REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

FATORES HUMANOS E ENGENHARIA SOCIAL: O ELO MAIS VULNERÁVEL DA CIBERSEGURANÇA CORPORATIVA

HUMAN FACTORS AND SOCIAL ENGINEERING: THE MOST VULNERABLE LINK IN CORPORATE CYBERSECURITY

FACTORES HUMANOS E INGENIERÍA SOCIAL: EL ESLABÓN MÁS VULNERABLE EN LA CIBERSEGURIDAD CORPORATIVA

Otávio Lacerda Oliveira Ferreira Leandro[1], Gabriel Divino Pereira de Souza[1], Diego Santos Almeida Pinto[2], Vinicius Portilho Pereira[3]

e6116955
https://doi.org/10.47820/recima21.v6i11.6955

PUBLICADO: 11/2025

RESUMO

O presente estudo tem como objetivo analisar como os fatores humanos e as técnicas de engenharia social configuram-se como o elo mais vulnerável da cibersegurança, mesmo diante do avanço constante das tecnologias de proteção digital. A pesquisa, de caráter descritivo e abordagem quali-quantitativa, baseou-se em revisão bibliográfica e análise de relatórios corporativos e institucionais recentes, como os da *Verizon*, IBM, ENISA e NIST. Os resultados demonstram que o comportamento humano está presente em aproximadamente 74% das violações de segurança reportadas globalmente, evidenciando que a maioria dos incidentes decorre de falhas de atenção, negligência, confiança excessiva e manipulação psicológica. Verificou-se também que a engenharia social evoluiu com o uso de inteligência artificial e *deepfakes*, tornando os ataques mais sofisticados e difíceis de detectar. Constatou-se que políticas de segurança centradas apenas em tecnologia são insuficientes sem o engajamento humano e uma cultura organizacional de segurança sólida. O estudo conclui que a vulnerabilidade humana, embora inevitável, pode ser significativamente reduzida por meio de educação digital contínua, conscientização comportamental e integração entre tecnologia, psicologia e gestão. Dessa forma, o elo mais fraco da cibersegurança pode transformar-se em um pilar de defesa, desde que sustentado por treinamento, cultura e responsabilidade compartilhada.

PALAVRAS-CHAVE: Fator humano. Engenharia social. Cibersegurança.

ABSTRACT

This study aims to analyze how human factors and social engineering techniques constitute the most vulnerable link in cybersecurity, even with the constant advancement of digital protection technologies. The descriptive research, with a qualitative and quantitative approach, was based on a literature review and analysis of recent corporate and institutional reports, such as those from Verizon, IBM, ENISA, and NIST. The results demonstrate that human behavior is present in approximately 74% of security breaches reported globally, highlighting that most incidents stem from attention lapses, negligence, overtrust, and psychological manipulation. Moreover, the research revealed that social engineering has evolved with the use of artificial intelligence and deepfakes, making attacks more sophisticated and difficult to detect. The findings also indicate that security policies focused solely on technology are insufficient without human engagement and a solid organizational security culture. The study concludes that human vulnerability, while inevitable, can

[1] Estudante de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba UNICERRADO.
[2] Orientador: Professor do curso de Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba. UNICERRADO.
[3] Coorientador do TCC no curso Gestão da Tecnologia da Informação no Centro Universitário de Goiatuba UNICERRADO.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

be significantly reduced through continuous digital education, behavioral awareness, and the integration of technology, psychology, and management. In this way, the weakest link in cybersecurity can become a pillar of defense, as long as it is supported by training, culture, and shared responsibility.

KEYWORDS: *Human factor. Social engineering. Cybersecurity.*

RESUMEN
Este estudio busca analizar cómo los factores humanos y las técnicas de ingeniería social constituyen el eslabón más vulnerable de la ciberseguridad, incluso con el avance constante de las tecnologías de protección digital. La investigación descriptiva, con un enfoque cualitativo y cuantitativo, se basó en una revisión bibliográfica y el análisis de informes corporativos e institucionales recientes, como los de Verizon, IBM, ENISA y NIST. Los resultados demuestran que el comportamiento humano está presente en aproximadamente el 74 % de las brechas de seguridad reportadas a nivel mundial, destacando que la mayoría de los incidentes se deben a lapsos de atención, negligencia, exceso de confianza y manipulación psicológica. También se descubrió que la ingeniería social ha evolucionado con el uso de inteligencia artificial y deepfakes, lo que hace que los ataques sean más sofisticados y difíciles de detectar. Se concluyó que las políticas de seguridad centradas exclusivamente en la tecnología son insuficientes sin la participación humana y una sólida cultura de seguridad organizacional. El estudio concluye que la vulnerabilidad humana, si bien inevitable, puede reducirse significativamente mediante la educación digital continua, la concienciación del comportamiento y la integración de la tecnología, la psicología y la gestión. De esta manera, el eslabón más débil de la ciberseguridad puede convertirse en un pilar de defensa, siempre que se apoye en la capacitación, la cultura y la responsabilidad compartida.

