STJ diz ter backup; advogados consideram que episódio é grave

O Superior Tribunal de Justiça informou nesta sexta-feira (6/11) que o backup dos sistemas de tecnologia da corte está "100% íntegro, bem como os dados dos cerca de 255 mil processos que tramitam". O tribunal foi alvo de hackers na terça (3) e desde então paralisou suas atividades. Os ministros e servidores não conseguem acessar seus próprios arquivos e e-mails.

STJ

STJCorte está fora do ar e com prazos suspensos

Em nota, o presidente do tribunal, ministro Humberto Martins, assegurou que o sistema estará disponível no dia 9 de novembro, conforme o previsto. O sistema reúne as principais funcionalidades do processo eletrônico e dos julgamentos colegiados.

A situação é considerada grave entre os ministros. Alguns demonstraram preocupação com uma mudança feita no sistema da corte no ano passado, que poderia ter aberto vulnerabilidades do site.

Um ministro da corte ouvido pela **ConJur** contou que o hacker não teve acesso aos arquivos e processos que estão guardados em nuvem. Com isso, o hacker conseguiu bloquear e criptografar apenas os dados que estão guardados nos computadores. Informações preliminares indicam que o ataque foi localizado de uma empresa particular estrangeira e estava sendo programado havia três meses.

Até agora, não está clara a dimensão do que foi atacado, se houve cópia dos dados e, consequentemente, do que poderá ser restaurado. Circula ainda a informação de que houve pedido de resgate dos dados, mas não há informação oficial da presidência sobre o tema.

A Polícia Federal e o setor de informática do STJ analisam a extensão do ataque e de que forma poderão contornar o problema. O Comando de Defesa Cibernética do Exército também colabora.

Outros sistemas oficiais também foram atingidos nesta quinta-feira (5/11) em Brasília: do Ministério da Saúde, da Secretaria de Economia do Distrito Federal e do governo do Distrito Federal. Não se sabe, porém, se há relação com o ataque ao STJ.

2023 - www.conjur.com.br - Todos os direitos reservados.

A Polícia Federal abriu inquérito para investigar o caso e destacou peritos em informática para trabalhar no assunto. Em sua *live* semanal, o presidente Jair Bolsonaro disse que a PF já identificou o responsável pelo ataque ao sistema do STJ. A informação, no entanto, não foi confirmada pelas autoridades.

Os prazos processuais foram suspensos até a próxima segunda-feira (9/11). O tribunal informa que as demandas urgentes estão centralizadas na presidência do STJ e pede que as petições sejam encaminhadas ao e-mail protocolo.emergencial@stj.jus.br.

Comunidade jurídica
Advogados ouvidos pela **ConJur** demonstraram bastante preocupação com o episódio e também consideraram que a situação é grave. Segundo eles, é preciso investigar as causas e adotar medidas para diminuir a insegurança jurídica.

Maria Hosken, do Nelson Wilians e Advogados Associados, especialista em Direito Digital e Privacidade, avalia que o caso gera preocupação, sobretudo pelo risco de vazamento de informações oriundas de processos que correm sob segredo de justiça.

"Ainda mais grave é a paralisação do órgão por indisponibilidade de seus sistemas informáticos. É uma situação de consequências ainda imprevisíveis e que deverá testar o preparo do Poder Judiciário não apenas no que se refere a medidas preventivas de segurança, mas também de maturidade em relação à gestão de incidentes dessa natureza", diz Hosken.

Lis Amaral, também sócia do Nelson Wilians Advogados, especialista em Direito Digital e Privacidade, destaca que as regras da LGPD, em vigor há pouco tempo, devem ser respeitadas.

"Em havendo incidentes como um vazamento, os controladores de dados pessoais devem observar regras estabelecidas para comunicação à autoridade nacional e, dependendo da gravidade, até aos titulares. Esse processo de investigação é fundamental para apurar as causas do incidente e estabelecer medidas de mitigação dos danos, razão pela qual não é aconselhável especular sobre boatos ainda não confirmados", explica a advogada.

Alan Thomaz, advogado especialista em Direito Digital e LGPD, entende que o incidente ainda carece de mais informações, mas a possibilidade de o backup dos dados também ter sido invadido é preocupante.

"Ainda não foram fornecidas informações oficiais sobre o incidente de segurança envolvendo o STJ. Informações dos bastidores indicam que se trata de um ataque de hacker grave, provavelmente de *ransomware*, que criptografou todos os dados de processos e e-mails do STJ, tornando-os inacessíveis. Aparentemente o backup dos dados também foi objeto de criptografia pelos hackers, e ainda não pode ser recuperado", opina o advogado.

2023 - www.conjur.com.br - Todos os direitos reservados.

Já para **Alex Santos**, advogado especialista em tecnologia do Nascimento e Mourão Advogados, o incidente é mais uma evidência de que existe uma "vulnerabilidade crônica nos sistemas de segurança cibernética utilizados pelo governo brasileiro".

"Há notícia de que todo o acervo de processos do STJ, além dos e-mails dos ministros e demais dados foram criptografados pelos hackers. E se essa informação se confirmar, milhões de jurisdicionados poderão ser prejudicados com uma possível extensão da suspensão das atividades no STJ até que a base seja restaurada", alerta Santos.

