FUNDAÇÃO PRESIDENTE ANTÔNIO CARLOS
FACULDADE PRESIDENTE ANTÔNIO CARLOS DE TEÓFILO OTONI
BACHAREL EM SISTEMAS DE INFORMAÇÃO

DILSIMEYRE GONÇALVES SANDER

JADE EMANOELHE ALVES PEREIRA

VAZAMENTO DE INFORMAÇÕES ONLINE

TEÓFILO OTONI
2022

DILSIMEYRE GONÇALVES SANDER[1]

JADE EMANOELHE ALVES PEREIRA[2]

VAZAMENTO DE INFORMAÇÕES ONLINE

Artigo científico apresentado à disciplina de Trabalho de Conclusão de Curso - TCC do Curso de Sistemas de Informação da Faculdade Presidente Antônio Carlos de Teófilo Otoni, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

BANCA EXAMINADORA

_____

Prof. Giovanni Camargo Silva
Orientador

_____

Prof. Renato Freitas Martins
Avaliador

_____

Prof. Lucas C. Oliveira Matsueda

Avaliador

Aprovado em __/__/____

[1]Aluna do 5º período de Bacharelado em Sistemas de Informação pela Faculdade Alfa Unipac de Teófilo Otoni. E-mail: dilsimeyresander16@gmail.com

[2]Aluna do 6º período de Bacharelado em Sistemas de Informação pela Faculdade Alfa Unipac de Teófilo Otoni. E-mail: jadeemanoelhealvespereira@gmail.com

Resumo

O objetivo do presente artigo é analisar o principal motivo para diversas exposições de dados, problema esse, que tem se tornado cada vez mais um enorme risco às informações privadas, discutindo-se a importância da conscientização dos usuários da rede mundial de computadores, que se encontram permanentemente vulneráveis. A metodologia utilizada no trabalho é de uma revisão bibliográfica, com a qual se busca trazer o panorama geral do assunto, apresentando o modo por meio do qual o sequestro de informações é realizado, bem como os principais dados expostos aos quais são possíveis citar exemplos, como: CPF, e-mail, endereço, fotos, telefone, senhas diversas e dados sigilosos, além de evidenciar maneiras de se proteger dos ataques cibernéticos relacionados a esse crime. Neste contexto, nota-se que apesar de ser um assunto bem discutido, é muito pouco priorizado por empresas, onde 80% de pesquisas feitas, acusam dados furtados ou ausência de informações dos clientes. Em alguns casos, é necessário passar por um conjunto de ações para evitar que aconteça um vazamento, encontrar implementações tecnológicas e automatizações para amenizar a manipulação de dados feita por um elemento humano, de maneira planejada ou não. Os usuários da grande rede permanecem, progressivamente, mais tempo conectados, e se submetem aos inúmeros casos de exposição trazendo cada vez mais vulnerabilidade que pode afetar a vida pessoal de um indivíduo e a segurança de uma empresa. Hoje, mais do que nunca, é necessário investir em medidas e métodos preventivos para melhorar a segurança dos sites e sistemas que armazenam as bases de dados. Além disso, devido à proporção das consequências de tais crimes, é necessário dar mais atenção aos profissionais que têm acesso a essas informações.

Palavras chaves: Segurança, vulnerabilidade, dados

Abstract

The objective of this article is to analyze the main reason for several data exposures, a problem that has increasingly become a huge risk to private information, discussing the importance of the awareness of users of the World Wide Web, who are permanently vulnerable. The methodology used in this work is a bibliographic review, which seeks to bring the general panorama of the subject, presenting the way in which the kidnapping of information is carried out, as well as the main exposed data, examples of which are possible to cite, such as: CPF, e-mail, address, photos, telephone, various passwords and sensitive data, in addition to showing ways to protect oneself from cyber attacks related to this crime. In this context, it is noted that despite being a well-discussed subject, it is very little prioritized by companies, where 80% of surveys made, accuse stolen data or absence of customer information. In some cases, it is necessary to go through a set of actions to prevent a leak, find technological implementations and automation to mitigate the manipulation of data made by a human element, planned or not. The users of the great network remain progressively more connected, and submit themselves to the countless cases of exposure bringing more and more vulnerability that can affect the personal life of an individual and the security of a company. Today, more than ever, it is necessary to invest in preventive measures and methods to improve the security of websites and systems that store databases. In addition, due to the proportion of the consequences of such crimes, it is necessary to pay more attention to the professionals who have access to this information.

Keywords: *security, vulnerability, data*

Introdução

A história da tecnologia está repleta de acontecimentos e momentos marcantes que moldaram a sociedade em algum ponto, dando novos direcionamentos de convivência e comunicação. Começa com a criação de ferramentas de caça pré-históricas e se estende até o lançamento de grandes tecnologias como *Apple e Microsoft*. Entretanto, assim como foram criadas grandes tecnologias que revolucionaram a forma de viver em sociedade, esse marco também transformou os usuários em vítimas de diversos ataques tanto no cotidiano, por exemplo, com furtos de aparelhos quanto de forma virtual com sequestro de informações.

