

FILIPE ROLO

Director de vendas da Trend  
Micro em Portugal

# Roubo de identidade: a verdade assustadora sobre perda de dados

O aumento crescente da perda de dados é uma preocupação constante para as empresas. De acordo com um estudo realizado em 2007 pelo King Research, a maior parte dos profissionais de TI sentem que os seus empregos entrariam numa espiral perigosa em caso de quebra de segurança. Por outro lado, não têm plena confiança nos mecanismos de combate à perda de dados pessoais e corporativos - cerca de três quartos dos mais de 250 profissionais de TI inquiridos manifestaram preocupação relativa à perda dos seus empregos na sequência de uma grave violação de segurança na sua empresa<sup>1</sup>.

## Roubo de Identidade

Nos EUA, o roubo de identidade está em pleno crescimento, apresentando uma média de 31 mil dólares gastos em cada caso em perdas para as empresas e utilizadores. Embora o roubo de identidade possa ocorrer quando é roubada uma carteira ou usados, com fins maliciosos, cartões de crédito de outras pessoas, a ameaça de fuga de dados e o acesso não autorizado a informações sensíveis de uma empresa é uma realidade cada vez mais crescente na protecção de dados e de privacidade.

Segundo a Attrition.org, uma organização de monitorização, mais de 162 milhões

de registos, tais como cartões de crédito e números da Segurança Social, foram comprometidos em 2007, em detrimento dos 49 milhões de registos identificados em 2006. Confirmando esta estatística, o Identity Theft Resource Center salienta que, até 18 de Dezembro de 2007, nos EUA, foram comprometidos mais de 79 milhões de registos, um aumento quatro vezes superior aos 20 milhões de registos de 2006<sup>2</sup>.

## Perda de dados - um problema generalizado

A perda de dados atinge consumidores e empresas. Todos os anos, nos EUA, as organizações registam perdas de milhões de dólares em propriedade intelectual quando software, design de produto, contratos, apresentações, formulários e planos de negócio são ilegalmente copiados. Surpreendentemente, são os colaboradores autorizados que provocam a maioria das perdas de dados corporativos - provavelmente porque têm fácil acesso a informação valiosa. De acordo com o Instituto Ponemon, 78% da perda de dados envolve acessos autorizados<sup>3</sup>. Apesar do facto de as empresas terem implementado medidas cautelares de protecção, como redes virtuais privadas (VPNs), firewalls e redes de vigilância, para prevenir o acesso externo não autorizado a informa-

ções privilegiadas, estas soluções não conseguem ainda enfrentar adequadamente a crescente ameaça dos utilizadores internos. A perda de dados pode ocorrer quer através da quebra de políticas da empresa, como o roubo de dados com fins lucrativos, quer por acidente, como a perda de portáteis.

Para além desta ameaça, a perda de dados ocorre quando "hackers" externos ou ladrões têm acesso às redes corporativas ou quando fisicamente entram nas instalações da empresa para roubar dados. Para além disso, os cibercriminosos são capazes de remotamente infectar os sistemas usando software malicioso para roubar informação valiosa e transferi-la para outros equipamentos que controlam.

## A indefinição entre o trabalho e casa

O crescimento de sistemas de mensagens instantâneas, rede sem fios, e dispositivos de armazenamento USB torna cada vez mais difícil a protecção de dados nas empresas. Além disso, cada vez mais os colaboradores transportam informação corporativa do trabalho para casa e vice-versa, o que aumenta a troca de informações através de dispositivos móveis. Esta realidade cria um enorme desafio para as empresas que pretendem proteger os seus dados contra a perda e o roubo de informações.

## Desafios de Segurança

Implementar soluções de segurança no ambiente de trabalho virtual é um desafio, especialmente com a proliferação de dispositivos móveis e sistemas de correio electrónico, Webmail, ftp, mensagens instantâneas (IM), Wi-Fi, discos USB, câmaras digitais, telemóveis, PDAs, laptops, CD/DVD e iPods.

É pouco prático e ineficaz bloquear o correio electrónico ou outras informações nos dispositivos móveis. Em vez disso, as soluções tecnológicas devem ser implementadas para proteger perdas de dados em cada end-point da empresa e qualquer rede corporativa ou privada, para que os dados empresariais permaneçam activos e seguros e os dados dos utilizadores permaneçam pessoais.

<sup>1</sup> "IT Professionals Fear Security Breach Could Cost Them Their Jobs, According to Recent Survey", [www.enterprise-networks-and-servers.com/newsflash/art.php?724](http://www.enterprise-networks-and-servers.com/newsflash/art.php?724), 30 de Abril de 2007

<sup>2</sup> Mark Jewell, AP, "Groups: Record Data Breaches in 2007", <http://attrition.org/news/content/08-01-03.html>

<sup>3</sup> Eric Sinrod, CNET News, "Going after the Bigger Insider Threats", [www.news.com/Going-after-the-bigger-insider-threats/2010-1029\\_3-6617692.html](http://www.news.com/Going-after-the-bigger-insider-threats/2010-1029_3-6617692.html), 20 Setembro de 2006