FATORES HUMANOS NA SEGURANÇA DA INFORMAÇÃO: COMO O RANSOMWARE EXPLORA AS VULNERABILIDADES PESSOAIS

HUMAN FACTORS IN INFORMATION SECURITY: HOW RANSOMWARE EXPLOITS PERSONAL VULNERABILITIES

Giovana Cristina Alves da Silva
Fatec Araraquara
giovana.silva9@fatec.sp.gov.br

Lucas Gabriel Camilo
Fatec Araraquara
lucas.camilo2@fatec.sp.gov.br

RESUMO

Este artigo explora a relação entre fatores humanos e segurança da informação, com ênfase em como o *ransomware* se aproveita de vulnerabilidades pessoais. A análise investiga como falhas comportamentais, de conhecimento e de percepção humana são exploradas por cibercriminosos para a realização de ataques bem-sucedidos. São destacadas práticas de segurança inconvenientes, como a falta de conscientização sobre *phishing*, o uso de senhas fracas e a negligência em atualizações de software, que abrem portas para essas ameaças. Também são discutidos diferentes cenários em que o *ransomware* se beneficia da engenhosidade ou da descoberta dos usuários, com destaque para o papel crucial na manipulação de indivíduos para revelar informações sensíveis ou interagir com links maliciosos. Além disso, é feita uma análise do impacto das decisões cotidianas dos usuários na segurança organizacional, abordando como políticas de segurança robustas, combinadas com treinamentos contínuos e práticas mais rigorosas, podem mitigar significativamente esses riscos e prevenir a disseminação de *ransomware* em ambientes corporativos.

Palavra-chave: Segurança da Informação, Ransomware, Phishing, Senhas Fracas, Ataques Cibernéticos.

ABSTRACT

This article explores the relationship between human factors and information security, with an emphasis on how ransomware exploits personal vulnerabilities. The analysis investigates how behavioral, knowledge, and perception failures are exploited by cybercriminals to carry out successful attacks. It highlights inconvenient security practices, such as a lack of awareness about phishing, the use of weak passwords, and negligence in software updates, which open the door to these threats. Different scenarios in which ransomware benefits from users' ingenuity or discovery are also discussed, with a focus on the crucial role of manipulating individuals to reveal sensitive information or interact with malicious links. Furthermore, an analysis of the impact of users' everyday decisions on organizational security is made, addressing how robust security policies, combined with ongoing training and stricter practices, can significantly mitigate these risks and prevent the spread of ransomware in corporate environments.

Keywords: Information Security, Ransomware, Phishing, Weak Passwords, Cyber Attacks.

1. Introdução

O estudo sobre como o comportamento das pessoas afeta a segurança da informação tem se tornado cada vez mais importante no mundo digital atual, principalmente com o aumento dos ataques de *ransomware*. Esses ataques exploram pontos fracos das pessoas, como a falta de cuidado com práticas de segurança, facilidade em cair em e-mails falsos e o uso de senhas fracas.

Além das questões técnicas, as ações e decisões dos usuários desempenham um papel crucial na segurança digital. No dia a dia, clicar em links desconhecidos ou baixar anexos suspeitos pode abrir caminho para que cibercriminosos infectem sistemas e exijam resgates para a recuperação.

Outro ponto preocupante é o uso inadequado de senhas. Muitas pessoas ainda escolhem senhas fáceis ou usam a mesma senha em várias contas, facilitando o trabalho dos invasores. Além disso, a falta de atualização regular de senhas aumenta os riscos. Isso mostra que a segurança não depende apenas de boas tecnologias, mas também de ações conscientes e responsáveis dos usuários.

Por isso, educar e conscientizar as pessoas é fundamental para prevenir ataques. Treinamentos que ensinem práticas seguras e como identificar ameaças comuns podem reduzir bastante o risco de ataques de *ransomware*. Promover uma cultura de segurança é crucial para proteger contra ameaças que frequentemente resultam de pequenos descuidos no cotidiano.

1.1 Objetivo Geral

O objetivo deste projeto é compreender como o comportamento humano influencia a segurança da informação, com ênfase em ataques de *ransomware*. O foco está em analisar como vulnerabilidades pessoais, como a falta de conscientização sobre práticas seguras, o uso de

senhas fracas e o descuido com links maliciosos, podem ser exploradas por cibercriminosos. Além disso, busca-se identificar maneiras de mitigar esses riscos por meio de treinamentos e políticas de segurança eficazes, visando criar uma cultura mais robusta de proteção digital tanto em empresas quanto entre usuários individuais.