Atualmente, quando se fala em privacidade, não há o mesmo entendimento, privacidade não significa mais isolamento, mas proteção. À medida que aumenta drasticamente o número de pessoas conectadas à Internet, que a utilizam para entretenimento, trabalho ou outros fins, é necessário a proteção legislativa, não apenas com penalidades criminais, mas também com obrigações civis e de responsabilidade administrativa. (CARRION *et al*, 2019)[3]

Ocorre que como as práticas de privacidade das redes sociais não garantem a segurança completa das informações enviadas a outras empresas, o usuário que conecta sua conta, em sua maioria sem ler os termos de uso, corre o risco de que muitas vezes não sabe, mas seus dados podem ser utilizados para outros fins, pois não são devolvidos mesmo em casos de invasão, ficando armazenados no banco de dados da empresa. (SULZ, 2020)[4]

Diante de crimes contra a integridade dos cidadãos foi criada a Lei Geral de Proteção de Dados (LGPD) para amparar as vítimas buscando meios de inibir as ações dos criminosos cibernéticos.

Além das redes sociais serem alvo de furto de dados, aplicativos que não possuem garantias para proteger os dados de seus usuários também enfrentam esse problema. Isso acontece como um sistema compartilhado, onde não apenas o próprio usuário está em risco, mas também toda a sua rede

[3]https://www.revistas.udesc.br/index.php/hfd/article/view/2316796308152019049
[4]https://rockcontent.com/br/blog/tudo-sobre-redes-sociais/

de amigos, todos comprometidos involuntariamente (ADVOGADOS, 2021)[5]. Uma pesquisa recente do *Massachusetts Institute of Technology* ("MIT") publicada no *Journal of Data and Information Quality* da ACM *(Association for Computing Machinery)* todos os dias, milhões de dados são expostos na internet. Sendo impossível manter a privacidade nas redes, mas não é a menor preocupação para as empresas informar as pessoas que usam a rede e compartilham suas informações que não estarão seguros quando suas informações pessoais estiverem nas mãos de alguém.

É necessário compreender que além de hackers mal-intencionados, também pode ser atribuído aos vazamentos de dados casos de falhas em sistemas e outros problemas internos de uma empesa, podendo ocasionar transtornos sociais aos usuários quanto ao desempenho da própria instituição em alcançar os objetivos de satisfazer seus clientes. (LIMA, 2020)[6].

O objetivo desse trabalho é avaliar as hipóteses de vazamento de dados pessoais na internet, e mostrar as maneiras de se prevenir e agir diante de um caso, explorando o objetivo geral é necessário especificar outros aspectos como: Verificar os dados mais vazado; Apresentar os riscos de se ter um dado vazado; Abordar as principais maneiras de acontecer um vazamento e propor soluções para aumentar a segurança das empresas e de pessoas físicas.

1. Revisão da literatura

Um vazamento de dados ocorre quando uma ação é arquitetada por criminosos, que consiste em sequestrar informações confidenciais de pessoas físicas ou jurídicas que são expostas sem a sua autorização. CPF, e-mail, endereço, fotos, telefone, senhas diversas e dados sigilosos são apenas alguns tipos de dados que podem ser expostos na Internet (ORTIZ, 2022)[7]. Um ponto importante para entender sobre vazamento de dados é que ocorrem ocasiões

[5] https://vocesa-abril-com-br.cdn.ampproject.org/v/s/vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/amp/?amp_gsa=1&amp_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_ct=1668130347318&amp_tf=De%20%251%24s&aoh=16681303419216&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Fvocesa.abril.com.br%2Fsociedade%2Fvazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit%2F

[6] https://tecnoblog.net/responde/o-que-fazer-em-caso-de-vazamento-de-dados-pessoais/>

[7] https://www.serasa.com.br/premium/blog/vazamento-de-dados-como-prevenir/

em que eles são consequências de ataques cibernéticos a empresas que mantém dados de seus clientes.

Com a ampliação intensa do número de usuários no meio digital, a internet somente beneficiou os crimes cibernéticos e o furto de proeminentes volumes de dados. Usuários de todo o mundo disponibilizam seus dados a todo momento para os mais diversos sites e entidades. Mesmo sendo para interações em mídias digitais, compras on-line e até transações bancárias.

Sob outra perspectiva, também há episódios em que as aplicações de segurança utilizadas na companhia são inapropriadas, o que facilita o acesso impróprio de criminosos a informações de outros. Os principais motivos de exposição não são unicamente dos ataques cibernéticos como *ransomware*[8], *spyware*[9], *phishing*[10], *malware*[11], etc, mas também falhas comuns de configurações de segurança que poderiam ser aperfeiçoadas, evitando, assim, enormes danos de reputação e desvantagens financeiras para as empresas vazadas. Distintas causas podem incluir insatisfação, erros sem pretensão e mal-intencionamento de funcionários, falta de experiência técnica ou habilidade para guardar os dados ou o ambiente.

