

Apesar de as empresas já investirem em soluções que diminuem esta vulnerabilidade

Mobilidade ameaça segurança...

Na verdade, é difícil retirar uma conclusão. A "Vida Económica" questionou alguns "players" do mercado sobre se a mobilidade efectivamente ameaça a segurança das redes empresariais. E tentou perceber até que ponto as empresas estão conscientes da vulnerabilidade a que ficam sujeitas a partir do momento em que tornam os seus recursos móveis. As respostas foram curiosas. Por um lado, há fornecedores que claramente não acreditam que a mobilidade afecte a segurança dos dados de uma organização. Até dizem mesmo que é um mito. Depois, temos outros "players" que dão a volta à pergunta e acabam por não responder directamente ao que foi formulado. E há ainda os que defendem com todas as letras que a mobilidade é de facto uma enorme ameaça para a segurança dos utilizadores e das empresas.

A mobilidade é de facto uma enorme ameaça para a segurança dos utilizadores e das empresas. Rui Oliveira, director-geral da iPortal Mais, representante em Portugal da Kaspersky foi quem de forma mais explícita respondeu à pergunta.

O responsável explica que, até os acessos à Internet não existirem nos telemóveis, a maior parte dos acessos à Internet eram feitos a partir das redes empresariais, que tem já hoje um mínimo de segurança, ou a partir de casa, onde as pessoas se habituaram a ter um firewall e um antivírus. Mas o que tem a maior parte dos telemóveis hoje que ligam à internet como protecção? Absolutamente nada, diz categoricamente Rui Oliveira. "E a ver pelo número de licenças vendidas pela nossa empresa no segmento móvel, no segmento empresarial e residencial, é para nós muito claro que o nível de protecção no segmento móvel é próximo de zero".

Quem é que hoje em dia se atreve a ligar-se com um PC ou um portátil à Internet sem se precaver com um antivírus? Quase ninguém, diz o director-geral, pelo menos quando se fala de pessoas que se preocupam com os conteúdos dos seus PC ou portáteis. "Muitos desses já notaram que mesmo o antivírus não chega e já tem um produto que junta o firewall pessoal ao antivírus".

Ora os telemóveis modernos são muito parecidos aos PC, diz Rui Oliveira, até porque têm quase tudo o que um PC tem e, sobretudo, tem as aplicações que são mais vítimas de infecções: leitor de correio electrónico, MSN e Skype. "Vamos assistir a uma verdadeira pandemia móvel. Ou seja, os programadores e vírus estão a adaptar os vírus dos PC para os móveis (o que é uma tarefa bem simples) e vão apanhar toda a gente desprevenida".

PHC e SMC não "acreditam" em insegurança

A PHC tem uma visão completamente diferente da de Rui Oliveira. Miguel Capelão, director de áreas tecnológicas, garante que de todo a mobilidade ameaça a segurança, apesar de referir esse é realmente o principal mito em relação à mobilidade.

Mas, afiança, "hoje existem ferramentas que permitem utilizar aplicações e dispositivos de mobilidade com toda a confiança. Nos diferentes produtos das gamas PHC Pocket e PHC Digital, as nossas soluções de mobilidade, incluímos várias dessas soluções de segurança, como um sistema de autenticação inter-

no. Além disso, permitem a utilização de diversos sistemas adicionais de segurança como SSL, que encripta todos os dados no acesso ao sistema, ou uma firewall que protege o servidor de ataques exteriores".

Em empresas com uma correcta aplicação das normas de segurança, a mobilidade é uma ameaça tão grande como a falta dela, diz Nuno Silveiro, country manager da SMC Networks. Tal como a visão da PHC, a SMC Networks igualmente garante que o conceito de que a mobilidade é mais insegura está já ultrapassado, visto existirem já diversas ferramentas de segurança que permitem minimizar os potenciais riscos.

Mobilidade pode ser ameaça se não se tomarem medidas

José Rocha, director-geral da Micro-Plus, representante em Portugal da AVG, é da opinião que a mobilidade pode ser uma ameaça se não foram tomadas as devidas precauções e utilizados sistemas de segurança adequados. O responsável alerta que devem ser usadas ligações VPN e encriptação de dados para se ligar ao servidor da empresa. "Isto cria um túnel seguro de ligação entre o computador e o servidor, protegendo os dados e os acessos. O portátil deve ter um sistema de antivírus eficiente, que tenha a capacidade de mudar de perfil de rede, de forma a adaptar-se às várias redes existentes, sempre de uma forma segura. Caso não o seja, pode correr o risco de entrar em redes infectadas, e depois infectar o computador e depois o servidor da empresa".

