



Por Adriano Filadoro(*)

Independentemente do tamanho de uma empresa, uma coisa é certa: ela está passando por importantes mudanças em termos de geração e gestão de informação, devendo buscar um nível de segurança, organização e agilidade que facilite o crescimento sem comprometer a estabilidade do sistema. Isso impõe novos desafios ao departamento de TI (Tecnologia da Informação), que está sempre buscando adequar suas necessidades ao poder de investimento.

Enquanto há muitas empresas aumentando sua representatividade em território nacional e presença global, outras também estão facilitando o acesso de executivos aos dados da base central – seja através de um home office, notebook ou smartphone. Esse processo precisa ser rápido e seguro. Empresas voltadas para o comércio eletrônico também dependem de que todos os dados e aplicativos estejam totalmente integrados, a fim de não dar margem a erros e colocar a carteira de clientes em risco.

Como toda informação de uma empresa, hoje em dia, está armazenada numa rede conectada a um ou mais servidores e vários computadores e dispositivos móveis, é preciso conhecer e investir em soluções que aumentem a segurança do conjunto. Afinal, hackers e crackers se empenham em descobrir vulnerabilidades e falhas que facilitem suas ações. Invadir sistemas, adulterar programas, obter e vender informações, usar senhas e dados bancários em benefício próprio, pichar ou tirar sites do ar, criar vírus e todas as pragas virtuais são um ‘divertimento’ lucrativo em muitos casos.

Vale dizer que o nível de segurança exigido está diretamente ligado às atividades da empresa, ao perfil e ao volume de usuários que acessam o sistema. Embora nenhum recurso ofereça 100% de segurança, há soluções que, quando usadas em conjunto, podem chegar muito perto disso. O importante é adequar o nível de segurança para cada departamento da empresa, fazendo uma varredura para detectar onde estão as falhas que precisam ser corrigidas. A seguir, conheça ONZE soluções que atendem vários níveis de segurança nas empresas:

1. Controle de rede.

Ao interromper o tráfego malicioso através de um sistema que controla o transporte de dados, a segurança da empresa é potencializada de um modo sem precedentes – já que a maioria classifica apenas velocidade e desempenho como prioridade. Outro ponto forte do controle da rede é aumentar a detecção do risco e da vulnerabilidade do negócio, fazendo com que o fluxo de informações esteja sempre bem protegido e seja o grande acelerador de negócios da empresa.

2. ‘Nuvem contínua’.

Empresas que necessitam de máxima proteção às suas operações e às informações geradas têm de garantir acesso seguro a redes, servidores, data centers, aplicações etc. A nuvem contínua (ou real cloud, como também é conhecida) representa um passo à frente de tudo o que está disponível, possibilitando que as aplicações da empresa estejam ativas em múltiplos sites, prontas para serem liberadas automaticamente sempre que forem solicitadas. Trata-se de um ganho imenso em termos de competitividade, permitindo que uma empresa faça em poucos minutos o que suas concorrentes provavelmente vão levar semanas para finalizar.

3. Backup na nuvem.

Essa solução inclui volume de backup, software de gestão e replicação de dados para um local remoto. Também contempla a centralização do volume de backup in-house, aplicando deduplicação nessa massa de dados para evitar repetição de segmentos. A empresa contrata a utilização de banda e o volume de disco necessários para a replicação para um local remoto, com um monitoramento efetivo dos processos de backup realizados por uma equipe em tempo integral,

todos os dias do ano.

4. Monitoramento e controle.

Além de desenvolver políticas de segurança para cada empresa ou departamento, é importante adotar um mecanismo de comunicação da política adotada, promovendo amplo entendimento das vulnerabilidades que devem ser evitadas. Esse processo deve ser revisado e retransmitido continuamente para melhor resultado.

5. Pacote de integridade.

São adotados alguns métodos de verificação da integridade de pacotes e rastreabilidade da procedência, evitando possíveis contágios na infraestrutura através de ataques virtuais quando da instalação de pacotes.

6. Perímetro de segurança.

Trata-se de um conjunto de políticas de segurança utilizado em programas e equipamentos que tem por objetivo reforçar o acesso físico e impedir a propagação de vírus por meio de dispositivos móveis (celulares, tablets, notebooks etc.).

7. Segurança de endpoints.

Neste caso, medidas de segurança são implantadas em todos os dispositivos móveis que em algum momento são conectados à rede: pendrives, smartphones, tablets, notebooks... Essa medida complementa a solução 'perímetro de segurança', evitando todo tipo de fraude e contaminação.

8. Gestão da largura da banda.

O objetivo é prevenir congestionamentos, tráfego lento de informações e abusos, bem como ataques à rede.

9. Inspeção de segurança.

Neste caso, a empresa conta com um monitoramento ativo, alinhado com sua política de segurança, para identificar os inúmeros tipos de ameaças e consequente solução de controle.

10. Filtro de IP.

Essa é uma solução de baixo custo para incrementar a segurança da rede. De acordo com as definições do protocolo, é realizada a filtragem por endereços de origem ou destino. Ou seja: alguns serviços poderão ser acessados somente por determinadas máquinas. Também é possível bloquear o tráfego de alguns pontos de origem.

11. Antivírus e AntiSpam.

Essas soluções são as mais populares, mas também são absolutamente necessárias hoje em dia, sob pena de haver uma queda brusca na produtividade ou a perda total de informações. São soluções que filtram mensagens e repelem intrusos, evitando que tenham acesso a informações estratégicas e comprometam a integridade da empresa. Apesar de simples, essas medidas jamais devem ser negligenciadas.

(*) Adriano Filadoro é diretor comercial e de marketing da [Online Data Cloud](#), empresa de serviços com mais de 20 anos de atuação na indústria de Tecnologia da Informação.

Fonte: [Canaltech](#), em 04.08.2014.