A IMPORTÂNCIA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA PREVENÇÃO A ATAQUES RANSOMWARE

Francisco Wideny Pereira Brito

RESUMO

Este trabalho tem como objetivo explorar a importância das políticas de segurança da informação na prevenção ao *ransomware*. Inicialmente, será dada uma visão geral do que é o *ransomware* e o seu funcionamento. Logo em seguida, serão abordados os conceitos e a relevância das políticas de segurança da informação, destacando os desafios envolvidos na sua implementação e as diretrizes fundamentais que devem fazer parte de uma PSI. A falta de uma cultura em segurança da informação pode contribuir muito para que os funcionários acabem sendo alvos fáceis, colocando em risco toda a organização. Por isso, além de se preocupar com as questões técnicas, uma política de segurança da informação também deve ser desenvolvida levando em consideração o fator humano. Espera-se que o presente trabalho possa contribuir para uma melhor compreensão dos danos que os ataques *ransomware* podem causar nos negócios das organizações de qualquer porte, bem como demonstrar os benefícios que uma PSI pode ter na prevenção a esses ataques.

Palavras-chave: Política de segurança da informação, Ransomware, Engenharia social.

1. INTRODUÇÃO

Nos últimos tempos, a área de segurança cibernética tem enfrentado um aumento considerável de ataques, principalmente os relacionados ao *ransomware*. O *ransomware*, um tipo de software malicioso que bloqueia o acesso a sistemas ou arquivos e exige resgate em criptomoedas para restaurar o acesso, tem afetado organizações em diversas partes do mundo. A prática do trabalho remoto e a disposição das organizações em pagar resgates quando seus dados são sequestrados contribuem significativamente para que esse cenário cresça de modo exponencial.

As ameaças cibernéticas crescem à medida que a sociedade fica cada vez mais dependente da tecnologia para realizar as suas tarefas no dia a dia. Nesse contexto, grupos e pessoas mal-intencionadas buscam formas de conseguir se aproveitar financeiramente de suas vítimas, podendo causar além de danos

financeiros, como também, em alguns casos, risco a vida das pessoas.

De acordo com uma matéria publicada no site Chainalysis (2024, tradução nossa):

> Os pagamentos de ransomware em 2023 ultrapassaram a marca de um bilhão de dólares, o número mais elevado já observado. Embora 2022 tenha registrado um declínio no volume de pagamentos de ransomware, a tendência geral de 2019 a 2023 indica que o ransomware vem sendo um problema crescente.

Além dos impactos financeiros diretos, ataques desse tipo podem causar um grande impacto na continuidade de muitos serviços essenciais. Em junho de 2024, um ataque *ransomware* acabou comprometendo os serviços de alguns hospitais do Reino Unido, resultando na transferência de pacientes para outras unidades, como também obrigando-os a adiarem resultados de exames (BRITO, 2024).

Diante desse contexto desafiador, torna-se essencial adotar uma Política de Segurança da Informação (PSI). Essa política estabelece regras e procedimentos que todos os colaboradores da empresa devem seguir à risca. Por meio de uma PSI bem estruturada e documentada, é possível identificar ameaças potenciais, implementar estratégias eficazes e estabelecer diretrizes para reduzir as vulnerabilidades na segurança. Além disso, a PSI fornece subsídios para atividades preventivas e educacionais, instruindo e orientando os colaboradores sobre as melhores práticas para mitigar as vulnerabilidades.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Visão geral sobre o ransomware

O *ransomware* tem sido uma ameaça constante às redes de computadores. Segundo Romar e Silva (2022, p. 2), “O primeiro ransomware da história surgiu em 1989. Era chamado de Trojan da AIDS.”. A origem desse nome se deu pelo seu criador, Joseph Popp, ter bastante interesse em estudar a AIDS. O cientista acabou, em 1989, por meio de um disquete, enviando o malware para algumas pessoas. Foi preciso que o sistema passasse por uma grande quantidade de reinicializações para que o *Ransomware* enfim pudesse ser ativado, criptografando as informações das vítimas. No entanto, o software malicioso aplicava um método de encriptação onde a chave que permitiria desbloquear os arquivos já se encontrava inserida no próprio código. Assim, a tarefa de descriptografar as informações não seria uma tarefa difícil (GRUSTNIY, 2021).

