

Por Sabrina Craide

O ciberataque global com o vírus WannaCry, que infectou milhares de computadores em diversos países do mundo na semana passada, acendeu o alerta para a importância da segurança cibernética no mundo corporativo e em órgãos públicos. Essa cultura de prevenção para diminuir o risco de ataques e prejuízos para as empresas ainda não está disseminada como deveria no Brasil, disse o presidente da SaferNet, Thiago Tavares Nunes de Oliveira.

O especialista lembra que, no ataque da semana passada, só foram infectadas máquinas que estavam com o sistema operacional desatualizado, e a atualização estava disponível há dois meses. “Essa é uma constatação que comprova que as boas práticas de segurança que deveriam ser seguidas por todos, tanto usuários finais e principalmente usuários corporativos, não têm sido seguidas”, diz Oliveira, que também é presidente da Câmara de Direitos e Segurança do Comitê Gestor da Internet no Brasil.

Oliveira diz que os usuários só percebem a importância de fazer um *backup* de seus dados quando perdem um *pen drive* ou quando o disco rígido do computador queima. “Isso vai desde as pequenas, médias e grandes empresas até órgãos públicos e o usuário final, que não têm grandes estruturas para dar suporte. E, junto com isso, se vão as fotos da família, os arquivos de trabalho e até informações confidenciais do usuário, que correm o risco de se tornar públicas

Prevenção e treinamento de funcionários

Outros especialistas em segurança da informação também alertam para a necessidade de melhorar as práticas de prevenção nas empresas. Para a diretora da Consultoria FTI, Thais Lopes, as empresas brasileiras ainda têm um nível de maturidade menor com relação à preocupação com ataques cibernéticos. “Mas isso está mudando, estamos dando os primeiros passos com relação à segurança das comunicações das empresas, tanto públicas quanto privadas”, avalia.

Ela cita pesquisa feita com mais de 500 executivos em diversos países, que mostra grande preocupação com o risco de ataques cibernéticos, tanto para prejuízos financeiros quanto para a reputação da empresa. Segundo a especialista, as empresas devem não apenas investir na área de tecnologia da informação, mas também treinar seus funcionários para saber como reagir e conhecer os possíveis tipos de ataques.

A falta de preocupação dos brasileiros com sua segurança digital também chama a atenção do presidente da empresa Psafe, especializada no assunto, Marco DeMello. Segundo ele, em geral as empresas e os usuários brasileiros não se preocupam “nem de perto” do que deveriam com a segurança digital. “Está na hora de as pessoas acordarem e terem mais cuidados com atualizações, senhas, redes sociais, aplicativos e sites que acessam. Não adianta trancar a porta de casa todos os dias e sua senha ser 12345. Sua vida digital estará totalmente exposta”, alerta.

Um cenário ainda mais sombrio é desenhado pelo especialista Dani Dilkin, diretor de Risco Cibernético da consultoria Deloitte. Ele alerta que nas próximas semanas o mundo poderá sofrer outros ataques, que serão variações do WannaCry. As causas, segundo ele, são o aprimoramento das técnicas de desenhos de programas maliciosos e a publicação de ferramentas que podem ser usadas para explorar a vulnerabilidade de outros sistemas. “Vamos ver, a partir daqui, esse tipo de incidente que aconteceu na semana passada o tempo todo”, prevê.

Banco do Brasil já havia se preparado

Todos os dias, o Banco do Brasil (BB) é alvo de ataques cibernéticos de toda natureza, desde os mais clássicos, como vírus, até os mais sofisticados, como o que atingiu diversas empresas na semana passada. “São centenas de milhares de ataques que empresas como a nossa estão sujeitas a receber. Todos os dias, minutos e segundos, o banco detecta, intercepta e bloqueia esses

ataques”, diz a gerente da Unidade de Arquitetura e Governança de Tecnologia da Informação do Banco, Mônica Luciana Martins.

