta todos os dias da sua actividade, para garantirem o seu normal funcionamento, o cumprimento com as suas responsabilidades contratuais, bem como os danos causados a terceiros. Casos relacionados com algumas destas questões surgem diariamente nas primeiras páginas dos jornais desta nossa 'aldeia global' e em



na integridade, confidencialidade e a disponibilidade de dados electrónicos e do sistema tecnológico.

Transferência de Risco

Gradualmente, com maior frequência, as empresas estão sujeitas às exigências nas suas responsabilidades - passíveis de serem

risco associado às falhas informáticas: possuem firewalls, antivírus e ferramentas de segurança para prevenir o roubo de dados e promovem as cópias de segurança. No entanto, muitas não estão preparadas para reagir a situações súbitas e imprevistas.

$$\text{Risco Informático} = \text{Ameaça} \times \text{Vulnerabilidade} \times \text{Valor dos Activos}$$

simultâneo fortalecem um público cada vez mais qualificado e exigente, aumentando a preocupação com tudo o que diga respeito a notoriedade e reputação das marcas.

Risco Informático

O risco informático refere-se a um componente do Risco Operacional que uma empresa enfrenta pelo facto de confiar

transferidas para o mercado segurador. Na medida em que a procura de soluções no mercado segurador tem vindo a crescer por parte das empresas de IT, também a indústria seguradora tem apresentado melhores soluções e com maior capacidade para assumir os riscos inerentes.

Mitigação de Risco

Teoricamente, as empresas estão preparadas para gerir o

Finalmente, mesmo as empresas que têm políticas e procedimentos claros, incutem uma "cultura de segurança" nos seus empregados e adquirem as melhores ferramentas disponíveis não estão imunes aos 'ciber-problemas'. A transferência para o mercado segurador será a estratégia adequada para a proteger a empresa.

© Copyright 2007. Marsh Lda
All rights reserved

A informação contida no presente documento, é baseada em fontes que acreditamos serem fiáveis; mas não garantimos a sua precisão; e devem ser entendidas como informações de carácter geral no âmbito dos seguros. A Marsh não faz representações ou fornece quaisquer garantias, expressamente, bem como implicitamente, respeitantes à condição financeira, solvência, ou aplicação do clausulado do contrato de seguradoras ou resseguradoras. A informação não tem como objectivo ser tomada como um conselho no que diz respeito a situações individuais e não podem ser consideradas como tal. Os segurados deverão consultar os seus conselheiros de seguros no que respeita a coberturas individuais. Este documento ou alguma parte da informação nele contida não pode ser copiada ou mesmo reproduzida sem a permissão da Marsh, Lda, à excepção de clientes Marsh que queiram utilizar esta informação para uso estritamente interno.

Marsh, Lda
Av. Fontes Pereira de Melo, 51 - 6.º E
Edifício Monumental
Apartado 1072 - 1052-803 Lisboa
T. +351 213 113 700 F. +351 213 113 701
R. Júlio Dinis, 676 - 1º
4050-320 Porto
T. +351 226 058 600 F. +351 226 058 601