COIMBRA
BUSINESS
SCHOOL
iscac
100 ANOS
Politécnico de Coimbra

COIMBRA BUSINESS SCHOOL | iscac Politécnico de Coimbra | 100 anos | since 1924

Ataques informáticos: divulgações nos relatórios empresariais

ISCAC | 2024 Susana Paula Nunes de Matos

COIMBRA
BUSINESS
SCHOOL
iscac
100 ANOS
Politécnico de Coimbra

Susana Paula Nunes de Matos

Ataques informáticos: divulgações nos relatórios empresariais

Coimbra, outubro de 2024

Susana Paula Nunes de Matos

Ataques informáticos:
divulgações nos relatórios empresariais

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Contabilidade e Fiscalidade Empresarial**, realizada sob a orientação da Professora Doutora Isabel Maria Mendes Pedrosa e coorientação do Professor Doutor Armando Dias Ramos e do Professor Doutor Carlos Miguel Dias Barros.

Coimbra, outubro de 2024

TERMO DE RESPONSABILIDADE

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de Ensino Superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

AGRADECIMENTOS

Quero expressar a minha profunda gratidão a todos os que contribuíram para a realização desta dissertação.

Em primeiro lugar, gostaria de agradecer à minha orientadora, Professora Doutora Isabel Maria Mendes Pedrosa e coorientadores, Professor Doutor Armando Dias Ramos e Professor Doutor Carlos Miguel Dias Barros pela orientação, sabedoria e sugestões valiosas durante todo este ano que dediquei a esta dissertação de mestrado. A vossa experiência e dedicação foram cruciais para o desenvolvimento deste trabalho e para o meu crescimento académico.

Agradeço à minha filha, cujo amor foi uma fonte constante de motivação e resiliência ao longo deste percurso. A sua compreensão pela minha ausência foi fundamental para que eu pudesse dedicar o tempo necessário a este trabalho.

E aos meus pais, agradeço por sempre acreditarem em mim. O vosso encorajamento e apoio inabalável foram essenciais, para que eu pudesse alcançar este objetivo.

A todos, o meu sincero obrigado.

RESUMO

O crescente aumento da utilização das tecnologias veio facilitar muito as atividades laborais, promovendo a otimização dos processos, a rapidez e a eficiência da execução dos trabalhos. No entanto, a era digital com a utilização massiva da *internet* e a possibilidade de armazenamento em *cloud*, onde facilmente se pode aceder à informação de onde quer que se esteja, trouxeram consigo aliados aos prós, alguns contras também. Um desses contras é a facilidade de acesso de forma indevida.

Com este trabalho pretende-se abordar a temática da segurança informática no contexto empresarial. Abordando os diferentes tipos de ataques informáticos, tais como *ransomware*, *phishing*, e ataques de negação de serviço (DoS, *Denial of Service*), explorando o impacto destas ameaças nas organizações portuguesas. A metodologia utilizada foi a Revisão Sistemática da Literatura com PRISMA 2020, permitindo a análise e síntese de estudos relevantes sobre o tema. Este trabalho incluiu a análise de relatórios de algumas empresas vítimas de ataques informáticos, com foco em palavras-chave relacionadas com segurança informática. Este trabalho permitiu constatar que a segurança informática é um desafio crescente para as empresas, evidenciando a necessidade de estratégias robustas de proteção e consciencialização, uma vez que os ataques informáticos, têm um impacto significativo na integridade e na continuidade dos negócios. Além disso, a análise dos relatórios empresariais revelou que muitas organizações ainda subestimam a importância de divulgar informações sobre incidentes de segurança, o que pode comprometer a confiança dos *stakeholders* e a reputação das próprias empresas.

Os resultados obtidos contribuem para uma compreensão mais aprofundada dos desafios enfrentados pelas empresas em relação à segurança da informação e destacam a importância da proteção contra ameaças informáticas.

Palavras-chave: Crimes informáticos, ataques informáticos, ciber-riscos, cibersegurança, segurança informática.

ABSTRACT

The increasing use of technology has greatly facilitated work activities, promoting the optimisation of processes, speed, and efficiency in the execution of tasks. However, the digital age, characterised by the massive use of the *internet* and cloud storage, where information can be easily accessed from anywhere, has also brought some downsides alongside its advantages. One of these downsides is the ease of improper access.