1.2 Objetivo Específico

- Analisar a relação entre a falta de conscientização em segurança digital e a ocorrência de ataques de ransomware.
- Identificar os principais comportamentos de risco adotados por usuários que facilitam a ação de cibercriminosos.
- Avaliar o impacto do uso de senhas fracas e a reutilização de credenciais em múltiplas plataformas.

2. Referencial Teórico

O fator humano refere-se à interação entre indivíduos e sistemas, destacando como características psicológicas e comportamentais influenciam a eficácia organizacional. Na segurança da informação, muitos riscos decorrem de decisões dos usuários, como falhas na percepção de ameaças e na adesão a políticas de segurança. Apesar do uso de tecnologias avançadas, os erros humanos, como clicar em links maliciosos e usar senhas fracas, são causas frequentes de incidentes de segurança. Assim, é fundamental considerar os fatores humanos nas estratégias de segurança, promovendo uma cultura de conscientização e responsabilidade entre os colaboradores.

De acordo com as informações fornecidas pelo Malwarebytes Labs (2020), os ataques de *ransomware* costumam ser distribuídos por meio de diversas técnicas, incluindo e-mails de *phishing*, links maliciosos, anexos de e-mail, e downloads de softwares maliciosos.

Conforme um estudo baseado nos dados da plataforma Egress Prevent (2021), o erro humano é identificado como o principal fator que aciona seus alertas de prevenção de perda de dados (DLP) em tempo real.

2.1.1 O conceito de Ransomware

Segundo Malwarebytes (2024) O *ransomware* começou a ser desenvolvido no final dos anos 1980, quando o pagamento precisava ser enviado via correio convencional. Atualmente, os cibercriminosos exigem que o resgate seja feito através de criptomoedas ou cartões de crédito, e os alvos variam entre indivíduos, empresas e organizações de diversos tipos. Além disso, alguns criadores de *ransomware* comercializam essa tecnologia para outros cibercriminosos, um modelo conhecido como *Ransomware-as-a-Service* (RaaS).

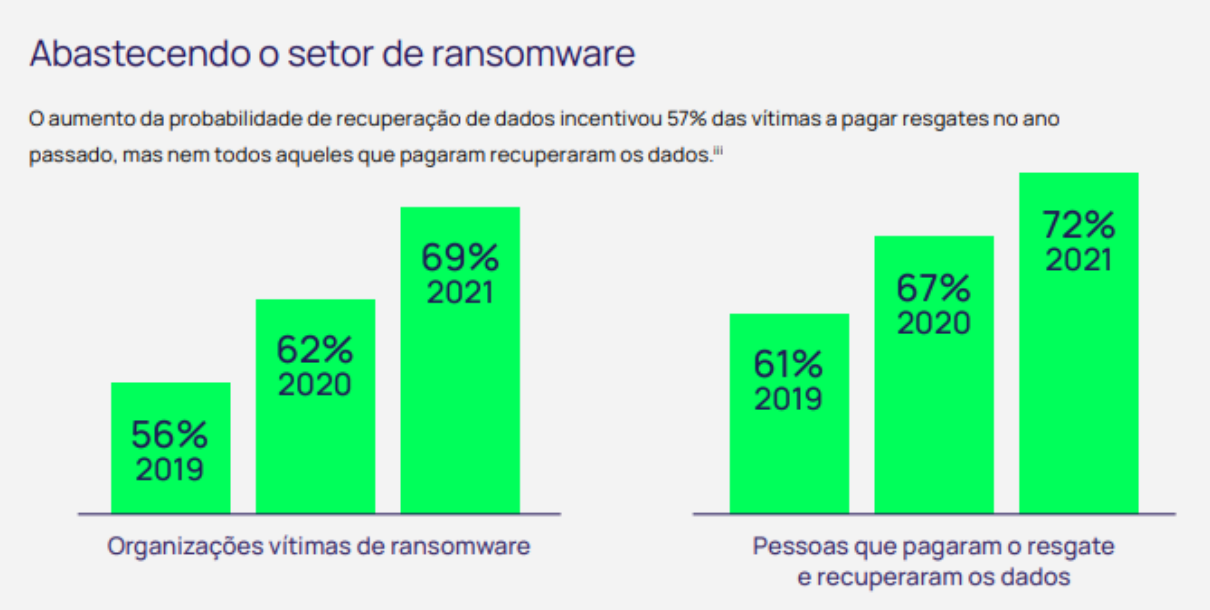
- **E-mails de Phishing**: Ataques de *ransomware* frequentemente começam com e-mails falsos que enganam os usuários para clicar em links maliciosos ou baixar anexos infectados. Esses e-mails são projetados para parecerem legítimos, imitando comunicações de empresas ou contatos conhecidos.

