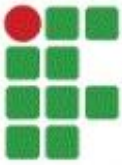

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
TECNOLOGIA EM REDES DE COMPUTADORES

ELISON VINÍCIUS DA SILVA ANUNCIAÇÃO
IGOR GONÇALVES BARBOSA AVELAR

MÉTODOS DE AUTENTICAÇÃO EM SEGURANÇA DA INFORMAÇÃO: redução de impactos em vazamento de dados.

MACAPÁ
2024

ELISON VINÍCIUS DA SILVA ANUNCIAÇÃO
IGOR GONÇALVES BARBOSA AVELAR

MÉTODOS DE AUTENTICAÇÃO EM SEGURANÇA DA INFORMAÇÃO: redução de impactos em vazamento de dados.

Trabalho de Conclusão de Curso apresentado a coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção do título de Tecnólogos.
Orientador: Prof. Me. Célio do Nascimento Rodrigues.

MACAPÁ
2024

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

A636m Anunciação, Elison Vinícius da Silva
Métodos de autenticação em segurança da informação: redução de impactos em vazamento de dados / Elison Vinícius da Silva Anunciação, Igor Gonçalves Barbosa Avelar. - Macapá, 2024.
28 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Tecnologia em Redes de Computadores, 2024.

Orientador: Me. Celio do Nascimento Rodrigues.

1. LGPD. 2. Segurança da Informação. 3. Vazamento de Dados. I. Avelar, Igor Gonçalves Barbosa. I. Rodrigues, Me. Celio do Nascimento, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

ELISON VINÍCIUS DA SILVA ANUNCIAÇÃO
IGOR GONÇALVES BARBOSA AVELAR

MÉTODOS DE AUTENTICAÇÃO EM SEGURANÇA DA INFORMAÇÃO: redução de impactos em vazamento de dados.

Trabalho de Conclusão de Curso apresentado a coordenação do curso de Tecnologia em Redes de Computadores como requisito avaliativo para obtenção do título de Tecnólogos.

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
CELIO DO NASCIMENTO RODRIGUES
Data: 20/02/2025 15:58:45-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Célio do Nascimento Rodrigues
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

gov.br Documento assinado digitalmento
LOURIVAL QUEIROZ ALCANTARA JUNIOR
Data: 20/02/2025 00:10:18-0300
Verifique em https://validar.iti.gov.br

Prof. Me. Lourival Queiroz Alcântara Júnior
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Prof. Me. Allan Meira de Medeiros
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Apresentado em: 14 / 01 / 2025.
Conceito/Nota: 7,5

Aos nossos pais que não mediram esforços para que tivéssemos uma educação adequada e baseada em adquirir conhecimentos.

AGRADECIMENTOS

Primeiramente, agradecemos a Deus que nos deu força, saúde e sabedoria para superar os desafios deste caminho. Foi com fé e perseverança que conseguimos enfrentar os momentos mais difíceis e seguir em frente. Agradecemos pelas bênçãos recebidas e pela oportunidade de realizar mais esta conquista em nossas vidas. Que possamos continuar trilhando nossos caminhos guiados por sua luz e proteção. Toda honra e glória sejam dadas a Ele.

Gostaríamos de expressar nossa mais profunda gratidão ao nosso orientador e professor Célio Rodrigues, cuja sua paciência, dedicação e conhecimento foram fundamentais para a realização deste trabalho. Seu compromisso em nos guiar durante todas as etapas do projeto foi inspirador e nos motivou a buscar sempre o melhor. Agradecemos por cada orientação precisa, por cada palavra de encorajamento e por acreditar no nosso potencial. Sua contribuição vai além do campo acadêmico, impactando também nossa formação pessoal. Somos imensamente gratos por todo o aprendizado proporcionado.

Aos nossos familiares, deixamos nosso mais sincero agradecimento por todo o apoio incondicional ao longo desta jornada. Foram vocês que, com palavras de incentivo, amor e compreensão, nos ajudaram a superar os desafios que surgiram. Obrigado por entenderem nossas ausências e por nos oferecerem um lar acolhedor que sempre foi nosso refúgio. Sem a base sólida e o suporte emocional de cada um de vocês, não teríamos chegado até aqui. Vocês são a nossa maior força e inspiração.

Aos nossos amigos, que estiveram ao nosso lado nos momentos mais difíceis e nas conquistas, nosso muito obrigado. Agradecemos pelas conversas, pelas trocas de ideias e pelo companheirismo que tornou esta caminhada mais leve. Vocês foram nossos parceiros de estudo, nossas vozes de incentivo e, muitas vezes, a alegria necessária em dias difíceis. Cada palavra de apoio e cada gesto de amizade marcaram profundamente esta etapa de nossas vidas. Levaremos cada um de vocês em nossos corações.

Por fim, aos professores do IFAP nosso sincero reconhecimento por todo o conhecimento compartilhado ao longo desta trajetória acadêmica. Vocês foram muito mais do que educadores; foram mentores que nos ajudaram a desenvolver nossa capacidade crítica, ética e profissional. Agradecemos a dedicação em sala de aula e fora dela, por cada dúvida esclarecida e por nos desafiar a ir além. Foi graças ao trabalho e empenho de vocês que pudemos alcançar este resultado.