Adib Abdouni, especialista em Direito Criminal e Constitucional, também vê no ataque fato da mais "alta gravidade". "Com vistas a amenizar a insegurança jurídica que a partir de então se projeta sobre os jurisdicionados, o STJ acionou a sistemática de atendimento em regime de plantão, de modo a garantir que a ausência de funcionalidade do processo eletrônico não impeça que demandas urgentes que reclamem atendimento jurisdicional imediato deixem de ser apreciadas, haja vista que o direito de acesso à justiça é um postulado fundamental e inalienável da pessoa, previsto no artigo 5º, XXXV da Constituição e, o seu artigo 93, XII, por sua vez, é expresso ao prever que 'a atividade jurisdicional será ininterrupta'", destaca Abouni.

O advogado lembra que no período de instabilidade digital, o presidente do Tribunal ficará responsável pelo enfrentamento de pedidos de tutela provisória, assim como matérias que importem em perecimento de direito ou que aflijam o direito de liberdade de locomoção. Também estarão sob responsabilidade do presidente da Corte pedidos de habeas corpus contra prisão, busca e apreensão, medida cautelar e mandado de segurança em razão de atos decretados por autoridade sujeita à competência originária do Tribunal, além de suspensão de segurança, suspensão de execução de liminar e de sentença e as reclamações a propósito das decisões do presidente cujos efeitos se operem durante o período de atendimento extraordinário.

Para o criminalista e especialista em LGPD **André Damiani**, sócio fundador do Damiani Sociedade de Advogados, o ataque demonstra a fragilidade no que concerne à segurança dos dados e, consequentemente, à privacidade das instituições públicas brasileiras.

"Há notícias de que este foi o pior ataque hacker da história do Brasil, visto que até os backups do STJ foram criptografados pelos criminosos, impedindo o acesso — por todos — de um incalculável banco de processos judiciais, acarretando enorme insegurança sobre o destino e a manutenção dos dados existentes nesses processos que podem, inclusive, vir a ser expostos por criminosos", afirma.

Associada do Damiani Sociedade de Advogados, **Blanca Albuquerque**, advogada especializada em proteção de dados pessoais pelo Data Privacy Brasil, afirma que, de acordo com a LGPD, o STJ deve se comunicar com a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares (de dados) que foram afetados em decorrência do incidente de segurança.

"Com a LGPD agora em vigor, o STJ deverá seguir seus preceitos e dar o exemplo de como as instituições devem atuar perante incidentes de segurança, além de que, tal catástrofe deve ser um alerta para todo o sistema governamental do país, que mesmo após o caso Snowden, continua frágil e

2023 - www.conjur.com.br - Todos os direitos reservados.

suscetível a ataques cibernéticos, comprometendo a privacidade dos dados sigilosos de todos os cidadãos do país", conclui Blanca.

Paula Sion, advogada criminalista e coordenadora do Grupo de Trabalho sobre Lei Geral de Proteção de Dados no âmbito da Comissão de Direito Penal da OAB-SP, lembra que nos anos de 1990 sequestravam pessoas e pediam altas somas em dinheiro vivo. Em 2020, sequestram dados e pedem resgate em criptomoedas, aproveitando-se de vulnerabilidades nos sistemas.

"Acredito que o STJ tenha uma rotina de backup de informações segura e que esteja preparado para ataques desta natureza. Do contrário, os danos serão inestimáveis."

Para **Daniel Gerber**, advogado criminalista com foco em gestão de crises e *compliance* político e empresarial. "Em virtude do ineditismo do ataque sofrido pelo STJ, mais importante do que uma solução ao problema da criptografia dos dados, é buscarmos caminhos que propiciem a análise de situações emergenciais. Nesse sentido, espera-se que o STF designe, o quanto antes, uma área competente para receber os recursos daqueles que, neste momento, estão impossibilitados de ver o seu pleito atendido por aquele tribunal."

Direito Internacional
O advogado **Solano de Camargo**, sócio da LBCA e especialista em Direito Digital e Internacional, alerta que é grave o crescimento dos ataques de hackers a instituições públicas durante a epidemia de Covid-19. Para ele, muitas das causas desses ataques é decorrente da própria ação ou omissão do Estado em que estão abrigados os ciberpiratas, sendo que cabe ao direito internacional público reger o comportamento dos Estados. "É urgente que se estabeleçam padrões internacionais de responsabilidades baseadas em provas que sejam fundadas em padrões técnicos como forma de trazer o direito internacional de cada Estado a aplicação, tanto das contramedidas, que interrompam as agressões cibernéticas , como da obtenção das reparações", diz.

Segundo Solano, a ação dos hackers transnacionais pode levar o Brasil e outros países a um blackout no âmbito da Justiça e de outros serviços públicos essenciais. Ele lembra que o conceito de "ataque cibernético" ainda não está resolvido no âmbito do Direito Internacional, mas que violações de direitos humanos em geral são da competência do Tribunal Penal Internacional, conforme estabelece o artigo 8º do Estatuto de Roma. "A guerra cibernética pode ser considerada uma violação dos tratados de direitos humanos, a depender de sua dimensão, de seus alvos e de suas consequências à população civil impactada", conclui.

Date Created
06/11/2020

2023 - www.conjur.com.br - Todos os direitos reservados.