- **Downloads de Software de Fontes Não Confiáveis**: A instalação de software de sites não confiáveis ou de redes *peer-to-peer* também pode resultar na infecção por *ransomware*. Esses softwares geralmente vêm disfarçados de programas úteis ou populares.
- **Exploração de Vulnerabilidades de Software**: *Ransomware* também pode se espalhar através da exploração de vulnerabilidades em softwares desatualizados. Se o sistema não estiver devidamente atualizado com os patches de segurança mais recentes, os cibercriminosos podem usar essas falhas para instalar o *malware* sem o conhecimento do usuário.

Uma vez que o *ransomware* infecta um sistema, ele criptografa os arquivos da vítima, utilizando métodos de criptografia fortes que tornam praticamente impossível a recuperação dos dados sem a chave de descriptografia. Após a criptografia, uma mensagem de resgate é exibida, exigindo pagamento, geralmente em criptomoedas, para liberar os arquivos.

Conforme mostra a tabela a seguir, cada vez mais o setor de *ransomware* tem obtido resultados. (DELINEA, 2024)

Figura 1 - Abastecendo o setor de ransomware



Fonte: DELINEA (2024) - Ransomware em ascensão

2.1.2 Tipos de Ransomware

Existem dois tipos gerais de *ransomware*. O tipo mais comum, chamado de *ransomware* criptografado ou *ransomware* cripto, mantém os dados da vítima como reféns criptografando-os. Em seguida, o invasor exige um resgate em troca do fornecimento da chave de criptografia necessária para decriptografar os dados. (IBM, 2024).

A forma menos comum de *ransomware*, chamada de *ransomware* não criptografado ou *ransomware* de bloqueio de tela, bloqueia todo o dispositivo da vítima, geralmente bloqueando o acesso ao sistema operacional. Em vez de ser inicializado como de costume, o dispositivo exibe uma tela que faz a exigência de resgate.

Esses dois tipos podem ser divididos nessas subcategorias:

- ***Leakware/doxware*:** é um *ransomware* que roub dados confidenciais e ameaça publicá-los. Enquanto formas anteriores de *leakware* ou *doxware* muitas vezes roubavam dados sem criptografá-los, as variantes atuai geralmente fazem as duas coisas.
- O ***ransomware* móvel** inclui todos os *ransomwares* que afetam dispositivos móveis. Entregue por meio de aplicativos maliciosos ou download direto, o *ransomware* móvel geralmente é um *ransomware* não criptografado, porque os backups automatizados de dados na nuvem, padrão em muitos dispositivos móveis, facilitam a reversão de ataques de criptografia.
- ***Wipers/ransomware* destrutivo:** ameaça destruir os dados se o resgate não for pago, exceto nos casos em que o *ransomware* destrói os dados mesmo que o resgate seja pago. Suspeita-se que esse último tipo de *wiper* seja implantado por agentes ou hacktivistas de estados-nação, em vez de cibercriminosos comuns.
- O ***Scareware*** é exatamente o que parece: *ransomware* que tenta assustar os usuários para que paguem um resgate. *Scareware* pode se passar por uma mensagem de uma agência fiscalizadora, acusando a vítima de um crime e exigindo uma multa. Alternativamente, ele pode falsificar um alerta de infecção por vírus legítimo, incentivando a vítima a comprar software antivírus ou *antimalware*. Às vezes, o *scareware* é um *ransomware*, criptografando os dados ou bloqueando o dispositivo; em outros casos, é o vetor do *ransomware*, que não criptografa nada, mas coage a vítima a baixar o *ransomware*.

2.2 Vulnerabilidades Humanas Exploradas pelo Ransomware

O sucesso do *ransomware* em grande parte depende da exploração de vulnerabilidades humanas, incluindo a falta de conscientização, confiança excessiva e comportamento negligente.

Segundo Garratech (2023), embora o investimento em ferramentas e sistemas seja essencial para a segurança dos dados, o fator mais importante na prevenção de ataques não reside na tecnologia, mas nas pessoas. O aspecto humano, com suas emoções e complexidades, é o componente mais vital na defesa contra ameaças cibernéticas e incidentes.

