A **segurança** da nuvem na perspectiva de um **CIO**

Stephen Orban

A segurança da nuvem na perspectiva de um CIO –

Stephen Orban – AWS Global Head of Enterprise Strategy

“Muitas pessoas estão pensando em segurança em vez de oportunidade. Parecem ter mais medo da vida do que da morte.” - James F. Bymes

Segurança é um tópico amplo, e se aplica de alguma forma a tudo o que acontece em TI. Em meus anos de trabalho em tecnologia, descobri que segurança era a única palavra com o poder de enfraquecer qualquer iniciativa. Nos primeiros dias da computação em nuvem, era comum para aqueles que não a entendiam questionar o quão confiável ela poderia ser. Ao invés de ajudar suas organizações a entender como eles poderiam se beneficiar da nuvem, eles criaram uma barreira para a sua evolução. Até recentemente, em 2012, quando comecei a usar a AWS para iniciativas empresariais significativas, ainda havia entre meus colegas e na minha organização um grande ceticismo que apenas a experiência poderia mudar. Os resultados, porém, convenceram mesmo os mais relutantes a confiar que a AWS nos ajudava a proteger nossos sistemas muito melhor do que se tentássemos protegê-los sozinhos.

Como ex-CIO e cliente AWS, aqui estão alguns pontos que mudaram a maneira como eu pensava sobre segurança na nuvem:

Eu sabia que a segurança é e sempre será a principal prioridade da AWS. É mandatório para servir uma base de clientes tão ampla e diversificada, em tantas indústrias e governos. Tínhamos sistemas PCI, dados PII, requisitos SOX e propriedade intelectual para proteger. Observar como outras empresas foram capazes de desenvolver soluções que cumpriam com as conformidades de segurança na nuvem foi instrutivo e gerou ainda mais confiança.

Eu tinha certeza que a AWS estava dedicando muito mais recursos para proteger sua plataforma do que o que eu tinha disponível para suportar todo o meu negócio, muito menos para investir só em segurança. Como muitas empresas que gerenciam seus

próprios data centers, estávamos constantemente fazendo análises para compensar custo, time-to-market, qualidade e segurança. Estas decisões nunca são fáceis, e nem sempre fica claro se você fez o caminho certo. Uma mudança de firewall sem uma avaliação cuidadosa, uma configuração incorreta de um cabo ou um provisionamento de SO apressado pode afetar a reputação da sua segurança. Se você trabalha na área de TI de uma empresa há algum tempo, tenho certeza que pode se identificar. É assustador pensar em quanta vulnerabilidade podemos causar a cada decisão. Se a segurança é sua prioridade número um, você não pode tomar atalhos.

Eu sabia que reduzir nossa superfície nos permitiria concentrar nossos esforços em nossos diferenciadores. Alavancar a segurança empregada nas instalações da AWS nos permitiu alocar alguns de nossos recursos dedicados à proteção de nosso hardware para proteger nossas aplicações. O crescente número de ameaças e a crescente comunidade de black hat eram questões que já nos exigiam mais esforços na segurança de aplicativos, independentemente de onde hospedávamos a nossa infraestrutura. Ser capaz de adicionar recursos a este esforço em um mesmo lugar me daria ainda mais paz de espírito. O modelo de responsabilidade compartilhada não implica menos responsabilidade, mas ajuda. Eu queria toda a ajuda que eu pudesse obter.

Eu sabia que a AWS tinha uma maior visibilidade da segurança global do que nós jamais teríamos de nossas próprias operações sozinhos. Eu estava ansioso para tirar proveito das economias de escala. Poderíamos nos beneficiar de todas as melhorias feitas para cada cliente da AWS.

Eu sabia que a automação reduz a probabilidade de erro humano. Isso se aplica à segurança da mesma maneira que se aplica ao desenvolvimento de aplicativos. Estávamos determinados a automatizar cada vez mais as tarefas de tecnologia repetitivas. Eu sabia que a AWS dependia fortemente da automação para escalar e reduzir as chances de erro humano, melhorando seu modelo de segurança. Ter um

parceiro para nos incentivar e para nos ensinar a automatizar melhor provou-se um grande benefício.

A CIO&LEADER entrevistou recentemente Stephen Schmidt, CISO da AWS, sobre uma variedade de tópicos relacionados à segurança. Na entrevista, Stephen fala sobre escala, investimento e automação e como essas questões se aplicam à segurança na AWS. Eu senti que esta entrevista reforçou minhas opiniões, e que valia a pena compartilhar com os que usam ou estão considerando usar a AWS. O artigo da entrevista foi publicado na edição de dezembro de 2014 da revista impressa da CIO & LEADER. A transcrição completa, abaixo, é reproduzida com permissão da CIO & LEADER.