O objetivo da segurança não é criar sistemas impenetráveis, mas sim aumentar o custo do ataque além do benefício para o invasor.
(Bruce Schneider)

RESUMO

A segurança da informação tem se tornado uma prioridade para organizações devido ao crescente número de incidentes relacionados ao vazamento de dados. Este trabalho explora os principais métodos de autenticação utilizados para proteger sistemas e dados, destacando suas características, benefícios e limitações. Com foco na redução de impactos decorrentes de violações, o estudo analisa desde métodos tradicionais, como senhas e PINs, até soluções mais robustas, como autenticação multifatorial (MFA) e biometria. A pesquisa também explora soluções inovadoras que minimizam riscos de ataques cibernéticos, contribuindo para um ambiente digital mais seguro e melhor equipado. Por meio de uma revisão bibliográfica, artigos e canais de comunicação, são avaliadas as tendências e as melhores práticas no uso de tecnologias modernas para mitigar os riscos associados à exposição de informações sensíveis. Os resultados apontam que a adoção de métodos mais avançados pode reduzir significativamente o impacto dos vazamentos, garantindo maior proteção às organizações e seus usuários.

Palavras-chave: segurança da informação; autenticação; vazamento de dados; biometria; autenticação multifatorial.

ABSTRACT

Information security has become a priority for organizations due to the increasing number of data leakage incidents. This study explores the main authentication methods used to protect systems and data, highlighting their features, benefits, and limitations. Focusing on reducing the impacts of data breaches, the research analyzes traditional methods, such as passwords and PINs, as well as more robust solutions like multifactor authentication (MFA) and biometrics. The research too explores innovative solutions that minimize cybersecurity risks, contributing to a safer digital environment and equiped better. Through a literature review, trends and communication channels, best practices in the use of modern technologies to mitigate risks associated with sensitive information exposure are evaluated. The findings suggest that adopting more advanced methods can significantly reduce the impact of data breaches, ensuring better protection for organizations and their users.

Keywords: information security; authentication; data breaches; biometrics; multifactor authentication.

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
IFAP	Instituto Federal do Amapá
SETEC	Secretaria de Educação Profissional e Tecnológica
TCC	Trabalho de Conclusão de Curso
LGPD	Lei Geral de Proteção de Dados
GDPR	Regulamento Geral de Proteção de Dados
NSA	Agência Nacional de Segurança dos Estados Unidos
GCHQ	Agência de Inteligência e Comunicação do Reino Unido
ISO	Organização Internacional de Normalização
IEC	Comissão Eletrotécnica Internacional

SUMÁRIO

1	**INTRODUÇÃO**	11
2	**ABORDAGEM DE CONCEITOS DE SEGURANÇA DA INFORMAÇÃO**	13
2.1	**Princípios básicos de segurança da informação**	14
3	**NORMAS E LEI PARA SEGURANÇA DA INFORMAÇÃO**	16
3.1	**Norma ISO/IEC 27001 – gerenciamento de segurança da informação**	16
3.2	**Norma ISO/IEC 27033-3 – segurança em redes de computadores**	16
3.3	**Impactos da lei geral de proteção de dados (LGPD)**	17
4	**FATORES DE RISCO**	18
4.1	**Incidentes e consequências**	18
5	**MÉTODOS DE AUTENTICAÇÃO**	21
6	**CONSIDERAÇÕES FINAIS**	26
	REFERÊNCIAS	27

1 INTRODUÇÃO

A segurança da informação é um dos pilares fundamentais para o funcionamento das organizações na era digital, especialmente diante do crescimento exponencial de dados sensíveis armazenados e processados em sistemas tecnológicos. Vazamentos de dados sejam eles, acidentais ou provocados por ataques cibernéticos tem se tornado cada vez mais frequentes como prejuízos financeiros, danos à reputação e violação a privacidade de indivíduos e instituições. Nesse contexto, a autenticação enquanto mecanismo de controle de acesso e identificação, assume papel central na proteção contra esses incidentes, sendo um dos métodos mais eficazes para minimizar os riscos associados à exploração de vulnerabilidades.

Entretanto isso, a crescente sofisticação de técnicas utilizadas por cibercriminosos exige que os métodos de autenticação evoluam constantemente, indo além de senhas tradicionais e incorporando abordagens multifatoriais, biométricas e baseadas em inteligência artificial. Assim, surge o problema central deste trabalho: como a escolha e a aplicação de métodos de autenticação podem contribuir para a redução dos impactos causados por vazamentos de dados?

O objetivo geral deste estudo é analisar a eficácia de diferentes métodos de autenticação no contexto da segurança da informação, com foco na mitigação dos impactos decorrentes de vazamentos de dados. Para alcançar esse objetivo, os seguintes objetivos específicos foram definidos abaixo.

Apresentar os principais tipos de métodos de autenticação utilizados atualmente, destacando suas características e limitações, investigar as vulnerabilidades mais comuns exploradas em vazamentos de dados e suas relações com falhas nos processos de autenticação, avaliar casos reais de vazamentos de dados para compreender como a aplicação de métodos de autenticação impacta na redução dos danos e propor recomendações e boas práticas para a implementação de métodos de autenticação mais robustos e eficazes.