PALABRAS CLAVE*: Factor humano. Ingeniería social. Ciberseguridad.*

INTRODUÇÃO

A cibersegurança contemporânea é frequentemente apresentada como uma disputa entre defesas técnicas e vulnerabilidades digitais: firewalls, antivírus, atualizações e criptografia são as respostas tradicionais às ameaças. Contudo, essa visão estritamente técnica ignora o elemento humano, os comportamentos, a atenção e as decisões que influenciam diretamente a segurança das organizações. Fatores como fadiga, pressa, confiança e conformidade social influenciam diretamente a eficácia das medidas de proteção. Assim, compreender os fatores humanos não é um complemento, mas um componente essencial para reduzir riscos. As defesas tecnológicas mais sofisticadas podem ser comprometidas por uma simples interação enganosa, tornando a engenharia social um tema central dentro da cibersegurança moderna. Este trabalho propõe analisar essa vulnerabilidade humana como o elo mais frágil das defesas digitais contemporâneas.

A engenharia social emergiu como vetor recorrente em incidentes de segurança, demonstrando que explorar comportamentos humanos é mais simples e lucrativo do que invadir sistemas complexos. Segundo o relatório *Verizon Data Breach Investigations Report* DBIR, (2024), aproximadamente 74% das violações de dados envolvem o fator humano, seja por erro, uso indevido de credenciais ou engano. O mesmo estudo destaca que o phishing continua sendo a técnica mais eficaz, seguido por ataques de pretexting e uso de engenharia social em redes

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

corporativas. Esses números revelam que as falhas humanas ultrapassam, em impacto, vulnerabilidades puramente técnicas. Portanto, compreender as dinâmicas psicológicas e organizacionais por trás desses ataques é fundamental para desenvolver defesas mais eficazes (Verizon, 2024).

Por que o comportamento humano ainda representa o elo mais vulnerável da cibersegurança, mesmo diante de tantas inovações técnicas?

A evolução tecnológica ampliou o alcance da engenharia social, permitindo ataques mais personalizados e automatizados. De acordo com a Agência da União Europeia para a Cibersegurança ENISA, (2023), o uso de inteligência artificial generativa já é um diferencial para cibercriminosos, que utilizam ferramentas como *deepfakes*, geração de voz sintética e e-mails automatizados para aumentar a credibilidade de golpes. A transição para modelos de trabalho remoto e híbrido também criou novos vetores de ataque, ao dispersar as equipes e enfraquecer as barreiras tradicionais. Assim, a engenharia social se adaptou às novas realidades de comunicação digital, tornando-se um fenômeno sociotécnico em constante evolução ENISA, (2023).

A abordagem sobre fatores humanos deve ultrapassar treinamentos pontuais e considerar aspectos mais amplos, como o desenho de processos, a usabilidade de sistemas e os incentivos institucionais. O Instituto Nacional de Padrões e Tecnologia NIST, em sua publicação *Special Publication 800-50* sobre conscientização em segurança, ressalta que a educação do usuário é mais efetiva quando incorporada à cultura organizacional e acompanhada por métricas comportamentais NIST, (2022). Dessa forma, programas contínuos de capacitação, políticas de comunicação transparente e práticas que recompensem a detecção de ameaças são medidas mais eficientes do que campanhas isoladas. A segurança, portanto, deve ser vista como um processo de aprendizado organizacional constante.

Os engenheiros sociais exploram princípios psicológicos universais para manipular vítimas e obter acesso a informações ou sistemas. Tais princípios foram amplamente descritos por Robert Cialdini, (2006), que identifica seis gatilhos de persuasão: reciprocidade, compromisso e coerência, prova social, autoridade, escassez e simpatia. Ao aplicar esses conceitos em contextos digitais, atacantes criam narrativas convincentes e convincentes que reduzem o senso crítico das vítimas. E-mails com linguagem de urgência, falsos comunicados corporativos e falsos pedidos de suporte técnico exploram esses mecanismos com grande eficácia. Assim, compreender a psicologia por trás da influência social torna-se indispensável para a prevenção e mitigação de ataques baseados em comportamento humano.