O crime cibernético em acontecimentos mais graves, é feito em bando. Na ordem jurídica e sistema jurídico do Brasil, existem insuficientes regras que presidem os delitos virtuais. Uma das primeiras leis feitas, é a Lei nº12.735/2012, conhecida como “Lei Carolina Dieckmann”, feita após a exposição de fotos e conversas pessoais da atriz em seu computador particular. Sucessivamente foi reconhecida em 2018 uma lei que se propõe a amparar os internautas da infração e dar autonomia às pessoas sobre suas informações pessoais, chamada Lei Geral de Proteção de Dados (LGPD) Lei

[8]Ransomware - é um malware de sequestro de dados, feito com criptografia, ele sequestra os próprios arquivos pessoais da vítima e é cobrado por um resgate para restaurar o acesso a esses arquivos. É cobrado em criptomoedas, tornando quase impossível rastrear os criminosos na prática.

[9]Spyware- Spyware é um software instalado em um computador comum, aplicativo de navegador ou telefone celular sem o seu conhecimento. Por causa disso, o spyware transmite seus dados pessoais confidenciais ao invasor.

[10]Phishing-(pronuncia-se: fishing) é um ataque que tenta roubar seu dinheiro ou sua identidade, permitindo que você revele informações pessoais (como números de cartão de crédito, informações bancárias ou senhas) em um site que finge ser legítimo.

[11]Malware - é a abreviação de "malware" e refere-se a um programa de computador projetado para infectar e danificar o computador de um usuário legítimo de várias maneiras.

nº13.709/2018, a qual exige que instituições acatem uma série de normas para proceder com o compartilhamento de dados dos usuários de maneira mais segura. Nesse sentido, cumpre dizer que dados sensíveis são informações de conteúdo privado, capazes de infringir a intimidade do usuário, envolvendo exposição de origem étnica, dados da ciência da hereditariedade, questões raciais, vida sexual, opinião religiosa, saúde, imagens naturais e honra. (Bisso *et al*, 2019).[12]

Apesar das leis e do tema vazamento de dados serem algo bem discutido há muito tempo nos círculos qualificados, ainda é um assunto muito novo para grande maioria das pessoas e é pouco priorizado por empresas e organizações.

Em contrapartida, destaca-se:

> [..] Dados pessoais vêm sendo coletados em larga escala e tanto as práticas de mercado quanto, cada vez mais, práticas sociais vêm considerando-os como algo que pode ser compartilhado sem grandes cuidados (BELLI, 2021)[13].

Enquanto, no mesmo momento em que, dados das pessoas são coletados de maneira grandiosa, e crescentemente, os atos sociais são olhados como algo que pode ser exposto sem cautelas (BALSAN, 2016)[14].

A IBM (*International Business Machines*) (DATA, 2019)[15] realizou uma pesquisa sobre vazamento de dados das organizações, e de acordo com o resultado, próximo de 80% da pesquisa com as empresas inclui ausência ou furto de informações pessoais dos clientes, o relatório foi realizado com 524 empresas em 17 países, englobando o Brasil. Vale ressaltar, que somente informações pessoais fazem parte da LGPD, portanto, dados que expõem um indivíduo, ou que na ocasião os fatos são ligados, e isso permite detectar o usuário.

---

[12] https://sol.sbc.org.br/index.php/errc/article/view/9230/9133

[13] https://portal.fgv.br/artigos/maior-vazamento-dados-pessoais-historia-brasileira-e-quais-licoes-devemos-aprender

[14]https://unisantacruz.edu.br/v4/download/revista-academica/18/2016-Revista-das-Faculdades-Santa-Cruz-18.pdf

[15] https://dataprivacy.com.br/pesquisas-revelam-informacoes-sobre-protecao-de-dados-no-brasil-e-no-mundo/

Outrossim, podemos citar como exemplo, o mega vazamento de dados de aproximadamente 223 milhões de brasileiros (incluindo brasileiros já falecidos) em janeiro de 2021, dados expostos como CPFs, benefícios do INSS, dados de veículos, entre outros. Essas informações foram colocadas por um criminoso em um fórum on-line específico para venda de informações pessoais. Esse número de CPFs vazados ultrapassa o número da população brasileira, pressupondo, que ao menos algum dado básico de cada cidadão tenha sido vítima do hacker, incluindo pessoas que já morreram. Não existe um detalhamento de dados vazados, por isso é reforçado o cuidado ao liberar informações confidenciais em sites que exigem a necessidade de incluir dados pessoais para acesso.

Vale ressaltar que o vazamento atinge diversos ramos e a sociedade. No ramo alimentício, um acontecimento que chamou bastante atenção foi o da franquia *Ceckers and Rally's,* em que 103 lojas foram atingidas por um programa que furtava informações dos cartões de crédito dos clientes. O detalhe mais importante: o programa estava ativado há três anos sem ser descoberto (KHANDELWAL, 2019)[16].