Essas vulnerabilidades são exploradas de várias maneiras:

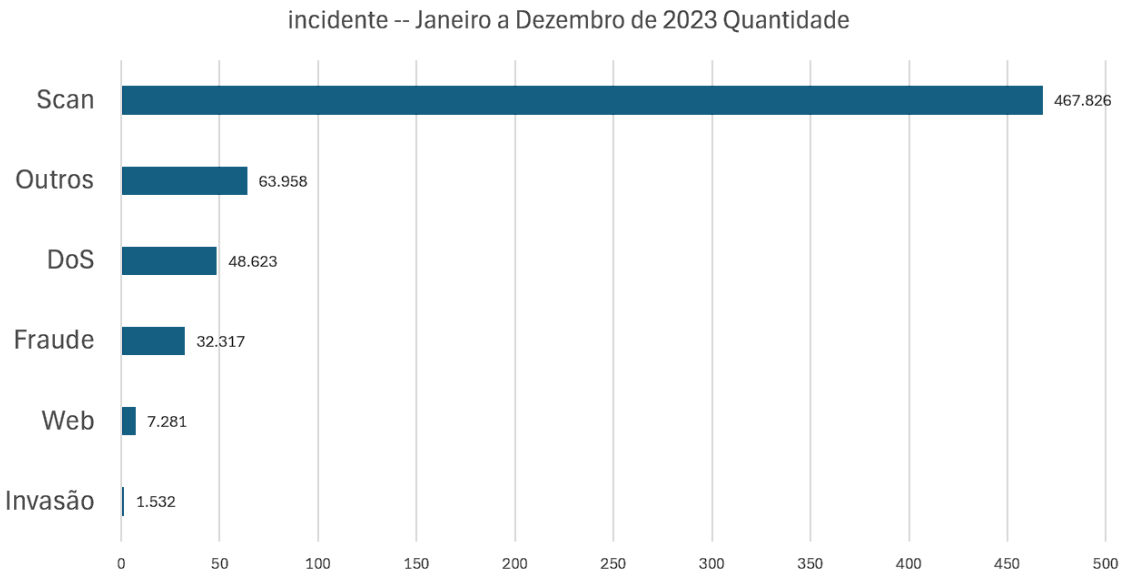
- **Falta de Conscientização e Treinamento**: Muitos usuários e funcionários não estão adequadamente treinados para identificar ameaças cibernéticas. A ausência de uma cultura organizacional focada em cibersegurança facilita a disseminação do

ransomware. Por exemplo, usuários que não reconhecem e-mails de *phishing* são alvos fáceis para ataques.

- **Confiança Excessiva**: A confiança natural dos usuários em comunicações que parecem legítimas pode ser explorada pelos cibercriminosos. E-mails que aparentam ser de fontes confiáveis podem induzir os usuários a clicar em links ou baixar anexos maliciosos sem questionar sua autenticidade.
- **Comportamento Negligente**: O descuido no uso de senhas fracas, a reutilização de credenciais em vários sites, e a falta de atualização de softwares são comportamentos que aumentam o risco de uma infecção por *ransomware*. A negligência em seguir as melhores práticas de segurança cibernética cria brechas que os atacantes podem explorar.

No Brasil, de acordo com dados publicados pelo CERT.br (2023), dos 467.826 incidentes notificados no período 2023, as fraudes correspondem a 32.317 ocorrências, ou seja, é um número expressivo, cabe aqui acrescentar o fato de que o "*phishing*" corresponde a 98% dessas fraudes. Conforme apresenta a Figura 2.

Figura 2 –Incidentes Notificados ao CERT.br –2023



Fonte: CERT.br (2023)

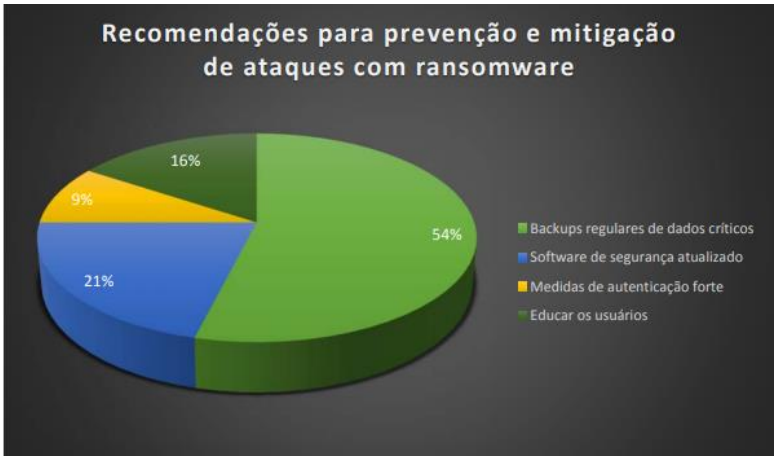
2.3 Implicações para a Segurança da Informação

