Aghazarm: A crescente onda de ataques cibernéticos no Brasil

09/07/2021

É correto afirmar que os ataques cibernéticos estão crescendo por todo o mundo. Porém, constata-se isso principalmente no Brasil, inclusive nas últimas semanas, pois os números são surpreendentes e aumentam cada vez mais, expondo o quanto as empresas em nosso território encontram-se despreparadas na prevenção de tais ataques, o que atrai os chamados *crackers*.

No ano de 2019, o Brasil foi atingido por uma quantidade assustadora de ataques cibernéticos, registrados como "sequestro de dados", tornando-se o número dois do mundo nesse tipo de ação, que é denominado *ransomware*. Esse tipo de ataque se caracteriza pela indisponibilidade e "sequestro" dos dados de uma companhia através de criptografia, bloqueando-os, seguido de contato para a exigência de resgate financeiro ou outro tipo, dependendo do grupo criminoso que o estiver executando.

Dessa forma, certamente o Brasil ficou exposto ao mundo, demonstrando fragilidade e vulnerabilidade nas redes digitais existentes. E isso tanto nas empresas privadas como no poder público e nos próprios usuários da tecnologia. Inúmeras fraudes foram executadas, furto de propriedade intelectual, dados pessoais, vazamento de fotos, clonagem e escuta de números celulares, prejuízos a redes privadas e espionagens diversas, sem contar ataques a redes corporativas, extorsão, sites e páginas falsas, furto de senhas e inúmeras clonagens de cartão de crédito.

Os estudos, à época, apontavam naquele ano um prejuízo de mais de US$ 1 trilhão!

A Nippon Telegraph and Telephone Corporation (NTT), empresa de telecomunicações que domina esse mercado no Japão, lançou o "Relatório de Inteligência de Ameaças Globais 2021 (GTIR)", em que explica como os cibercriminosos tiram proveito da desestabilização global na mudança para o trabalho remoto e exploram suas vulnerabilidades.

Os ataques a aplicativos específicos e da web aumentaram, respondendo por 67% de todos os ataques, o que mais que dobrou nos últimos dois anos, e o setor de saúde sofreu um grande impacto na sua mudança para a telessaúde e o atendimento remoto, com 97% de todas as atividades hostis direcionadas ao setor.

No Brasil, o grupo de medicina diagnóstica Fleury sofreu, no último dia 23, um ataque cibernético que deixou a maior parte de seus sistemas de tecnologia indisponível, prejudicando as operações dos laboratórios.

Além da repercussão negativa pelo ataque propriamente dito, a imagem do laboratório foi abalada pela vulnerabilidade escancarada pelos criminosos. As consequências para a empresa e as ações de mercado podem se agravar ao longo do tempo. Com a persistência dos sistemas desabilitados pode ocorrer um prejuízo financeiro direto e um indireto, ligado à reputação e à insatisfação dos clientes/pacientes, que é a deterioração da imagem da empresa, como já citado.

Vale lembrar que houve outros dois ataques recentemente, sendo que um deles paralisou as fábricas da JBS nos Estados Unidos, no final de maio; reportagem da Bloomberg divulgou que os funcionários do frigorífico afirmaram que a

Copyright © 2026 Consultor Jurídico

companhia rejeitou iniciativas para gastar mais com segurança cibernética pela "falta de retorno imediato", e o outro ataque que desconectou um oleoduto da Colonial Pipeline, bloqueando 45% do suprimento de combustíveis da costa leste americana no mesmo mês.

Fica claro que os eventos de *ransomware*, trouxeram à baila mais um fator de risco a ser considerado fortemente pelos investidores de todas as empresas antes de quaisquer operações, tendo de pesar o quão seguro está o parque tecnológico daquela empresa e quais seriam suas vulnerabilidades.

Estudos da Fortinet, empresa multinacional da Califórnia que desenvolve e comercializa *software*, produtos e serviços de cibersegurança, revelam que o Brasil sofreu mais de 3,2 bilhões de tentativas de ataques cibernéticos só no primeiro trimestre de 2021, e, portanto, nosso país lidera o ranking da América Latina, que contabilizou um total de 7 bilhões de tentativas durante o período.

Segundo o jornal *Valor Econômico*, *"o Grupo Fleury é vítima do código malicioso (ransomware) Sodinokibi, o mesmo que afetou a JBS, e que os cibercriminosos pediram um resgate em bitcoin para liberarem as informações bloqueadas por criptografia"*.

Outra empresa do setor de saúde, a Hapvida, antes do laboratório Fleury, foi atacada por *hackers* em 2020, ficando claro que os processos de digitalização das empresas vêm falhando em termos de planejamento de segurança e etapas completas de prevenção, elevando o risco cibernético.

Houve, também em 2020, um ataque à Copel, que atingiu alguns servidores, mas os sistemas se mantiveram íntegros; à Eletronuclear, subsidiária da Eletrobras responsável pelas usinas nucleares do complexo de Angra dos Reis, que também não chegou a ter impactos sobre a operação das unidades ou riscos de segurança, e assim por diante, por todo o Brasil.

O âmago da questão é quando as empresas irão, de fato, acreditar que a área de proteção digital é fundamental para elas próprias, para sua continuidade operacional, para a satisfação e proteção dos dados pessoais de seus clientes, para a manutenção de sua imagem, de sua marca, de seus investimentos?

Deverão ainda passar por outras inúmeras invasões digitais, regates de dados, vazamento de informações confidenciais e desonra mercadológica para fazer o que é correto na área de segurança cibernética?

Essas questões são fundamentais para todos os gestores não só de tecnologia, mas para os próprios membros da alta administração, no *compliance* às leis e na prevenção de incidentes dessa monta, que só traz prejuízos para todos, inclusive para o Brasil enquanto nação.

Fonte: https://conjur.jumps.com.br/2021-jul-09/aghazarm-crescente-onda-ataques-ciberneticos-brasil/

Copyright © 2026 Consultor Jurídico