CRIMES VIRTUAIS, PREJUÍZOS REAIS

AS TENTATIVAS DE ATAQUES HACKER CRESCERAM 75% DURANTE A PANDEMIA. QUANDO BEM-SUCEDIDOS, OS DELITOS GERAM PERDAS FINANCEIRAS E DE REPUTAÇÃO PARA AS COMPANHIAS

PAULA SIMÕES

Marcus Garcia, VP de tecnologia e produto da FS Security: adequação à LGPD foi uma boa oportunidade para revisar a proteção digital

Na manhã de domingo de 30 de maio deste ano, a JBS enfrentou um sério problema: uma invasão hacker desativou as operações de fábricas nos Estados Unidos, no Canadá e na Austrália. Os criminosos fizeram um ataque do tipo *ransomware*, no qual hackers conseguem controlar o equipamento da vítima e só liberam o uso após o pagamento de um resgate — como em um sequestro. Por orientação de uma consultoria de cibersegurança, a JBS decidiu pagar 11 milhões de dólares em bitcoins aos bandidos — de acordo com a exigência do grupo —, depois de negociar que o depósito seria feito após o restabelecimento dos sistemas. Isso aconteceu em 3 de junho. Foram dois dias inteiros de paralisação nas fábricas da companhia.

Em declaração para o *The Wall Street Journal*, André Nogueira, CEO da JBS nos Estados Unidos,

FOTO: CELSO DONI

PROTEÇÃO EM 10 PASSOS

Eduardo Bezerra, líder de seguros cibernéticos da Wiz Corporate, traz conselhos para melhorar a segurança corporativa

1. Nos ambientes físicos, é preciso haver acesso restrito a locais onde se trabalhe com dados sensíveis, como os departamentos jurídico e de gestão de pessoas

2. Nunca deixe documentos expostos e com fácil acesso — às vezes o hacker está dentro da empresa

3. Triture todos os documentos em papel que tenham sido digitalizados e estejam seguros no sistema

4. Não deixe senhas em post-its colados no computador, nem salvas em blocos de notas ou anotadas em cadernos

5. Crie momentos periódicos para trocar as senhas

6. Adote um sistema de validação de senha em duas etapas. O token, que envia uma mensagem de confirmação da senha, costuma ser eficiente

7. Evite receber currículos e documentos externos em pendrives, que podem conter vírus

8. Faça treinamentos para impedir que os funcionários caiam em golpes virtuais

9. Adote antispam e antivírus com tecnologia *endpoint detection and response* (EDR)

10. Considere contratar um seguro de cibersegurança

Renata Maiorino, diretora de desenvolvimento humano do escritório de advocacia Mattos Filho: criação de cultura de segurança de dados

disse que a decisão foi difícil, mas necessária para evitar qualquer risco potencial aos clientes e paralisação das operações. Em nota, a companhia afirmou que os servidores de backup foram preservados. Assim que o ataque ocorreu, a JBS informou o FBI sobre o problema, e o gabinete concluiu que o responsável havia sido o grupo russo REvil, também conhecido como Sodinokibi, que já esteve por trás de uma invasão contra a Quanta Computer, fornecedora da Apple.

Esse é apenas um exemplo de caso de ataque cibernético, já que o crime está em expansão pelo mundo. Só no Brasil, houve um crescimento de 220% em invasões

hacker no primeiro semestre de 2020, segundo dados do grupo MZ, especializado em relações com investidores. Além disso, um levantamento da consultoria espanhola Minsait mostrou que as tentativas de invasão virtual aumentaram 75% durante a pandemia e que 80% das empresas não estão prontas para encarar o problema. "A mudança para o trabalho remoto foi feita de forma muito rápida, então várias companhias não tiveram tempo, nem caixa, para investir na segurança necessária", afirma Eduardo Bezerra, líder de seguros cibernéticos da Wiz Corporate.