As consequências de ataques que exploram o elo humano ultrapassam o impacto técnico, alcançando dimensões financeiras, reputacionais e legais. De acordo com o relatório IBM Cost of a Data Breach, (2024), o custo médio global de uma violação de dados atingiu 4,88 milhões de dólares, sendo que incidentes iniciados por engenharia social ou phishing representam parte

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

significativa desse valor. Além dos prejuízos diretos, há perda de confiança de clientes, processos regulatórios e interrupções operacionais prolongadas. Esses dados evidenciam que o investimento em conscientização e políticas de segurança baseadas em comportamento é, além de estratégico, financeiramente justificável IBM, (2024).

Do ponto de vista metodológico, a pesquisa sobre fatores humanos na cibersegurança demanda uma abordagem interdisciplinar, que una ciência cognitiva, psicologia social e gestão da informação. Métodos quantitativos como análise de incidentes e simulações de phishing podem ser combinados com técnicas qualitativas, como entrevistas e observação de campo. Essa combinação permite compreender não apenas o "o que" das falhas humanas, mas o "porquê" por trás delas. A análise contextual, levando em conta cultura organizacional, pressão por produtividade e desenho de processos, é essencial para evitar conclusões simplistas. Essa integração metodológica é o que diferencia uma simples descrição de incidentes de uma compreensão aprofundada sobre o comportamento humano em ambientes digitais.

Portanto, reconhecer o fator humano como vulnerabilidade não implica culpabilizar o indivíduo, mas redesenhar sistemas e políticas que reduzam a probabilidade de erro. O usuário deve ser visto não como o problema, mas como parte da solução um agente ativo na construção de uma cultura de segurança mais resiliente. Assim, este trabalho propõe discutir os fatores humanos e a engenharia social como elementos complementares na análise de vulnerabilidades, reforçando que tecnologia e comportamento precisam caminhar juntos. O elo mais vulnerável da cibersegurança pode, com educação, design e cultura, transformar-se também no mais forte.

1. REFERENCIAL TEÓRICO

A segurança da informação sempre foi um dos pilares fundamentais para o funcionamento das organizações modernas. No entanto, nas últimas décadas, o avanço das tecnologias e o crescimento da interconectividade digital ampliaram as possibilidades de ataque, revelando um fator que ultrapassa os limites técnicos: o ser humano. Segundo Sêmola, (2014), a cibersegurança deve ser entendida como um processo contínuo e multidisciplinar, no qual pessoas, processos e tecnologias precisam atuar em conjunto. Nesse contexto, a vulnerabilidade humana surge como o elo mais frágil das defesas digitais, tornando o estudo dos fatores humanos e da engenharia social um elemento essencial na proteção de dados.

A engenharia social pode ser definida como o conjunto de técnicas de manipulação psicológica utilizadas para induzir indivíduos a revelar informações confidenciais, realizar ações indevidas ou conceder acesso a sistemas protegidos. De acordo com Mitnick e Simon (2011), a manipulação psicológica é a arma mais poderosa dos invasores, pois explora emoções e fraquezas cognitivas, e não falhas de software. Assim, a engenharia social é, em essência, uma ciência do

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

comportamento aplicada à segurança, explorando princípios de influência, confiança e autoridade para contornar mecanismos técnicos de proteção.

1.1. O fator humano na cibersegurança

O comportamento humano está no centro das falhas de segurança cibernética. Mesmo em ambientes com políticas e ferramentas avançadas, erros humanos continuam a representar a maior parte das violações. Conforme o *Verizon Data Breach Investigations Report* DBIR, (2024), cerca de 74% dos incidentes de segurança envolvem o fator humano, seja por negligência, erro operacional, má configuração ou resposta inadequada a tentativas de fraude. Esses dados evidenciam que o elo humano não pode ser tratado como um simples risco residual, mas como uma variável central a ser gerenciada nas estratégias de segurança organizacional (Verizon, 2024).