Essa ameaça é um malware de computador que se instala de uma forma silenciosa na máquina do usuário. O principal objetivo desse software malicioso é impossibilitar acesso a arquivos importantes, por meio da criptografia dos arquivos, por exemplo. Logo após realizar a criptografia dos arquivos, é solicitado ao usuário que pague um resgate para seu criador remover a restrição e poder acessar os dados novamente. (HASSAN, 2019).

Fonte: Infobusiness, 2019.

2.1.1. Evolução das táticas de ataque ransomware e impactos causados nos últimos anos

Ao longo dos anos, tem ocorrido uma evolução significativa nas táticas de ataque de *ransomware*, as quais estão se tornando mais sofisticadas e prejudiciais. Os números de ataques estabilizaram, mas principalmente empresas e serviços públicos vem sendo cada vez mais afetados. Isso se deve ao fato de que os ataques estão se tornando cada vez mais direcionados.

Conforme Prescott (2024) aborda em uma notícia, depois do aumento de ataques do tipo *ransomware* durante a pandemia da Covid-19, os números estabilizaram e houve queda, mas ocorreu uma mudança na forma de agir dos cibercriminosos. A autora complementa ainda que:

> Na comparação com outros países, o Brasil tem a menor taxa de ataque de ransomware: 59% das organizações globais disseram ter sido atacadas contra 44% no País. Em 2023, o porcentual era de 66% global e 68% no Brasil. Houve, portanto, uma queda nos ataques e ela está relacionada ao fato de que os criminosos estão direcionando os ataques (PRESCOTT, 2024).

Essa mudança de foco para alvos mais lucrativos tem trazido impactos significativos. Empresas de grande porte e instituições financeiras são frequentemente visadas, resultando em prejuízos milionários e interrupções prolongadas em seus serviços. Além disso, hospitais e outras infraestruturas críticas também se tornaram alvos preferenciais.

O uso de táticas como a dupla extorsão, onde os criminosos não apenas criptografam os dados, mas também ameaçam vazar informações sensíveis, aumentou a pressão sobre as vítimas para pagar o resgate.

De acordo com a empresa CloudFlare (2022), a prática de roubar dados com a intenção de vazá-los era incomum antes de 2019. No entanto, até o terceiro trimestre de 2021, a ameaça de vazamento estava presente em 83,3% dos ataques. Além disso, esses ataques se tornaram mais elaborados, com criminosos utilizando engenharia social para enganar funcionários e comprometer sistemas de maneira mais eficiente. Por fim, a crescente sofisticação dos ataques e a mudança de tática para alvos mais lucrativos e críticos ressaltam a necessidade de uma abordagem mais completa relacionada à proteção de dados. As empresas devem investir em tecnologias de detecção e resposta avançadas, além de treinar seus funcionários para reconhecer e responder a ameaças de *ransomware*.

2.2. Política de segurança da informação

No contexto atual, as organizações estão cada vez mais focadas em proteger o seu ativo mais valioso: a informação. Nesse sentido, uma medida essencial é a implementação de uma política de segurança da informação. Conforme apresenta Hintzbergen *et al* (2018) "A política de segurança inclui documentos de política, procedimentos e orientações que visam determinado aspecto de segurança da informação e fornecem expectativas detalhadas".

Os autores ainda acrescentam que essa política deve estar alinhada com as exigências organizacionais, assim como com as diretrizes vigente. É fundamental que esse documento tenha a autorização do conselho de administração, assim como disponibilizá-la a todos os envolvidos (HINTZBERGEN *et al*, 2018).