A metodologia adotada será de natureza exploratória e descritiva, com abordagem qualitativa. O trabalho será fundamentado em revisão bibliográfica e documental, envolvendo artigos científicos, livros e relatórios técnicos sobre segurança da informação, autenticação e vazamentos de dados. Além disso, estudos de caso serão utilizados para exemplificar e validar os conceitos abordados, possibilitando uma análise prática do impacto dos métodos de autenticação na contenção de riscos.

Ao final, espera-se que este estudo contribua para a conscientização sobre a importância de métodos de autenticação robustos, apresentando subsídios teóricos e práticos para sua

aplicação estratégica na segurança da informação, especialmente no cenário crítico dos vazamentos de dados.

2 ABORDAGEM DE CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

De acordo com SÊMOLA (2003), podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Para ALVES (2006), a segurança da informação possui a missão de proteger as informações garantindo a continuidade de seus negócios, com o objetivo de reduzir os danos causados e aumentar o retorno de investimentos além de uma vasta oportunidade de negócios.

A segurança da informação era definida por sistemas de normas especializadas como a ISO e a IEC, pois ambos a definiram como uma forma de proteção contra ameaças com a função de assegurar, minimizar os riscos e/ou danos e maximizar retornos em oportunidades comerciais. Complementando a abordagem nos tempos atuais, a informação se transformou em um ativo com altíssimo grau de importância, pois necessita dos devidos cuidados e restrições já que a sua demanda exige um extremo cuidado possuindo um valor essencial para as corporações e como consequência tendo que ser protegido de forma adequada, conforme é determinado na norma ISO/IEC 17779:2001.

Na ABNT (2003) com a sua norma ISO/IEC mencionada anteriormente acima, define a segurança da informação como “a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos.”. A norma ISO/IEC 17799:2001 ainda complementa que “a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade”.

CID como é abreviado, são 3 principais pilares da segurança da informação também chamados de tripé de segurança, começando pelo atributo da confidencialidade que aborda às proteções de determinadas informações das quais não devem ser acessadas em hipótese alguma por indivíduos não-autorizados. Por exemplo, alguém mal-intencionado acaba obtendo acesso a dados bancários, informações sigilosas e dados pessoais de clientes e resolve vazar essas mesmas informações pela internet. Para que isto não ocorra, a confidencialidade é aplicada com a implantação de logins, senhas, tokens, criptografias etc.

O atributo da integridade é focado no armazenamento de dados, pois do mesmo modo em que tais informações poderão ser fornecidas aos usuários, também poderão ser armazenadas sem nenhuma interferência de alteração. Exemplificando de forma mais sucinta, onde você que é um usuário acessa um site, você clique em um link esperando ser redirecionado para alguma

página específica, é na verdade um invasor, entre você e o site, desviando seu acesso para outra página maliciosa. Para poder evitar esse transtorno será necessário fazer um backup, utilizar mecanismos de definições de permissão e códigos de verificação, pois assim não perderá seus dados.

Por fim, o atributo da disponibilidade que deixa claro que foca na garantida de disponibilidade de informações, pois é focado na eficácia do sistema de segurança da informação, tendo como consequência poder acessas suas informações quando achar necessário. Para isso, a organização ou o usuário físico precisará ter uma estrutura altamente adequada, pois backups feitos de forma periódica em nuvens e atualizações regulares e necessárias são essenciais para evitar possíveis quedas de navegação.

2.1 Princípios básicos de segurança da informação

É importante frisar mudança ou atualizações de normas, especificamente na ISO/IEC 17799, sendo essa atualizada para numeração 27002, em que a abordagem sobre os atributos básicos da informação, também chamado de princípios básicos da segurança da informação. Que são: confidencialidade, integridade, autenticidade, disponibilidade e irretratabilidade ou não repúdio, sendo esses dois princípios sendo pilares adicionais que contribuem para a segurança da informação

a) Princípio da confidencialidade: Este princípio leva-se em consideração que engloba a proteção dos dados dos usuários contra acessos não autorizados e medidas a fim de preservar a privacidade deles.

b) Princípio da integridade: Dispõe-se sobre as condições dos dados, os quais devem ser mantidos e inalterados. O emissor emite um documento e este ser direcionado para o destinatário sem que haja possibilidade de ser alterado de forma proposital ou acidental.

c) Princípio da autenticidade: Refere-se à confirmação de que o usuário é realmente quem alega ser, desde quem está emitindo a informação até quem irá recebê-la.

d) Princípio da disponibilidade: Refere-se à confirmação de que o usuário é realmente quem alega ser, desde quem está emitindo a informação até quem irá recebê-la, como por exemplo os códigos enviados por e-mail ou SMS.

e) Princípio da irretratabilidade ou não repúdio: É focado na legitimidade da informação, funciona como uma forma de rastrear todas as ações de um indivíduo dentro do sistema de forma que não seja possível negar a autoria de uma ação. Sendo um exemplo prático, a criação e assinatura de um documento ou arquivo específico.