A crescente sofisticação do *ransomware* e sua capacidade de explorar vulnerabilidades humanas representam um grande desafio para a segurança da informação. Organizações e indivíduos devem adotar uma abordagem proativa para mitigar o risco de ataques. Isso inclui:

- **Educação e Treinamento Contínuos**: Implementar programas de conscientização sobre cibersegurança para todos os funcionários, com ênfase em identificar e evitar ameaças de *phishing* e outras formas de ataque social.
- **Políticas de Segurança Rigorosas**: Estabelecer e manter políticas de segurança robustas, como o uso obrigatório de autenticação de múltiplos fatores, senhas fortes, e a aplicação regular de patches de segurança.
- **Backup Regular de Dados**: Manter backups atualizados e testados de todos os dados críticos é essencial para mitigar os danos de um ataque de *ransomware*. Esses backups devem ser armazenados em locais seguros e isolados da rede principal.
- **Atualizações e Patches:** Mantenha todos os seus sistemas e softwares atualizados. Muitos ataques de *ransomware* exploram vulnerabilidades conhecidas que poderiam ser corrigidas por patches de segurança.

A figura a seguir mostra quais são as recomendações para prevenção e mitigação de ataques com *ransomware*. (IBM, 2024)

Figura 3 – Prevenção e Mitigação



Fonte: IBM (2024) - Ataque Cibernético: O que é e como prevenir

O referencial teórico destaca a natureza perniciosa do *ransomware*, evidenciando-o como uma ameaça cibernética capaz de paralisar sistemas inteiros ao bloquear o acesso a dados críticos, frequentemente usada para extorquir vítimas por meio de pedidos de resgate. A vulnerabilidade humana é apresentada como um dos principais incidentes de perda de dados, revelando que comportamentos inadvertidos ou negligentes muitas vezes servem como porta de entrada para ataques cibernéticos.

2.4 Ransomware como um serviço

Segundo o site Delinea (2024) um dos fatores que contribui para o aumento dos casos de RaaS é o estabelecimento de redes de afiliados ou programas de parceria pelos criadores de *ransomware*. Nesse modelo emergente, os desenvolvedores oferecem o *ransomware* gratuitamente aos cibercriminosos, que o utilizam para realizar ataques, coletar resgates das vítimas e repassar uma parte desse valor aos criadores. Esse esquema reduz o risco para os desenvolvedores e amplia suas chances de sucesso.

Ransomware como um serviço, conhecido como *Ransomware-as-a-Service* (RaaS), é um modelo de negócio ilícito no qual desenvolvedores de *ransomware* criam e fornecem ferramentas prontas para outros cibercriminosos, que podem então lançar ataques sem precisar de conhecimento técnico avançado. Nesse esquema, os criadores do *ransomware* oferecem o software malicioso em plataformas da *dark web*, muitas vezes com suporte técnico e atualizações, em troca de uma parcela do pagamento do resgate ou de uma taxa fixa.

Esse modelo facilita a proliferação de ataques de *ransomware*, pois permite que praticamente qualquer pessoa, mesmo sem habilidades de programação, realize extorsões digitais. Ao utilizar *RaaS*, os criminosos alugam ou compram o software, personalizam o ataque e implementam o *ransomware* em sistemas de vítimas, que podem ser indivíduos, empresas ou organizações. A facilidade de acesso ao *RaaS* tem contribuído para o aumento significativo de ataques cibernéticos nos últimos anos.

A ascensão do *ransomware* como Serviço é uma realidade preocupante no cenário de segurança cibernética atual. No entanto, com a conscientização adequada e as medidas de segurança corretas, é possível se proteger contra essas ameaças e manter seus ativos digitais seguros. (Clearsale, 2024)

3. Metodologia

A metodologia deste artigo baseia-se em uma revisão de materiais acadêmicos e técnicos sobre *ransomware* e sua relação com os fatores humanos na segurança da informação. O objetivo é compreender as principais teorias, práticas e exemplos que mostram como as vulnerabilidades humanas são exploradas, além de identificar estratégias eficazes para ajudar a reduzir esses riscos.