2.3. Componentes de uma política de segurança da informação eficaz

Sabendo dos riscos que um *ransomware* pode causar, é essencial que uma política de segurança da informação contenha diretrizes adequadas que possam visar prevenir ataques *ransomware* da melhor forma possível. Um dos itens importantes que devem constar numa PSI é a utilização de backup. A realização de backup feita com frequência e armazenando os dados em locais seguros, longe de acesso não autorizado pode prevenir a perda de informações por eventuais acidentes (SAFETYWARE, 2017).

Há algumas normas que podem auxiliar a implementar uma PSI a ter um controle de backup eficaz. Além de realizar backup com frequência e armazenar as cópias em locais seguros, de acordo com a norma NBR ISO/IEC 27002 (2013):

> Convém que cópias de segurança de sistemas e serviços específicos sejam testadas regularmente para garantir que elas estão aderentes aos requisitos definidos nos planos de continuidade do negócio. Para serviços e sistemas críticos, convém que sejam criados mecanismos de geração de cópias de segurança que abranjam todos os sistemas de informação, aplicações e dados necessários

> para a completa recuperação do sistema em um evento de desastre. (ABNT, 2013, p 54).

A elaboração de uma PSI também precisa levar em conta o fator humano, que é considerado o elo mais fraco. Grimes (2021) comenta que a engenharia social é a principal causa de ataques *ransomware*. A respeito disso, ainda com Grimes (2021), uma boa maneira de prevenir esses ataques é pela capacitação das vítimas para reconhecer, por exemplo, e-mails maliciosos. Desde modo, é de vital importância que a conscientização da segurança da informação seja levada a sério, pois somente com o envolvimento e ajuda de todos os colaboradores é que a prevenção a ataques malware poderá ser eficaz. Sobre isso, Liska e Gallo (2017) comentam que:

> No final, a conscientização e o treinamento em segurança devem ser mais do que apenas assinar digitalmente uma política e assistir a uma apresentação de slides todos os anos. Treinamentos curtos e envolventes e apresentações em vídeo sobre tópicos como reconhecer um e-mail de phishing podem fornecer treinamento contínuo para seus usuários finais de uma forma que não impeça sua capacidade de trabalhar, mas forneça um lembrete constante de que os adversários estão lá fora, e eles precisam manter um estado de vigilância ao lidar com qualquer coisa que recebam, seja por e- mail, SMS ou chamada de voz. (LISKA; GALLO, p 84, tradução nossa).

Em um ataque *ransomware*, um plano de continuidade também deve fazer parte de uma PSI em uma situação crítica, que segundo Stallings e Brown (2014) ajudará a preservar os serviços que venham a passar por uma interrupção brusca.

2.4. Desafios na prevenção ao ransomware

Devido a rápida e constante evolução das técnicas de ataque de *ransomware* que os cibercriminosos vem desenvolvendo ao longo do tempo, prevenir adequadamente esses ataques torna-se uma tarefa complexa, que envolve não somente questões técnicas, mas também pessoais. Como dito anteriormente, é importante que um plano de backup esteja incluído na política de segurança da informação de qualquer organização, no entanto, quando uma organização decide implementar um plano de backup, ela precisa levar em conta algumas questões importantes que, se não for planejado da maneira correta, pode desperdiçar recursos financeiros que poderiam ser evitados.

Implementar um plano de backup tem seus custos, porém é necessário para prevenir a perda de acesso aos dados caso um possível ataque *ransomware* venha a acontecer. Em um artigo publicado em um site pela Century telecom (2024) sobre o backup em nuvem: “O investimento inicial para implementar Cloud Backup pode parecer alto, e os benefícios nem sempre são imediatamente aparentes para as partes interessadas”. Muitas empresas ainda subestimam a importância de se investir em segurança da informação, apesar dos riscos. A Century telecom (2024) ainda menciona uma possível solução para que as partes interessadas possam compreender melhor a necessidade de investimento:

> Realizar uma análise detalhada de custo-benefício, considerando não apenas os custos diretos, mas também os benefícios a longo prazo, como redução de downtime e custos de recuperação de desastres. Apresentar casos de estudo e exemplos reais onde o Cloud Backup reduziu custos e melhorou a eficiência operacional pode ajudar a justificar o investimento. (CENTURY TELECOM, 2024).