This work aims to address the theme of cybersecurity in the business context, discussing the different types of cyberattacks, such as *ransomware*, *phishing*, and denial-of-service attacks, while exploring the impact of these threats on portuguese organisations. The methodology used was a Systematic Literature Review with PRISMA 2020, allowing for the analysis and synthesis of relevant studies on the subject. This work included the analysis of reports from several companies that were victims of cyberattacks, focusing on keywords related to cybersecurity. It was possible to conclude thatcybersecurity is an increasing challenge for companies, highlighting the need for robust protection and awareness strategies, as cyberattacks have a significant impact on the integrity and continuity of businesses. Furthermore, the analysis of corporate reports revealed that many organisations still underestimate the importance of disclosing information about security incidents, which can compromise stakeholder trust and the reputation of the companies.

The results obtained contribute to a deeper understanding of the challenges faced by companies regarding information security and highlight the importance of protection against cyber threats.

Keywords: Cybercrime, cyber-attack, cyber risk, cybersecurity, cyber-security.

ÍNDICE GERAL

TERMO DE RESPONSABILIDADE iii

AGRADECIMENTOS v

RESUMO vii

ABSTRACT ix

ÍNDICE GERAL xi

ÍNDICE DE TABELAS xiii

ÍNDICE DE FIGURAS xv

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS xvii

GLOSSÁRIO xxi

Capítulo 1 - INTRODUÇÃO 1

1.1 Enquadramento 1

1.2 Motivação 1

1.3 Objetivos 2

1.4 Metodologia 3

1.5 Contribuições 3

1.6 Estrutura da Dissertação de Mestrado 3

Capítulo 2 - REVISÃO DE LITERATURA 5

2.1 Caracterização do Problema 5

2.2 Ataques informáticos 8

2.3 Tipos mais comuns de ataques informáticos 10

2.3.1 *Ransomware* 10

2.3.2 *Phishing* 12

2.3.3 *Man-in-the-middle* (MitM) 14

2.3.4 *Cross-site scripting attacks* 15

2.3.5 *Cryptojacking* 18

2.3.6 *Denial of Service* (DOS) e *Distributed Denial of Service* (DDoS).....19
2.3.7 DNS *spoofing or "poisoning"*.....20
2.3.8 DNS *tunneling*.....21
2.3.9 Drive-by Download Attacks.....22
2.3.10 *Inside threats*.....23
2.3.11 *Internet of Things (IoT) attacks*.....24
2.3.12 Password attacks.....25
2.3.13 SQL *injection attacks*.....26
2.3.14 Manipulação de URL.....27
2.3.15 *Zero-day exploits and attacks*.....27
2.4 Impacto das ameaças informáticas.....28
2.5 Cibersegurança.....29
2.6 Tendências emergentes das técnicas aplicadas nos ataques informáticos.....35
Capítulo 3 - METODOLOGIA DE INVESTIGAÇÃO.....39
Capítulo 4 - ESTUDO DOCUMENTAL.....41
4.1 Resultados.....41
4.2 Análise e Discussão dos Resultados.....52
Capítulo 5 - CONCLUSÃO.....55
5.1 Principais contributos.....56
5.2 Limitações.....57
5.3 Proposta de trabalhos futuros.....57
REFERÊNCIAS BIBLIOGRÁFICAS.....59

ÍNDICE DE TABELAS

Tabela 1 - Incidentes por tipo registados pelo CERT.PT, 2021 e 2022 - TOP 10 6

Tabela 2 - Incidentes por tipo registados pelo CERT.PT por ano 9

Tabela 3 - Variação de Incidentes por tipo registados pelo CERT.PT entre 2018 e 2023 10

Tabela 4 - Tabela identificativa de ataques.....45

Tabela 5 - Medidas de segurança / cibersegurança implementadas após os ataques informáticos 48