O fator humano abrange não apenas a suscetibilidade individual a enganos, mas também aspectos culturais e estruturais que moldam o comportamento dos colaboradores. Segundo Schneier (2018), a maioria dos incidentes ocorre não por malícia, mas pela falta de compreensão sobre o impacto das próprias ações. Isso demonstra que segurança da informação é, antes de tudo, uma questão de comportamento coletivo, onde a conscientização e a cultura organizacional são determinantes para o sucesso das defesas digitais. Dessa forma, o desenvolvimento de programas de segurança deve considerar os limites cognitivos, as pressões de trabalho e os incentivos institucionais que influenciam as decisões humanas.

1.2. Engenharia social e seus mecanismos de manipulação

A engenharia social baseia-se em princípios universais de persuasão e influência. Cialdini (2006) identifica seis gatilhos psicológicos frequentemente explorados por atacantes: reciprocidade, compromisso e coerência, prova social, autoridade, escassez e simpatia. Em ataques de phishing, por exemplo, o senso de urgência e a aparência de legitimidade são usados para provocar decisões impulsivas. Já em golpes corporativos, o uso de figuras de autoridade ou de colegas falsificados cria um ambiente de confiança artificial. A eficácia dessas táticas mostra que a engenharia social opera explorando vulnerabilidades emocionais tanto quanto tecnológicas.

Além disso, a modernização dos ataques intensificou o uso de inteligência artificial generativa e *deepfakes* para aumentar a credibilidade das fraudes. De acordo com o Relatório ENISA Threat Landscape, (2023), a manipulação de áudio e vídeo, somada à automação de mensagens personalizadas, tornou os ataques de engenharia social mais convincentes e difíceis de detectar. Assim, os limites entre realidade e simulação tornam-se cada vez mais tênues, exigindo novas abordagens de defesa centradas na detecção comportamental e na análise contextual das comunicações.

ISSN: 2675-6218 - RECIMA21
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

1.3. Cultura organizacional e conscientização

A conscientização é uma das principais ferramentas de mitigação do risco humano. O NIST, (2022) enfatiza que programas de segurança devem ir além de treinamentos pontuais e integrar práticas contínuas de aprendizagem, alinhadas à cultura da organização. Quando os colaboradores compreendem o *porquê* das políticas de segurança, a adesão torna-se natural e sustentável. Nesse sentido, o engajamento humano não é alcançado por imposição, mas por empatia e clareza comunicacional. A criação de ambientes de trabalho que não punam erros, mas incentivem o reporte de incidentes, fortalece a cultura de segurança e reduz o impacto das falhas humanas.

A educação em segurança digital, quando aplicada de forma contextualizada, permite que o usuário atue como uma linha adicional de defesa. Conforme estudo de Parsons *et al.,* (2017), treinamentos baseados em cenários práticos e simulações de ataques reais aumentam significativamente a percepção de risco e a taxa de resposta adequada. Assim, programas de capacitação devem incluir simulações de phishing, alertas personalizados e feedback constante, promovendo o desenvolvimento de uma mentalidade de vigilância ativa.

1.4. A interdependência entre tecnologia e comportamento

Embora as soluções tecnológicas sejam essenciais, elas não substituem o papel do comportamento humano. Firewalls, antivírus e sistemas de detecção de intrusão podem mitigar riscos, mas dependem de decisões humanas para serem corretamente configurados e utilizados. Segundo Ross e Benigni (2020), a segurança deve ser projetada considerando o “fator humano como parte do sistema”, e não como um obstáculo. Essa integração entre tecnologia e psicologia organizacional é o caminho para alcançar defesas adaptativas e resilientes.

Entretanto, a análise de fatores humanos pode orientar o design de interfaces mais seguras. Sistemas com excesso de alertas, linguagem técnica ou fluxos complexos podem gerar fadiga cognitiva e levar usuários a ignorar avisos críticos. A aplicação de princípios de security by design e human-centered security reduz a probabilidade de erros e aumenta a adesão às políticas de segurança. Assim, o equilíbrio entre usabilidade e proteção se mostra indispensável para reduzir vulnerabilidades originadas pelo próprio comportamento humano.

2. MÉTODOS

A metodologia tem como objetivo descrever os caminhos percorridos para alcançar os resultados pretendidos nesta pesquisa, apresentando os métodos, as técnicas e as abordagens utilizadas. Segundo Marconi e Lakatos (2003), a metodologia científica representa o conjunto de procedimentos sistematizados adotados pelo pesquisador na busca de respostas a um problema de investigação. Assim, este trabalho adotou uma abordagem estruturada, visando compreender

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

como o fator humano e as técnicas de engenharia social se configuram como os principais vetores de vulnerabilidade dentro da cibersegurança organizacional.

