versão março/2023

CONTRATAÇÃO DE TIC

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

1. SOLUÇÃO DE TIC A SER CONTRATADA

Consultoria especializada para realização de testes de segurança no ambiente tecnológico do Tribunal

2. IDENTIFICAÇÃO DA UNIDADE DEMANDANTE

Unidade/Setor:	Coordenadoria de Segurança da Informação e Proteção de Dados
Responsável:	Lucas Pozatti
Integrante Demandante indicado	

3. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

Segundo notícias recentes, o número de ataques a órgãos públicos atingiu seu maior patamar nos últimos 4 anos[1], com 989 casos ocorridos em janeiro/2024, uma média de 32 casos por dia. Essa crescente onda de ameaças cibernéticas demanda, por sua vez, maiores investimentos em recursos humanos, tecnológicos e financeiros na proteção do ambiente tecnológico - para exemplificar, em 2024 o TJ-RS estima investir 15 milhões de reais em segurança cibernética[2].

Diante do cenário dinâmico e em constante evolução das ameaças cibernéticas, tem se destacado, cada vez mais, a importância da realização de testes de segurança do ambiente tecnológico (principalmente em aplicações web e na infraestrutura de TI). Essa recomendação é fundamentada em uma abrangente análise do panorama de ameaças dos últimos anos, com

---

1 https://oglobo.globo.com/brasil/noticia/2024/03/01/ataques-ciberneticos-contra-orgaos-do-governo-federal-crescem-em-janeiro-puxados-por-vazamentos-de-dados.ghtml

2 https://gauchazh.clicrbs.com.br/colunistas/humberto-trezzi/noticia/2024/02/saiba-quanto-o-judiciario-gaucho-ja-gastou-para-prevenir-ataques-hackers-cls4l0ux9000v0132pr33cs2g.html

base em informações de relatórios especializados como o *Relatório de Violações de Dados* - 2023[3], da Verizon, e o *Custo de Violações de Dados*[4] - 2023, da IBM.

Com base nos relatórios, tem-se o seguinte panorama de ameaças:

- **Origem dos ataques**: verifica-se que a maior parte dos ataques origina-se de ameaças externas às organizações, correspondendo a cerca de 80% das violações:

Figura 1 - Gráfico demonstrando a fonte das ameaças nas violações observadas (fonte: 2023 Data Breach Investigation Report, Verizon, 2023)

- **Evolução das Táticas de Ataque:** de acordo com o Relatório de Violações de Dados da Verizon, as táticas de ataque têm evoluído rapidamente, tornando-se mais sofisticadas e difíceis de detectar. Os cibercriminosos estão aproveitando cada vez mais vulnerabilidades em aplicações web para realização de ataques.

[3] https://www.verizon.com/business/en-nl/resources/reports/dbir/
[4] https://www.ibm.com/br-pt/reports/data-breach

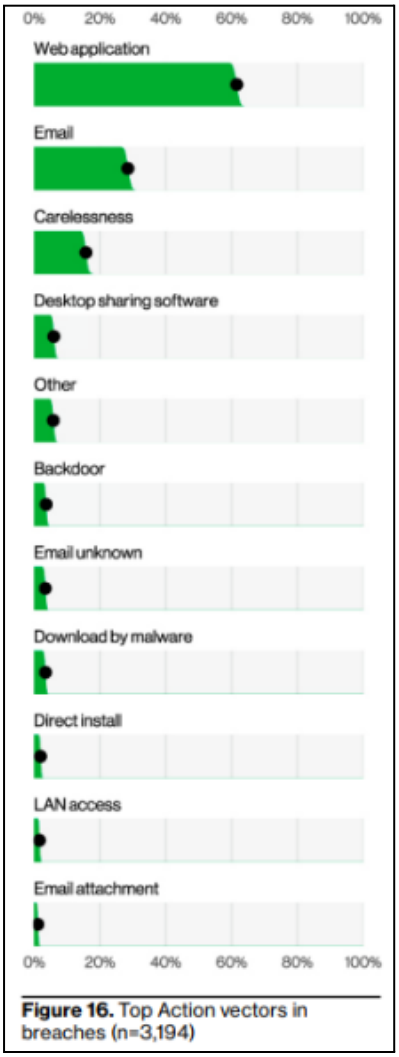

Figura 2 - Gráfico demonstrando os vetores de ataques mais utilizados (fonte: 2023 Data Breach Investigation Report, Verizon, 2023)

- **Aumento das Violações de Dados:** o relatório da IBM sobre o custo de violações de dados destaca um aumento alarmante no número e na gravidade das violações de dados nos últimos anos. Esses incidentes resultaram em danos significativos às organizações afetadas, incluindo perdas financeiras, danos à reputação e interrupções operacionais.