Já no setor governamental, o acontecimento que ganhou as manchetes, foi o caso da Bulgária. De acordo com relatórios, um *hacker* conseguiu roubar mais de 5 milhões de dados dos cidadãos búlgaros, contando com o fato de ter aproximadamente 7 milhões de pessoas no país (CIMPANU, 2019)[17]. Além disso foram enviados cerca de 110 dados governamentais para meios de comunicações local.

No ramo financeiro, os casos envolvendo as empresas *Mastercard* e *Capital One* é digno de destaque. Dezenas de milhares dos clientes do *Mastercard* que participavam do plano de fidelização *Priceless Specials* da Bélgica e Alemanha, tiveram os seus dados vazados na Internet (GATLAN,

[16]https://thehackernews.com/2019/05/credit-card-checkers-restaurants.html
[17]https://www.zdnet.com/article/hacker-steals-data-of-millions-of-bulgarians-emails-it-to-local-media/

2019)[18]. Agora, na *Capital One*, os dados de mais de 140 milhões de americanos e 6 milhões de canadenses foram disseminados.

Com essas informações, há a possibilidade de observar que nem grandes empresas de tecnologia que possui pessoas especializadas e preparadas para proteger os seus dados consegue escapar de notícias sobre episódios de falha na segurança.

No ano de 2018, no EUA, uma despesa envolvendo vazamento de dados, agregando 654 bilhões de dólares, com a exposição de 2,4 bilhões de dados dos usuários (SECURITY,2018)[19].

Sistemas relacionados à internet apresentam inúmeros riscos, mas a falta de investimento de ativos em segurança e uma manutenção contínua, deixa o sistema vulnerável, abrindo uma porta de oportunidade para os criminosos em diversos tipos de golpes. (ORTIZ,2022)[20]

Segundo o conceito retirado do sítio eletrônico da Universidade Federal de Pelotas/RS – UFPEL:

> [...] Ativos: qualquer coisa que tenha valor para a organização.[...] Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.[...] Segurança da Informação e Comunicações: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (UFPEL, 2022)[21].

Quanto ao tema, as imagens abaixo ilustram bem o assunto:

[18]https://www.bleepingcomputer.com/news/security/mastercard-reports-data-breach-to-german-and-belgian-dpas/
[19]https://www.securitymagazine.com/articles/90320-data-breaches-cost-654-billion-in-2018
[20]https://www.serasa.com.br/premium/blog/vazamento-de-dados-como-prevenir
[21]https://wp.ufpel.edu.br/seginfo/termos-e-definicoes/

Figura 1 - Vulnerabilidade e risco

Fonte: Cert.br (2012). Disponível em: <https://cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 29 out. 2022.

É possível notar, na primeira imagem, que o ativo está justamente relacionado a risco, visto que tem um valor importante na organização (STALLINGS,2015 *apud* LEONEL, 2018, p. 21)[22].

Na segunda imagem, é apresentado os riscos centrais, de ameaças e vulnerabilidade:

Fonte: Cert.br (2012). Disponível em: <https://cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 29 out. 2022.

[22]https://repositorio.utfpr.edu.br/jspui/bitstream/1/17295/1/CT_GESER_X_2018_03.pdf

Apesar de existir diversos tipos de vazamento de dados, essas situações têm motivos variados e podem ocorrer de diferentes formas. *Data Breach* ou vazamento de dados, é identificado com crime cibernético pois se trata de procedimentos que transgridem a integridade das informações pessoais de terceiros e acometem sistemas. É considerado crime quando os dados pessoais ou privados são acedidos por *hackers*, com intenções criminosas, seja para ameaças, golpes, fraude de identidade ou extorsões das vítimas. Casos como de furto de celulares, computadores e demais dispositivos também são classificados como crime cibernético pois os *hackers* também conseguem acesso às informações pessoais dos usuários, ou seja, não ocorrem exclusivamente no âmbito digital. No cenário de cumprimento da lei, as sanções administrativas da LGPD passaram a valer em agosto de 2021. Diversas empresas enfrentam dificuldade em se adequar aos requisitos da LGPD sendo que a lei visa punir com multas e advertências com até 2% do faturamento anual das empresas. Pela inteligência do art. 1º da LGPD, vejamos:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019).

Mesmo que constantemente ocorra o desenvolvimento de tecnologias inovadoras para a segurança nas redes, o vazamento de dados é um problema frequente. Pesquisas mostram que algumas das principais causas de vazamento de dados estão em falhas simples de configuração de segurança que deveriam ser corrigidas, prevenindo assim maiores danos à reputação e supressão financeira nas empresas. (STASSUN, 2012)[23]. A empresa de cibersegurança Syhunt, em um relatório, afirma que mais de 220 milhões de indivíduos foram expostos a danos morais e econômicos, pois tiveram seus dados pessoais comprometidos em 2021. Isso significa que seus dados confidenciais, segredos comerciais, código-fonte, dados de clientes, dados

[23]https://periodicos.ufsc.br/index.php/cadernosdepesquisa/article/view/1984-8951.2012v13n102p153/22679

pessoais e qualquer outra coisa armazenada em sistemas de informação podem ser expostos ou usados como parte de espionagem corporativa. Outrossim, os serviços em nuvem oferecem grandes vantagens para o local, mas trazem novos riscos que podem resultar em violações de segurança por meio de vazamentos de dados. Uma forma conhecida dos vazamentos de dados, é chamada de vazamento de nuvem e o incômodo é gerado quando se tem os dados expostos e não é possível saber quais informações foram acessadas. (ZIMMER, 2022)[24].

