JUDICIÁRIO SOB ATAQUE HACKER: FATORES DE RISCO PARA A SEGURANÇA DO PROCESSO DECISÓRIO EM SISTEMAS JUDICIAIS ELETRÔNICOS

Transformação digital, ciberespaço e novas tecnologias da informação na Justiça

Renato Solimar Alves (Universidade de Brasília) Marcus Aurélio Carvalho Georg (Universidade de Brasília) Rafael Rabelo Nunes (UnB) (Universidade de Brasília)

RESUMO

O Poder Judiciário promoveu a transformação do sistema judicial brasileiro por meio da ampla adoção da tecnologia no processo judicial. A transformação experimentada pela utilização do processo eletrônico aumentou a agilidade da distribuição e tramitação dos processos, bem como no aumento da produtividade em razão da maior produção de julgados, o que resultou na celeridade e na melhora da prestação do serviço jurisdicional (Hino & Cunha, 2020). A pandemia acelerou ainda mais esse processo de transformação e criou novas formas de inserir a tecnologia na Justiça, com destaque para o incremento da realização de videoconferências e audiências virtuais (Martins, 2021), além da possibilidade de citações por meios eletrônicos, o atendimento remoto por meio de "balcão virtual" e utilização de inteligência virtual na análise dos processos (Conselho Nacional de Justiça, 2021). Neste cenário, a tecnologia, que já era um fator crítico, passa a ter um papel ainda mais relevante para o alcance dos objetivos estratégicos do Judiciário e para a efetiva prestação jurisdicional ao cidadão. Contudo, juntamente com os benefícios introduzidos pelo uso da tecnologia, são inseridos também novos fatores de risco. Em anos recentes, de 2019 a 2022, pode-se observar ataques cibernéticos de grandes proporções, que impactaram negativamente ou paralisaram a atividade-fim de diversos órgãos do Poder Judiciário, afetaram a órgãos tais como: STJ, TJ-RS, TRF da 1ª Região, TSE, STF, TRT-ES, TRF da 3ª Região, TRT-RS e Justiça Federal em Pernambuco (Reina, 2022). Além da indisponibilização dos serviços, há o risco relacionado à integridade dos dados. A título de exemplo, no Tribunal Regional Federal da 3ª Região, foi observado que um hacker obteve acesso ao sistema processual eletrônico, o que possibilitou a mudança de pareceres do MPU, a conversão de sentenças de condenação em absolvição e a alteração das contas destinatárias para o recebimento de valores legítimos em outros processos (Moura & Borges, 2022) (Tribunal Regional Federal da 3ª Região, 2021). Quando tais ataques chegam a afetar o funcionamento do sistema jurídico, se revelam fragilidades que abalam a confiança depositada na Justiça, sendo necessário que o nível de segurança seja o mais elevado possível (Hirata & Oliveira, 2022). Considerando que os riscos são os efeitos das incertezas sobre os objetivos, torna-se essencial que sejam adequadamente identificados (ABNT, 2018), de forma que gestão de riscos seja capaz de reduzir a probabilidade ou os efeitos dos incidentes sobre a integridade, disponibilidade e/ou confidencialidade das atividades-críticas. No Poder Judiciário, destacam-se as atividades de recebimento e distribuição de processos, análise e relatoria de processos, produção de decisão, julgamento, processamento judicial e execução de atos cartorários e o cumprimento de despachos e decisões (Supremo Tribunal Federal, 2018). Em outra perspectiva, constitui um desafio aplicar os controles de segurança necessários para proteger os sistemas de informação. O framework MITRE ATT&CK documenta as táticas e técnicas utilizadas por hackers em situações reais, apresentando 14 táticas, 191 técnicas, 363 sub-técnicas e milhares de procedimentos utilizados por hackers nos ataques cibernéticos (MITRE Corporation, 2021). Existem outros frameworks que listam os controles de segurança necessários para se proteger contra esses comportamentos maliciosos. A título de exemplo, o Cybersecurity Framework do