Segundo ela, o BB já havia sido alertado para um possível ataque como esse, e se preparou com atualizações de *softwares* e bloqueios de vulnerabilidades. Atualmente, cerca de 120 funcionários trabalham para garantir a segurança dos dados da instituição.

O banco tem um comitê de prevenção, que se reúne a cada dois meses, para definir medidas de segurança que serão implementadas, de acordo com os objetivos de negócio da empresa. A política estratégica de segurança é revista pelo menos a cada ano.

Também são realizadas campanhas internas, cursos a distancia e presenciais e várias ações de comunicação para disseminar a cultura de segurança da informação para os funcionários. “Para disseminar a consciência de que as informações dos clientes e do banco têm extrema importância para nós, é um ativo de altíssima importância e deve ser tratada de forma correta”, diz o gerente de Segurança Institucional do BB, Adilson Augusto Lobato.

As determinações para funcionários vão desde orientações sobre abertura de *e-mails*, arquivos que podem ser salvos, onde devem ser armazenadas as informações corporativas, o uso do *e-mail* corporativo apenas para serviço e os cuidados com credenciais de acessos. Os servidores também são orientados sobre como tratar as informações corporativas, até o que pode ou não fazer em redes sociais e em aplicativos de trocas de mensagens.

Segurança elevada para dados do governo

O gerenciamento de sites, sistemas e *e-mails* do setor público federal é feito pelo Serviço Federal de Processamento de Dados (Serpro). “Trabalhamos para ter um padrão de segurança elevadíssimo”, diz a presidente do órgão, Glória Guimarães.

Além da aplicação de “vacinas”, que são antivírus para evitar que as redes e computadores sejam infectados, o Serpro atua com um Grupo de Resposta Rápida a Ataque, que bloqueia imediatamente qualquer entrada de ameaças. “Estamos sempre colocando todas as nossas posições atualizadíssimas com relação à segurança e educação”, diz a presidente do Serpro,

Segundo ela, também é feito um trabalho de educação dos servidores para evitar problemas de segurança. Entre as orientações estão a de desligar os computadores à noite, não abrir *e-mails* ou mensagens maliciosos e fazer *backup* das máquinas para salvar os arquivos. O sistema de *e-mail* utilizado pelo Serpro, chamado de Expresso, utiliza criptografia de ponta a ponta para garantir a segurança das informações enviadas e recebidas.

Também são de responsabilidade do Serpro os serviços da Receita Federal, como a declaração do Imposto de Renda. “A vida fiscal de todo cidadão está aqui, por isso temos que ter bastante cuidado e critério com essas informações”, diz Glória.

Regras de ouro

Além das empresas, os usuários comuns devem incorporar, no seu dia a dia, hábitos para garantir a segurança de dados, como o uso de antivírus e a realização periódica de *backup* dos dados.

“É o preço que se paga para se manter seguro online. Da mesma forma que você faz seguro de carro e plano de saúde para não usar, deve fazer o *backup* para não precisar usar, mas, se precisar um dia, ter aquela segurança”, diz o presidente da SaferNet, Thiago Tavares Nunes de Oliveira.

Ele dá cinco “regras de ouro” para garantir a segurança do uso da internet:

1 – Manter o sistema operacional sempre atualizado. As atualizações de segurança dos sistemas tanto de computadores quanto de celulares devem ser feitas regularmente, de preferência de

forma automática.

2 – Manter um antivírus atualizado. “Não se concebe hoje usar um computador sem antivírus atualizado”, diz o especialista.

3 – Ter sistemas de *antispyware* e *antimalware*, que protegem contra códigos maliciosos que interceptam as comunicações. É similar ao antivírus, mas tem a finalidade de impedir programas espiões.

4 – Manter um *backup* atualizado dos dados, de preferência em um HD externo.

5 – Ter muito cuidado com os links que você clica por aí. Normalmente, o vetor de propagação dos vírus e códigos maliciosos se dá por *e-mail* e por mensagens instantâneas. Então, isso vem normalmente na forma de um link, isso pode infectar sua máquina.

Fonte: Agência Brasil, em 21.05.2017.