O processo de pesquisa iniciou-se com a seleção de fontes, como como Google Scholar, Scopus e IEEE Xplore, além de livros, artigos de conferências e relatórios de organizações especializadas em cibersegurança. Foram priorizados os materiais mais recentes, abrangendo os últimos cinco anos, para garantir que as informações fossem atuais. As fontes foram selecionadas com base em sua relevância para o tema do *ransomware*, com ênfase nos fatores humanos na segurança da informação, prevenção de ataques e a credibilidade das publicações, como aquelas revisadas por especialistas.

Após a seleção das fontes, foi realizada uma análise crítica dos textos, buscando identificar conceitos importantes, estratégias de prevenção e exemplos reais sobre *ransomware* e vulnerabilidades humanas. Essa análise ajudou a reconhecer padrões, identificar pontos que precisam de mais estudo e sugerir formas de reduzir os riscos. As informações foram, então, organizadas de forma clara, para mostrar o impacto dos fatores humanos na segurança da informação, com recomendações práticas para aumentar a conscientização e educação em cibersegurança.

4. Situação-Problema

A organização em análise é a Chip Racing Brasil**,** uma empresa de tecnologia que fornece soluções de software para o setor automotivo. O problema identificado é a crescente vulnerabilidade a ataques de *ransomware*, que tem gerado preocupações sobre a integridade dos dados e a continuidade dos negócios. A falta de conscientização e de práticas de segurança adequadas entre os colaboradores tem sido um dos principais fatores que contribuem para essa situação. Com a crescente sofisticação dos cibercriminosos, a empresa corre o risco de sofrer ataques que poderiam resultar em perda de dados, danos financeiros e prejuízo à reputação.

5. Mecanismos Adotados

- **Consultoria:** Realizamos um programa de consultoria com o objetivo de identificar soluções para os problemas de gerenciamento de projetos, especialmente no que se refere à segurança da informação. A consultoria envolveu reuniões com a equipe de TI e com gestores de projeto para discutir as práticas atuais e as lacunas na segurança.

- **Assessoria:** O trabalho de assessoria consistiu em acompanhar e avaliar o processo de segurança da informação já existente na organização. Realizamos entrevistas com os colaboradores e uma análise das práticas de segurança em vigor. Identificamos que muitos colaboradores não estavam cientes dos riscos associados ao *phishing* e utilizavam senhas fracas.

- **Força Tarefa:** Formamos uma força-tarefa composta por membros das equipes de TI e Recursos Humanos, com o objetivo de abordar o problema do *ransomware*. A equipe investigou casos recentes de ataques na indústria e as vulnerabilidades comuns. Durante esse processo, foram identificados pontos críticos, como a falta de atualizações de software e a resistência dos colaboradores em adotar práticas de segurança.

5.1 Parecer Técnico

O parecer técnico resultou na seguinte análise da situação:

- **Diagnóstico das Vulnerabilidades**: A pesquisa revelou que 60% dos colaboradores admitiram não mudar suas senhas regularmente e 70% não participaram de treinamentos sobre segurança digital. Além disso, 80% dos colaboradores não reconheciam e-mails de phishing.
- **Recomendações**: É fundamental implementar um programa de conscientização sobre segurança, que inclua treinamentos regulares e testes simulados de *phishing*. Também é recomendado revisar e atualizar as políticas de segurança da informação da organização.

5.2 Plano de Ação para Intervenção

Objetivo Geral: Mitigar os riscos de ataques de *ransomware* e fortalecer a segurança da informação na Chip Racing Brasil.

Ações Específicas:

A) **Programa de Conscientização e Treinamento:**

- Desenvolver um programa de treinamento em segurança da informação, abordando temas como *phishing*, uso seguro de senhas e importância das atualizações de software.
- Realizar sessões de treinamento trimestrais, incluindo atividades práticas e simulações de ataques.

B) **Revisão das Políticas de Segurança:**

- Atualizar as políticas de segurança da informação, incluindo a exigência de senhas fortes e a obrigatoriedade de trocas regulares.
- Criar um manual de boas práticas em segurança da informação a ser distribuído a todos os colaboradores.