Tabela 6 - Análise dos relatórios período de 2018-2023.....51

ÍNDICE DE FIGURAS

Figura 1 - Esquema de Ransomware.....11
Figura 2 - Esquema de Phishing.....13
Figura 3 - Esquema de ataque MITM.....15
Figura 4 - Esquema de ataque XSS.....16
Figura 5 - Esquema de Cryptojacking.....18
Figura 6 - Esquema de Denial os Service.....19
Figura 7 – Esquema de envenenamento de DNS.....21
Figura 8 - Esquema DNS tunneling.....22
Figura 9 - Esquema Drive-by download.....22
Figura 10 – Ameaças internas.....24
Figura 11 - Esquema ataque IoT.....24
Figura 12 - Esquema de ataque de password.....25
Figura 13 - Esquema de ataque SQL injection.....27
Figura 14 - Esquema de ataque Zero-day exploits.....28
Figura 15 - O ciclo de vida do roubo de credenciais.....32

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

AL - Agência Lusa

AR - Assembleia da República

BCP - Banco Comercial Português

BTC - *Bitcoin*

CEO - *Chief Executive Officer* (Diretor Executivo)

CERT.PT - Equipa de Resposta a Incidentes de Segurança Informática Portuguesa

CML - Câmara Municipal de Loures

CNCS - Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

CSC - Código das Sociedades Comerciais

CSIRT - *Computer Security Incident Response Team* (Equipa de Resposta a Incidentes de Segurança em Sistemas Computacionais)

CSIS - *Centre for Strategic and International Studies* (Centro de Estudos Estratégicos e Internacionais)

CUF - Companhia União Fabril - Grupo José de Mello Saúde

DNS - *Domain Name System* (Sistema de Nomes de Domínio)

DOM - *Document Object Model* (Modelo de Objeto de Documento)

EDA - Eletricidade dos Açores

EDP - Eletricidade de Portugal

EUA - Estados Unidos da América

EUROPOL - Agência da União Europeia para a Cooperação Policial

FC - Fundação Champalimaud

FCP - Futebol Clube do Porto

FTP - *File Transfer Protocol* (Protocolo de transferência de ficheiros)

GGS - Grupo Germano de Sousa

GI - Grupo Impresa

GN - Grupo *Newsplex*

HDES - Hospital Divino Espírito Santo

HGO - Hospital Garcia de Orta

IA - Inteligência Artificial

IRC - *Internet Relay Chat* (Conversação de retransmissão de *internet*)

M2M - *Machine-to-machine* (Máquina a máquina)

MFA - *Multifactor authenticator* (autenticação multifator)

MitM - *man-in-the-middle* (Homem do meio)

ML - *Machine learning* (aprendizagem máquina)

MMS - *Multimedia Messaging Service* (Serviço de mensagens de multimédia)

OSINT - *Open Source Intelligence* (Inteligência de Fontes Abertas)

PJ – Polícia Judiciária

PME - Pequenas e médias empresas

PRISMA - *Preferred Reporting Items for Systematic reviews and Meta-Analyses* (Itens de relatório preferidos para revisões sistemáticas e meta-análises)

REMGFA - Rede do Estado Maior General das Forças Armadas

RGPD – Regulamento Geral sobre a Proteção de Dados

SCP - Sporting Clube de Portugal

SMS - *Short Message Services* (Serviços de Mensagens Curtas)

SMTUC - Serviços Municipalizados de Transportes Urbanos de Coimbra

SOC - *Security Operations Center* (Centro de Operações de Segurança)

SRSD - Secretaria Regional da Saúde e Desporto

SSL - *Secure Sockets Layer* (Camada de Segurança na *Internet*, substituída pelo TLS)

TAP - Transportes Aéreos Portugueses

TI - Tecnologias de informação

TIC - Tecnologia da informação e comunicação

TLS - *Transport Layer Security* (Camada de Segurança de Transporte, veio substituir o SSL)

TIN - *Trust in News*

VIP - *Very Important Person* (Pessoa muito importante - famosa)

VPN - *Virtual Private Network* (Rede privada virtual)

WLAN - *Wireless Local Area Network* (Rede de área local sem fio)

GLOSSÁRIO

Botnet - é uma rede de dispositivos que foi infetada com *software* mal-intencionado, como por exemplo um vírus.

Bitcoin – é uma moeda digital, que foi criada em 2009 por um grupo de pessoas sob o pseudónimo de Satoshi Nakamoto. Utiliza um código complexo que não pode ser alterado e todas as transações são protegidas por criptografia, daí também ser denominada de criptomoeda. É através do processo de mineração que se criam *bitcoins*.