Sendo assim, representa que as suas informações sigilosas, a privacidade, dados de clientes, ou qualquer dado armazenado em sistemas de informação pode ser divulgada ou usada de forma ilegal para espionagem. Embora dificilmente detectado, a medida mais cautelosa para aplacar o propínquo risco é inserir gestões de risco para detecção, contendo e alertando em casos de vazamentos, pois quanto mais rápido for descoberto menor será o prejuízo. (GATLAN, 2019)[25].

Vazamento via fornecedores

Mesmo se a empresa utilizar a melhor postura de segurança cibernética internamente, e não gerenciar adequadamente o risco do fornecedor, poderá acabar expondo os dados por meio de violações de segurança. (FGLTDA, 2021)[26]

SQL Injection

A injeção de SQL é um tipo simples de ataque que requer muito pouco conhecimento técnico para ser executado. Ele explora a falta de segurança do site para obter acesso não autorizado ao seu banco de dados. Além de simples, esse ataque também pode ser automatizado. (BELCIC,2020)[27]

[24]https://www.lumiun.com/blog/o-que-fazer-e-o-que-nao-fazer-contra-vazamento-de-dados-por-funcionarios/>
[25]https://www.bleepingcomputer.com/news/security/mastercard-reports-data-breach-to-german-and-belgian-dpas/
[26]https://fgltda.com.br/5-niveis-de-seguranca-cibernetica-na-automacao
[27]https://www.avast.com/pt-br/c-sql-injection

Phishing

Um pouco mais complicado, esse ataque requer engenharia social para manipular as pessoas para obter dados confidenciais. Exemplos típicos são e-mails falsos que parecem reais ou se assemelham a alguns e-mails que você conhece. Este e-mail pode pedir informações, dar crédito ou qualquer outra coisa. Ao clicar em um link em um e-mail, você pode acabar instalando *malware*, *spyware* ou até mesmo sendo direcionado para um login falso em uma página semelhante a uma que você já conhece, fornecendo suas informações confidenciais. (Nelson,2021)[28]

Exploração de Vulnerabilidades

Esse tipo de ataque explora vulnerabilidades ou bugs de *software* para obter acesso não autorizado a um sistema ou a dados. Pesquisadores que desejam publicar um CVE ou criminosos que procuram vulnerabilidades com intenção maliciosa de causar danos a uma empresa. Sistemas operacionais, navegadores e aplicativos populares são alguns dos principais alvos, e existem kits de exploração que permitem que criminosos explorem facilmente vulnerabilidades sem conhecimento técnico. (KASPERSKY,2022)[29]

Ransomware

Ransomware é um *software* fraudulento usado para bloquear dados em computadores e servidores usando alguma forma de criptografia. Os hackers usam esse malware para exigir um resgate pela publicação de informações, geralmente em criptomoedas como *bitcoin.* Quando um computador ou rede é infectado por esse software o *ransomware* bloqueia o acesso ao sistema ou criptografa os dados, assim cibercriminosos podem exigir um resgate de suas vítimas pela divulgação de informações. (KLUSAITĖ,2022)[30]

[28]https://www.avg.com/pt/signal/what-is-social-engineering
[29]https://www.kaspersky.com.br/resource-center/threats/malware-system-vulnerability
[30] https://nordvpn.com/pt-br/blog/o-que-e-ransomware/

Além do fato de as redes sociais serem alvo de roubo de dados, aplicativos que não possuem garantias de proteção dos dados de seus usuários também enfrentam esse problema, como:

Os acontecimentos mostraram que ninguém está protegido o suficiente de invasão virtual, todavia, revela também como reconhecer a falha e tentar melhor o sistema, por exemplo:

A empresa Nitendo, grande desenvolvedora e publicadora japonesa de jogos eletrônicos e consoles, foi bem ágil em descobrir que 160 mil contas haviam sido invadidas e vazadas por hackers. Ao perceber o vazamento, foi comunicado aos usuários afetados para que fosse feito a alteração do login imediatamente, assim, evitando futuros prejuízos e sequestro das contas. Como método de prevenção para o problema, a empresa eliminou a possibilidade de cadastros feitos em sites terceiros ou por contas legado.(GARRETT, 2020)[31]

Em paralelo, ressalta-se que 500 mil contas dos usuários do aplicativo Zoom tiveram as suas contas expostas no fórum da *Dark Web*. As informações continham endereços eletrônicos e senhas de acesso, que foram distribuídos de forma gratuita pelos autores do crime (GARRETT, 2020)[32]. A empresa se pronunciou alegando que as correções do problema estavam sendo feitas, e afirmou que seria improvável as informações de usuários corporativos estarem no meio milhão de contas vazadas. E para provar a autenticidade do vazamento, a empresa usou o site *Bleeping Computer*[33] para avaliar os e-mails e senhas divulgadas.