Quando o sistema fica “fora do ar”, não possibilitando o acesso ao mesmo, consequentemente às informações estarão indisponíveis. Segundo Garde (2019) explica que quando o governo brasileiro se viu obrigado a acelerar a regulamentação da lei e se adequar aos moldes europeus. Pela urgência e pressão internacional, a LGPD se apresenta como uma versão compacta e simplificada da GDPR, mas com os mesmos pilares que garantem a privacidade dos usuários digitais.

3 NORMAS PARA PROTEÇÃO E SEGURANÇA DE DADOS

As normas ISO/IEC especificamente focadas na segurança de informações e dados tem sido altamente essencial no mundo da tecnologia que tem se seguido instável com tantos ataques cibernéticos fora de proporções nunca vistas. Especialmente as ISO/IEC 27001 e 27033-3, essas duas especificamente da família de normas 27000, foram altamente signicativas para a melhoria de segurança de informação de dados ressaltando que tais informações importantes pudessem ser asseguradas e protegidas tendo ali relações com a Lei Geral de Proteção de Dados (LGPD).

3.1 Norma ISO/IEC 27001 – gerenciamento de segurança da informação

A norma ISO/IEC 27001, aborda sobre gestões de segurança que procuram definir seus métodos e requisitos para melhorar os atendimentos e necessidades de uma empresa em questões de correção e detecção de pontos de falhas visando melhorias no gerenciamento de sistemas de segurança, onde aprimora as boas relações de empresas parceiras de segurança da informação com seus clientes e futuros cliente em potencial.

Um fator importante é em suas definições de objetivos nos quais focam nas constantes melhorias e auditorias em métodos de segurança da informação onde fazem análises detalhadas de formas bastante críticas e minuciosas, sendo certificados nos quais estão demonstrando que seus sistemas de segurança estão muito bem protegidos em seus próprios ambientes corporativos, deixando altamente claros que essas melhorias nas gestões devem ser adotadas de imediato.

3.2 Norma ISO/IEC 27033-3 – segurança em redes de computadores

A norma ISO/IEC 27033-3, funciona como um guia que foca na segurança da informação em redes de computadores que se aplicam na segurança de dispositivos para proteção de seus serviços e proteção de seus usuários, meios físicos e em conexões de comunicação.

A ISO também faz análises de riscos relacionados a segurança de rede, voltada também aos procedimentos a serem adotados a fim de sanar tais riscos que são identificados. Através desta norma, também começam a ser feito análises em pontos específicos de rede, nos quais

analisam filtros de pacotes (patches), traduções em endereços de rede, filtros de conteúdos específicos e análises de navegação, redes virtuais privadas (VPN), etc.

3.3 Impactos da Lei Geral de Proteção de Dados (LGPD)

A lei nº 13.709/2018, também nomeada de Lei Geral de Proteção de Dados (LGPD) possui um impacto significativo durante o cotidiano do mundo digital, porém, esse impacto acaba por gerar consequências nunca antes vista. Pois, uma vez que esses dados de usuários são coletados independente da plataforma seja X (antiga Twitter), Facebook ou Google, caso vazados na internet, causam resultados catastróficos. No caso das penalidades de forma geral, a LGPD tem a obrigação de proteger o usuário de utilizações abusivas dos seus dados como por exemplo, a Netshoes que em Julho de 2018 sofreu vazamentos dos seus dados contendo dados importantes, o que claro causou prejuízos a empresa como perdas de dados bancários, informações pessoais de clientes e funcionários, etc. No ano seguinte, foi condenada a pagar em até 500 mil reais de indenização a mais de 2 milhões de usuários que foram prejudicados por ordem do Ministério Público do Distrito Federal de acordo com o site G1.

Os impactos que causam no mundo digital são vastos, pois segundo *Yuri Sahione* no caso de compartilhamento de dados que quando é relacionado a tecnologia de informação e publicidade, os impactos tendem a ser bem diretos, onde as empresas consigam adaptar suas operações. Esses mesmos impactos podem afetar diversos setortes de tecnologia, pois algumas empresas ou instituições importantes acabam sofrendo, porém, contendo informações bem mais detalhadas além do necessário para garantir mais segurança nas informações obtidas em seus bancos de dados.

Porém, esses tipos de dados, tanto de usuários quanto de empresas ou organizações, são extremamente valiosos já que até mesmo as corporações precisam constantemente contratar equipes especializadas em segurança da informação, para proteger seus dados e realizar relatórios que estejam ligados a vazamentos de informações sigilosas, além de seguirem requisitos específicos de proteção de dados, caso incluam dados pessoais de seus clientes.

4 FATORES DE RISCO

Qualquer falha de segurança pode sim, se mostrar algo catastrófico quando se revelado publicamente vulnerabilidades que possam afetar e prejudicar empresas privadas, órgãos públicos, e até mesmo instituições de ensino (fundamental, médio e superior). Claro que, nenhum deles quer que isso aconteça futuramente em algum momento. É levado em consideração que uma hora ou outra vai acontecer pois até mesmo é necessário que possam se preparar para tais incidentes e terríveis consequências.

