

A Segurança da geração que voa na Nuvem

A geração Y provocou a computação em nuvem – uma grande nuvem, que “não é passageira” e se expande na forma do e-universo social e corporativo da Internet, onde bilhões de internautas navegam e exigem conveniência e tempestividade. Esta juventude demanda uma segurança mais natural, menos invasiva.



Paulo Sergio Pagliusi, Ph.D.

(paulo.pagliusi@arcon.com.br)

O autor é Gerente de Portfólio & Produtos na Arcon Serviços Gerenciados de Segurança, e Diretor de Comunicação da Information Systems Audit and Control Association (ISACA), no Rio de Janeiro.

Julho de 2011

A geração Y, também chamada de geração *Net*, engloba os nascidos entre 1980 e 2000. É composta por uma juventude multitarefa e arrojada, que respira tecnologia em tudo o que vê e faz. Um traço marcante destes jovens concebidos na era digital, segundo Don Tapscott¹, é que desejam conveniência e tempestividade: não são fiéis a marcas e demandam resposta em tempo real. São velozes e querem tudo muito mais rápido. Além disto, são impulsivos, impacientes, ansiosos e intensos. Por isto, eles já foram acusados de tudo: distraídos, superficiais e até egoístas. Mas se preocupam com o meio ambiente, possuem fortes valores morais e estão prontos para mudar o mundo.

Na opinião deste autor, o mundo já foi modificado de forma marcante por essa juventude. Com sua demanda por conveniência e tempestividade, a geração Y provocou o desenvolvimento da *computação em nuvem*². Novas demandas em computação em nuvem e em virtualização surgiram por conta dessa geração, pois a Internet precisou aprender a se comunicar com esse público, que quer tudo para ontem. As instituições que ignoram isso só têm a perder e não estão no século XXI.

“Por que não posso ler um artigo na tela enquanto termino de baixar um vídeo no computador?”, questionou um universitário de Cuiabá, de 19 anos, durante uma apresentação. Seu amigo sentado ao lado, de 17 anos, completou: “Minha mãe não consegue entender como consigo fazer tanta coisa ao mesmo tempo na Internet. Mas isso funciona muito bem”, disse ele. Frases como estas, comumente ouvidas por este autor, destacam algumas das características da geração Y, que costuma ser público e também tema de suas palestras sobre segurança do ambiente em nuvem. Estes são exemplos de como a geração Y relaciona-se com o ambiente da nuvem. Estes jovens cresceram conectados à Internet.

Em particular, a nuvem se desenvolve devido à *elasticidade ágil*, uma característica fundamental deste novo modelo tecnológico de computação. Ela consiste no conjunto de capacidades que podem ser rápida e elasticamente provisionadas pela nuvem, em

¹ Don Tapscott. *Grown up digital: how the net generation is changing your world*. McGraw-Hill, 2009.

² *Computação em nuvem*: modelo tecnológico que provê alta disponibilidade e habilita ao usuário, de modo simplificado, o acesso sob demanda a uma rede (autosserviço por demanda). Esta rede possui recursos computacionais configuráveis (ex. banda, processamento, memória, máq. virtuais, espaço disco, aplicações e serviços), alocados dinamicamente, mediante um serviço de rede mensurado.

alguns casos automaticamente. Essa característica permite aumentar ou diminuir a utilização de recursos virtuais, de forma que pareçam ilimitados e possam ser adquiridos em qualquer quantidade, a qualquer hora, para se ajustarem às oscilações de demanda.

Isto reduz a ineficiência do modelo de computação tradicional, em que normalmente se projeta uma capacidade acima do uso normal, para garantir um desempenho aceitável em picos de demanda, pois depende de uma infraestrutura física, pré-existente – como a do centro de dados de uma empresa. Por isto, este modelo é limitado a uma *escalabilidade*³, que pode ser lenta e complexa de se obter, à medida que se aproxima dos limites de sua capacidade e disponibilidade de acesso.

Portanto, o modelo tecnológico da computação tradicional pode tornar-se incapaz de atender aos anseios da qualidade percebida⁴ pela geração *Net*. Em oposição, a elasticidade ágil da nuvem provê recursos virtuais, sob demanda e com gerenciamento mínimo. Esta característica é essencial para o crescimento da nuvem, pois permite às corporações satisfazerem às exigências desta nova geração, de modo adequado em custo benefício.

Mas a nuvem trás um nível adicional de riscos, diretamente associados à terceirização de serviços essenciais (serviços em nuvem). Isto exige atenção especial na observância aos princípios da segurança da informação: disponibilidade, integridade, confidencialidade e autenticidade, bem como na privacidade, no suporte e na conformidade. Entretanto, a computação em nuvem traz benefícios relacionados ao fato de que, nela, não se necessita desenvolver controles internos de segurança nem capacitar pessoas neste segmento. Neste novo modelo de prestação de serviços, é fundamental o estabelecimento de uma relação de confiança entre o cliente e o provedor. A transparência da forma como o provedor implementa, desenvolve e gerencia a segurança é fator decisivo para se atingir este objetivo. Outro importante desafio imposto à computação em nuvem é possibilitar o atendimento dos anseios da Geração Y.

Há, assim, o grande desafio de se oferecer uma nuvem que concilie segurança com mobilidade, interação e rapidez, para esse público que se insere cada vez mais no mercado. São jovens que gostam de interação, andam em tribos - formadas por redes sociais e sítios de relacionamento -, e consideram primordial preservar a segurança e a mobilidade no acesso à Internet. Porém, há uma forte tendência das redes sociais serem o principal vetor de propagação de ameaças, e a nuvem que as hospeda encontra-se fora

³ Em telecomunicações e engenharia de *software*, *escalabilidade* é uma propriedade de um sistema, rede, ou um processo, que indica sua habilidade para gerenciar quantidades crescentes de trabalho. Para se aumentar a escalabilidade, na computação tradicional é preciso acrescentar recursos físicos, incluindo mais máquinas (escalabilidade horizontal), ou mais recursos às máquinas existentes (escalabilidade vertical), tais como processadores, memória, discos rígidos ou um link mais poderoso com a rede. Por se ater ao mundo físico, esta expansão demanda mais tempo e exige mais recursos para se concretizar do que no mundo virtual.

⁴ Vide: SOCOLOWSKI, Jorge Carlos. *A disponibilidade de acesso como componente da qualidade percebida do serviço de Internet Banking e seu tratamento por um banco brasileiro de varejo: um estudo de caso*. Dissertação de Mestrado. Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas, São Paulo, 2008. (Em: http://www.gv.br/nova_intranet/Secretarias/posgraduacao/envio/MP/AE/176599.pdf)

do controle das organizações. Entre tais ameaças, destacam-se os ataques DDoS (*Distributed Denial of Service* - negação de serviço), fraudes, perda ou furto de dados, por meio de *Phishing Scam* e *Malware*, muitas vezes acessados inadvertidamente por meio de “encurtadores” de URL (como os produzidos pelo Twitter), falsificação e furto de identidade, pirataria e evasão de propriedade intelectual, crimes contra a honra (difamação, injúria e calúnia), e até mesmo *cyber bullying*.

Destaca-se que tais ameaças não são “vapor d’água”, ou seja, há razões para se preocupar, principalmente porque os problemas se localizam onde as empresas não têm controle. Ressalta-se que, no Brasil, 99,9% (46,7 milhões) dos internautas estão conectados em alguma rede social, segundo o comScore⁵. O país possui o maior número de usuários de Orkut do mundo, além da 2ª maior audiência do YouTube, e a 3ª maior audiência do Twitter. Além disto, 36% dos internautas no Brasil fazem diariamente *upload* de fotos e vídeos, e 2,6 milhões atualizam *blogs*.

É preciso, então, utilizar inteligência no contexto da nuvem. Ao invés de se proteger ativos em um perímetro, por meio de uma ação de *segurança*, como ocorre na computação tradicional, deve-se antecipar à ameaça na nuvem, identificando-a fora do ambiente de controle, antes que ela se materialize em um ataque, por meio de uma ação de *defesa*. O mercado financeiro foi o primeiro a utilizar esta estratégia de defesa, bem antes do surgimento da nuvem, ao tomar medidas preventivas para controle de ameaças a bolsas de valores. Assim, pode-se, por exemplo, monitorar diariamente na Internet a marca da empresa ou organização, para verificar se alguém clonou a página da corporação, se não está havendo desvio de tráfego em motores de busca (Google, Yahoo), entre outras ações de defesa.

Como solução para permitir o acesso a redes sociais e demais canais de relacionamento da Internet, com uma segurança ágil e ao mesmo tempo eficaz e alinhada aos anseios desta juventude, a biometria, os padrões comportamentais e a holografia podem apontar algumas saídas. Além disto, podem promover uma segurança não intrusiva, mais natural e menos invasiva. O desafio maior é conciliar esta almejada segurança com as exigências de mobilidade e rapidez de resposta no acesso ao ambiente de computação em nuvem. Um problema fundamental é a identidade na rede, considerando a multiplicidade de canais existentes. Tais desafios precisam ser vencidos em tempo real, para se atender à demanda de inclusão digital e de comunicação dessa dinâmica geração. A conclusão a que se chega é a de que há evidências apontando a Geração Y como responsável pelo crescimento da nuvem, ou seja, de que "a Geração Y provocou a computação em nuvem".

⁵Link: <http://www.comscore.com/>, acessado em 28Jun2011.