Já como método de proteção, as empresas como *Adobe, Allianz, Andreessen Horowitz, Ant Group* entre outros, optaram por utilizar o conceito de corrente de blocos mais conhecido como *blockchains*[34], cada um contendo um arquivo e um hash, garantindo que as informações desse bloco de dados

[31]https://www.techtudo.com.br/listas/2020/12/relembre-os-oito-maiores-vazamentos-de-dados-em-2020.ghtml
[32]Ibidem
[33]Bleeping Computer é um site que cobre notícias de tecnologia e oferece ajuda gratuita de informática através de seus fóruns.
[34]Blockchain é a tecnologia que garante a segurança das transações com criptoativos, pois permite rastrear o envio e o recebimento de informações pela internet.

não sejam alteradas. O aglomerado criado incluiu seu hash e o do bloco anterior, criando uma conexão entre os blocos. (Forbes, 2022)[35].

Considerações Finais

Perante os dados apresentados nesse trabalho, verifica-se que é salutar a adoção de certos cuidados no mundo virtual onde há a necessidade das empresas formularem uma política de informações mais transparentes e acessíveis ao usuário. Para esclarecer quando será necessário armazenar dados e qual é o procedimento para solicitar a exclusão desses dados, uma vez que nenhuma das políticas de privacidade analisadas, existe essa informação.

Outro ponto que precisa ser acordado é o grau de consentimento, pois trata das principais etapas do tratamento de dados pessoais do usuário. É essencial saber como as suas informações pessoais serão processas e o impacto do tratamento.

O consentimento do sujeito deve ser óbvio, ou seja, a autorização de compartilhamento de dados deve ser inequívoca, franquiando a empresa o fornecimento das aludidas informações a terceiros, motivo pelo qual a empresa autorizada deve informar de forma objetiva acerca do compartilhamento dos dados, bem como as possíveis consequências.

Não obstante, verificada a possibilidade de vazamento de dados, notadamente no âmbito das empresas, nota-se o empreendimento de esforços para corrigir a falha e blindar a instituição alvo, aperfeiçoando o sistema de segurança, com objetivo de restaurar a confiabilidade perante o mercado.

Como pessoa física, todos estão expostos às práticas acima independentemente de não estarem em um centro de informações vazadas, podendo ser a próxima vítima. Em golpes de vazamento de dados, a melhor solução é ir atrás da informação, verificando e desconfiando de todas as mensagens, ligações ou outras maneiras de contato. Além disso, deve-se optar por ativar a autenticação de dois fatores, reforçar senhas, usar dados

[35]https://forbes.com.br/forbes-money/2022/02/forbes-top-50-blockchain-conheca-as-empresas-bilionarias-que-utilizam-a-tecnologia/

dinâmicos, escolher a biometria para assegurar o aparelho e a sua vida útil. Outra forma de proteção é *liveness detection*, que é o reconhecimento da face (ao vivo), trazendo uma identificação mais segura, dentre outros.

Por mais que exista leis, não há métodos específicos a serem praticados nesse tipo de situação, exceto quando ocorre algum dano verdadeiro, que possa causar prejuízos (como abertura em crediários ou débitos em nome da vítima, por exemplo). Diante disso, cabe um ressarcimento pelos danos sofridos, perquirido judicialmente.

Referências

ADVOCACIA, Galvão. **Vazamento e Roubo de Dados: Como Acontecem e Como se Precaver?**. Brasília, 2022. Disponível em: <https://www.galvaoesilva.com/roubo-de-dados/> Acesso em: 1 11. 2022.

ADVOGADOS, Veirano. **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.** 2021. Disponível em: <https://vocesa-abril-com-br.cdn.ampproject.org/v/s/vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/amp/?amp_gsa=1&_js_v=a9&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_ct=1668130347318&_tf=De%20%251%24s&aoh=16681303419216&referrer=https%3A%2F%2Fwww.google.com&share=https%3A%2F%2Fvocesa.abril.com.br%2Fsociedade%2Fvazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit%2F>. Acesso em: 3 11. 2022.

ALVES, Cássio Bastos. **Segurança da informação vs. engenharia social: como se proteger para não ser mais uma vítima**. 2010. 63f. Artigo (Graduação em Sistemas de Informação) – Coordenação do Curso de Sistemas da Informação, Centro Universitário do Distrito Federal, Brasília, 2010. Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm> Acesso em 06.09.2022.

BELCIC, Ivan. **O que é injeção de SQL e como ela funciona?**. 2020. Disponível em: <https://www.avast.com/pt-br/c-sql-injection>. Acesso em: 8 11. 2022.

BISSO, Rodrigo *et al*. Vazamentos de Dados:Histórico, Impacto Socioeconômico eas Novas Leis de Proteção de Dados.**ANAIS DA ESCOLA REGIONAL DE REDES DE COMPUTADORES (ERRC)**, Porto Alegre, 17, 2019, Alegrete. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, p. 154-159, 2019. Disponível em: 2022.