Geralmente softwares duvidosos ou desatualizados, falta de firewalls e até falta de melhorias com focos em montagem e usos em equipamentos de segurança digital e cibernética para fins de proteção de dados, segundo à LGPD (Lei Geral de Proteção de Dados) criada em 2014 e atualizada em 2018 pode gerar multas pesadas que demonstre falhas irreversíveis em sistemas avançados de seguranças.

Entre fatores conhecidos, é também possível demonstrar tais consequências notáveis como roubos e vendas de dados, falhas diretas e indiretas em empresas privadas e órgãos governamentais públicos, até mesmo em bancos públicos e privados, o estrago causado por ataques cibernéticos é exponencialmente e altamente devastador. É comprovado por meios digitais de comunicação e mídia, podendo provar que esses fatores de risco podem sim causar falhas podendo gerar prejuízos ocasionando em perdas totais de informações e/ou dados importantes até tendo atrasos significativos em quaisquer setores corporativos importantes, sejam públicos, privados ou em ambos.

4.1 Incidentes e Consequências

Como já sabemos, incidentes relacionados à roubos de dados tem sido bem mais frequentes do que o normal, o que a longo prazo tem afetado muitos usuários em diversos setores ao longo dos anos. Um dos exemplos desses, podem ser roubos e vazamentos de dados a plataformas de redes sociais, dados bancários, informações sigilosas etc.

Algumas das repercussões que já aconteceu foi em um exato período de 3 anos, roubos e vazamentos de dados onde tais alvos entre eles, o Senado, Tribunal Superior Eleitoral (TSE) e até mesmo o exército. Contudo, vem um questionamento importante, qual fator eles têm em comum que a longo prazo afeta a população como um todo? A resposta é bem simples, todos foram atacados pelo mesmo autor nos roubos e vazamentos cibernéticos de dados. De acordo

com site de comunicação de notícias G1 ao todo, foram três operações responsáveis por prendê-lo nos anos de 2019, 2020 e 2021:

a) Operação *Defaced* (2019)

A nomeada *operação defaced*, foi executada em meados de 2019 com a prisão do hacker Marcos Roberto Correia da Silva, sob o pseudônimo de *"Vandathegod"*. Ele foi responsável por invadir sites e sistemas da Polícia Civil, Ministério Público de Minas Gerais, Tribunal de Justiça de Goiás e até o Exército Brasileiro.

Durante a sua prisão um computador havia sido apreendido, diversos dados sigilosos e importantes dos governos estaduais foram copiados pelo hacker. Durante esse ataque onde o dito cujo fez isso por mera "diversão" e não fez por questões financeiras inicialmente. Nota-se que esse foi um dos primeiros ataques já realizados pelo hacker em questão, o que pode demonstrar terríveis falhas nos seus sistemas de segurança de dados que deveriam ser os mais avançados tecnologicamente, o que neste primeiro incidente demonstrou ser totalmente o contrário.

b) Operação *Exploit* (2020)

Também envolvendo o mesmo hacker, havia sido detido em meados de novembro de 2020 durante a operação *exploit.* Ele estava sendo investigado juntamente com outros hackers que cujos nomes não haviam sido revelados por participar de ataques ocorridos contra o TSE (Tribunal Superior Eleitoral), onde expos informações importantes de ex-servidores do órgão público e ter tentado vende-los na *deepweb* no qual afetou diretamente o primeiro turno nas eleições municipais de 2020, porém, não obteve sucesso no seu objetivo em questão.

c) Operação *Deepwater* (2021)

Por fim, a prisão do mesmo hacker ocorre finalmente na operação *Deepwater* que foi deflagrada em 19 de janeiro de 2021 no qual participou do maior vazamento de dados da história contando justamento com os dois anos anteriores, onde o mesmo foi preso novamente, pois foi encontrado com ele um notebook e um smatphone e em ambos os dispositivos foram

encontradas informações pessoais e sigilosas de mais de centenas de milhões de usuários brasileiros e foi descoberto que já haviam sido divulgadas na internet.

5 MÉTODOS DE AUTENTICAÇÃO

Entre as inúmeras técnicas de invasão, podemos citar a backdoor (porta dos fundos) que consiste principalmente em criar uma abertura para ataques a sistemas privados ou públicos podendo ser tanto dispositivos, rede ou sistemas. O backdoor, pode ser tanto resultado de um trabalho específico que busca alcançar um sistema pré-determinado ou resultado de lacunas a abertas que passam despercebidas podendo ser encarada com uma vulnerabilidade não intencional.

Como por exemplo, podemos citar o caso magalenha que se usou de tanto phising e backdoor. A partir de links fraudulentos, e-mails de phishing e outros vetores, os usuários são induzidos a interagirem com arquivos e sites maliciosos, que por sua vez, executam um script Visual Basic que permite a implementação do backdoor PeepingTitle.

O backdoor também pode ser usado para realizar atividades de manutenção, desde que seja configurado de forma correta, ele se torna uma ferramenta útil segundo o blog backup seguro. Para se ter uma boa ideia desse cenário, basta pensar em dispositivos inteligentes de *Internet of Things*, como a famosa Alexa, da Amazon. Muitas vezes, dispositivos do tipo contam com a instalação prévia de *backdoors* para permitir que um técnico estabeleça acesso remoto e solucione possíveis problemas, se for necessário.

