Especialista indica caminhos para tornar a segurança parte da missão da empresa e evitar ataques virtuais

Cresce o número de empresas que reportam ataques cibernéticos. Nos últimos dois casos, os CEOs das companhias pediram demissão logo após os acontecimentos. Não é novidade que os ataques estão cada vez mais sofisticados e prejudiciais, tendo como alvo o que as organizações mais valorizam: os dados de clientes, a propriedade intelectual e a reputação.

A frequência dos ataques mostra que as companhias precisam de uma nova abordagem para a segurança. Por isso, Nathaniel Fick, ex-oficial da Marinha dos Estados Unidos e CEO da Endgame, aconselha: veja o tema com os olhos dos seus atacantes. O objetivo é entrar na mente do inimigo e ver como eles conduzem a invasão, a fim de antecipar e se preparar para o que está por vir.

Infelizmente, segundo ele, essa mentalidade é rara. Apesar de gastar bilhões todos os anos em produtos de segurança e na contratação dos melhores engenheiros e analistas de segurança, empresas estão mais vulneráveis do que nunca. Duas tendências são responsáveis por isso, afirma. A primeira é a rápida convergência das arquiteturas corporativas de TI, e a segunda é a proliferação de adversários cada vez mais sofisticados.

Para olhar sob a perspectiva do cibercriminoso, Fick lista, na revista Harvard Business Review, quatro passos importantes que podem ser seguidos.

1. Entenda seus principais riscos e como os criminosos pretendem explorá-los

Se a segurança pudesse ser calculada, então o adversário seria o numerador. As empresas devem compreender suas técnicas únicas para blindar o cibercriminoso. Uma segurança eficaz deve integrar indicadores de compromisso (temos sido atacados?), táticas, técnicas e procedimentos (como estamos sendo alvo?), inteligência de identidade (quem pode nos alcançar, e por quê?), inteligência de vulnerabilidade (o que está sendo explorado?) e atribuição de ataque (é uma ou commoditie).

Com uma inteligência de ameaças direcionada, analistas podem direcionar seu tempo investigando os incidentes mais importantes, priorizando os maiores riscos para os negócios. Identifique seus bens mais essenciais e concentre recursos apenas nas ameaças que realmente representam um risco para a sua empresa.

2. Faça um inventário de seus bens e o monitore continuamente

Se a segurança pode ser calculada, então você precisa de um inventário. No nível mais simples, as empresas devem identificar e monitorar todos os seus ativos, respondendo perguntas como: quais aplicativos estão rodando nos servidores de banco de dados que guardam suas informações mais valiosas? Será que um funcionário pode plugar um novo dispositivo à sua rede corporativa?

Empresas devem manter um inventário dinâmico em tempo real dos ativos, monitorando-o de forma contínua. Além disso, é preciso torná-lo visualmente simples e intuitivo para as equipes de segurança e operações.

3. Faça da segurança parte da sua missão

O novo modelo de segurança precisa assegurar que a companhia tem os melhores defensores contra os melhores atacantes. Segurança não é delegável, e a missão de equipes de segurança deve ser sinônimo da missão da empresa.

4. Seja ativo, não passivo, na caça a adversários em sua rede

Já que você não pode atacar outra equipe em seu próprio território, você pode, e deve, ter cada vez de ter uma postura pró-ativa de proteção contra adversários dentro de suas redes.

Isso significa não apenas assumir que você está sob ataque, mas que o atacante está dentro, e por isso você deve conter e corrigir o risco antes que eles causem prejuízos, reduzindo drasticamente o tempo entre a violação e a detecção em mais de 200 dias.

Fonte: IT Forum 365, em 25.03.2015.