CARRION, P.; QUARESMA, M. Internet da Coisas (IoT): **Definições e aplicabilidade aos usuários finais.**HumanFactors in Design, Florianópolis, v. 8, n. 15, p. 049-066, 2019. DOI: 10.5965/2316796308152019049. Disponível em: https://www.revistas.udesc.br/index.php/hfd/article/view/2316796308152019049 . Acesso em: 10 nov. 2022.

CARVALHO, WiníciosEduardo. **A INFLUÊNCIA DOS VAZAMENTOS DE DADOS PESSOAIS PARA A CONSTRUÇÃO DA LEGISLAÇÃO ATUAL**. São Paulo, 2020. Disponível em: <https://uniesp.edu.br/sites/_biblioteca/revistas/20201125003402.pdf> Acesso em: 1 11. 2022.

CIMPANU, Catalin. **Hacker steals data ofmillionsofBulgarians, emails it to local media: Sourceofthe data breachappearstobethecountry'sNationalRevenueAgency**, 2019. Disponível em: <https://www.zdnet.com/article/hacker-steals-data-of-millions-of-bulgarians-emails-it-to-local-media/> Acesso em: 1 10. 2022.

FGLTDA, FGLTD. **5 níveis de segurança cibernética na automação**. Belo Horizonte, 2021. Disponível em: <https://fgltda.com.br/5-niveis-de-seguranca-cibernetica-na-automacao/>. Acesso em: 9 11. 2022.

FORBES, Forbe. **Forbes Top 50 Blockchain: conheça as empresas que usam a tecnologia .** 2022. Disponível em: < https://forbes.com.br/forbes-money/2022/02/forbes-top-50-blockchain-conheca-as-empresas-bilionarias-que-utilizam-a-tecnologia/>. Acesso em: 19 10. 2022.

GATLAN, Sergiu. **Mastercard Reports Data Breachto German andBelgianDPAs**, 2019. Disponível em: <https://www.bleepingcomputer.com/news/security/mastercard-reports-data-breach-to-german-and-belgian-dpas/> Acesso em: 9 9. 2022.

https://www.syhunt.com/pt/?n=News.2022

KASPERSKY, Kaspersk. **Exploits e vulnerabilidades.** Disponível em: <https://www.kaspersky.com.br/resource-center/threats/malware-system-vulnerability>. Acesso em: 10 11. 2022.

KHANDELWAL, Swati. **Hackers StoleCustomers' Credit Cards from 103 CheckersandRally'sRestaurants**, 2019. Disponível em: <https://thehackernews.com/2019/05/credit-card-checkers-restaurants.html> Acesso em: 30.10. 2022.

KLUSAITĖ, Laura. **Ransomware: o que é e como se proteger?.** 2022. Disponível em: <https://nordvpn.com/pt-br/blog/o-que-e-ransomware/>. Acesso em: 15 10. 2022.

LIMA, Lucas. **O que fazer em caso de vazamento de dados pessoais?**.São Paulo, 2020. Disponível em: <https://tecnoblog.net/responde/o-que-fazer-em-caso-de-vazamento-de-dados-pessoais/> Acesso em: 20 10. 2022.

NELSON, Brittany. **O que é engenharia social e saiba se você está em risco.** 2021. Disponível em: <https://www.avg.com/pt/signal/what-is-social-engineering>. Acesso em: 08 10. 2022.

ORTIZ, Elaine. **CPF vazado**: quais os riscos e como prevenir o vazamento de dados? São Paulo, 2022. Disponível em: <https://www.serasa.com.br/premium/blog/vazamento-de-dados-como-prevenir/> Acesso em: 02 11. 2022.

PRIVACY, Data. **Proteção de dados e vazamento de informações – IBM**. São Paulo, 2019. Disponível em: <https://dataprivacy.com.br/pesquisas-revelam-informacoes-sobre-protecao-de-dados-no-brasil-e-no-mundo/> Acesso em: 02 11. 2022.

SÁ, Marcelo. **Análise do Impacto da Nova Lei de Proteção de Dados Pessoais nas aplicações de Internet das coisas**: Aplicações mobile do governo. Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdfAcesso em: 15 9. 2022.

SECURITY, Securit. **Data BreachesCost $654 Billion in 2018**. 2019. Disponível em: <https://www.securitymagazine.com/articles/90320-data-breaches-cost-654-billion-in-2018> Acesso em: 29 30. 2022.

SILVA, Hemuryel. **Segurança da informação**: estudo de caso sobre o vazamento de senhas. 2017. 91 f. Monografia de Especialização (Curso de EspecializaçãoSemipresencial em Configuração eGerenciamento de Servidores eEquipamentos de Redes) - Universidade TecnológicaFederal do Paraná, Curitiba, 2018. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/17295/1/CT_GESER_X_2018_03.pdf>. Acesso em: 2 11. 2022.

