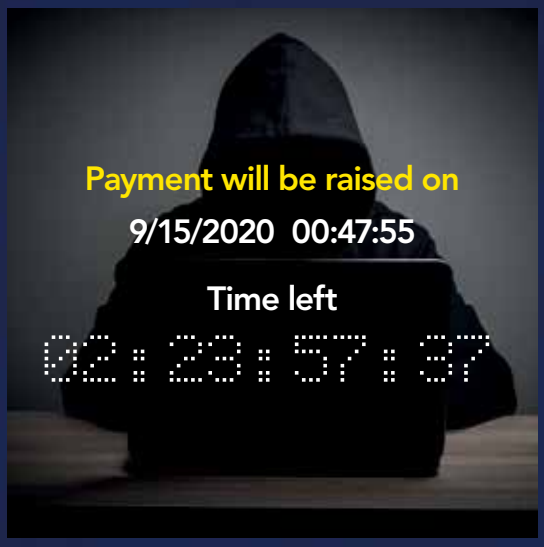

VULNERABILIDADES NA INTERNET

Apesar do aumento de crimes virtuais no país, baixo investimento dificulta expansão de empresas nacionais de cibersegurança

Domingos Zaparolli

A fabricante de cosméticos Natura e a montadora de veículos Honda foram alvo de ataques cibernéticos em suas operações no Brasil, em junho. As duas companhias optaram por não divulgar detalhes do ocorrido e o impacto das invest idas nos negócios. Natura e Honda não estão sozinhas. Em 2020, grandes grupos no país sofreram atentados do gênero, entre eles operadoras de energia e logística e empresas do agronegócio. A multinacional russa de cibersegurança Kaspersky registrou 1,6 bilhão de tentativas de agressões cibernéticas no Brasil entre fevereiro e abril, o equivalente a 60% das ameaças registradas na América Latina. A preocupação com o tema duplicou a procura por seguros corporativos no primeiro semestre no país.

As principais ameaças no Brasil são os ataques do tipo *ransomware*. Neles, o hacker utiliza um software malicioso (*malware*) para invadir e assumir o controle do computador ou do smartphone do usuário. Uma mensagem na tela exige o pagamento de resgate (*ransom* em inglês) em criptomoeda, como bitcoin, para que os arquivos do usuário não sejam apagados (*ver box na página 76*). Numa variação, conhecida como *double extortion* (extorsão dupla), os dados são acessados e a vítima sofre a ameaça de ter suas informações sigilosas divulgadas ou vendidas em leilões virtuais. Pesquisa da empresa anglo-americana de soluções em segurança cibernética Sophos revela que o Brasil foi o quarto país mais afetado por ataques de *ransomware* em 2019, atrás da Malásia, Índia e Austrália.

Outros crimes cibernéticos são cada vez mais comuns no país, como o *trojan horse*, ou cavalo de troia. A vítima clica inadvertidamente em um link aparentemente inofensivo e abre a porta para que suas informações financeiras sejam roubadas. Há ainda os *spywares* (*malwares* de espionagem), que visam obter informações estratégicas de empresas e órgãos públicos, como a Polícia Federal e tribunais de Justiça. Em 2019 foram notificadas 19,1 mil ameaças de segurança às redes computacionais do governo, sendo que mais de 10 mil se confirmaram como ataques, segundo dados do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR-Gov), vinculado ao Gabinete de Segurança Institucional da Presidência da República.

Segundo recomendam os especialistas, é preciso investir em segurança para lidar com o problema, amplificado nos últimos meses por causa da pandemia do novo coronavírus, quando a intensificação do trabalho em *home office* deixou mais vulneráveis arquivos e sistemas de empresas. A consultoria de inteligência de mercado norte-americana IDC aponta que as companhias brasileiras investiram US$ 1,6 bilhão em segurança da informação em 2019 – no mundo, os gastos foram de US$ 107 bilhões. Globalmente, o valor médio aplicado em segurança da informação no mundo corporativo é de 18% do orçamento total de tecnologia da informação (TI).

No Brasil, esse valor médio de gastos não chega a 4%, estima Roberto Gallo, presidente da Associação Brasileira das Indústrias de Materiais de Defesa e Segurança (Abimde). Essa média é puxada para cima pelos investimentos do setor financeiro, que aplica em segurança virtual por volta de 10% do orçamento de TI, conforme a Federação Brasileira de Bancos (Febraban). "Se subtrair os bancos dessa média, os investimentos do restante da economia são irrisórios", afirma Gallo.