Em relação a conscientização em segurança da informação como medida de contenção a engenharia social, Aldawood e Skinner (2019, p. 114, tradução nossa) comentam que "Como a engenharia social está relacionada às capacidades humanas, as limitações comportamentais dos funcionários representam um desafio à eficácia do programa de treinamento e conscientização". Os autores ainda citam que:

> Mesmo com as mais recentes ferramentas de programas de treinamento e conscientização, os funcionários podem ter vulnerabilidades, como o medo de serem vítimas. Os hackers podem se aproveitar do uso de psicologia reversa para garantir que os alvos escolhidos possam morder a isca. (ALDAWOOD; SKINNER, p. 115, 2019).

Nesse sentido, é importante ressaltar que a conscientização em segurança da informação nunca é o bastante. Capacitar os colaboradores a criarem uma cultura em segurança da informação é a melhor maneira de prevenir que criminosos venham a conseguir se aproveitar da falta de conhecimento dos profissionais, prejudicando, assim, toda a organização.

3. METODOLOGIA

A metodologia é uma disciplina que tem como objetivo abordar o estudo, a compreensão e a avaliação dos diversos métodos que estão à disposição para a realização de uma pesquisa científica. Além disso, também objetiva descrever os vários procedimentos de uma pesquisa que facilitam a aquisição, bem como o tratamento de informações, com o objetivo de encaminhar e auxiliar na resolução de qualquer adversidade e questões que tenham cunho investigativo. (FREITAS; PRODANOV, 2013).

Esse trabalho foi desenvolvido com o intuito de analisar e compreender a importância da criação e utilização de políticas de segurança da informação na prevenção a ataques *ransomware*. Para a elaboração desse trabalho, foi utilizada uma abordagem qualitativa, visto que esse tipo de abordagem permite uma análise mais profunda e detalhada sobre o tema em questão. Foram realizadas revisões bibliográficas, usando como fonte livros, artigos, norma e sites, com a finalidade de buscar entender as melhores práticas e estratégias adotadas por empresas e organizações para se protegerem contra esse tipo de ameaça.

Ademais, considera-se que também foi realizada a utilização de uma pesquisa descritiva, visto que ao elaborar o trabalho, foi descrito o que ocorre na sua realização, com o intuito de entendê-la e também a analisar, sem interferir diretamente nela. Nesse tipo de pesquisa o objetivo é tentar descrever as manifestações de eventos ou situações dentro de um determinado contexto. (CAMPOS, 2015; SAMPIERI; COLLADO; LUCIO, 2013).

Diante do exposto, o propósito deste trabalho é identificar medidas eficazes que possam ser adotadas para fortalecer a segurança cibernética, promover a disseminação de conhecimento e aprimorar as políticas de segurança da informação nas organizações.

4. RESULTADOS E DISCUSSÃO

Os resultados deste estudo destacaram a relevância que as políticas de segurança da informação (PSI) tem na prevenção a ataques de *ransomware*. Implementar uma PSI eficaz apresenta vários desafios, incluindo o custo inicial de medidas como backups em nuvem e a resistência interna das partes interessadas que podem não ver imediatamente os benefícios. Realizar uma análise de custo-benefício detalhada e apresentar estudos de casos reais podem ajudar a justificar esses investimentos.

Além disso, esse trabalho ressalta que os ataques *ransomware* costumam usar a engenharia social que continua a ser uma ameaça significativa, pois explora as vulnerabilidades comportamentais dos funcionários. Programas de treinamento e conscientização devem ser contínuos e adaptados de acordo com a realidade de cada negócio para abordar essas vulnerabilidades, garantindo que os funcionários estejam sempre alertas e prontos para conseguir reconhecer e responder da maneira correta a ameaças de *ransomware*.