C) **Implementação de Ferramentas de Segurança:**

- Investir em software de segurança cibernética que inclua proteção contra *ransomware* e *phishing*.
- Implementar autenticação de dois fatores (2FA) para acessar sistemas sensíveis.

D) **Monitoramento e Avaliação:**

- Estabelecer um comitê de segurança da informação que se reunirá mensalmente para avaliar a eficácia das medidas implementadas e fazer ajustes conforme necessário.
- Realizar auditorias semestrais para garantir que as políticas de segurança estão sendo seguidas e que as vulnerabilidades estão sendo tratadas.

E) **Feedback Contínuo:**

- Criar um canal de comunicação onde os colaboradores possam relatar incidentes de segurança ou sugerir melhorias nas práticas de segurança.

6. Cronograma de Implementação:

- **1º Mês:** Revisão das políticas de segurança e desenvolvimento do programa de treinamento.
- **2º Mês:** Início do programa de treinamento e implementação de ferramentas de segurança.
- **3º Mês:** Estabelecimento do comitê de segurança da informação e início das auditorias.

7. Análise dos Resultado e Discussões

A pesquisa confirma que o comportamento humano é essencial na segurança da informação, especialmente na prevenção de ataques de *ransomware*. Os dados mostram que a falta de conscientização e de treinamento aumenta significativamente a probabilidade de que as pessoas sejam vítimas desses ataques. A maioria dos casos de *ransomware* analisados envolveu algum tipo de erro humano, como abrir e-mails falsos ou usar senhas fracas.

Os resultados também mostram como é importante investir em programas de educação em cibersegurança. Em empresas onde os funcionários recebem treinamentos frequentes, houve uma queda no número de ataques bem-sucedidos. Isso indica que a educação pode ser uma das maneiras mais eficazes de reduzir os riscos de ataques de *ransomware*.

A pesquisa reforça a ideia de que o comportamento humano é uma das maiores fragilidades na segurança digital. Embora a tecnologia seja importante, ela sozinha não é suficiente para evitar ataques de *ransomware*. A combinação de medidas tecnológicas com conscientização e mudanças de comportamento se mostrou fundamental.

Além disso, a pesquisa aponta que o impacto dos treinamentos é maior em lugares onde a segurança já é levada a sério. Em empresas que não têm a segurança como prioridade, o efeito dos treinamentos tende a ser menor. Isso sugere que, além de educar as pessoas, é importante criar uma cultura que valorize a segurança da informação.

Por fim, os resultados indicam que, apesar das vulnerabilidades humanas, quando as pessoas são bem treinadas e preparadas, elas podem se tornar uma forte defesa contra-ataques. A pesquisa, portanto, apoia a ideia de que é preciso equilibrar o uso de tecnologia com a educação e conscientização das pessoas para combater o *ransomware*.

8. Conclusão

O *ransomware* continua sendo uma ameaça em crescimento, mostrando que é preciso lidar não só com os problemas técnicos, mas também com as fraquezas humanas.

A combinação de educação, treinamento, políticas de segurança claras e boas práticas de backup podem diminuir bastante o impacto desses ataques. Tanto empresas quanto indivíduos precisam estar atentos e prontos para enfrentar essa ameaça em constante evolução, protegendo assim suas informações.

Este artigo teve como objetivo entender como o comportamento humano afeta a segurança da informação, focando em como o *ransomware* aproveita as falhas pessoais para atacar sistemas e roubar dados. A pesquisa analisou que atitudes como a falta de cuidado, o uso de senhas fracas e a negligência em práticas de segurança facilitam esses ataques.

Por outro lado, o estudo apresenta algumas limitações. Ele focou em comportamentos conhecidos e comuns, o que pode não cobrir toda a complexidade dos fatores humanos que influenciam a segurança. Além disso, o foco foi nas empresas, deixando de lado o impacto dessas vulnerabilidades em outros contextos, como na esfera doméstica.

Para pesquisas futuras, seria interessante fazer uma análise mais detalhada de diferentes tipos de organizações e como elas lidam com a cibersegurança, além de acompanhar por mais tempo as mudanças de comportamento e seus efeitos. Também seria útil investigar outras fraquezas humanas menos conhecidas que podem ser exploradas por novas formas de *ransomware* ou outras ameaças.

Em resumo, este trabalho contribuiu para uma melhor compreensão dos fatores humanos na segurança da informação, mostrando que é necessário combinar tecnologia com educação para reduzir os riscos. Tanto empresas quanto indivíduos precisam entender que a segurança da informação é uma responsabilidade compartilhada, que exige tanto medidas técnicas quanto comportamentais para ser realmente eficaz.