O risco das criptomoedas

Popularização das moedas digitais pode impulsionar o mercado de segurança virtual

A procura por tecnologia de cibersegurança no Brasil deve crescer nos próximos anos em decorrência de uma maior percepção de risco no país gerada pela popularização das criptomoedas. Essa é a avaliação de Ulisses Penteado, sócio da BluePex, empresa de Limeira (SP) especializada em soluções como antivírus, *firewall*, anti-*malwares*. "Até então, os hackers brasileiros invadiam para pichar sites e se exibir. Hackers estrangeiros não viam a maioria das empresas do país como alvos estratégicos para roubos de informação. Os ataques aqui não geravam grandes prejuízos", descreve.

As criptomoedas abriram novas perspectivas aos criminosos. É difícil seguir o movimento realizado com essas moedas e existem recursos tecnológicos bastante difundidos para despistar o rastreador. "A possibilidade de sucesso na monetização do crime é grande", avalia Penteado. A execução do crime virtual também não demanda expertise, uma vez que há uma ampla oferta de ferramentas prontas e de fácil manipulação para o ataque. Essa nova realidade levou criminosos comuns a migrarem para o crime virtual, e os ataques se tornaram mais intensos e lesivos. "As ameaças mudaram de patamar e as empresas vão ter que investir para se proteger."

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD), aprovada pelo Senado em agosto, também deve impulsionar os investimentos em segurança virtual, no Brasil. As empresas passam a ser legalmente responsáveis pela manutenção da privacidade dos dados de seus clientes e parceiros comerciais e terão que fazer uma gestão preventiva da segurança da informação para evitar roubos e vazamentos indevidos. Segundo a Associação Brasileira de Software (Abes), 60% das empresas brasileiras ainda não estão prontas para atender os requisitos da nova lei. Têm pouco tempo para se adaptar.

O baixo nível de investimento dificulta a criação de um ecossistema expressivo em cibersegurança no Brasil, aponta o engenheiro eletricista e cientista da computação Paulo Licio de Geus, do Instituto de Computação da Universidade Estadual de Campinas (IC-Unicamp). "Temos empresas nacionais com capacidade técnica. No entanto, são poucas e de pequeno porte, sem expressão global", constata. O problema, na opinião de Geus, é que não se valoriza esse tipo de segurança no país. "É difícil uma empresa local inovar, desenvolver soluções e sobreviver em um ambiente onde não há uma massa de recursos disponível para financiar suas iniciativas", conclui.

Outro problema é a escassez de mão de obra qualificada, tanto nas desenvolvedoras de soluções quanto nas empresas usuárias, que precisam da orientação de profissionais para implementar programas adequados aos desafios impostos pelos criminosos virtuais. Segundo o relatório *Cybersecurity workforce study*, da organização internacional de profissionais de segurança (ISC), há uma lacuna de 600 mil especialistas em segurança cibernética na América Latina, com destaque para o Brasil.

O professor de engenharia da computação da Pontifícia Universidade Católica do Paraná (PUC-PR) Altair Olivo Santin, coordenador da comissão de segurança da informação da Sociedade Brasileira de Computação (SBC), avalia que, além da carência de profissionais, também falta qualidade na mão de obra. "Muitos dos que trabalham em segurança da informação não têm formação adequada", sustenta.

Uma reivindicação da SBC é a normatização da graduação em segurança da informação pelo Ministério da Educação. O projeto de um currículo básico já foi desenvolvido por instituições internacionais de computação em 2017 e está sendo analisado pela SBC. Para Santin, o criminoso virtual é dinâmico e está sempre buscando novas formas de ataque. O combate demanda um grande número de profissionais dedicados, com capacidade para desenvolver pesquisa acadêmica e novas soluções nas empresas. "A segurança cibernética não é massificada no Brasil. É inevitável que sejamos percebidos pelos criminosos como vulneráveis", sentencia o professor.

O mercado de cibersegurança no país é atendido majoritariamente por multinacionais, que respondem por mais de 80% das encomendas. O ambiente de negócios adverso não impede, porém, que desenvolvedores brasileiros de soluções em cibersegurança conquistem espaço no mercado local e iniciem uma trajetória de internacionalização, em busca de escala mercadológica.

Segundo Gallo, da Abimde, o Brasil conta com empresas reconhecidas pela qualidade técnica de soluções em antivírus, *firewall* (dispositivo que monitora o tráfego de rede e a conexão com a internet) e sistemas de criptografia – programas que cifram a mensagem e a tornam ininteligível para quem não tem acesso ao código de segurança. De acordo com o especialista, Estados Unidos, Reino Unido, Rússia, China e Israel, nessa ordem, são as nações de maior destaque no mundo. "Em um ranking internacional de cibersegurança, estaríamos entre os melhores", especula Gallo.

