A onda de invasões hackers às estruturas tecnológicas dos tribunais

15/04/2022

Em 18 meses — de novembro de 2020 até abril de 2022 —, os tribunais brasileiros foram vítimas de 13 ataques cibernéticos de *hackers*, paralisando os trabalhos e provocando transtornos para advogados e a população. Isso significa, em média, um ataque a cada 41 dias.

123RF

As invasões aos sistemas de dados e informações ocorreram em São Paulo, Distrito Federal, Pernambuco, Rio Grande do Sul e Espírito Santo, e tiveram como alvo as cortes federais, criminais e eleitorais, estaduais e do Trabalho; mas, principalmente, as cortes superiores, como o Supremo Tribunal Federal, o Superior Tribunal de Justiça e o Tribunal Superior Eleitoral (TSE).

Essa estatística expõe uma situação grave, uma vez que as bases de dados dos tribunais ficam à mercê dos invasores e os serviços prestados para advogados e aos cidadãos, inacessíveis por vários dias, atrasando e adiando julgamentos e o andamento de todos os procedimentos judiciais.

Por exemplo, os sistemas do Tribunal Regional Federal da 3ª Região ficaram fora do ar por mais de uma semana após sofrerem ataque *hacker* no último dia 30. Essa invasão ocorreu quando o TRF-3 iria cumprir o prazo constitucional da expedição de precatórios, o que o levou a adiar a data. Os *hackers* paralisaram os sistemas do tribunal federal e atingiram as ferramentas utilizadas para elaboração de minutas, conferência de dados pelas partes e transmissão de ordens de pagamento de precatórios.

"A maioria das invasões é no ambiente de tecnologia dos tribunais. É muito preocupante essa situação", alerta **Fernando Tasso**, juiz de Direito no Tribunal de Justiça de São Paulo que atuou como gestor de Tecnologia da Informação (TI) da corte no último biênio.

Segundo **Alexandre Libonati de Abreu**, juiz auxiliar da presidência do Conselho Nacional de Justiça, a frequência de ataques cibernéticos aos tribunais brasileiros não é elevada, mas assim mesmo ele admite que o problema preocupa.

"A média de um *(ataque)* a cada 41 dias não é alta se comparada a ataques sofridos por estabelecimentos bancários ou sítios de compra, por exemplo, mas, independentemente da frequência, qualquer ataque a um órgão do Judiciário pode gerar consequências gravíssimas, e deve servir de alerta para que o assunto 'segurança cibernética' seja visto com a mesma (ou até maior) seriedade com que se vê a segurança física de instalações", disse o juiz. "Os tribunais lidavam, até bem pouco tempo, apenas com processos físicos. A transformação digital se iniciou há 20 anos, tendo se acelerado apenas nos últimos anos. A ameaça digital, portanto, é um fenômeno recente no Judiciário".

Os objetivos
A finalidade dos ataques na internet violando a segurança desses sistemas é danificar ou destruir a rede de informações dos tribunais, mas também há motivação financeira e de competição pessoal entre os grupos *hackers*.

"Há uma predileção, e a motivação nem sempre é financeira. Há a motivação de mostrar a vulnerabilidade, a fraqueza e a debilidade dos sistemas com as invasões aos órgãos públicos, como os tribunais, mas também em outros órgãos federais" explica Tasso.

Ao paralisar as ferramentas do sistema de informações, há casos em que os *hackers* pedem resgate para liberar as atividades normalmente. Geralmente o pagamento precisa ser feito em criptomoedas.

Para **Omar Kaminski**, especialista em Direito Informático e internet, "o que tem prevalecido no Brasil, na esfera pública, é a chamada segurança por obscuridade — em que se acredita que, sem transparência, sem publicidade e sem detalhamento há uma menor expectativa de prejuízos e danos. Temo que esse número (13 ataques em 18 meses) possa ser ainda maior, a depender da competência e interesse dos *hackers* envolvidos".

Especialistas em TI também afirmam que os *hackers* visam, entre outras coisas, ao dinheiro que circula nesses locais, originados de taxas judiciárias. São mais de dez taxas, que vão desde aquelas para petições, apelações, recursos e agravos de instrumento até as de inventários, divórcios e ações penais, entre outras.

Mas essas violações também visam a capturar dados sigilosos de identidade das pessoas dentro dos processos. De posse desse material, partem para sua venda no submundo do crime ou para extorsão do titular desses dados.

Venda de dados
No submundo do ativismo digital, esses dados de pessoas são extremamente valorizados e vendidos na *deep web*, que é uma parte da internet que não está indexada pelos mecanismos de busca, ficando fora do alcance do grande público.

É na *deep web* que fica guardado todo tipo de informação que requer senhas, logins, *tokens* e usa criptografia para ser acessada. Por exemplo, os sistemas de administração de sites e redes sociais, assim como informações bancárias de um correntista, e-mails pessoais e funcionais, mas, principalmente, os sistemas de administração de instituições estão na *deep web*.

Além disso, os dados sequestrados também podem ser vendidos na *dark web*, uma camada ainda mais profunda da internet, que contém um mundo de informações e conteúdo que não fica disponível para usuários comuns. Atividades ilícitas prosperam dentro da *dark web*.

De acordo com o advogado **Alexandre Atheniense**, especialista em Direito Digital e Tecnologia da Informação e sócio fundador da Alexandre Atheniense Advogados, o sequestro de dados pessoais dentro de uma corte tem como objetivo ganhos financeiros. "Isso hoje vale muito dinheiro na *deep web*", observa.

