Cultura de Segurança da Informação - Um Relato de Oficinas para Conscientização de Servidores em Organizações Públicas

Maria A. P. F. Losse[1], Ana C. C. M. Morais[1], Edgard T. Sousa[1], Rennan L. B. Cabral[1,2], George A. V. Santos[2], Fernando A. A. Lins[2]

[1]Tribunal de Contas do Estado de Pernambuco (TCE-PE)

[2]Departamento de Computação – Universidade Federal Rural de Pernambuco

{alice,anacarolina,edgard,rennancabral}@tcepe.tc.br,
{fernandoaires,george.valenca}@ufrpe.br

Abstract. *Currently, the increase in the number of cyberattacks and data leaks from organizations is undeniable. In an increasingly digitalized world, Information Security tips and techniques have become even more critical for improving the organization's awareness. However, taking traditional face-to-face courses, or even remote courses, has a limited impact on people's motivation. In this context, this paper proposes holding a Security Workshop as an alternative capable of motivating interest in this topic and helping to learn and support the generation of security content specific to the company's context. The results showed that employees could propose and discuss innovative security tips and techniques based on the organization's context.*

Resumo. *Atualmente, é inegável o aumento da quantidade de ataques cibernéticos e vazamento de dados de organizações. Em um mundo cada vez mais digitalizado, dicas e técnicas de Segurança da Informação se tornam ainda mais importantes para a melhoria da conscientização da organização. Contudo, a realização de cursos tradicionais presenciais, ou mesmo cursos remotos, tem um alcance limitado sobre a motivação das pessoas. Neste contexto, este artigo propõe a realização de Oficina de Segurança como uma alternativa capaz de motivar o interesse nesta temática e também como forma de tanto auxiliar o aprendizado como também apoiar a geração de conteúdo de segurança específico para o contexto da empresa. Os resultados mostraram que os funcionários foram capazes de propor e discutir dicas e técnicas inovadoras de segurança baseadas no contexto da própria organização.*

1 Contexto

A sociedade vem acompanhando, ao longo dos anos, um crescente aumento na transformação digital, que impacta praticamente todas as áreas de conhecimento. Contudo, o número de riscos de Segurança da Informação (SI) também aumentou: cada vez mais, o armazenamento se dá em meio digital, muitas vezes externo à organização, e o acesso ocorre por redes de comunicação, que podem não ser confiáveis. Neste contexto, cresce o número de ataques cibernéticos e violações a dados confidenciais e pessoais. O resultado é a necessária valorização das áreas de Segurança da Informação e Cibersegurança[1]. Processos, técnicas e ferramentas de SI tornam-se críticas e urgentes não só no setor privado, mas também em organizações públicas, que possuem verdadeiros

[1] https://www.computerweekly.com/news/ 366537314/IT-Priorities-2023-security-dominates-IoT-investment-plans.

"armazéns de dados" de cidadãos, dos mais variados tipos (de dados contábeis a registros de saúde).

O fator humano ganha ainda mais destaque, como evidencia a recente criação do Comitê Nacional de Cibersegurança [BRASIL 2024] que, dentre outras atribuições, buscará fortalecer a conscientização de segurança computacional a nível nacional. Dessa forma, atacantes mal intencionados terão menos espaço para aplicar estratégias de engenharia social. É possível destacar que alguns trabalhos já trazem contribuições interessantes neste contexto. Por exemplo, a UFC [UFC 2024] e a UFBA [UFBA 2024] propõem programas formais e materiais específicos de conscientização. Contudo, existe uma lacuna a ser preenchida referente a formas inovadoras e ativas de aprendizagem que busquem não apenas o repasse de conteúdo mas também maior engajamento dos funcionários da organização, contribuindo para que eles sejam também agentes do processo de ensino-aprendizagem e de mudança comportamental.

Este cenário motivou a condução de oficinas de Segurança da Informação, destinadas a servidores de uma organização pública, como estratégia de engajamento dos participantes e identificação de boas práticas para proteção de dados e sistemas. Este estudo foi conduzido em meio a um convênio de cooperação técnica entre a organização, pertencente ao setor de fiscalização, e uma universidade federal, com aplicação do método de pesquisa-ação (processo de investigação interativo que combina ações de resolução de problemas implementadas em um contexto colaborativo, à luz de definições da academia). A oficina aqui descrita, intitulada Você +Seguro, buscou envolver seus participantes, a partir de atividades colaborativas e criativas, estimulando o debate e a elaboração de respostas para questões relacionadas à segurança cibernética.

2 Processo Adotado

A oficina foi realizada em setembro de 2023, durante a II Semana de Inovação do TCE-PE, e contou com um total de 89 participantes. Estes participantes, em geral, não eram da área de Tecnologia da Informação, e não possuíam conhecimentos avançados desta área. A oficina foi conduzida por duas servidoras ligadas à gestão de SI da instituição. Esta oficina foi construída em cima de princípios da Aprendizagem Baseada em Problemas (PBL - *Problem Based Learning*) e *Design Thinking* (DT), em que problemas são apresentados através de desafios. Neste caso, foram apresentados desafios como: "como fortalecer a cultura da segurança da informação de forma inovadora?", "quais são os principais cuidados que você deve ter com o seu celular para proteger as informações contidas nele?" e "o que fazer quando o seu celular for roubado?". A oficina teve início com uma breve **apresentação do conceito e importância** da Segurança da Informação. Em seguida, houve a **descrição da dinâmica** a ser realizada e a **formação de grupos** (oito, no total). Cada grupo, formado por servidores de diferentes áreas da instituição, conduziu uma **reflexão sobre os desafios elencados** utilizando técnicas intuitivas do DT, como *Brainstorming* e *Brainwriting*. Após esta reflexão, houve **compartilhamento dos resultados** por todos os grupos.