O presente estudo classifica-se como pesquisa básica e descritiva, pois busca gerar conhecimento sem aplicação prática imediata, mas com foco em ampliar a compreensão teórica sobre o comportamento humano no contexto da segurança da informação. O objetivo descritivo se justifica pela intenção de observar, descrever e analisar fenômenos relacionados às ações humanas e às estratégias de manipulação utilizadas em ataques de engenharia social, sem, no entanto, intervir diretamente sobre eles.

Quanto à abordagem do problema, a pesquisa é qualitativa e quantitativa. É qualitativa por utilizar interpretações teóricas e descritivas provenientes de livros, relatórios e artigos científicos, com foco na compreensão dos fatores humanos e comportamentais. É também quantitativa, pois utiliza dados estatísticos provenientes de fontes secundárias como relatórios da *Verizon*, (2024) e da IBM Security, (2024) para sustentar a relevância do tema com base em números e percentuais de incidentes de segurança relacionados a falhas humanas.

Em relação aos procedimentos técnicos, o trabalho enquadra-se como pesquisa bibliográfica, visto que foi desenvolvido a partir da análise de materiais já publicados, como artigos científicos, livros, relatórios técnicos e publicações institucionais nacionais e internacionais. Conforme Gil (2019), a pesquisa bibliográfica é fundamental para a construção de uma base teórica sólida, permitindo ao pesquisador compreender as contribuições e lacunas existentes na literatura. Dessa forma, foram consultadas fontes como o NIST Special Publication 800-50 (2022), o ENISA Threat Landscape (2023), e obras de autores renomados como Mitnick (2011), Schneier (2018) e Cialdini (2006).

O método científico adotado foi o hipotético-dedutivo, partindo da hipótese de que “o comportamento humano é o elo mais vulnerável da cibersegurança moderna”. Essa hipótese foi construída com base em estudos anteriores e testada por meio da análise de evidências empíricas encontradas em relatórios e pesquisas sobre incidentes de engenharia social. Assim, o raciocínio dedutivo parte de princípios gerais observados na literatura para explicar casos concretos e recorrentes de falhas humanas em ambientes corporativos.

Para a coleta de informações, utilizou-se a técnica de levantamento documental em bases acadêmicas e relatórios corporativos especializados, como Google Scholar, Scopus, ENISA, NIST, *Verizon* e IBM *Security Reports.* As fontes foram selecionadas de acordo com sua relevância científica e atualidade, priorizando publicações dos últimos cinco anos. As informações coletadas foram analisadas e organizadas de forma comparativa, permitindo identificar padrões de comportamento e tendências de exploração de vulnerabilidades humanas.

A análise dos dados foi conduzida por meio de interpretação analítica e comparativa, buscando estabelecer relações entre os conceitos teóricos e os dados empíricos encontrados.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

A abordagem comparativa permitiu observar semelhanças entre os mecanismos de manipulação identificados em diferentes contextos e compreender de que forma as organizações respondem a esses desafios. Essa etapa foi essencial para confirmar a hipótese inicial e fundamentar as discussões apresentadas nas seções posteriores.

Enfim, a metodologia adotada neste estudo permitiu construir uma visão crítica e interdisciplinar sobre o papel do fator humano na cibersegurança, unindo evidências empíricas, conceitos teóricos e análises comportamentais. Assim, este trabalho contribui para o debate acadêmico e prático sobre a necessidade de integrar psicologia, tecnologia e educação digital na formulação de políticas de segurança mais eficazes.

3. RESULTADOS E DISCUSSÃO

Para a fundamentação da hipótese proposta, foram analisados artigos científicos, relatórios corporativos e publicações de órgãos especializados em segurança da informação, os quais abordam o impacto do fator humano e das técnicas de engenharia social em incidentes cibernéticos. Os dados coletados reforçam a ideia de que a principal vulnerabilidade das organizações não está nos sistemas, mas nas pessoas que os operam. Os resultados demonstram que, mesmo diante de tecnologias avançadas, os erros humanos e os ataques de manipulação continuam sendo os vetores mais explorados por cibercriminosos.

Na primeira etapa da análise, observou-se que o *Verizon Data Breach Investigations Report* DBIR, (2024) identificou o fator humano como elemento presente em 74% das violações de segurança globalmente. Esse número inclui ações como cliques em links de phishing, compartilhamento indevido de credenciais, erros de configuração e negligência em protocolos básicos de segurança. Tais estatísticas comprovam que o elo humano é, de fato, o componente mais frágil das defesas corporativas. A análise desses dados também indica que a maioria dos incidentes poderia ter sido evitada com treinamentos contínuos e políticas institucionais de conscientização digital.

A segunda etapa da pesquisa evidenciou o papel crescente da engenharia social como ferramenta de ataque sofisticada. O relatório ENISA Threat Landscape (2023) mostra que os criminosos estão utilizando inteligência artificial e *deepfakes* para automatizar golpes e criar comunicações mais convincentes. E-mails e mensagens fraudulentas são gerados com base em dados coletados de redes sociais e sistemas corporativos, tornando a fraude quase indistinguível de comunicações legítimas. Essa evolução tecnológica amplia o alcance dos ataques e exige que as empresas adotem estratégias preventivas mais complexas, baseadas em comportamento e contexto, e não apenas em filtros automáticos.

Em paralelo, o relatório IBM Cost of a Data Breach (2024) indica que o custo médio global de uma violação de dados atingiu 4,88 milhões de dólares, sendo que incidentes originados em

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

falhas humanas ou engenharia social estão entre os mais caros para remediação. Além das perdas financeiras diretas, há impactos indiretos, como danos à reputação, perda de confiança dos clientes e sanções legais decorrentes da má gestão de dados sensíveis. Esse panorama reforça que o investimento em cultura de segurança e educação digital é financeiramente justificável, representando não um custo, mas uma forma de mitigação de prejuízos de longo prazo.

A análise também revelou que a maioria das organizações ainda trata o comportamento humano como um problema técnico, e não como uma questão de cultura organizacional. De acordo com estudos de Parsons *et al.,* (2017), programas de conscientização baseados em simulações práticas e feedback constante reduzem significativamente a taxa de sucesso de ataques de phishing. No entanto, muitas empresas ainda adotam treinamentos esporádicos, sem continuidade ou mensuração de resultados. Essa prática se mostra ineficiente diante do cenário atual, em que o ataque social é dinâmico e adaptável. As organizações que desenvolvem uma cultura de segurança contínua, aliando aprendizado e incentivo à notificação de incidentes, apresentam resultados mais consistentes na redução de vulnerabilidades humanas.

Outro ponto importante observado foi a influência dos fatores psicológicos e sociais nos ataques de engenharia social. Baseando-se nos estudos de Cialdini, (2006), percebe-se que os invasores exploram princípios como autoridade, reciprocidade e escassez para obter respostas rápidas e automáticas de suas vítimas. Esses gatilhos emocionais reduzem a capacidade crítica das pessoas e as levam a tomar decisões impulsivas. A compreensão desses mecanismos permite desenvolver políticas de segurança mais realistas, que considerem as limitações cognitivas dos usuários e estimulem a tomada de decisão segura em ambientes de pressão ou urgência.

A discussão dos resultados também aponta que a simples implementação de tecnologias de proteção como autenticação multifator ou firewalls inteligentes não é suficiente para eliminar os riscos relacionados ao fator humano. Como defende Schneier (2018), a segurança deve ser compreendida como um sistema sociotécnico, em que o comportamento humano é parte integrante da arquitetura de proteção. A negligência desse aspecto transforma as tecnologias em barreiras ilusórias, facilmente contornáveis por estratégias de manipulação e engenharia social. Portanto, a integração entre psicologia, treinamento e design de sistemas é essencial para reduzir vulnerabilidades reais.

Por fim, os resultados confirmam a hipótese inicial deste estudo: o fator humano permanece sendo o elo mais vulnerável da cibersegurança, e sua exploração por meio da engenharia social representa um dos maiores desafios contemporâneos da segurança digital. Para mitigar esse cenário, é fundamental que as organizações adotem uma abordagem holística que envolva tecnologia, processos e principalmente pessoas. A construção de uma cultura de segurança consciente e participativa é o caminho mais eficaz para transformar o elo mais fraco em uma barreira ativa contra-ataques cibernéticos.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

4. CONSIDERAÇÕES

O presente estudo teve como objetivo compreender de que forma os fatores humanos e as técnicas de engenharia social se configuram como o elo mais vulnerável da cibersegurança, mesmo diante de constantes avanços tecnológicos. A pesquisa partiu da hipótese de que a principal fragilidade dos sistemas de proteção digital não está nas ferramentas utilizadas, mas no comportamento dos indivíduos que as operam. Com base nas análises realizadas, essa hipótese foi confirmada, evidenciando que a vulnerabilidade humana permanece sendo o maior desafio das organizações no campo da segurança da informação.