Além dos sistemas de informação e paralisação dos processos judiciais eletrônicos e acesso ao banco de dados dos tribunais, as ações *hackers* também podem afetar a emissão de mensagens por e-mail e até mesmo o sistema telefônico. Foi o que aconteceu em março na Justiça Federal de Pernambuco, um ataque que deixou o site e os sistemas da seção judiciária totalmente fora do ar por alguns dias. O que levou à suspensão de prazos processuais e atendimentos virtuais.

Ego em alta
Diversão e competição também estão entre os objetivos das invasões *hackers*. Os criminosos, dentro de suas bolhas de ações, ganham destaque e prestígio quando conseguem entrar nos sistemas de informações dos grande e importantes cortes judiciais.

"Informação é poder. Essa onda de invasão é uma tentativa de obter poder. Mas também serve para desmoralizar o tribunal que não possui segurança compatível com a atividade que exerce. É uma glória para o *hacker* em sua tribo dizer que conseguiu tornar indisponível o sistema de um determinado tribunal por alguns dias", destaca Atheniense.

São muitas as categorias de invasores em operação no Brasil. "Já acompanhei mais o hacktivismo, hoje em dia acho que se profissionalizaram, ou os que faziam isso há dez anos já devem ter procurado outra ocupação ou se aperfeiçoaram. É um submundo difícil de acompanhar, há desde os novatos, script kiddies (hacker novato), worms (pupa, verme, hacker ainda embrionário), até os que se julgam poderosos o suficiente para causar uma guerra", explica Omar Kaminski. Mas todos conseguem provocar problemas nos sistemas invadidos.

LGPD
E os ataques devem se intensificar e se tornam cada vez mais preocupantes. Por isso, todos defendem a correta aplicação da Lei Geral de Proteção de Dados (LGPD) e o investimento em segurança e governança.

Lívia Bíscaro Carvalho, advogada coordenadora da área cível no Diamantino Advogados Associados, afirma que a questão traz à tona "a fragilidade do ponto de vista da proteção de dados, uma vez que os processos guardam desde informações pessoais das partes até documentos sigilosos e, inclusive, menção a contas bancárias que são vinculadas aos autos".

"Visando ao restabelecimento da segurança foram necessárias medidas que suspenderam o atendimento e também os prazos, com reflexo inegável de atraso nos trâmites processuais; julgamentos terão de ser remarcados e haverá sobrecarga quando da retomada dos trabalhos", destaca a advogada.

Beatriz Haikal, sócia de privacidade, proteção de dados e regulatório de novas tecnologias no BBL Advogados, também lamenta que ataques *hackers* tenham se tornado cada vez mais frequentes — e, em muitos casos, sua ocorrência está além

do controle dos órgãos públicos e empresas.

"Embora nem tudo esteja sob a esfera de controle, algumas ações são fundamentais para mitigar e até evitar a ocorrência de danos. Nesse sentido, a LGPD estabelece princípios importantes a serem seguidos, como os da segurança e da prevenção", comenta a advogada.

Na noite de uma sexta-feira, dia 1º de outubro de 2021, por exemplo, a infraestrutura tecnológica do TRT da 4ª Região, em Porto Alegre, registrou atividades maliciosas e suspeitas no sistema de informação e dados. O ataque cibernético havia ocorrido por volta do meio-dia do dia anterior. A ação pirata fez com que os serviços prestados fossem suspensos até que a equipe de TI solucionasse a situação e evitasse a extensão do ataque para outras estruturas do tribunal.

A criação de uma cultura de privacidade e proteção de dados, além da realização de treinamentos que preparem os colaboradores para lidar com os incidentes e afastar a vulnerabilidade digital, é defendida pela advogada Beatriz Haikal. Ela entende também que o processo de implementação de um sistema de segurança e de resposta a incidentes é uma tarefa permanente, que deve ser constantemente atualizada. "Mas, sem dúvida, as iniciativas de governança contribuem para a detecção mais eficaz e para uma resposta mais satisfatória, buscando afastar danos reputacionais e preservando os titulares de dados pessoais", complementa.

O trabalho desenvolvido por parte de servidores nos tribunais também pode ser classificado como ponto facilitador para a atividade *hacker* nos sistemas de informação e dados dos tribunais. "As pessoas trabalham de maneira muito informal no que tange à operação dos sistemas. O fator humano é um problema. Os tribunais não se adequaram com naturalidade em termos de governança digital. São muito ingênuos na segurança de informação", critica Atheniense, que pede maiores investimentos em sistemas e capacitação das pessoas.

Da mesma forma enxerga o problema Omar Kaminski. "Os desafios não param, e cada vez serão mais sofisticados. Há também de se investir em segurança corporativa e capacitação dos funcionários para que tratem e cuidem dos dados dos jurisdicionados com o máximo de atenção e cuidado. Ao menos até que a inteligência artificial assuma o trâmite".

Uma das modalidades de invasão é chamada de *ransomware*, que é um *software* que entra no sistema e pode bloquear os computadores. O *hacker*, então, exige pagamento de resgate para desbloqueá-lo. "Essa invasão, geralmente, acontece onde os softwares são desatualizados", alerta **Renato Ópice Blum**, *chairman* e sócio-fundador do Opice Blum, Bruno e Vainzof Advogados, especialista em Direito Digital.

Ataques *hackers* aos tribunais brasileiros

De NOV/20 a ABR/22

nov/20	TRF-1
nov/20	STJ
nov/20	TSE
jan/21	TRF-3
jul/21	7ª Vara Criminal Federal SP
mai/21	STF
abr/21	TJ-RS
ago/21	TSE
out/21	TRT-RS
fev/22	TRT-ES
mar/22	TRF-3
abr/22	JF-PE

Fonte: https://conjur.jumps.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais/