PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

AMEAÇAS CIBERNÉTICAS EM ASCENSÃO: OS ATAQUES HACKERS NO MUNDO

RISING CYBER THREATS: HACKER ATTACKS IN THE WORLD

Mateus Rodrigues Romano[1], Sandro Roberto Armelin[2]

1- Discente na Faculdade de Tecnologia de Itapira “Ogari de Castro Pacheco”; 2- Docente na Faculdade de Tecnologia de Itapira “Ogari de Castro Pacheco”.

Contato: sandro.armelin@fatec.sp.gov.br

RESUMO

Em uma atualidade onde a tecnologia domina em todos os sentidos e atuações da nossa existência como seres humanos, cresce também a importância de que as organizações desenvolvam proteções e cuidem da segurança não somente caracterizado por cercas ou muros físicos, que protegem o seu bem material, mas sim a proteção do seu espaço virtual, compreendendo suas informações digitais e físicas. A segurança da informação de uma empresa está relacionada com proteção de um conjunto de dados no sentido de preservar o valor que essas informações representam para o negócio da empresa. Com base nesta preocupação, as organizações passaram a investir uma grande parte dos seus lucros em equipamentos e softwares com objetivo de preservar seu negócio, que está passível de sequestro ou roubo de informações, resultando no comprometimento do funcionamento do negócio da empresa. O objetivo desse artigo é abordar através da metodologia de pesquisa bibliográfica, a importante relevância do tema de segurança de dados e, utilizando a história como método de comparação, apresentar possíveis prejuízos que as organizações podem sofrer em seus negócios. Através da discussão de 10 casos divulgados amplamente pela mídia desde 2011, pode-se constatar principalmente o prejuízo financeiro registrados nas organizações. Constatado também na pesquisa para confecção desse artigo que muitos casos não foram divulgados até mesmo por receio da empresa de apresentar uma visão de fragilidade para o mercado, logo, esses casos ficam no anonimato e não aparecem nas pesquisas e impossibilitando obter estatísticas reais. Com os dados comentado nesse artigo pode-se constatar os principais prejuízos para as organizações que tiveram informações roubadas por *hackers*, que além de ter seus dados sigilosos de projetos compartilhado para todo o mundo nas redes, sofrem com indisponibilidade de infraestrutura, e-mails, site, sistemas para os clientes e funcionários, e que todos esses itens impactam diretamente no âmbito financeiro pois toda a organização “trava”. A segurança da informação compreende de uma série de ações que são adotadas estrategicamente para controlar e evitar os riscos de danos ou perda dos dados nas organizações. Baseado em confidencialidade, integridade e disponibilidade das informações, essas práticas sustentam a política de proteção de dados nas empresas. Políticas de segurança devem ser implementadas na organização de forma clara e objetiva, definindo claramente a responsabilidade de cada área e de seus colaboradores na utilização dos recursos tecnológicos. As políticas devem fornecer um

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

enquadramento para a implementação de mecanismos de segurança, definido através de procedimentos de segurança e processos de auditoria.

Palavras-Chave: Proteção. Informação. Segurança.

ABSTRACT

In a current situation where technology dominates in all senses and actions of our existence as human beings, the importance of organizations developing protections and taking care of security is also growing, not only characterized by physical fences or walls, which protect their material goods, but also the protection of their virtual space, including their digital and physical information. The security of a company's information is related to the protection of a set of data in order to preserve the value that this information represents for the company's business. Based on this concern, organizations began to invest a large part of their profits in equipment and software in order to preserve their business, which is subject to kidnapping or theft of information, resulting in compromising the functioning of the company's business. The objective of this article is to approach, through the methodology of bibliographical research, the important relevance of the theme of data security and, using history as a method of comparison, to present possible losses that organizations may suffer in their business. Through the discussion of 10 cases widely publicized by the media since 2011, it can be seen mainly the financial loss registered in the organizations. It was also found in the research for the preparation of this article that many cases were not disclosed even for fear of the company presenting a vision of fragility for the market, so these cases remain anonymous and do not appear in the surveys, making it impossible to obtain real statistics. With the data discussed in this article, it can be seen the main losses for organizations that had information stolen by rackers, who, in addition to having their confidential project data shared worldwide on networks, suffer from unavailability of infrastructure, emails, website, systems for customers and employees, and that all these items directly impact the financial scope because the entire organization “locks”. Information security comprises a series of actions that are strategically adopted to control and avoid the risk of damage or loss of data in organizations. Based on confidentiality, integrity and availability of information, these practices support the data protection policy in companies. Security policies must be implemented in the organization in a clear and objective way, clearly defining the responsibility of each area and its employees in the use of technological resources. Policies should provide a framework for implementing security mechanisms, defined through security procedures and auditing processes.

Keywords: Protection. Information. Security.

INTRODUÇÃO

De acordo com o avanço das tecnologias envolvendo os cenários físicos e virtuais, houve o surgimento de diversas práticas para o âmbito de segurança da informação, essas práticas ajudam as organizações a se protegerem de vazamentos de dados. Os vazamentos podem acontecer tanto internamente quanto externamente, e por isso, faz-se necessário a criação de um padrão contendo orientações e regras que devem ser seguidas para um melhor policiamento quanto ao uso da informação. Afinal, ao mesmo tempo que a empresa atinge um alto patamar de tecnologia implementado, pode ficar exposta, fazendo

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

com que o seu bem mais precioso, a “informação”, navegue neste mundo virtual à mercê de pessoas mal-intencionadas.

Segundo a empresa de antivírus Kaspersky (2022), cybersecurity é o ato de proteger os ativos da empresa, ou seja, servidores, sistemas eletrônicos, redes, e dados contra possíveis ataques maliciosos. Além disso, é importante ressaltar que não se trata apenas de ameaças hackers, mas também de ameaças naturais, como por exemplo, queda de energia.

Dentro deste cenário, foi instituído a Política de Segurança da Informação, que faz parte da Norma Internacional ISO 27000. Trata-se de um conjunto de boas práticas utilizadas para o gerenciamento da segurança da informação, cujo objetivo é garantir a confidencialidade, integridade e disponibilidade.

Segundo Offidani (2023), a Global Data estima um investimento global na cibersegurança de R$1 trilhão de reais até 2025, e apesar desse investimento, o sucesso das empresas ainda não é garantido. Afinal, além de todo esse dinheiro investido, é necessário ter uma governança consolidada dentro da organização, visando sempre a proteção virtual, melhorando os processos e suas operações.

O Fórum Econômico Mundial reafirmou que, aqueles que não elaborarem uma boa governança em segurança cibernética, usando ferramentas e métricas adequadas, serão menos flexíveis e menos sustentáveis. O risco cibernético é o risco de sustentabilidade mais imediato e financeiramente material que as organizações enfrentam atualmente (OFFIDANI, 2023).

Com base nestas informações, mostra-se cada vez mais necessário reforçar a importância do tema abordado. Portanto, o escopo do trabalho trata-se em transparecer o crescimento das ameaças cibernéticas nos últimos anos, além de demonstrar os prejuízos causados e os mecanismos utilizados pelos hackers, tendo- por objetivo geral apresentar casos recentes de empresas que sofreram ataques cibernéticos e suas consequências para os negócios.

REFERENCIAL TEÓRICO

Para verificar as causas e consequências de ataques cibernéticos, é necessário entender os conceitos por trás do assunto. Dessa forma, o trabalho traz as definições referente à Governança de TI, Cibersegurança, Segurança da Informação e Ataques Hackers, além de seus principais tipos, normas e importância. A definição de governança de TI segundo Batalha et al. (2020), trata da especificação dos processos decisórios e do framework de responsabilidade, focando em interessantes comportamentos no emprego da TI. A governança de TI também pode ser descrita como um grupo de procedimentos, normas, políticas e atividades, as quais têm o propósito de compor o setor de tecnologia das empresas. Portanto, com essas ferramentas, torna-se possível a implementação de melhorias nas instituições, principalmente referente à produtividade e serviços técnicos das áreas (LOURENÇO et al., 2022).

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

Segundo o Congresso de Segurança da Informação das Fatec, há três tipos de governanças dentro de uma empresa, sendo elas: governança de corporativa, governança corporativa de TI e governança de TI. Governança corporativa, é também conhecida como governo das sociedades ou das empresas, refere-se ao conjunto de processos, costumes, políticas, leis, regulamentos e instituições que orientam como uma empresa é gerenciada, administrada ou controlada. Implica na avaliação e direcionamento do uso da TI para ofertar suporte à organização bem como monitorar a sua utilização para realização de seus planos. Envolve a metodologia, diretrizes e as políticas de uso da TI dentro da organização (NBR ISO/IEC 38500:2009). Tem como meta, futuramente modelar há área de TI dentro das empresas. É o detalhamento das prescrições e responsabilidades para motivar a TI da empresa referente ao suporte e prolongue os planos e os objetivos da organização (WEILL, ROSS, P8, 2006) (LOURENÇO et al., 2022). Para salientar a importância da governança em TI, alguns guias de melhores práticas foram definidos, alinhando a melhor maneira de aplicação, como por exemplo, o *Information Technology Infrastructure Library (ITIL)* e *Control Objectives for Information and Related Technologies (COBIT) e* reforça que diversos prejuízos podem ser ocasionados nas empresas caso a governança de TI não esteja de acordo, principalmente danos relacionados à informação, o item mais valioso, e a ameaça da integridade dos dados da instituição. (BRANDÃO et al. 2021).

A Organização Internacional de Padronização, conhecida como International Organization for Standardization (ISO) desenvolve e publica normas internacionais. De acordo com o próprio site da organização, os padrões são como uma fórmula que descreve a melhor maneira de fazer algo e abrangem diversas atividades. ISO/IEC 38500 – Governança de TI é uma norma internacional que trata da governança corporativa de tecnologia da informação. Orienta sobre o uso eficaz e aceitável referente à governança aos condutores de uma organização. ISO/IEC 27002 – Boas práticas para gestão de segurança da informação, está dentro da segurança da informação da família ISO 27000. Designa instruções para iniciar, implementar, melhorar e manter a gestão da segurança da informação (EDITORA ABNT, 2013a, p.1) (LOURENÇO et al., 2022).

ISO 27000

Esta norma discorre os itens abaixo de acordo com a Tabela 1.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

Tabela 1. Norma ISO 27000.

Política de Segurança da Informação	Para começar é de extrema importância a empresa realizar a elaboração de um documento de política de segurança da informação. O Documento necessita a inclusão de diversas diretrizes e estipular uma estrutura para conseguir alcançar seus objetivos. Adicionalmente, incluir outros aspectos para ter a segurança dos dados da empresa mais satisfatório, lembrando sempre de incorporar a alta direção, para esse documento estar sempre alinhado com os objetivos que a empresa quer alcançar.
Organização da Segurança da Informação	A aplicação da Segurança da Informação em uma organização demanda um gerenciamento apropriado. Nesse propósito, é primordial que as tarefas de segurança da informação sejam encaminhadas e administradas por representantes nomeados pela empresa, que terão responsabilidades claramente determinada para preservar as informações vulneráveis. Esse enfoque atesta uma gestão pratica da segurança da informação e colabora para a blindagem dos registros da organização.
Gestão de ativos	Para ficar em conformidade com as normas e diretrizes da Segurança da Informação, considera-se como um ativo itens adquiridos pela empresa que tem valor e requer conservação. Deve-se categorizá-los, identificá-los, para ser criado um registro e preservar a sua integridade ao longo do tempo. É necessário documentar e estabelecer diretrizes para uniformizar a autorização e utilização dos ativos.
Segurança em recursos humanos	O intuito desta divisão é mitigar a possibilidade de dolo, furto ou má administração dos ativos. Para realizar o ingresso de novos colaboradores ou fornecedores é significativo que ele seja adequadamente avaliado, primordialmente se for tratar de dados confidenciais. Os funcionários devem estar conscientes das ameaças pertinentes à segurança da informação, seus encargos e compromissos.
Segurança física e do ambiente	Nesta etapa faz-se necessário a implementação de ambientes resguardados, controle de acesso e medidas de proteção contra perigos físicos e ambientais, para certificar-se da segurança das instalações e equipamentos sensíveis de processamento de informações.
Segurança das operações e comunicações	É importante que o planejamento para reduzir o risco de falhas, gerenciamento de serviços terceirizados, criação diretrizes para efetivação de backups de segurança e sua restauração e administração a proteção de redes e comunicações internas estejam em comum acordo com as obrigações e protocolos pela operação e gestão de todos os equipamentos que processam as informações.
Controle de acesso	A organização precisa sempre saber quem está tendo acesso as suas informações e essencialmente garantir que apenas pessoas autorizadas tenham acesso, evitando assim perdas de arquivos e recursos da organização. Sempre obter um controle no acesso as informações com base nos requisitos de negócio e na segurança da informação.

Fonte: Lourenço et al., (2022)

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

Conforme descrito por Ribeiro et al. (2020), cibersegurança trata-se de uma fração da segurança da informação, conceito que abrange a proteção das informações no ciberespaço, evitando o vazamento de dados. Dessa forma, estratégias são necessárias para gerenciar os potenciais riscos referente à segurança das informações (NUNES, 2012). A *International Telecommunications Union – ITU* define cibersegurança como um conjunto de guias, ferramentas, enfoques na gestão de risco, boas práticas e tecnologias de proteção de ativos organizacionais e usuários do ambiente virtual (ITU, 2009) (RIBEIRO et al., 2020).

Tereso et al., (2021) identifica cibersegurança como a atividade em proteção de sistemas e redes à ataques virtuais. Estas ameaças são realizadas com o objetivo de roubar informações privilegiadas ou alterá-las, podendo resultar na interrupção das atividades da empresa ou a exposição de dados confidenciais para possíveis interessados, como empresas concorrentes.

(FORNASIER, 2020 apud AKHILESH; MÖLLER, 2020), evidencia a importância da cibersegurança, pois a tecnologia está crescendo diariamente e abrange diversas possibilidades para ser utilizada e modificada pelos seres humanos. Os crimes virtuais movimentam grandes quantidades de dinheiro no mundo, podendo ser a fonte de renda de inúmeros criminosos, os quais se aprimoram para realização dessas infrações. Portanto, faz-se necessário o investimento nesta área para que seja monitorada e não haja o crescimento de crimes e violações no universo virtual (FORNASIER et al., 2020).

Segue abaixo uma tabela com os principais tipos de ataques virtuais, com base no documento de Boas Práticas de Cibersegurança em Teletrabalho, elaborado pelo CNCS (ANDRADE, et al., 2020) (TERESO et al., 2021).

Tabela 2 – Principais tipos de ataque virtuais.

Ciberespionagem	Baseia no roubo de informações comerciais e privilegiadas e seu foco são instituições políticas.
Malvertising	Atua através de publicidades online, buscam que o usuário clique na propaganda e seja direcionado para páginas maliciosas, as quais instalam um malware e podem realizar clones dos dados da pessoa.
Phishing	Consiste no envio de e-mails com links ou anexos maliciosos com o direcionamento para páginas suspeitas, para induzir usuários a inserir dados pessoais e posterior chantagens.
WannaCry	Trata-se do vírus *ransomware*, onde o ataque consiste no bloqueio de acesso do usuário à sua máquina. Usualmente está seguido de um pedido de resgate em criptomoedas para liberação do acesso.

Fonte: Tereso et al., (2021)

Segurança da Informação trata-se da proteção dos perigos relacionados à informação, com o foco na diminuição dessas ameaças e riscos. Relata também sobre a diferença entre Segurança e Segurança da Informação (SI). Sendo que em Segurança da Informação, trabalha-se com um ativo específico, a informação. São ativos que geram,

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

processam, manipulam, transmitem e armazenam informações, além das informações em si (CONSELHO NACIONAL DE JUSTIÇA, 2021). A Segurança da Informação (SI) é baseada em três pilares fundamentais, os quais são: confidencialidade, integridade e disponibilidade. Confidencialidade se resume em sigilo, onde é necessário proteger as informações e permitir que somente as pessoas autorizadas tenham acesso a elas. A integridade está relacionada ao ato de manter as informações em seu formato original, com o foco em protegê-las de qualquer alteração acidental ou intencional. Disponibilidade - existem situações acidentais ou intencionais que podem interferir no acesso às informações que são disponíveis aos usuários, os quais as acessam sempre que precisam e no momento que precisam (CONSELHO NACIONAL DE JUSTIÇA, 2021).

Os ativos de uma organização, significa tudo aquilo que possui valor e demanda proteção dentro de uma empresa. Nas organizações, encontra-se diversos tipos de ativos, os quais podem ser classificados de diferentes maneiras e muitas vezes são divididos de acordo com semelhantes características referente às necessidades, estratégicas e ferramentas de proteção. Como os ativos possuem particularidades, abordagens específicas devem ser utilizadas de acordo com suas necessidades de segurança. Proteção é nome da medida focada em evitar prejuízos aos ativos (SENA et al., 2022).

Feitosa et al., (2017, P. 1-3) descreve ataques cibernéticos como algo ofensivo e defensivo, destinado a explorar ou danificar informações digitais e até mesmo bloquear o acesso às suas informações. Silva et al., (2020) menciona que o termo ataque cibernético ainda não é bem definido entre os países. O governo dos EUA define ataques cibernéticos como atividade cibernética maliciosa, já o Ministério da Defesa do Brasil trata como ataque cibernético quaisquer “ações que objetivam interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL, 2014a, p. 23).

Ransomware é um *software* danoso que infecta os arquivos armazenados em um computador, geralmente através de sites ou links maliciosos, fazendo com que sejam criptografados, além da exigência de resgate, usualmente com pagamentos em Bitcoin. Distributed Denial of Service (DDoS) trata-se de uma “negação de serviço”. Ocorre através da infecção de dispositivos com malware para torná-los um *bot*. São controlados para fazer solicitações repetidas a um determinado servidor, afastando os usuários normais. Spear-phishing são golpes onde o criminoso convence o destinatário do e-mail a realizar download de algum malware ou o obriga a fornecer informações confidenciais, se passando por uma fonte confiável. São eficazes e podem ser feitos sob medida para determinados alvos (LOUREIRO, 2022).

METODOLOGIA

De acordo com Mendes, Silveira e Galvão (2008), a pesquisa bibliográfica integrativa trata-se de um método de pesquisa que investiga trabalhos relevantes para apoiar decisões e melhorar a prática. Permite compactar o conhecimento sobre um assunto e identificar

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

déficits que precisam de novos estudos. É valioso para facilitar a obtenção de conclusões gerais em áreas de estudo com grande volume de conhecimento científico. Isso é especialmente útil quando os profissionais têm pouco tempo para ler todas as pesquisas disponíveis e enfrentam dificuldades na análise crítica dos estudos. Diferentes autores empregam formas distintas no processo de elaboração da revisão integrativa, que se encontra bem definida na literatura. Para a construção da revisão integrativa, no geral, precisa-se percorrer seis etapas diferentes, vamos percorrer os passos realizados utilizando o presente artigo.

Na primeira etapa consiste em identificar o tema e selecionar a hipótese ou questão de pesquisa para a elaboração da revisão integrativa, o processo de construção da revisão integrativa se inicia com a definição de um problema e a formulação de uma hipótese ou questão de pesquisa pertinente. Portanto, optar por um tema de interesse torna o processo mais estimulante. Essa etapa é considerada essencial para redigir uma revisão integrativa bem estruturada. O tema deve ser definido de forma transparente e específica, permitindo uma análise focada e completa. Após o autor estabelecer a questão de pesquisa, os descritores e palavras-chave, a busca dos estudos acaba sendo reconhecida com tranquilidade. Delimitação de parâmetros para a segunda etapa, a inserção e exceção de estudos/amostragem ou busca na literatura e na terceira etapa a definição das informações a serem extraídas dos estudos optados/organizados dos estudos. À princípio, o trabalho foi realizado através de pesquisa bibliográfica integrativa e teve início a partir de buscas por artigos no google acadêmico, exemplares físicos de livros em biblioteca, artigos, periódicos, a partir de 2019 até publicação deste artigo, com as palavras-chave: governança, cibersegurança, segura da informação, ataques cibernéticos, ataques *hackers,* ciberataques. Para a quarta etapa do processo é feita uma avaliação dos estudos incorporados a revisão integrativa que a partir da seleção dos estudos, realizou-se a leitura, análise e resumo das informações, elegendo os trechos relevantes para a composição do trabalho. A quinta etapa diz respeito a análise e interpretação dos resultados, onde foi adicionado as empresas alvas de ataques nos últimos 12 anos, uma tabela foi elaborada com as principais informações dos ocorridos, para demonstração da frequência dos acontecidos, os prejuízos causados e os tipos de vírus mais utilizados, que diariamente causam grandes estragos nas empresas e deixa-as vulneráveis a ponto de acabar precisando fechar suas portas. Sexta etapa revisa e consolida a apresentação e síntese do conhecimento (MENDES; SILVEIRA; GALVÃO, 2008).

RESULTADOS E DISCUSSÃO

Com base nas informações apresentadas, a tabela 3 abaixo aborda 10 ataques cibernéticos em grandes empresas no mundo, acontecidos desde 2011 e principalmente em 2021, ano em que o Brasil atingiu a posição de 5º país que mais sofreu crimes cibernéticos, com 9,1 milhões de ocorrências, somente no primeiro trimestre (SECURITY REPORT, 2022).

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

Tabela 3 - Ataques cibernéticos em grandes empresas

Empresa	Ano	País	Resgate	Responsáveis	Vírus
TJ-RS	2021	Brasil	US$ 5 milhões	Revil	Ransomware
Renner	2021	Brasil	US$ 1 bilhão de dólares	Não localizado	Ransomware
CVC Corp	2021	Brasil	Não localizado	Não localizado	Ransomware
Ministério da Saúde	2021	Brasil	Não localizado	Lapsu$ Group	Ransomware
Poly Network	2021	China	US$ 500.000	Mr. White Hat	Falha de segurança na plataforma
Kaseya	2021	Estados Unidos	US$ 70 milhões	Revil	Ransomware
JBS	2021	EUA, Canadá e Austrália	US$11 milhões	Revil (Sodinokibi)	Ransomware
Dyn	2016	Países da América do Norte e Europa	5 bitcoins (cerca de R$ 11 mil)	Não localizado	DDoS
Yahoo	2013 e 2014	Estados Unidos	Não localizado	Karim Baratov	Não localizado
Epsilon	2011	Estados Unidos	Não localizado	Não localizado	Spear-phishing

Fonte: Elaborada pelo autor.

Em abril de 2021, o Tribunal de Justiça do Rio Grande do Sul foi alvo de um ataque de *ransomware*, deixando os funcionários sem acesso ao sistema e até mesmo sem conseguir ligar o computador. Para que as operações não parassem completamente, os funcionários utilizaram WhatsApp e e-mails de entidades parceiras (IT FORUM, 2021). Segundo o delegado André Anicet, da Delegacia de Repressão aos Crimes Informáticos, do Departamento Estadual de Investigações Criminais (Deic), equipamentos eletrônicos foram apreendidos na casa de uma pessoa para investigação. O jornal digital ainda apurou que as buscas ocorreram na residência de um servidor do próprio Judiciário, em Porto Alegre, que trabalha no setor de informática da corte (GZH, 2021). Ainda em 2021, no mês de agosto, a Renner afirmou ter sido vítima de um ataque cibernético criminoso, gerando indisponibilidade em seus sistemas. Logo iniciaram seus protocolos de controle e segurança para deter ao ataque e seus possíveis danos (IT Forum, 2021). As operações foram normalizadas dois dias depois e o site de compras voltou a funcionar (ÉPOCA NEGÓCIOS, 2021).

A CVC anunciou em seu site, no mês de outubro de 2021: “A CVC Corp informa que foi vítima de um ataque cibernético”. Tratava-se de um ataque de ransomware e informações sobre o resgate não foram divulgadas (IT FORUM, 2021). De acordo com

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

matéria publicada pela revista Época Negócios (2021), a central de atendimento da companhia ficou indisponível e o site fora do ar. Entretanto, o embarque de clientes com viagens marcadas e as reservas confirmadas não foram impactados, segundo comunicado do grupo. O ConecteSUS, aplicativo que disponibiliza o Certificado Nacional de Vacinação Covid-19, e o site do Ministério da Saúde, foram atacados por hackers, na madrugada do dia 10 de dezembro de 2021. Os dados sobre a vacina ficaram indisponíveis por vários dias. Segundo o Forum, "o e-SUS Notifica, que recebe notificações dos estados e cidades sobre a síndrome gripal suspeita e confirmada de covid-19; e o Programa Nacional de Imunização (SI-PNI) também foram afetados." (IT FORUM, 2021). Um dia depois, no domingo, os registros de vacinação foram recuperados, sem perdas (ÉPOCA NEGÓCIOS, 2021).

A Poly Networks, empresa fundada pelo empresário chinês Da Hongfei em 2020, é uma prestadora de serviços financeiros descentralizados (Decentralized Finance [DeFi]). Funciona como um banco de criptomoeda, oferecendo serviços desvinculados às regulações governamentais (THE HACK, 2021). Em 2021, no mês de agosto, aconteceu um dos maiores roubos de criptomoedas da história, em agosto de 2021. Criminosos roubaram cerca de US$ 600 milhões (R$ 3,1 bilhões) da plataforma Poly Network, os hackers exploraram uma vulnerabilidade em seu sistema. Posteriormente, ocorreu um diálogo entre os criminosos e a empresa, e após apelo da Poly Network, devolveram quase todos os fundos. Além disso, divulgaram em um site que roubaram para mostrar as falhas de segurança na plataforma. O hacker foi convidado para ser conselheiro de segurança da empresa (ÉPOCA NEGÓCIOS, 2021).

A empresa de tecnologia da informação com sede em Miami, Kaseya, foi atacada em julho de 2021, pouco antes do fim de semana prolongado do Dia da Independência nos Estados Unidos. O G1 (2021) informou "De acordo com a Kaseya, menos de 40 clientes foram afetados, mas alguns deles também têm outros clientes, e o ataque pode ter se espalhado para centenas ou até milhares deles." O ataque a JBS aconteceu no dia 30 de maio de 2021 e a empresa recuperou os acessos 4 dias depois, em 3 de junho (ÉPOCA NEGÓCIOS, 2021). De acordo com a revista Exame (2021), "o frigorífico JBS confirmou ao *The Wall Street Journal* nesta quarta-feira, 9, que pagou 11 milhões de dólares aos hackers que atacaram os sistemas da empresa no Estados Unidos e na Austrália no final de maio."

Epsilon, uma empresa de e-mail marketing, teve seus dados de endereços de e-mail roubados em 2011 por hackers, tratava-se de uma das violações de dados de maior alcance de todos os tempos. Os hackers roubaram uma lista imensa de e-mails e conseguiram contato com os usuários, resultando em um impacto gigantesco (LOUREIRO, 2022). Segundo o G1 (2011), "a empresa de marketing Epsilon sofreu há duas semanas um vazamento de dados que pode ser o maior de história. Pela lei dos EUA, empresas devem avisar clientes sobre dados roubados." Yahoo foi vítima de ataque hacker em dois anos seguidos, 2013 e 2014, resultando na exposição de 3 bilhões de contas de usuário. As informações roubadas foram colocadas à venda e tratava-se de nomes completos, endereços de e-mail, datas de nascimento e números de telefone (LOUREIRO, 2022). A

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

revista Exame (2017) informou: “O ciberataque de 2013 à gigante online Yahoo afetou todas as três bilhões de contas da empresa, disse, nesta terça-feira (3), a Verizon, que adquiriu os ativos online da Yahoo no começo deste ano, após uma nova análise sobre o incidente.”

Dyn, empresa responsável por grande parte do sistema de nomes de domínio (DNS) da Internet e de infraestrutura, foi alvo de uma série de ataques distribuídos de negação de serviço (DDoS) em 2016 (LOUREIRO, 2022). A empresa possui diversos clientes e a lista de afetados era imensa, com mais de 60 sites: PayPal, GitHub, Pinterest, Reddit, Netflix, Disqus e Box, além das páginas dos veículos *CNN* e *New York Times* (TECNOBLOG, 2016).

CONCLUSÃO

A importância de as organizações investirem em segurança de dados contra hackers é indiscutível e essencial nos tempos atuais, em que a tecnologia desempenha um papel fundamental em quase todas as áreas dos negócios. A partir das pesquisas realizadas neste artigo, foi possível apurar a importância deste tema para os dias atuas. É notório a relevância do assunto entre as organizações, que ultimamente estão investindo em profissionais e equipamentos de segurança com propósito de proteger o seu negócio. Apresentamos ao longo desse artigo 10 casos de empresas que nos últimos 10 anos sofreram algum tipo de ataque de cibernético. Esses casos foram constatados através de serem divulgados amplamente pela mídia nacional. Com a avaliação esses casos podemos chegar em algumas conclusões fundamentais como a proteção de dados dos clientes, preservação e prevenção de perdas financeiras, manutenção e preservação da marca, preservação da espionagem industrial, indisponibilidade de recursos para atender aos clientes, furto de criptomoeda, dados das empresas criptografadas, recursos digais sem possibilidade de utilização pelos colaboradores.

Essas organizações apresentadas lidam com uma grande quantidade de informações confidenciais de clientes, incluindo dados pessoais e financeiros. A segurança robusta é crucial para proteger esses dados contra acesso não autorizado e garantir a confiança dos clientes na empresa. As violações de segurança podem levar a sérias consequências financeiras, desde perdas de receitas até penalidades regulatórias e ações judiciais. Investir em segurança reduz o risco de violações e os custos associados a elas. Uma violação de segurança pode causar um dano significativo à reputação da marca. A confiança dos clientes e parceiros comerciais pode ser abalada, levando a perda de negócios e oportunidades futuras. Empresas podem ser alvo de hackers que visam roubar informações confidenciais, como projetos, estratégias de negócios e propriedade intelectual. Investir em segurança de dados ajuda a proteger esses ativos valiosos.

Os prejuízos aos negócios de uma companhia são imensuráveis após um ataque cibernético, a segurança de dados é uma responsabilidade primordial das organizações que prezam por garantir a proteção de seus clientes, a integridade de suas operações e a sustentabilidade de sua reputação. O investimento em medidas de segurança adequadas

DOI: 10.5281/zenodo.10083791 Artigo original

é uma estratégia importante e necessária para proteger-se contra as crescentes ameaças cibernéticas e manter-se competitivo no mercado atual. Em complemento a todas as conclusões sugere-se a elaboração de um manual de segurança cibernética para as organizações utilizarem como guia, principalmente aquelas que acreditam que esses ataques nunca iram acontecer com elas. Este manual deveria seguir a premissa da prevenção e tendo com guia os históricos de ocorrências.

REFERÊNCIAS

Ataque de 2013 violou todas as 3 bilhões de contas, diz Yahoo. EXAME, 3 de outubro de 2017. Disponível em: <https://exame.com/negocios/ciberataque-ao-yahoo-afetou-as-3-bilhoes-de-contas-da-empresa/>. Acesso em: 09 de maio de 2023.

Brasil foi o 5º país com mais ataques cibernéticos em 2021. Security Report**,** 11 de abril de 2022 Disponível em: <https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em-2021/> Acesso em: 09 maio de 2023.

BATALHA, Victor Barreto. **Análise da Conformidade da política de Governança de TI um estudo de caso ANATEL**. 2020. 56 f. TCC (Graduação) - Curso de Engenharia Eletrônica, Faculdade Unb Gama - Fga, Brasília – Df, 2020.

BRANDÃO, Dhyego Silva Domingos. **Diagnóstico do uso de Tecnologia da Informação como Estratégia para Implementação das Práticas de Governança de TI em IES**. 2021. 92 f. Dissertação (Mestrado) - Curso de Poleduc, Universidade Federal do Ceará, Fortaleza, 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital.** 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/03/AnexoVManualReferenciaPrevencaoMitigacaoDeAmeacasCiberneticasConfiancaDigitalRevisadoREV.docx.pdf. Acesso em: 30 mar. 2023.

Empresa de marketing vazou dados sobre consumo de medicamentos. G1, 18 de abril de 2011. Disponível em: <https://g1.globo.com/tecnologia/noticia/2011/04/empresa-de-marketing-vazou-dados-sobre-consumo-de-medicamentos.html>. Acesso em: 09 de maio de 2023.

FEITOSA, Caio Vinícius Cesar. **Ataques Cibernéticos: Estudo do Caso STUXNET.** Repositório UFF Institucional, Niterói, 2017.

FORNASIER, M. O.; SPINATO, T. P.; RIBEIRO, F. L. **Ransomware e cibersegurança: a informação ameaçada por ataques a dados**. Revista Thesis Juris, [S.L.], v. 9, n. 1, p. 208-236, 23 jun. 2020. University Nove de Julho. http://dx.doi.org/10.5585/rtj.v9i1.16739.

PROSPECTUS
ISSN 2674-8576

DOI: 10.5281/zenodo.10083791 Artigo original

HIGA, Paulo. **Uma série de ataques DDoS está quebrando a internet hoje**. Tecnoblog, 21 de outubro de 2016. Acesso em: <https://tecnoblog.net/noticias/2016/10/21/ddos-dyn-ferrou-internet/>. Acesso em 11 de maio de 2023.

JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. G1, 09 de junho de 2021. Disponível em: <https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml>. Acesso em: 09 de maio de 2023.

KASPERSKY. **O que é cibersegurança?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security. Acesso em: 30 maio 2023.

LOUREIRO, Vitoria. **Curiosidade: conheça os 5 maiores ataques cibernéticos da história**. Nova8. Barueri, 12 de julho de 2022.

LOURENÇO, F. A.; BARNABÉ, L. A.; OLIVEIRA, W. **A Área de Governança de T.I: Suas Diretrizes e Processos.** 2022. 18 f. Dissertação (Mestrado) - Curso de Congresso de Segurança da Informação das Fatec, Fatec Araraquara, Araraquara, 2022. Cap. 2.

LAVADO, Thiago. **JBS pagou US$ 11 milhões em resgate a autores de ataque ransomware**. EXAME, 9 de junho de 2021.

MATOS, Eduardo. **Computadores de servidor e de juíza podem ter sido porta de entrada de ataque hacker aos sistemas do TJ-RS**. GZH, 30 de julho de 2021. Disponível em: <https://gauchazh.clicrbs.com.br/geral/noticia/2021/07/computadores-de-servidor-e-de-juiza-podem-ter-sido-porta-de-entrada-de-ataque-hacker-aos-sistemas-do-tj-rs-ckrpp3vcf00b00193s18l28hs.html>. Acesso em: 09 de maio de 2023.

MENDES, Karina dal Sasso; SILVEIRA, Renata Cristina de Campos Pereira; GALVÃO, Cristina Maria. Revisão integrativa: método de pesquisa para a incorporação de evidências na saúde e na enfermagem. **Texto & Contexto - Enfermagem**, [S.L.], v. 17, n. 4, p. 758-764, dez. 2008. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0104-07072008000400018.

OFFIDANI, Adriana. Abes – Associação Brasileira das Empresas de Software. **ESG: a relação entre governança e cibersegurança**. 2023. Disponível em: https://abes.com.br/esg-a-relacao-entre-governanca-e-ciberseguranca/. Acesso em: 30 maio 2023.

Os maiores ataques hackers de 2021. Época Negócios, 28 de dezembro 2021. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2021/12/os-maiores-ataques-hackers-de-2021.html>. Acesso em: 10 de maio de 2023.

PETRY, Guilherme. **TJ-RS é vítima do ransomware REvil. Gangue pede U$ 5 milhões pelo resgate**. The Hack, 2021. Disponível em: <https://thehack.com.br/tj-rs-e-vitima-do-ransomware-revil-gangue-pede-u-5-milhoes-pelo-resgate/>. Acesso em 08 de maio de 2023.

PETRY, Guilherme. **O Grande Assalto (de criptomoedas): a história do roubo de U$ 611 milhões da Poly Network**. The Hack, 2021. Disponível em: <https://thehack.com.br/o-grande-assalto-de-criptomoedas-a-historia-do-roubo-de-us-611-milhoes-da-poly-network/>. Acesso em: 08 de maio de 2023.

RIBEIRO, Ramiro et al. **Cibersegurança e Segurança da Informação Contábil: Uma Análise da Percepção do Profissional Contábil.** Ragc, Monte Carmelo, v. 8, n. 32, p. 71-85, 20 abr. 2020.

SILVA, W. R.; NOGUEIRA, J. M. **Ataques Cibernéticos e Medidas Governamentais para Combatê-los.** O Comunicante, v. 9 n. 1 (2019).

TERESO, Marco; PRATAS, António. **Cibersegurança e teletrabalho: Um mundo de oportunidades de riscos.** 2021. 11 f. Dissertação (Mestrado) - Curso de Encontro Científico da Unidade de Investigação & Desenvolvimento, Escola Politécnica em Santarém, Portugal, Instituto Superior de Gestão e Administração, Isla Santarém - Portugal, 2021.

WEILL, Peter; ROSS, J. W. **Governança de TI**. São Paulo, M. Books: 2006. Cap 1

SENA, J. W. P; DE OLIVEIRA, P. F. A. Política de segurança da informação nas organizações de saúde. **Recisatec - Revista Científica Saúde e Tecnologia** - ISSN 2763-8405, [S. l.], v. 2, n. 7, p. e27149, 2022. DOI: 10.53612/recisatec.v2i7.149. Disponível em: https://recisatec.com.br/index.php/recisatec/article/view/149. Acesso em: 11 maio. 2023.

6 ataques cibernéticos que abalaram o Brasil em 2021. **IT Forum**, 27 de dezembro de 2021. Disponível em: <https://itforum.com.br/noticias/06-ataques-ciberneticos-que-abalaram-o-brasil-em-2021/>. Acesso em: 09 de maio de 2023.