Durante o desenvolvimento do trabalho, observou-se que o fator humano está diretamente ligado à maioria dos incidentes cibernéticos relatados mundialmente. Dados do *Verizon* DBIR, (2024) e da IBM Security, (2024) demonstram que a negligência, a falta de treinamento e a manipulação psicológica estão presentes em mais de dois terços das violações de dados. Esse resultado reforça que a cibersegurança deve ser tratada como uma questão tanto tecnológica quanto comportamental, em que a educação e a cultura organizacional exercem papel fundamental na prevenção de ataques.

Verificou-se também que a engenharia social continua sendo um dos métodos mais eficazes utilizados por cibercriminosos, justamente por explorar aspectos emocionais e cognitivos das pessoas. A utilização de técnicas de persuasão descritas por Cialdini (2006) e o avanço de ferramentas baseadas em inteligência artificial, como *deepfakes* e automação de mensagens, ampliaram significativamente o alcance e a eficiência desses ataques. Assim, conclui-se que os profissionais de segurança precisam compreender os mecanismos psicológicos explorados pelos atacantes para desenvolver estratégias de defesa mais eficazes e humanas.

Os resultados ainda mostraram que políticas de segurança centradas apenas em tecnologia são insuficientes para garantir proteção plena. A criação de uma cultura de segurança organizacional, sustentada por treinamentos contínuos, comunicação clara e incentivo ao reporte de incidentes, mostrou-se a forma mais eficaz de reduzir o impacto das vulnerabilidades humanas. Conforme Schneier, (2018), a segurança é um sistema sociotécnico, e só pode ser efetiva quando as pessoas são parte integrante do processo de defesa, e não o elo esquecido.

Portanto, é essencial que as organizações adotem uma visão integrada, na qual pessoas, processos e tecnologias atuem de forma conjunta e harmônica. A implementação de programas de conscientização, aliados a políticas de incentivo e feedback, pode transformar os usuários antes vistos como vulnerabilidades em aliados estratégicos da cibersegurança. Essa mudança cultural demanda tempo e investimento, mas representa um passo decisivo rumo à construção de ambientes digitais mais seguros e resilientes.

Por fim, conclui-se que o fator humano, embora seja o principal vetor de risco, também pode se tornar o maior aliado na proteção cibernética. Cabe às empresas, instituições e gestores

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

compreenderem que segurança não se resume a barreiras técnicas, mas à educação, à conscientização e ao fortalecimento do comportamento ético e responsável no uso das tecnologias. O elo mais vulnerável pode, com preparo e conhecimento, tornar-se o mais resistente da cadeia da cibersegurança.

REFERÊNCIAS

CIALDINI, Robert B. **Influence:** The Psychology of Persuasion. New York: Harper Business, 2006.

ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. **ENISA Threat Landscape 2023**. Athens: ENISA, 2023.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 7. ed. São Paulo: Atlas, 2019.

IBM SECURITY. **Cost of a Data Breach Report 2024**. Armonk, NY: IBM Corporation, 2024.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MITNICK, Kevin D.; SIMON, William L. **The Art of Deception:** Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2011.

NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication 800-50:** Building an Information Technology Security Awareness and Training Program. Gaithersburg, MD: NIST, 2022.

PARSONS, Kathryn; MCCORMAC, Agata; BUTAVICIUS, Marcus; PATTINSON, Malcolm. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. **Computers & Security**, v. 66, p. 40–51, 2017.

ROSS, John; BENIGNI, Michael. **Human Factors in Cybersecurity:** Aligning Security and Behavior. Oxford: Routledge, 2020.

SCHNEIER, Bruce. **Click Here to Kill Everybody:** Security and Survival in a Hyper-Connected World. New York: W. W. Norton & Company, 2018.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma Visão Executiva. 3. ed. Rio de Janeiro: Elsevier, 2014.

VERIZON. **Data Breach Investigations Report 2024**. New York: Verizon Enterprise Solutions, 2024.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.