Pessoas que usam backdor em grande parte usam scaner que localizam lacunas. Vale acrescentar que os atacantes geralmente identificam alvos ou vítimas através de *scanners*, que identificam sites com componentes não corrigidos (sem patches) ou desatualizados que vão permitir a inclusão de arquivos maliciosos. Através dessa prática gera uma porta através do servidor que pode ser acessada a qualquer instante, ainda existe o empecilho sobre a questão de atualização.

Segundo informações adquiridas e apuradas pelo site ciscodvisor a implantação de backdoors em redes corporativas foi a principal ação dos invasores em quase um quarto de todos os incidentes registrados no ano passado. Os usuários desse meio utilizam essa ferramenta como um método escapatório para burlar os sistemas que escapam das ferramentas de criptografia de sistemas computacionais inteiros ou de um único dispositivo.

Segundo matéria disponibilizada pelo site Technoblog a Agência Nacional de Segurança dos Estados Unidos e a Agência Britânica (GCHQ), fizeram uma operação onde eles quebraram protocolos já existentes sendo: HTTPS, SSL, VPN, SSH entre outros. Segundo o Jornal New York times, O Guardian e a Agência jornalística pro pública todas as formas de

criptografia já foram quebradas pela NSA com objetivo de ter acesso as comunicações feitas pela internet.

O NY Times explica que a agência conseguiu burlar ou quebrar grande parte dos métodos de encriptação utilizados atualmente na rede, incluindo aí sistemas utilizados pelo comércio, indústria e setor financeiro. Aqueles dados que todo mundo espera que estejam resguardados também estariam suscetíveis ao acesso dos agentes: emails, históricos de pesquisa, chamadas por VoIP, bate-papos em texto por aplicativos de IM e documentos salvos na nuvem.

A NSA investiu “bilhões de dólares” desde o ano 2000 para iniciar uma campanha clandestina, depois de ter perdido uma batalha judicial para instalar uma porta dos fundos (backdoor) em todas as formas de criptografia. Se não foi possível fazer com o auxílio da lei, os agentes da agência recorreram à engenharia reversa e ao velho método do stealth (a invasão silenciosa) para obter todas as informações de que precisavam – e aquelas de que não precisavam também.

Por exemplo, o monitoramento em tempo real pode vigiar muitos arquivos sendo acessados ou alterados em um período curto. Ele também pode detectar a abertura de arquivos que não são usados há muito tempo. Mesmo se for provado que essa atividade não é ransomware, pode ser outro problema de segurança, como uma ameaça interna.

Para montar uma linha de defesa contra qualquer vírus e ramsowares, é fundamental como primeiro item montar um firewall e um sistema de detecção de intrusão (IDS) atuam com primeira linha de defesa e funciona com outros tipos de taques mesmo não sendo ramsowares. Um firewall analisa a atividade de entrada e saída da rede e bloqueia conexões que considerar como não autorizadas.

Atividades não autorizadas podem ser uma varredura de portas, em que um invasor tenta se conectar a portas aleatórias para descobrir quais serviços estão sendo executados em um servidor. Alternativamente, pode ser um invasor tentando fazer login em um servidor usando força bruta ou simplesmente para executar um ataque de negação de serviço contra um servidor, enviando um número enorme de solicitações em rápida sucessão.

Os sistemas de detecção de intrusão são similares aos firewalls, pois também detectam atividades maliciosas. Essas ferramentas então agem com base em um conjunto de regras predefinidas. Por exemplo, elas podem ativar outras ferramentas para execução ou alertar o administrador do sistema para que ele possa analisar o problema e intervir manualmente.

A defesa contra ransomware é uma verdadeira corrida armamentista tecnológica, e não é possível confiar apenas em regras estáticas e definições de malware. Até a verificação antivírus heurística não garante a identificação de todo código maligno. Portanto, é importante usar monitoramento em tempo real e análise comportamental para identificar alterações em atividade no seu sistema.

Usar essa forma de monitoramento aumenta a probabilidade de qualquer atividade suspeita ser notada. Manter os programas sempre atualizados, porque estes estão sempre em desenvolvimento de proteção para novas ameaças. Importante baixar aplicativos apenas de fontes confiáveis, verificando se as permissões de instalação e execução são coerentes e desabilitar a auto execução de mídias removíveis e de arquivos que estejam anexados.

Algumas empresas de cibersegurança também desenvolvem ferramentas gratuitas para descriptografar dados infectados por ransomware, tendo como exemplo, o site *www.nomoreransom.org.* Um dos principais fatores de sucesso dos ciberataques é a exploração das vulnerabilidades do usuário final. Ainda não se deram conta das ameaças que se escondem por trás de uma simples visita à internet.

As empresas e os governos devem investir pesado em campanhas de conscientização de seus funcionários para a execução de uma navegação segura. Visando à prevenção e à minimização dos danos, é de extrema importância fazer uma cópia periódica (backup) de todos os dados das máquinas em mídia física externa. Outro ponto, outras medidas simples, porém não menos importantes, como a ativação da extensão dos arquivos, bem como o monitoramento dos anexos dos e-mails, para evitar que um arquivo executável malicioso seja ativado.