Referências

CLEARSALE. **A Ascensão do Ransomware como Serviço**: Uma Nova Ameaça Cibernética, 2023. Disponível em: https://blogbr.clear.sale/ascens%C3%A3o-do-ransomware-amea%C3%A7a-cibern%C3%A9tica . Acesso em: 09 set. 2024.

CROWDSTRIKE. **Relatório de Ameaça Global**, 2024. Disponível em: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf . Acesso em: 22 ago. 2024.

DELINEA. **Ransomware em Ascensão:** Como reduzir riscos e reagir a ataques, 2024. Disponível em: https://cdn.directions.pt/uploads/2022/09/Delinea_PDF_whitepaper-ransomware-on-the-rise-pt.pdf . Acesso em: 09 set. 2024.

EGRESS SOFTWARE TECHNOLOGIES**. Egress CISO Guide:** Preventing Human Error on Email, 2023. Disponível em: https://www.egress.com/media/lq0bj5bj/egress_ciso_guide_preventing_human_error.pdf . Acesso em: 09 set. 2024.

ESTATISTICAS DO CERT.BR**. Incidentes Notificados ao CERT.br**, 2024. Disponível em: https://stats.cert.br/incidentes/ . Acesso em: 20 ago. 2024.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação:** O Fator Humano, 2009. Disponível em: https://www.cursosavante.com.br/cursos/curso533/conteudo7486.pdf . Acesso em: 21 ago. 2024.

FORNASIER, Mateus de Oliveira. SPINATO, Tiago Protti. RIBEIRO, Fernanda Lencina. Ransomware e Cibersegurança: A informação ameaçada por ataques a dados. **Revista Thesis Juris**, 2020. Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739/8272 . Acesso em: 21 ago. 2024.

FREIRE, Rodolfo Francisco Paz. SILVA, Humberto Caetano Cardoso da. QUEIROZ, Ricardo Gomes de. BATISTA, Amélia Acácia de Miranda. O fator humano como uma vulnerabilidade em segurança da informação. **Revista Brasileira de Administração Cientifica, 2017.** Disponível em: https://www.sustenere.inf.br/index.php/rbadm/article/view/SPC2179-684X.2017.003.0012/1259 . Acesso em: 21 ago. 2024.

GARRATECH SOLUÇÕES EM TI. **A importância do fator humano na segurança da informação**. Disponível em: https://garratech.com.br/importancia-fator-humano-seguranca-da-informacao/#:~:text=Em%20outras%20palavras%2C%20as%20pessoas,normalmente%20ou%20entrar%20em%20colapso . Acesso em: 09 set. 2024.

IBM. **O que é ransomware?.** Disponível em: https://www.ibm.com/br-pt/topics/ransomware . Acesso em: 09 set. 2024.

KANAGUSKU, Ana Rita Akayama. GASETA, Edison. Fator Humano na Segurança da Informação: Desmistificando o Elo Mais Fraco, 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/114/33 . Acesso em: 20 ago. 2024.

MALWAREBYTES LABS. **Ransomware trends in 2020**, 2020. Disponível em: https://resources.malwarebytes.com/files/2020/12/2020-State-of-Ransomware-Report.pdf . Acesso em: 22 ago. 2024.

MEORIN, Caio. **Ransomware**: Extorsão Digital, 2017. Disponível em: https://repositorio.feituverava.com.br/srv-c0002-s01/api/core/bitstreams/54a83d18-9bf2-4a7a-9e5c-b61fc176e654/content . Acesso em: 20 ago. 2024.

SILVA, Denise Ranghetti Pilar da. STEIN, Lilian Milnitsky. Segurança da Informação: Uma Reflexão Sobre o Componente Humano. Disponível em: http://revista.cienciasecognicao.org/index.php/cec/article/view/628/410 . Acesso em: 21 ago. 2024.

SILVA, Victor. OLIVEIRA, Rogerio. Ataque Cibernético de Ransomware: O que é e Como se Prevenir. **Revista Ciências e Cognição**, 2007 Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/16242/1/analise_e_desenvolvimento_de_sistemas_2023_1_victor_luiz_lopes_da_silva_ataque_cibernetico_ransomware_o_que_e_e_como_prevenir.pdf . Acesso em: 20 ago. 2024.