No mercado global, as companhias brasileiras desfrutam de uma vantagem em potencial, defende Gallo. "O Brasil não tem tradição em espionagem internacional e não se imagina que as empresas brasileiras estejam a serviço de seu governo. Essa desconfiança afeta empresas de algumas das principais potências geopolíticas. Também não temos no país leis que permitem ao governo quebrar o sigilo de dados de usuários no exterior, como o Cloud Act norte-americano", afirma.

Gallo é o fundador da campineira Kryptus, empresa especializada em criptografia fundada em 2003. A companhia contou com quatro auxílios do programa Pesquisa Inovativa em Pequenas Empresas (Pipe) da FAPESP para desenvolver um módulo de segurança criptográfica de alto desempenho em *hardware* (*hardware security module*, HSM). A solução foi adotada por diversos clientes corporativos e integra o sistema de voto eletrônico da Justiça Eleitoral brasileira. Também é usado pelo Sistema de Monitoramento de Fronteiras (Sisfron), projeto que as Forças Armadas implementam com o objetivo de coibir atos ilícitos na fronteira terrestre brasileira (*ver* Pesquisa FAPESP *nº 282*).

Em julho, a Kryptus recebeu um aporte financeiro de R$ 20 milhões do Fundo de Investimento em Participações (FIP) Aeroespacial, formado por Embraer, Banco Nacional do Desenvolvimento Econômico e Social (BNDES), Financiadora de Estudos e Projetos (Finep) e agência de fomento paulista Desenvolve-SP. Os recursos foram liberados com o objetivo de desenvolver um plano de expansão e exportação de expertise brasileira em criptografia e segurança.

Rapidamente após o anúncio do aporte, a companhia anunciou a abertura de um escritório de representação na Suíça. "O mercado europeu exige proximidade. É importante ter uma equipe local", diz Gallo. Segundo ele, a Suíça foi uma escolha estratégica por sua reputação de não ter ingerência política do Estado em suas empresas e com profissionais qualificados na área de TI.

A Kryptus obtém 30% de sua receita – cujo valor não divulga – com exportações. Na Europa, atende clientes na Alemanha, Suíça, Espanha e Portugal. Também realiza negócios em nações africanas como Angola, Cabo Verde e Marrocos. Mas o forte são as exportações para a América Latina, direcionadas a empresas de Colômbia, Peru, Equador, Argentina e Chile. Com o escritório na Suíça a expectativa é de um aumento de vendas na Europa, África e Oriente Médio. "Em três anos, mais de 50% de nosso faturamento deverá vir dessas regiões", projeta Gallo.

Outra movimentação recente ocorrida no setor nacional de cibersegurança foi a compra da empresa pernambucana Tempest pela fabricante de aeronaves Embraer, que já incluía soluções de segurança cibernética em seu portfólio. Segundo Fernando Silva, vice-presidente de estratégia e marketing da Tempest, o acordo manteve intocada a estrutura administrativa da companhia recifense. "Vamos passar a desenvolver novos produtos e serviços voltados para a área de defesa, segurança aeroespacial, controle de tráfego aéreo e infraestruturas críticas, como as mantidas por empresas de energia", lista Silva.

O principal segmento de atuação da Tempest, criada em 2000, é o financeiro, responsável por 60% do faturamento de R$ 120 milhões em 2019. Um software de prevenção a fraudes virtuais desenvolvido pela companhia, o Allow Me, está presente nos aplicativos de mobile banking dos principais bancos do país em 30 milhões de aparelhos celulares. Em 2012, a empresa abriu um escritório em Londres, no Reino Unido, e fornece seus sistemas para a revista *The Economist*, o jornal *The Guardian* e a rede de supermercados Tesco. Hoje, 5% de seu faturamento vem do exterior. "A Embraer vai abrir novos mercados para a Tempest, principalmente na área de defesa em países latino-americanos, onde já tem uma presença forte", diz Silva. ■

Projetos

1. HSM Kryptus: Complementos técnicos inovadores em HSM brasileiro para inserção em mercado nacional e internacional (nº 15/50579-0); **Modalidade** Pesquisa Inovativa em Pequenas Empresas (Pipe); **Convênio** Finep Pipe/Pappe Subvenção; **Pesquisador responsável** Roberto Alves Gallo Filho (Kryptus); **Investimento** R$ 956.344,00.
2. Projeto de módulo criptográfico de alto desempenho (HSM) (nº 04/02906-8); **Modalidade** Pesquisa Inovativa em Pequenas Empresas (Pipe); **Pesquisador responsável** Roberto Alves Gallo Filho (Kryptus); **Investimento** R$ 16.584,46.

Os demais projetos consultados estão listados na versão on-line.