As equipes de segurança da informação também utilizam a chamada *sandbox* (caixa de areia), que é uma ferramenta capaz de executar os programas suspeitos de forma isolada, num ambiente virtual dentro da própria máquina, possibilitando ao usuário analisar seus procedimentos de forma segura, num perímetro limitado e sem afetar a máquina.

Outro procedimento utilizado é o chamado método honeyfile ou honeypot (arquivo de mel ou pote de mel), onde se apresenta um sistema exposto como uma isca para um ataque. Diante desse ataque, a equipe de segurança da informação poderá estudá-lo, podendo desenvolver novos mecanismos de defesa para novos vírus. Por óbvio que os procedimentos de prevenção não se esgotam aqui, diversos procedimentos técnicos são utilizados, mas não caberia maior aprofundamento, tendo em vista correr o risco de desviarmos da análise jurídica do presente estudo.

Os usuários particulares ainda não se deram conta das ameaças que se escondem por traz de uma simples visita à internet. As empresas e os governos devem investir pesado em campanhas de conscientização de seus funcionários para a execução de uma navegação segura. Visando à prevenção e à minimização dos danos, é de extrema importância fazer uma cópia periódica (backup) de todos os dados das máquinas em mídia física externa.

Outro ponto, outras medidas simples, porém não menos importantes, como a ativação da extensão dos arquivos, bem como o monitoramento dos anexos dos e-mails, para evitar que um arquivo executável malicioso seja ativado. Manter os programas sempre atualizados, porque estes estão sempre em desenvolvimento de proteção para novas ameaças. Importante baixar aplicativos apenas de fontes confiáveis, verificando se as permissões de instalação e execução são coerentes e desabilitar a auto execução de mídias removíveis e de arquivos que estejam anexados.

Algumas empresas de cibersegurança também desenvolvem ferramentas gratuitas para descriptografar dados infectados por *ransomware*, tendo como exemplo, o site www.nomoreransom.org. As equipes de segurança da informação também utilizam a chamada *sandbox* (caixa de areia), que é uma ferramenta capaz de executar os programas suspeitos de forma isolada, num ambiente virtual dentro da própria máquina, possibilitando ao usuário analisar seus procedimentos de forma segura, num perímetro limitado e sem afetar a máquina.

Outro procedimento utilizado é o chamado método *honeyfile* ou *honeypot* (arquivo de mel ou pote de mel), onde se apresenta um sistema exposto como uma isca para um ataque. Diante desse ataque, a equipe de segurança da informação poderá estudá-lo, podendo desenvolver novos mecanismos de defesa para novos vírus. Por óbvio que os procedimentos de prevenção não se esgotam aqui, diversos procedimentos técnicos são utilizados, mas não caberia maior aprofundamento, tendo em vista correr o risco de desviarmos da análise jurídica do presente estudo.

Em nosso ordenamento jurídico, a competência para a apuração das infrações penais cabe às Polícias Civis dos Estados e à Polícia Federal, conforme preceitua o artigo 144 da Constituição da República, bem como aos membros do Ministério Público. Diante da evolução tecnológica, a prática de crimes cibernéticos se tornou uma realidade, havendo uma constante necessidade para os órgãos de investigação acompanharem essa evolução. As organizações criminosas têm explorado esse mercado cada vez mais lucrativo

e interessante, onde a busca pelo anonimato tem dificultado a atuação desses órgãos de investigação.

Ao tratarmos de crimes cibernéticos, precisamos também entendê-los como uma ameaça real à segurança dos países. Diante disso, também há necessidade de planejamento para a construção de uma defesa cibernética com a finalidade de proteger, a força tarefa internacional (união entre a Polícia Nacional Holandesa, a Europol, a Intel Security e a Kaspersky para combater o ransomware), elencou seis tópicos para prevenção e reação são os seguintes:

1 – Backup: é a cópia dos arquivos importantes, sempre faça.
2 – Antivírus: são softwares que combatem os programas maliciosos, tenha um bom antivírus.
3 – Atualização Contínua: é importante que seu sistema operacional esteja sempre atualizado.
4 – Desconfie Sempre: nunca clicar em links sem ter certeza de que seja legitimo.
5 – Exibir Extensões de Arquivos: define seu formato, nunca baixe um executável.
6 – Off-line: se perceber algum arquivo suspeito, desligue o dispositivo e a internet.

Os principais motivos para que os *ransomwares* ainda tenham um alto índice de infecção é a sua constante evolução como "negócio", a alta capacidade técnica dos cibercriminosos e a facilidade que eles têm em disponibilizar seus serviços para "hackers" leigos. Entretanto, existem medidas simples que, se bem observadas minimizam bastante a possibilidade desse tipo de malware causar algum tipo de transtorno.

6 CONSIDERAÇÕES FINAIS

No contexto atual, onde a informação é um dos ativos mais valiosos para empresas e indivíduos, garantir a segurança dos dados tornou-se uma prioridade essencial. Este trabalho abordou os métodos de autenticação como uma das principais ferramentas no combate aos vazamentos de informações, ressaltando a importância de práticas robustas para proteger sistemas e usuários contra ameaças cibernéticas cada vez mais sofisticadas.