Com o aumento dos ataques, a procura por seguros cibernéticos também cresceu. Segundo dados apurados pela Superintendência de Seguros Privados (Susep), no ano passado os prêmios desse tipo emitidos pelas seguradoras dobraram em relação ao ano anterior. Algumas companhias encontram formas criativas de se proteger. "O Facebook dá recompensas para quem invade seus sistemas e reporta sobre a vulnerabilidade", diz Poliana Szernek, advogada especializada em cibersegurança do escritório Campos Mello. O fato de os ataques se tornarem um mercado lucrativo também mostra a tendência de que esse tipo de problema aumente no futuro. "Vamos ver cada vez mais jovens querendo ser hackers nos próximos 16 anos. Primeiro pela curiosidade, e também porque isso está virando um negócio", afirma Eduardo.

Cultura de proteção

Não é por acaso que o aumento dos crimes aconteceu na pandemia, período em que pessoas e empresas passaram a depender mais da tecnologia para exercer suas atividades à distância — sejam profissionais, sejam pessoais. A implantação às pressas do home office também pode piorar o problema. Empresas com equipes de trabalho remoto devem refletir com muito cuidado sobre o acesso a sistemas por meio de equipamentos que não são da própria companhia, o que gera mais vulnerabilidade pela impossibilidade de monitoramento de sites, aplicativos de mensagens e e-mails pessoais, comumente usados como porta de entrada pelos hackers.

Com isso em mente, a multinacional de tecnologia Thales investiu 500.000 reais no processo de adaptação para o trabalho remoto na pandemia. Entraram nesse pacote compra de equipamentos para todos os funcionários que trabalhariam de casa, ferramentas de segurança digital e treinamentos. "A gente parte do princípio de que não existe nada que seja 100% seguro, então investimos em diferentes tecnologias, como antivírus, token com senha de segurança, VPN *[virtual private network]*, firewall e criptografia de dados", explica Luciano Macaferri Rodrigues, diretor-geral da Thales no Brasil.

Mas a segurança de dados vai

FOTO: CELSO DONI

além das barreiras de proteção: passa pela educação. Inspirados pela experiência em home office durante a pandemia, o escritório de advocacia Mattos Filho decidiu adotar o trabalho híbrido, com dois dias da semana em casa quando a crise passar. Mas isso só foi possível porque, desde 2013, a empresa está em um processo de transformação digital baseado em três pilares: tecnologia para o desenvolvimento do negócio, experiência online do cliente e dos empregados, e segurança da informação. Treinamentos sobre temas como proteção de dados fazem parte da formação da nova cultura digital. "Todos os computadores e laptops são do escritório e têm criptografia e sistema antivírus, de forma que nós temos total acesso aos dados e a possíveis tentativas de invasão", diz Leonardo Brandileone, diretor de tecnologia e conhecimento do Mattos Filho. "Há anos fazemos treinamento sobre esse tema para que os profissionais entendam quais cuidados devem ser tomados. O trabalho híbrido não daria certo sem essa cultura", diz Renata Maiorino, diretora de desenvolvimento humano.

Informações sensíveis

Além de se protegerem de criminosos, as empresas que atuam no Brasil estão com outra questão delicada: as adequações à Lei Geral de Proteção de Dados (LGPD), que regulamenta o uso de dados pessoais pelas companhias — sejam eles de clientes, fornecedores ou de funcionários. Caso as organizações descumpram as regras, poderão ser penalizadas pela Autoridade Nacional de Proteção de Dados (ANPD). E a exposição de informações sensíveis, uma das consequências comuns de ataques hacker, é uma das violações previstas na lei.

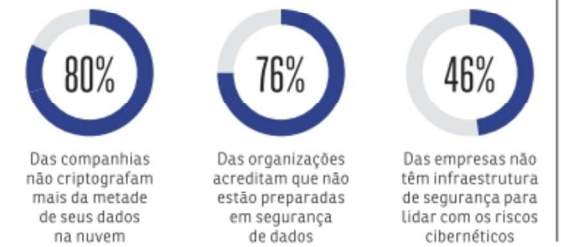
A nova legislação é uma boa oportunidade para as companhias criarem uma mentalidade de segurança digital. Foi isso o que pensou a a empresa de tecnologia FS Security que, para se adequar às normas da LGPD, contratou um escritório de advocacia. O primeiro passo foi mapear a situação da companhia para, depois, traçar um plano de ação com as adequações necessárias. Por meio de um comitê formado pelas áreas jurídica e de gestão de pessoas, a FS Security está cascateando as ações. "A LGPD envolve não só a proteção de dados mas também a maneira de trabalhar. Há impacto sobre o modo como desenvolvemos um software, sobre as ferramentas de apoio nos sistemas e sobre como capturamos e armazenamos dados", diz Marcus Garcia, VP de tecnologia e produto da companhia. "A gente já possuía protocolos de segurança para processos de contratação e demissão, mas a importância dis-