SILVA, Narjara et al. **Engenharia social nas redes sociais online:** um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. Brasília, 2013. Disponível em: <http://eprints.rclis.org/23215/1/Engenharia%20social%20nas%20redes%20sociais%20online.pdf>. Acesso em: 19 10. 2022.

SOUZA, Diane. BALSAN, Jorge. BASTOS, Eurides. EXPOSIÇÃO DE DADOS NA INTERNET. **Revista das Faculdades Santa Cruz**, Santa Cruz, v. 1, n. 1, p. 87-98, jan./jun.2016. Disponível em: <https://unisantacruz.edu.br/v4/download/revista-academica/18/2016-Revista-das-Faculdades-Santa-Cruz-18.pdf#page=87> Acesso em: 13 10. 2022.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas / WilliamStallings; tradução Daniel Vieira; revisão técnica Paulo Sérgio LicciardiMesseder Barreto, Rafael Misoczki. 6.ed. São Paulo: PearsonEducation do Brasil, 2015. 578 p. <https://www.docdroid.net/BebtXZO/criptografia-e-seguranca-de-redes-6a-ed-2014-pdf#page=5> Acesso em: 15 10. 2022.

STASSUN, Cristian; ASSMANN, Selvino. **Hipermobilidade Estética e Dispositivos de Controle de Circulação:** O Desejo de Ser Notado e Encontrado na Internet. Florianópolis, 2012. Disponível em: <https://periodicos.ufsc.br/index.php/cadernosdepesquisa/article/view/1984-8951.2012v13n102p153/22679> Acesso em: 05 09. 2022.

SULZ, Paulino. **O guia completo de Redes Sociais: saiba tudo sobre as plataformas de mídias sociais!**. 2020. Disponível em: <https://rockcontent.com/br/blog/tudo-sobre-redes-sociais/>. Acesso em: 01 10. 2022.

ZIMMER, Kelvin. **O que fazer e o que não fazer contra vazamento de dados por funcionários**. São Paulo, 2022. Disponível em: <https://www.lumiun.com/blog/o-que-fazer-e-o-que-nao-fazer-contra-vazamento-de-dados-por-funcionarios/> Acesso em: 15 10. 2022.

Faculdade Presidente Antônio Carlos de Teófilo Otoni

FICHA DE ACOMPANHAMENTO INDIVIDUAL DE ORIENTAÇÃO DE TCC

Atividade: Trabalho de Conclusão de Curso – Artigo/Monografia.
Curso: Sistemas de Informação **Período:** 5 **° Semestre:** 2 **° Ano:** 2022
Professor (a): GIOVANNI CAMARGO SILVA
Acadêmico: Dilzimeyre Gonçalves Sander

Tema:	**Assinatura do aluno**
Vazamento de informações online	Dilzimeyre G. Sander

Data(s) do(s) atendimento(s)	Horário(s)
2 de novembro de 2022	20:00
9 de novembro de 2022	19:30
10 de novembro de 2022	07:40
4 de novembro de 2022	19:30

Descrição das orientações:
Analisando o desenvolvimento do artigo e auxiliando na correção da escrita

Considerando a concordância com o trabalho realizado sob minha orientação, **AUTORIZO O DEPÓSITO** do Trabalho de Conclusão de Curso do (a) Acadêmico (a) Dilzimeyre Gonçalves Sander.

Assinatura do Professor

Relatório de Plágio

Resumo

[1,25%] sol.sbc.org.br/index.p…
[0,91%] sol.sbc.org.br/index.p…
[0,20%] hacknotice.com/2019…
[0,20%] oodaloop.com/briefs/…
[0,17%] zdnet.com/article/hac…
[0,16%] itsecuritynews.info/ha…
[0,16%] bleepingcomputer.co…
[0,16%] cyware.com/news/ha…
[0,14%] github.com/ffffffff0x/D…
[0,09%] reddit.com/r/privacy/c…

Arquivo de entrada: Artigo TCC.pdf (4755 termos)

Arquivo encontrado	Qtd. de termos	Termos comuns	Similaridade (%)	
sol.sbc.org.br/index.php/errc/article/download/9230/9133	2856	94	1,25	Visualizar
sol.sbc.org.br/index.php/errc/article/view/9230	651	49	0,91	Visualizar
hacknotice.com/2019/07/16/hacker-steals-data-of-millions-…	747	11	0,20	Visualizar
oodaloop.com/briefs/2019/07/16/hacker-steals-data-of-milli…	528	11	0,20	Visualizar
zdnet.com/article/hacker-steals-data-of-millions-of-bulgaria…	1031	10	0,17	Visualizar
itsecuritynews.info/hacker-steals-data-of-millions-of-bulgari…	2049	11	0,16	Visualizar
bleepingcomputer.com/news/security/mastercard-reports-d…	1177	10	0,16	Visualizar
cyware.com/news/hacker-steals-data-of-millions-of-bulgari…	113	8	0,16	Visualizar
github.com/ffffffff0x/Dork-Admin/blob/master/README.md	7291	17	0,14	Visualizar
reddit.com/r/privacy/comments/cdu6ag/hacker_steals_data…	11731	16	0,09	Visualizar