Além disso, os relatórios citados mencionam algumas estatísticas relevantes, tais como:

- **Táticas de Ataque Mais Comuns:** conforme o relatório da Verizon, os métodos de ataque mais comuns incluem exploração de vulnerabilidades, ataques de phishing e

comprometimento de credenciais, largamente utilizados em tentativas de intrusão a ambientes tecnológicos. Outro tipo de ataque que visa afetar as organizações são os ataques a aplicações web, com vistas a indisponibilizar a prestação dos serviços. Essas técnicas destacam a necessidade de avaliar regularmente a segurança do ambiente tecnológico do Tribunal contra possíveis brechas.

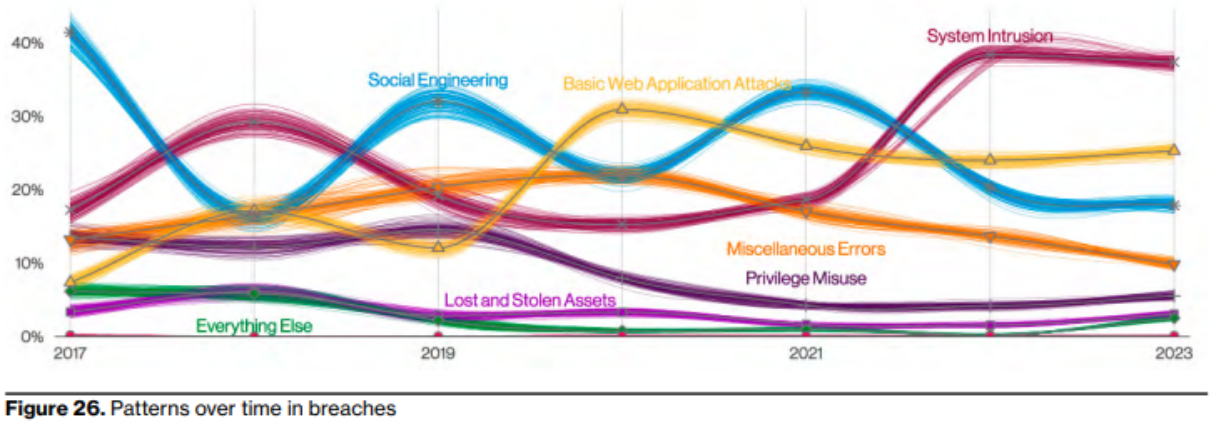

Figura 3 - Principais tipos de ataque (fonte: 2023 Data Breach Investigation Report, Verizon, 2023)

- **Impacto Financeiro das Violações de Dados:** o relatório da IBM revela que o custo médio de uma violação de dados aumentou significativamente nos últimos anos, atingindo cifras consideráveis. Isso inclui custos diretos, como investimentos em remediação e compensação de vítimas, bem como custos indiretos, como perda de receita e danos à reputação da marca.

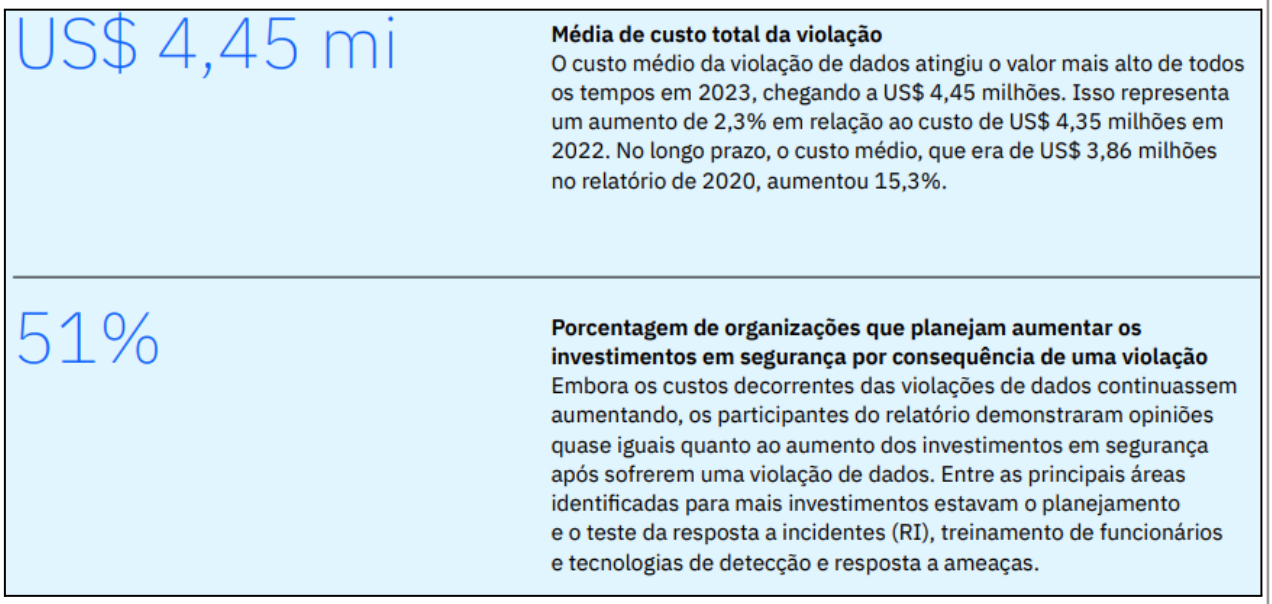

Figura 4 - Custos de uma violação de dados (fonte: Custo de Violações de Dados, IBM, 2023)

Diante desse cenário desafiador, os testes de segurança do ambiente tecnológico emergem como ferramenta essencial para avaliar a eficácia das medidas de proteção de TI contra ameaças cibernéticas. Esses testes simulam ataques controlados por especialistas em segurança (sem, no entanto, causar danos) identificando vulnerabilidades e pontos fracos que poderiam ser explorados por atores maliciosos, de acordo com o escopo definido pelo Tribunal.

Uma vez realizados os testes, a empresa elabora um relatório com a identificação e sugestão de correção das vulnerabilidades encontradas no teste, com o intuito de evitar que essas fragilidades sejam exploradas por atores maliciosos, incorrendo em comprometimento das atividades do Tribunal.

Ademais, os testes também avaliam a eficácia das medidas de segurança cibernética existentes em mitigar ameaças e fortalecer a resiliência do ambiente, contribuindo significativamente para a proteção de dados sensíveis e a garantia da integridade dos sistemas de informação.

A indústria de cartões de pagamento/crédito, responsável por transacionar dados sensíveis e um alto fluxo financeiro, tem a obrigação de estar em conformidade com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI-DSS, em inglês). Nele, é estabelecido que os testes de segurança são obrigatórios, por meio do controle 11.4, que exige a realização de testes de penetração regularmente.

No âmbito do Judiciário, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), instituída pela Resolução CNJ nº 396/2012[5], estabelece o seguinte:

- Art. 6º São objetivos da ENSEC-PJ: … II – aumentar a resiliência às ameaças cibernéticas;
- Art. 9º São ações da ENSEC-PJ: … II – elevar o nível de segurança das infraestruturas críticas;

Já a Portaria CNJ nº 162/2021[6], que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, define diversos controles para proteção do ambiente tecnológico, tomando por referência frameworks de segurança cibernética robustos, como CIS Controls[7] e ABNT NBR 27002:2022.