3 Solução e Resultados

Os resultados obtidos nos grupos foram registrados na forma de mapa mental, como mostra a Figura 1, facilitando a interpretação dos mesmos pela equipe de SI do órgão.

Figura 1. Resultado do desafio sobre fortalecimento da cultura de segurança.

O mapa mental acima revela que os participantes sugeriram ações técnicas interessantes, mesmo em geral pertencendo a setores de fora da TI do órgão. Por exemplo, a promoção de capacitações frequentes está intimamente ligada à promoção da cultura de cibersegurança. Já a promoção de testes, jogos e alertas inesperados demonstra a apreciação por um formato lúdico, baseado no paradigma crescente de gamificação. Também cabe destacar que a proposição de uso de inteligência artificial está de acordo com orientações da IEEE, em seu documento sobre principais tendências [IEEE 2023].

A Figura 2 apresenta os resultados relacionados ao segundo desafio, e pode-se notar que o público também conseguiu produzir dicas técnicas relevantes e atuais, como autenticação multifatorial. Inclusive, houve sugestões menos conhecidas como salvar o IMEI do aparelho - iniciativa defendida pelo programa "Celular Seguro" [BRASIL 2023].

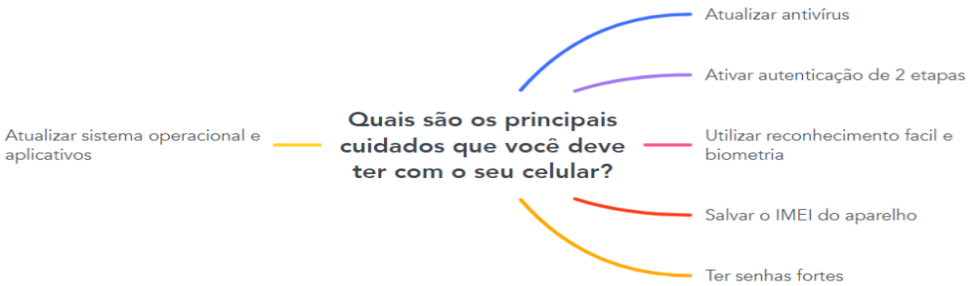

Figura 2. Resultado do desafio sobre cuidados com o celular.

Os exemplos acima demonstram que, mesmo um público sem experiência profunda em TI, foi capaz de evidenciar conhecimento de segurança digital e prover sugestões de segurança ligadas tanto à sua vida pessoal como à sua vida profissional.

Pode-se afirmar que um dos pilares atuais da Segurança da Informação são as pessoas. Elevar o nível de conhecimento de segurança digital delas se mostra vital para o sucesso dos objetivos de negócio da organização. Este trabalho descreveu a realização de Oficinas de Segurança, uma forma ativa de aprendizagem onde os participantes aprendem e produzem o conteúdo técnico a ser disseminado pela organização. Os resultados evidenciaram que a oficina de segurança é capaz de prover aprendizagem ativa e geração de conteúdo relevante. Inclusive, este conteúdo está sendo usado pela organização em campanhas de conscientização de SI. É possível também destacar que a metodologia proposta para a oficina pode ser aplicada em outros nichos, como outros órgãos públicos.

REFERÊNCIAS

[BRASIL 2023] Comunicar roubo/furto de aparelho pelo aplicativo Celular Seguro. Disponível em https://www.gov.br/pt-br/servicos/comunicar-roubo-furto-de-aparelho-pelo-aplicativo-celular-seguro (último acesso: 18 fev. 2024).

[BRASIL 2024] Portaria nº 6 de Fevereiro de 2024. (2024). Comitê Nacional de Cibersegurança - CNCiber. Disponível em https://www.in.gov.br/en/web/dou/-/portaria-n-6-de-9-de-fevereiro-de-2024-542752145. (último acesso: 15 abr. 2024).

[IEEE 2023] Top Technology Trends for 2023. Disponível em https://innovationatwork.ieee.org/top-technology-trends-for-2023/#:~:text=Cloud%20Computing%2C%205G%2C%20Metaverse%2C,2023%2C%20Says%20New%20IEEE%20Study (último acesso: 19 fev. 2024).

[UFBA 2024]. 5ª Campanha de Conscientização em Segurança da Informação. Disponível em https://www.sti.ufba.br/5a-campanha-de-conscientizacao-em-seguranca-da-informacao (último acesso: 15/02/2024).

[UFC 2024] Programa de Conscientização em Segurança da Informação. Disponível em https://seginfo.ufc.br/programa-de-conscientizacao-em-seguranca-da-informacao/ (últim acesso: 16/02/2024).