Enfrentando os Ataques Hackers: Controles de Segurança da Informação Prioritários para o Tratamento dos Riscos de Negócio do Poder Judiciário

Renato Solimar Alves (Universidade de Brasília), Carlos Eduardo Miranda Zottmann (Universidade de Brasília), Marcus Aurélio Carvalho Georg (Universidade de Brasília), Luiz Guilherme Schiefler de Arruda (Universidade de Brasília) e Rafael Rabelo Nunes (Universidade de Brasília)

Tema: Inovações, inteligência artificial e tecnologias de informação e comunicação em sistemas de justiça

RESUMO

Ataques de hackers contra órgãos do Poder Judiciário têm ocorrido com frequência e causado danos significativos à sua imagem (Fuccia, 2022; Lobo, 2022; Moura & Borges, 2022; Reina, 2022). O Poder Judiciário, no desempenho de suas funções, está exposto a uma ampla gama de eventos de riscos, cada um com suas próprias variadas causas e potenciais consequências graves para as instituições, servidores públicos e sociedade como um todo (Alves et al, 2023). Para uma adequada avaliação desses riscos, é crucial identificar não apenas os riscos, suas causas e consequências, mas também as ameaças e as vulnerabilidades existentes (Shameli-Sendi et al., 2016). Considerando que uma ameaça é qualquer evento ou circunstância com potencial de impactar a missão, funções, imagem, reputação ou ativos de uma organização (National Institute of Standards and Technology, 2012), é fundamental identificar controles de segurança que podem ser implementadas para reduzir ou neutralizar as ações ou efeitos dessas ameaças sobre a confidencialidade, integridade e disponibilidade de sistemas e informações (National Institute of Standards and Technology, 2020). É por meio da implementação de um conjunto deles que a segurança é alcançada. Isso inclui a adoção de políticas, processos, procedimentos, estrutura organizacional e tecnologias para reduzir o risco de exploração das vulnerabilidades (ABNT, 2022; Almeida & Respício, 2018). Existem guias de boas práticas para a implementação de controles de segurança, como a publicação especial 800-53 e o CSF do NIST, o CIS Controls e o MITRE ATT&CK. No entanto, a seleção dos controles pode ser desafiadora, pois essas referências não fornecem orientações sobre quais controles de segurança são mais recomendados para a situação específica do negócio, seus requisitos de segurança e a

dependência da tecnologia da informação (Barnard & Von Solms, 2000; Yevseyeva et al., 2015). Isso pode levar a uma seleção sem critério, resultando em falta de clareza na demonstração dos benefícios trazidos em relação aos investimentos realizados (Al-Safwani et al., 2018; Yevseyeva et al., 2016). Da mesma forma que o Setor Elétrico procurou fazer ao selecionar os controles adequados para o seu contexto (Lima et al., 2022), este trabalho busca avançar e oferecer caminhos para a efetiva mitigação desses riscos para o Poder Judiciário. Propõe-se a definição de uma linha de base de controles para se estabelecer o nível recomendado de segurança como uma alternativa à seleção aleatória de controles ou a necessidade de um extenso e complexo processo de avaliação de riscos (Barnard & Von Solms, 2000). Uma adequada gestão de riscos permite aplicar de forma efetiva, o princípio constitucional da eficiência (Nunes et al, 2021). Trata-se de um estudo de natureza aplicada, qualitativa e com objetivos exploratórios (Gil, 2018). Como procedimentos técnicos foi realizada a análise bibliográfica da literatura, entrevistas com profissionais das áreas jurídica, administrativa e de tecnologia, bem como grupos focais com especialistas de segurança da informação e gestão de riscos. Como resultado, foi obtida uma relação de aproximadamente 200 controles de segurança específicos para o tratamento dos riscos relacionados a 40 causas geradoras dos 10 principais riscos de negócio do Poder Judiciário (Alves et al., 2023) que incluem medidas preventivas, detectivas ou compensatórias para reduzir os riscos associados à gestão de pessoas, implementação de processos e o uso de tecnologias da informação. Os controles propostos abrangem diversas áreas de conhecimento e atuação na estrutura organizacional do Poder Judiciário. Na seleção dos controles, foi adotado como ponto de partida o framework CIS Controls v8, devido à sua adoção como referência pelo Governo Federal e pelo TCU em auditorias (TCU, 2020). Contudo, para abranger o escopo de riscos específico, foi necessário indicar controles complementares que incluem atividades para evitar espionagem, litispendência ou litigância de má-fé, estratégias de segurança para autoridades e a definição de controles tecnológicos, entre outros aspectos relevantes. Como trabalhos futuros, vislumbra-se a possibilidade de criação de um método ágil para diagnóstico e medição do nível de risco de segurança da informação para os órgãos do Poder Judiciário, com base na autoavaliação da aplicação dos controles propostos. Além disso, pode-se indicar controles