Actualmente, a mobilidade representa a grande autonomia das pessoas tendo em conta que podem aceder à informação de forma global, independentemente do local onde se encontrem. Traduz-se também numa nova forma de trabalhar e pode evidenciar um incremento da produtividade dos trabalhadores, permitindo-lhes aceder à informação corporativa, mesmo estando fora do escritório.

Mas, para Albano Formiga, Business Sales Consultant da CESCE SI, a mobilidade e a segurança possuem uma relação umbilical, uma relação que poucas vezes se concretiza, pois é dada pouca relevância à segurança. "A comunicação social, de algum tempo a esta parte, tem veiculado diversos artigos em que se denunciam diversos casos de perda de portáteis, pen-usb e pda, os quais contém informação confidencial pessoal ou do negócio". O responsável assume que

esta situação está atinente à "maravilha" de a mobilidade poder levar ou aceder à informação em qualquer lado. No entanto, diz, a segurança com que tal mobilidade se verifica constitui, para a maioria das pessoas, uma questão ficcionada e própria de um bom filme. "Esta ligação - mobilidade/segurança - requer algum trabalho de sensibilização por parte das organizações, nomeadamente, desde o aconselhar à utilização de ferramentas para protecção da informação até à criação de procedimentos de segurança".

A opinião de Sérgio Viana, Business Developer da Sybase, vem no alinhamento das anteriores. O responsável admite que a mobilidade tem vantagens para as empresas que decidam implementá-la, mas tem questões de segurança que não deverão ser descuradas. "No entanto,

A mobilidade e a segurança possuem uma relação umbilical, uma relação que poucas vezes se concretiza, pois é dada pouca relevância à segurança.

actualmente existem já ferramentas que permitem responder aos diversos problemas de segurança que podem ser identificados".

Mobilidade e globalização representam desafio

A mobilidade do utilizador e a globalização do ambiente corporativo representam um desafio para o qual o perímetro tradicional de segurança é ultrapassado, diz Renato Lopes, Account Manager Mid-Market da McAfee para Portugal. Este responsável explica que, nos últimos anos, a mobilidade das empresas no ambiente global criou uma classe de riscos de segurança. Este desenvolvimento, continua, faz com que o perímetro de rede, que normalmente é protegido por dispositivos de segurança, "desapareça". "Isto faz com que seja mais difícil manter uma rede segura. PDA e telefones "inteligentes", por exemplo, utilizam os sistemas operativos e aplicações que incluem vulnerabilidades que podem ser exploradas

de forma semelhante nos computadores portáteis". O desenvolvimento da tecnologia nas empresas permitiu às ameaças utilizarem vários pontos de entrada alternativos para penetrar numa rede, como, por exemplo, através dos empregados da empresa que trazem os seus computadores portáteis e PDA infectados para o escritório. "Isto permite ao malware e a outros tipos de ataques propagar-se livremente na rede protegida".

Atacantes estão sempre à procura dos elos mais fracos

O actual desafio para as empresas é conseguir proteger a informação corporativa, assegurando o acesso ubíquo à mesma através de uma multiplicidade de dispositivos, de redes e sistemas heterogéneos cada vez mais difíceis de gerir. Esta é a visão da Symantec.

Para Timóteo Meneses, director técnico da Symantec Portugal, os atacantes estão sempre à procura dos elos mais fracos (com novos vectores de ataques) para conseguir penetrar nas redes e roubar informação confidencial e crítica. "Verifica-se assim uma correlação de crescimento: à medida que cada vez mais administradores de sistemas implementam redes baseadas na conectividade sem fios, criam oportunidades adicionais para invasões e exploração de outros tipos de fragilidades nas mesmas, quer através de estratégias técnicas como sociais, tendo em conta os comportamentos dos utilizadores".

Com as LAN sem fios, diz o responsável, apenas precisam de estar dentro do alcance aéreo da ligação e apanhar o sinal, mesmo de fora do edifício. Mesmo as mais recentes normas de ligação aérea não são seguras e é importante que os utilizadores tenham consciência disso e adoptem posturas apropriadas de segurança.

Para além das LAN sem fios, as redes de voz utilizadas pelos portadores comerciais sem fios, para telefones inteligentes e PDA, são também potencialmente vulneráveis a intrusos e ataques maliciosos. Ainda que a maioria dos vírus da actualidade seja escrita para os sistemas operativos DOS e Windows, baseados em PC, temos já diversos exemplos de casos em que os hackers deitaram as mãos aos sistemas operativos mais compactos como os utilizados nos dispositivos móveis, tais como o PalmOS, o Windows CE/Pocket PC e o Symbia.