Por sua vez, o CIS Controls v8, define o Controle 18 - Teste de Invasão, com o seguinte objetivo: *Teste a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controles (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante.*

Já a ABNT NBR 27002:2022[8] - Controles de segurança da informação, possui os seguintes controles relacionados à necessidade de efetuar testes de segurança do ambiente tecnológico:

- 8.8 - Gestão de Vulnerabilidades Técnicas
- 8.29 - Testes de segurança em desenvolvimento e aceitação
- 8.34 - Proteção de sistemas de informação durante os testes de auditoria

Diante do exposto, ao realizar esse tipo de contratação, o Tribunal estará provendo meios para aumentar ainda mais a proteção da organização contra o cenário de ameaças em constante evolução. Essa abordagem proativa é crucial para a manutenção de um nível adequado de proteção do ambiente tecnológico, auxiliando o Tribunal a prestar jurisdição de forma célere e eficiente.

[5] https://atos.cnj.jus.br/atos/detalhar/3975
[6] https://atos.cnj.jus.br/atos/detalhar/3982
[7] https://www.cisecurity.org/controls
[8] https://www.abntcatalogo.com.br

4. QUANTIDADE A SER CONTRATADA E JUSTIFICATIVA

O número de horas de consultoria a ser contratado foi estimado com base na quantidade de testes de segurança a serem realizados e o tempo médio para execução dos testes.

Há que ser levado em consideração não apenas o tempo de execução dos testes por parte da empresa especializada, esse sim debitado da quantidade contratada, mas também o tempo que a equipe do TRT levará para implementar eventuais correções indicadas para corrigir as fragilidades identificadas nos testes.

Dessa forma, entende-se que a quantidade de **1000 horas** contratadas/registradas atenderá, de forma satisfatória, a demanda de testes de segurança do ambiente tecnológico a serem executadas em um período de **24 meses**.

5. PREVISÃO DA DATA EM QUE DEVE SER ENTREGUE O BEM OU INICIADA A PRESTAÇÃO DOS SERVIÇOS

Data ____/___/____ Motivo:

(x) Não se aplica

6. ALINHAMENTO COM O PLANO DE CONTRATAÇÕES

A demanda está prevista no Plano de Contratações de TIC?

(x) Sim: **ID SETIC - 61/2024** ( ) Não

7. INDICAÇÃO DA FONTE DE RECURSOS

( ) Programa de Apreciação de Causas da Justiça do Trabalho

( ) Manutenção do Sistema Nacional de TI

(x) Segurança da Informação nas Unidades do Poder Judiciário - SIUPJ

( ) Outra:

8. ALINHAMENTO ESTRATÉGICO[9]

A contratação está alinhada a algum objetivo do Plano Estratégico Institucional do Tribunal?

(x) Sim – Qual?
- **( )** Fortalecer a comunicação e as parcerias institucionais
- **( )** Promover o trabalho decente e a sustentabilidade
- **( )** Garantir a duração razoável do processo
- **( )** Promover a integridade e a transparência em relação aos atos de gestão praticados
- **( )** Assegurar o tratamento adequado dos conflitos trabalhistas
- **( )** Garantir a efetividade do tratamento das demandas repetitivas
- **( )** Fortalecer a governança e a gestão estratégica
- **( )** Aperfeiçoar a gestão orçamentária e financeira
- **( )** Incrementar modelo de gestão de pessoas em âmbito nacional
- **(x)** Aprimorar a governança de TIC e a proteção de dados

( ) Não

A contratação está alinhada a algum objetivo da Estratégia Nacional de TIC do Poder Judiciário?

(x) Sim – Qual?
- **( )** Aumentar a Satisfação dos Usuários do Sistema Judiciário;
- **( )** Promover a Transformação Digital;
- **( )** Reconhecer e Desenvolver as Competências dos Colaboradores;
- **( )** Buscar a Inovação de Forma Colaborativa;
- **( )** Aperfeiçoar a Governança e a Gestão;
- **( )** Aprimorar as Aquisições e Contratações;
- **(x)** Aprimorar a Segurança da Informação e a Gestão de Dados;
- **( )** Promover Serviços de Infraestrutura e Soluções Corporativas.

( ) Não

RESPONSÁVEL DA ÁREA DEMANDANTE

Documento assinado digitalmente
LUCAS POZATTI
Coordenador de Segurança da Informação e Proteção de Dados

[9] A consulta detalhada aos objetivos estratégicos pode ser realizada no Plano Estratégico Institucional 2021-2026, disponível no site do Tribunal (Planejamento Estratégico).