prioritários para se alcançar o nível desejado de risco, conforme as necessidades específicas de cada órgão.

Palavras-Chave: Segurança cibernética; controles de segurança; gestão de riscos; tratamento de riscos; poder judiciário.

Referências

ABNT. (2022). ABNT NBR ISO/IEC 27002.

Almeida, L., & Respício, A. (2018). Decision support for selecting information security controls. Journal of Decision Systems, 27, 173–180. https://doi.org/10.1080/12460125.2018.1468177

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. Computers and Security, 77, 565–577. https://doi.org/10.1016/j.cose.2018.05.009

Alves, R. S., Georg, M. A. C., & Nunes, R. R. (2023). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. RISTI. https://doi.org/10.5281/zenodo.7920441

Barnard, L., & Von Solms, Prof. R. (2000). A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. https://doi.org/https://doi.org/10.1016/S0167-4048(00)87829-3
Fuccia, E. V. (2022). Fraudes em alvarás no TRT-1 superam R$ 4 mi e sistema de pagamento é suspenso. Revista Consultor Jurídico. https://www.conjur.com.br/2022-nov-13/fraudes-emissao-alvaras-trt-ultrapassam-milhoes

Gil, A. Carlos. (2018). Como Elaborar Projetos de Pesquisa: Vol. 6o ed. Atlas.

Lobo, A. P. (2022, novembro 14). TRT do Rio de Janeiro sofre golpe de R$ 4 milhões com certificados digitais falsos. Convergência Digital.

Moura, R. M., & Borges, L. (2022). A impunidade dos hackers que colocaram o Judiciário de joelhos _ VEJA. Veja. https://veja.abril.com.br/politica/a-impunidade-dos-hackers-que-colocaram-o-judiciario-de-joelhos/

National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments - SP 800-30. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations - SP 800-53. https://doi.org/10.6028/NIST.SP.800-53r5

Nunes, R. R., Batista Sidrim Perini, M. T., & Melo Mourão Pinto, I. E. (2021). A gestão de riscos como instrumento para a aplicação efetiva do Princípio Constitucional da Eficiência. Revista Brasileira de Políticas Públicas, 11(3).

Lima, E., Moreira, F., de Deus, F., Nze, G., Sousa Júnior, R., & Nunes, R. R. (2022). Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética. RISTI, E49, 301–312. https://doi.org/10.5281/zenodo.7900434

Reina, E. (2022). ConJur - A onda de invasões hackers às estruturas tecnológicas dos tribunais. Revista Consultor Jurídico. https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14–30. https://doi.org/10.1016/J.COSE.2015.11.001

TCU. (2020). Acompanhamento de SegCiber. https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/

Yevseyeva, I., Basto-Fernandes, V., Emmerich, M., & Van Moorsel, A. (2015). Selecting Optimal Subset of Security Controls. Procedia Computer Science, 64, 1035–1042. https://doi.org/10.1016/j.procs.2015.08.625

Yevseyeva, I., Fernandes, V. B., Van Moorsel, A., Janicke, H., & Emmerich, M. (2016). Two-stage Security Controls Selection. Procedia Computer Science, 100, 971–978. https://doi.org/10.1016/j.procs.2016.09.261