CRESCIMENTO DAS AMEAÇAS

O relatório *Threat Report Global* de 2021, feito pela multinacional de tecnologia Thales, mostra quais são os principais riscos e como as empresas se saem na segurança de dados

FONTES DE ATAQUE

FALTAM CUIDADOS



Luciano Macaferri Rodrigues, diretor-geral da Thales no Brasil: 500.000 reais em equipamentos, proteção e treinamentos na migração ao home office

so aumentou depois da aplicação das diretrizes da LGPD."

Fator humano

É consenso entre os especialistas que, independentemente de todas as ferramentas de segurança adotadas, o elo mais fraco continua sendo nós — os usuários da tecnologia. Criminosos se utilizam da engenharia social para descobrir informações sobre pessoas, a empresa em que trabalham, do que gostam e demais informações que são voluntariamente publicadas nas redes sociais. Dessa forma, eles enviam um e-mail de golpe, o famoso *phishing*, para que o usuário clique em um link suspeito e deixe o hacker entrar na empresa por meio de um vírus que rouba senhas e dados.

Além disso, ainda há o fato de que funcionários mal-intencionados podem ser os próprios hackers. Ricardo Caiado, advogado especializado em compliance e cibersegurança do escritório de advocacia Campos Mello, conta que um de seus clientes sofreu com o vazamento de dados. Após a demissão de alguns empregados, uma pessoa que trabalhava no RH da empresa enviou a um advogado trabalhista os contatos dos ex-funcionários. O objetivo era que o advogado prospectasse clientes para sugerir processos trabalhistas. "Fomos acionados para avaliar se era o caso de informar a Autoridade Nacional de Proteção de Dados", diz Ricardo.

Embora não seja possível garantir que não haverá um comportamento errado de um funcionário, as empresas podem se proteger. Por isso que o investimento em segurança digital não deve ser subestimado — embora 35% das companhias na América Latina e na Europa tenham diminuído o orçamento dessa área em 2020, segundo a Minsait. Adotar mecanismos de proteção, capacitar pessoas e adquirir dispositivos de trabalho próprios geram custos que, embora altos, devem ser vistos como inegociáveis. Afinal, os prejuízos de ataques e vazamentos são financeiros, penais e de reputação. E nem sempre a imagem corporativa sobrevive.

Um caso elucidativo é o da americana SolarWinds, especializada em tecnologia e que possui diversos contratos com o governo norte-americano. Em março de 2020, seu sistema foi invadido por hackers que, uma vez dentro da rede, invadiram diversos clientes, como órgãos do governo dos Estados Unidos e companhias como a Microsoft. Até hoje, apesar de a SolarWinds alegar que já resolveu o problema, muitos especulam que não é exatamente o caso. Há dúvidas sobre a origem do ataque, com suspeitas de espionagem Russa (o que não foi possível detectar) e de que há informações sensíveis que continuam expostas e acessadas. Em audiência pública para comitês federais, o CEO da SolarWinds culpou um ex-estagiário pelo uso de uma senha fraca, que seria "solarwinds123"e teria vazado em um fórum na *deep web* (usada, entre outros crimes, para divulgação e venda de dados). A empresa, segundo ele, falhou em identificar o problema e alterar a senha. Se a explicação for verdadeira, é chocante que o sistema de uma companhia de tecnologia tenha permitido um erro tão primário quanto uma senha fraca. ●

FOTO: DIVULGAÇÃO