Por fim, diante de inúmeros ataques cibernéticos que a cada dia vem ficando mais frequente e mais sofisticados, implementar uma política de segurança da informação torna-se essencial. Esse documento pode permitir que uma organização ou empresa, independentemente de seu tamanho, consiga proteger seus ativos digitais, assegurando a integridade de sua reputação.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALDAWOOD, H; SKINNER, G. Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. **Cybersecurity and Cyberforensics Conference**, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013**: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

BRITO, Paulo. **Ataque cibernético atinge serviços de saúde em Londres**. [*S. l.*], 4 jun. 2024. Disponível em: https://www.cisoadvisor.com.br/ataque-cibernetico-atinge-servicos-de-saude-em-londres/. Acesso em: 7 jun. 2024.

CAMPOS, L. F.L. **Métodos e técnicas de pesquisa em psicologia**. 5. ed. rev. Campinas, SP: Alínea, 2015.

CENTURY TELECOM. **Desafios e soluções na implementação do cloud backup no data center**. 2024. Disponível em: https://centurytelecom.com.br/desafios-e-solucoes-na-implementacao-do-cloud-backup-no-data-center/. Acesso em 15 maio 2024.

CHAINALYSIS. **Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline**. 2024. Disponivel em: https://www.chainalysis.com/blog/ransomware-2024/. Acesso em 27 abr. 2024.

CLOUDFLARE**. Os invasores de ransomware escalam táticas de extorsão**. 2022**.** https://www.cloudflare.com/pt-br/the-net/ransomware-extortion/. Acesso em 27 abr 2024.

FREITAS, Ernani Cesar; PRODANOV, Cleber de Freitas. Ebook **Metodologia do Trabalho Científico:** Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2. Ed. 2013.

GRIMES, R. A. **Ransomware Protection Playbook**. 1. ed. Haboken: Wiley & Sons, 2021.

GRUSTNIY, Leonid. **A saga do ransomware**: Ransomware, outrora representados como quase inofensivos, atingiram a maioridade e tem de ser levados a sério. [*S. l.*], 9 abr. 2021. Disponível em: https://www.kaspersky.com.br/blog/history-of-ransomware/17280/. Acesso em: 5 maio 2024.

HASSAN, Nihad A. **Perícia forense digital**. Traduzido por Aldir Coelho Corrêa da Silva. São Paulo: Novatec Editora Ltda, 2019. 25 p.

HINTZBERGEN, J. *et al*. **Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002.** 3. ed. Rio de Janeiro: Brasport, 2018.

LISKA, A; GALLO, T. **Ransomware Defending Against Digital Extortion**. 1. ed. Sebastopol: O'Reilly Media, 2017.

INFOBUSINESS. **A anatomia básica de um ataque por ransomware**. 2019. Disponível em: https://infob.com.br/o-que-e-ransomware/. Acesso em 19 maio 2024.

PRESCOTT, Roberta. **Ataques ransomware estão mais direcionados e cresce o pagamento de resgate**. Associação Brasileira de Internet, 2024. Disponível em: https://www.abranet.org.br/Noticias/Ataques-ransomware-estao-mais-direcionados-e-cresce-pagamento-de-resgate-4917.html. Acesso em: 22 maio. 2024.

ROMAR , Carlos Eduardo Chagas; SILVA, Rodrigo Cardoso. **Estudo de Métodos de Detecção de Ransomware Utilizando Inteligência Artificial**. Sao Paulo, 9 dez. 2022.

SAFETYWARE. **Boas práticas para prevenção de ransomware**. 2017. Disponível em: https://www.safetyware.com.br/boas-praticas-para-prevencao-de-ransomware/. Acesso em: 29 abr. 2024.

SAMPIERI, R. H; COLLADO, C. F.; LUCIO, M. P. B. **Metodologia da pesquisa**. 5. ed. Porto Alegre: Penso, 2013.

STALLINGS, William; BROWN, Lawrie. **Computer Security**: Principles and Practice. 3. ed. [*S. l*]: Pearson, 2014.