Por Andressa Soares (*)

Há mais de um ano transformamos nossas casas em escritórios devido à pandemia da Covid-19. Entretanto, o cenário de trabalho à distância já estava em ritmo crescente nas empresas brasileiras dada às novas tecnologias e mentalidades corporativas. A pandemia, então, apenas acelerou este processo, forçando as organizações a seguirem por um caminho sem qualquer planejamento. Como resultado, gargalos provavelmente surgiram, abrindo a porta para invasões cibernéticas.

Somente em 2020, foram detectadas 8,4 bilhões de tentativas de invasões maliciosas no Brasil, segundo a Confederação Nacional das Seguradoras (CNSeg). De acordo com a instituição, a adoção do regime de home office contribuiu para elevar ainda mais essas ocorrências de ataques cibernéticos, pois os criminosos virtuais estão aproveitando o novo cenário para invadir as redes corporativas por meio de senhas fracas e phishing - técnica de engenharia social usada para enganar usuários e obter informações confidenciais, gerando prejuízos incalculáveis.

Diariamente, milhões de mensagens eletrônicas são enviadas com o objetivo de fisgar vítimas e introduzi-las voluntariamente ao erro por fornecerem determinadas informações que, como consequência, expõem dados pessoais e, ou, coorporativos. Cair num golpe on-line resulta em inúmeras dificuldades e prejuízos para a vítima, mas, àquelas empresas que tiveram seus dados roubados e expostos, têm muito mais problema.

Portanto, este tem sido o principal foco dos criminosos: um sistema de segurança falho ou um funcionário que não esteja seguindo procedimentos de segurança, sendo necessário apenas um clique para sequestrar informações sensíveis e confidenciais que, dependendo da situação, só podem ser recuperadas mediante a pagamentos milionários. A IBM (International Business Machines Corporation) afirma que o custo para reparar um vazamento de dados em uma empresa no Brasil pode chegar à média de US$ 1,24 milhão.

A utilização de senhas fracas por colaboradores também é um dos principais fatores que contribuem com o cibercrime. Teoricamente, as senhas são a porta de entrada para o on-line e, portanto, precisam ser tratadas com muita atenção. Mas, a realidade é outra. A senha 123456 ainda está entre as mais utilizadas pelos colaboradores, segundo a NordPass, uma empresa de gerenciamento de palavras-chave.

Num momento como esse, questiona-se "qual o caminho para minimizar possíveis riscos, tornando o novo cenário corporativo mais seguro?" A resposta é que a prática e a prevenção precisam caminhar juntas. Neste sentido, medidas de segurança precisam ser revisadas e aplicadas, mas, principalmente, todos os colaborados precisam entender os riscos existentes por meio de treinamentos.

Uma das principais boas práticas é a utilização de VPN’s (do inglês, Virtual Private Network) para acessar redes coorporativas internas, como forma de garantir que os dados não sejam interceptados. Além disso, é necessário aplicar a autenticação em dois fatores, utilizar controles para a transferência de arquivos via USB e implementar uma política de senhas fortes auxiliada a sistemas que permitam apagar dados caso um aparelho seja roubado ou perdido. Aqui, é muito importante que o controle esteja com a TI da empresa ao invés do usuário.

Num outro ponto, capacitar os colaboradores para lidar com as ameaças de engenharia social é tão fundamental quanto cuidar de softwares ou aplicações, pois a capacitação combinada com a informação continua sendo a melhor prevenção. Atualmente, o mercado conta com ferramentas que integram o treinamento à conscientização em segurança e simulação de phishing por meio de e-mails similares aos golpes virtuais, tendo bons resultados e sendo capazes de apontar os funcionários que estão propensos a tais armadilhas.

Agora, mais que nunca, é preciso direcionar esforços para essas possibilidades, pois o home office,

que era uma medida momentânea, veio para ficar. Segundo a consultoria Cushman & Wakefield, 73,8% das empresas brasileiras pretendem instituir essa modalidade como definitiva, mesmo após a pandemia. Portanto, treinar seus colaboradores para reconhecer os truques de engenharia social é mandatório. A mensagem é: pensar antes e clicar depois. Afinal, basta um clique para comprometer uma corporação.

(*) **Andressa Soares** é consultora de Cyber Insurance and Risk Controls na ICTS Protiviti, empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados.

Fonte: IMAGE, em 02.07.2021