CIO & LEADER: *A maioria dos líderes de segurança de informações corporativas estão perdidos quando se trata de ameaças da próxima geração, como DDoS e APT. Quão grande é uma ameaça para vocês e como conseguem contê-la?*

Stephen Schmidt*: Nós vemos quase tudo o que acontece na Internet. Gostaria de compartilhar algumas estatísticas interessantes para ajudar a quantificar isso. Cerca de 1 em cada 500 endereços IP que são roteados da Internet para a Amazon, e cerca de 1 em cada 700 são mapeados ativamente para uma instância EC2. Você pode pensar em nós como uma matriz de telescópio muito grande implantado para encontrar um objeto muito pequeno. Isso nos permite identificar ameaças que estão vindo contra nossos clientes e construir nossos serviços para ajudá-los a se proteger contra essas ameaças. Por exemplo, muitos dos atores do APT tentam reunir nomes de usuários e senhas legítimos. Esta é uma das razões pelas quais não permitimos nomes de usuário e senhas nas redes que contêm dados de clientes. Demos cartões inteligentes, por ser um dispositivo físico que você deve ter em sua posse e é realmente difícil para esses atores roubarem.*

CIO & LEADER: *Riscos de terceiros também são motivo de preocupação para os profissionais de segurança. Como você, como CISO, supera esses riscos?*

***Schmidt**: Para minimizar esses riscos, é importante garantir que o terceiro com quem trabalhamos atenda aos mesmos padrões de segurança que nós. Temos de ser capazes de transmitir um conjunto comum de práticas de segurança para nossos clientes. Nós nos certificamos que sigam isso estritamente. A maneira como fazemos isso é através de auditorias. Por exemplo, se tivermos um ambiente CloudFront que está em um local de co-localização em algum país, exigimos que o provedor de co-localização forneça exatamente os mesmos requisitos de segurança que nós. Isso faz parte do nosso acordo com eles e os testamos regularmente. Então, eu tenho uma equipe cujo trabalho é visitar fisicamente cada local que temos em todo o mundo várias vezes por ano. Fazemos inspeções inesperadas, nós apenas aparecemos lá e certificamo-nos de que estão fazendo exatamente o que devem fazer. Nossas exigências são tão rigorosas que as reduzimos ao nível da construção. Por exemplo, se eles estão usando fasteners aprovados, pinos e parafusos ou não, para que você não possa de fato desaparafusar nada do lado de fora. Verificamos as dimensões dos furos nas paredes para garantir que não são maiores do que um determinado tamanho, para que você não possa passar uma mão através dele e fazer algo. Garantimos que o cabeamento que sai de nossas instalações está dentro de condutas invioláveis. Então há uma lista inteira de critérios que nós atravessamos para certificarmos de que nossos fornecedores seguem as nossas exigências particulares.*

***CIO & LEADER**: Vocês certamente têm uma estratégia robusta de mitigação de riscos de terceiros. Mas como vocês contrariam ameaças internas?*
***Schmidt**: A melhor maneira de combater a ameaça interna é limitar o acesso humano aos dados. Então, uma das coisas que fazemos internamente é reduzir ativamente o número de pessoas que podem acessar informações. Mesmo que nosso negócio esteja crescendo loucamente, todas as semanas nós reduzimos o número de seres humanos com acesso à informação que pertence aos nossos clientes. Podemos conseguir isso através da automação. Por exemplo, se um ser humano precisa fazer algo repetidamente mais de uma ou duas vezes, decidimos corrigir isso. Nós tentamos construir uma ferramenta que pode fazê-lo automaticamente. Esta abordagem tem dois*

benefícios. Em primeiro lugar, as ferramentas raramente correm mal. Eles fazem a coisa certa, a mesma coisa todas as vezes. Os seres humanos, por outro lado, podem fazer um erro tipográfico e causar um problema. Em segundo lugar, aumenta a disponibilidade. A automação, portanto, melhora a segurança e a disponibilidade.

***CIO & LEADER**: Então, onde a AWS planeja gastar em 2015? Em quais tecnologias e soluções a empresa vai se concentrar?*
***Schmidt**: Para a AWS, a única área em que nos focaremos fortemente é a criptografia. Será criptografia onipresente, ou seja, criptografia em todos os pontos. A outra área onde direcionaremos nossas energias seria fornecer mais controle do cliente sobre essa criptografia para que eles possam também controlar as chaves. O terceiro seria garantir que damos aos nossos clientes ferramentas para ajudá-los a tomar boas decisões de segurança. Os clientes estão acostumados a serem informados pelos fornecedores de que, se surgir um problema, os próprios clientes vão corrigi-lo. Na AWS, tomamos uma abordagem diferente. Em vez disso, a AWS faz da seguinte maneira: aqui está a situação onde você pode melhorar, e aqui está o botão que diz como melhorar ou corrigi-lo. O ponto é: damos aos clientes as ferramentas que eles precisam, muito baratas ou livres, para que eles possam corrigir sozinhos.*

***CIO & LEADER**: Como CISO, onde você planeja investir?*
***Schmidt**: Nós investimos muito na automação, então uma das coisas que mais construímos são ferramentas. E fazemos enormes quantidades de automação em práticas comuns de segurança, em testes comuns de penetração e de gerenciamento de configuração, entre muitos outros, para garantir que as coisas estão fazendo o que precisam estar fazendo. Essas são áreas onde fazemos um grande investimento a cada ano. Por duas razões: uma, os benefícios definitivos de segurança; e a outra é que eu simplesmente não consigo operar com a escala que temos sem automação. Não há nenhuma maneira que eu possa contratar engenheiros de segurança em número e qualidade suficiente para cobrir os serviços AWS, tão grande como eles são, se eu não automatizar rapidamente. Investimos muito esforço em automação.*

Criar sistemas seguros para a sua empresa é um princípio fundamental do trabalho de qualquer executivo de TI. Por que não usar as melhores ferramentas disponíveis para isso? A maioria dos atletas profissionais irá dizer-lhe que seus equipamentos importam. Não é um substituto para o talento, prática e trabalho duro, mas se o uso de melhores equipamentos tiver o potencial de melhorar o desempenho, eles vão usá-lo. A nuvem não é um substituto para ter o melhor talento, disciplina e governança em seus sistemas, mas aumenta as suas chances.

Keep building,

-Stephen

@stephenorban

orbans@amazon.com