Ao longo do estudo, foi possível observar que métodos tradicionais de autenticação, como o uso de senhas simples, apresentam vulnerabilidades significativas, sendo insuficientes para lidar com os desafios impostos por ataques modernos. Nesse sentido, soluções mais avançadas, como a autenticação multifator (MFA), biometria e métodos baseados em inteligência artificial, têm se mostrado eficazes na redução do impacto de incidentes relacionados ao vazamento de dados.

Outro ponto relevante abordado foi a necessidade de equilibrar segurança e usabilidade. Métodos de autenticação extremamente complexos podem desencorajar os usuários, enquanto soluções mais práticas, mas seguras, como o uso de tokens, reconhecimento facial e autenticação por dispositivos móveis, têm ganhado destaque por proporcionarem proteção sem comprometer a experiência do usuário.

Conclui-se que a adoção de métodos de autenticação modernos é indispensável para mitigar os riscos associados a vazamentos de dados. No entanto, essa implementação deve estar alinhada com uma cultura organizacional voltada para a conscientização e treinamento dos usuários, bem como a atualização contínua de tecnologias e práticas de segurança.

Por fim, o estudo reforça que a segurança da informação é um campo dinâmico e em constante evolução. Assim, é crucial que organizações e indivíduos estejam preparados para acompanhar as mudanças tecnológicas e as novas ameaças, garantindo, dessa forma, a integridade, a confidencialidade e a disponibilidade das informações, pilares fundamentais da segurança da informação.

REFERÊNCIAS

ARAÚJO, Fábio Lucena de. **Aspectos jurídicos no combate e prevenção ao ransomware**. Disponível em: https://www.mprj.mp.br/documents/20184/1287128/Fabio_Lucena_de_Araujo.pdf. Acesso em: 23 ago. 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. **NBR ISO/IEC 17799:** tecnologia da Informação: código de Prática para Gestão da Segurança da Informação. Rio de Janeiro, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. **NBR ISO/IEC 27001:** gerenciamento de segurança da informação. Disponível em: https://debsolutionsti.com/iso-27000/iso-27001/. Acesso em: 13 mai. 2023.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. **NBR ISO/IEC 27033-3:** segurança em redes de computadores. Disponível em: https://debsolutionsti.com/iso-27000/iso-27033-3/. Acesso em: 13 mai. 2023.

CISO. **Backdoor supera ransomware como principal ação de hackers.** Disponível em: https://www.cisoadvisor.com.br/backdoor-supera-ransomware-como-principal-acao-de-hackers. Acesso em: 10 jul. 2024.

COMPUTERWORLD. **6 consequências devastadoras de um vazamento de dados corporativos.** 24 jul. 2021. ComputerWorld. Disponível em: https://computerworld.com.br/seguranca/6-consequencias-devastadoras-de-um-vazamento-de-dados-corporativos/. Acesso em: 25 out. 2021.

DURVAL, Carolina. **Pishing:** entenda os riscos e proteja sua empresa. Disponível em: https://gestaoclick.com.br/blog/phishing/. Acesso em: 26 jul. 2024.

FILHO, Napoleão Póvoa Ribeiro**. Ransomware:** origens, consequências e prevenção**.** Disponível em: https://ojs.studiespublicacoes.com.br/ojs/index.php/sees/article/view/2145/1762. Acesso em: 10 out. 2024.

GARDE, Guilherme. **O paradoxo da privacidade e a LGPD.** 22 ago. 2019. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=51507&sid=15. Acesso em: 29 set. 2021.

JULIO, Clara**. Malware backdoor:** entenda esse tipo de ameaça e saiba como evitar. Disponível em: https://backupgarantido.com.br/blog/malware-backdoor/. Acesso em: 15 mai. 2024.

KASPERSKY**. Brasil e os ataques de pishing por whatsapp.** Disponível em: https://www.kaspersky.com.br/blog/brasil-ataques-phishing-2022/20943/. Acesso em: 21 jul. 2024.

NETSHOES diz que dados de clientes podem ter sido vazados após “incidente cibernético”. **G1,** 17 jul. 2024. Disponível em:

https://g1.globo.com/tecnologia/noticia/2024/07/17/netshoes-diz-que-dados-de-clientes-podem-ter-sido-vazados-apos-incidente-cibernetico.ghtml. Acesso em: 19 set. 2024.

RAMOS, Rahellen**. Marco civil da Internet.** Disponível em: https://www.politize.com.br/marco-civil-da-internet/. Acesso em: 27 nov. 2021.

RANGEL, Misha. **Ransomware defense**. Disponível em: https://www.veeam.com/blog/pt/ransomware-defense.html. Acesso em: 26 jun. 2024.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

SILVA, A. C. **Metodologia da pesquisa aplicada à contabilidade.** 2.ed. São Paulo: Atlas, 2008.

SUSPEITO do maior vazamento de dados do brasil é preso em uberlândia. **G1,** 19 mar. 2021. Disponível em: https://g1.globo.com/mg/triangulo-mineiro/noticia/2021/03/19/suspeito-do-maior-vazamento-de-dados-do-brasil-e-preso-em-uberlandia.ghtml. Acesso em: 08 abr. 2024.

STARLLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. Editora Pearson, 6.ed. 2015.