NIST descreve 22 categorias, 98 subcategorias e aproximadamente 1200 possíveis controles de segurança necessários para identificar, proteger detectar, responder ou se recuperar de ataques cibernéticos criminosos (NIST, 2022). Contudo, todos esses frameworks são essencialmente técnicos e não vinculados ao negócio o que dificulta a tradução, para os gestores da alta administração, as ações e iniciativas para mitigação dos riscos técnicos. Nesse sentido, este estudo tem como objetivo identificar os principais fatores de riscos que podem afetar os sistemas judiciais. Trata-se de um estudo de natureza aplicada, qualitativa, com objetivos exploratórios. Como procedimento técnico foi utilizada análise bibliográfica da literatura especializada, grupos focais com profissionais multidisciplinares (área judiciária, área administrativa e de tecnologia), e análise de causa-raiz para identificar os riscos de negócio nas atividades-chave do Poder Judiciário. Os resultados obtidos indicam que os principais riscos de negócio que precisam ser tratados no processo judicial eletrônico são: previsibilidade da distribuição dos processos, modificações de fatos ou informações necessárias para o processo decisório, fraudes documentais, falhas na verificação da autenticidade de documentos, vazamento de informações de processos sigilosos. Como trabalhos futuros, sugere-se novas abordagens que correlacionem os controles operacionais aos riscos de negócio com o objetivo de auxiliar no tratamento e comunicação dos riscos entre as equipes técnicas, gestores de nível tático e estratégico dos órgãos.

PALAVRAS-CHAVE: Segurança da Informação, Tribunais. Riscos cibernéticos no processo judicial, Estratégia Nacional de Segurança Cibernética, Frameworks.

REFERÊNCIAS

ABNT. (2018). NBR ISO 31000. Gestão de riscos ? Diretrizes. Rio de Janeiro, RJ, Brasil: ABNT.

Conselho Nacional de Justiça. (2021). Justiça 4.0. Acesso em 21 de maio de 2022, disponível em https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/

Hino, M. C., & Cunha, M. A. (2020). Adoção de tecnologias na perspectiva de profissionais de direito. Revista Direito GV, v. 16(n. 1), e1952. doi:10.1590/2317-6172201952

Hirata, A., & Oliveira, C. G. (2022). 39 dias após o ataque cibernético ao STJ: reflexões e desafios. Acesso em 22 de Maio de 2022, disponível em Migalhas: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/337701/39-dias-apos-o-ataque-cibernetico-ao-stj--reflexoes-e-desafios

Martins, T. d. (2021). Acesso à Justiça e pandemia. Revista Jus Navegandi, 6412. Acesso em 21 de maio de 2022, disponível em https://jus.com.br/artigos/88048/acesso-a-justica-e-pandemia

MITRE Corporation. (2021). MITRE ATT&CK. Acesso em 25 de maio de 2022, disponível em MITRE: https://attack.mitre.org/matrices/enterprise/

Moura, R. M., & Borges, L. (28 de março de 2022). A impunidade dos hackers que colocaram o Judiciário de joelhos. Acesso em 19 de maio de 2022, disponível em Veja:

https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/

NIST. (2022). NIST Cybersecurity Framework. (National Institute of Standards and Technology) Acesso em 25 de maio de 2022, disponível em NIST: https://www.nist.gov/cyberframework/framework

Reina, E. (2022). Ameaça Virtual - Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias. (Revsita Consultor Jurídico) Acesso em 22 de maio de 2022, disponível em Conjur: https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais

Supremo Tribunal Federal. (2018). Cadeia de Valor. Acesso em 1 de junho de 2022, disponível em https://www.stf.jus.br/arquivo/cms/intranetAGE/anexo/MapProcessos/CadeiaValor/CadeiadevalorSTF2018.pdf

Tribunal Regional Federal da 3ª Região. (2021). Justiça Federal condena hackers por falsificação de documento público em sistema processual. (Assessoria de Comunicação Social do TRF3) Acesso em 19 de maio de 2022, disponível em TRF3: https://web.trf3.jus.br/noticias/Noticiar/ExibirNoticia/414225-justica-federal-condena-hackers-por-falsificacao-de