Blockchain - consiste numa cadeia de blocos, onde cada bloco contém um conjunto de transações ou dados, um carimbo de tempo e um *hash* (resumo / representação criptográfica) do bloco anterior. Isto cria uma sequência contínua e interligada de blocos. É a tecnologia subjacente a criptomoedas (*Bitcoin*, *Ethereum, Ripple* e *Litecoin*), mas também tem aplicações em diversas áreas, tais como cadeias de abastecimentos, contratos inteligentes, votação eletrónica, etc.

Cache – um arquivo *cache* é uma ferramenta que atua como um processo temporário e permite ao processador recuperar os dados mais rapidamente. *Cache* consiste assim no armazenamento temporário de um conjunto de informações, que permite que o navegador trabalhe mais rápido acedendo às informações guardadas na memória temporária.

Cloud Storage – O armazenamento em nuvem é um modo de armazenamento de dados de computador em que os dados digitais são armazenados em servidores em locais fora do *site*. Os servidores são mantidos por um fornecedor, responsável por hospedar, gerir e proteger os dados armazenados na infraestrutura. O fornecedor garante que os dados nos servidores estão sempre acessíveis por ligações de *Internet* públicas ou privadas.

Cookies - são pequenos arquivos de texto que são armazenados no dispositivo do utilizador (como um computador, *tablet* ou *smartphone*) quando ele visita um *site*.

Criptografia - é uma técnica utilizada para proteger a confidencialidade, integridade e autenticidade de informações sensíveis, durante o armazenamento, transmissão ou processamento das mesmas. Este método consiste em converter o chamado texto simples num formato ilegível chamado texto cifrado, através da utilização de algoritmos e chaves criptográficas.

Existem dois tipos principais de criptografia:

- A criptografia simétrica onde a mesma chave é usada tanto para criptografar quanto para de*script*ografar os dados. Neste caso, o remetente e o destinatário devem concordar previamente com uma chave compartilhada. Embora seja eficiente e rápido, o principal desafio deste tipo é a distribuição segura da chave entre as partes.

- A criptografia assimétrica, também conhecida como criptografia de chave pública, que utiliza um par de chaves relacionadas, ou seja, uma chave pública e uma chave privada. A chave pública é utilizada para criptografar os dados, enquanto a chave privada correspondente é utilizada para de*script*ografá-los. Estas chaves estão matematicamente ligadas de tal forma, que a informação criptografada com a chave pública só pode ser decifrada pela chave privada correspondente. Isto elimina a necessidade de uma chave compartilhada, tornando mais fácil a distribuição segura das informações. Além disso, a criptografia assimétrica é frequentemente utilizada em protocolos de segurança, como o SSL/TLS, para estabelecer ligações seguras na *internet*. A criptografia desempenha um papel fundamental na segurança da informação, sendo amplamente utilizada em várias aplicações tais como, comunicações seguras, transações financeiras, autenticação de utilizadores e proteção de dados confidenciais. É uma ferramenta essencial para garantir a privacidade e a segurança no mundo digital.

Criptomoeda - é uma moeda digital, com lógica similar à da moeda fiduciário, que utiliza a tecnologia de *blockchain* e da criptografia para assegurar a validade das transações e a criação de novas unidades da moeda através da mineração.

Cyber-range - é um ambiente simulado onde indivíduos ou equipas podem praticar e desenvolver as suas competências e conhecimentos em cibersegurança num ambiente seguro e controlado**.**

Deepfake – é uma técnica de Inteligência Artificial (IA) que utiliza redes neurais para criar ou manipular conteúdo audiovisual, trocando o rosto de pessoas em vídeos, sincronizando movimentos labiais, expressões e outros detalhes.

Deep Web - é a parte da *internet* que não pode ser detetada facilmente pelos tradicionais motores de busca, garantindo privacidade e anonimato aos seus utilizadores.

Encriptação - é o processo específico de transformar dados legíveis (texto simples) num formato ilegível (texto cifrado) usando um algoritmo de criptografia e uma chave. É uma aplicação prática da criptografia.

Engenharia Social – são formas de obtenção de informação pessoal através de OSINT, *Open Source Intelligence*, ou de meios enganosos sobre o proprietário dos dados fidedignos.

Firewall - é um sistema de segurança de rede de computadores que restringe o tráfego da *Internet* para, de ou numa rede privada.

Hacker - designa alguém capaz de invadir dispositivos eletrónicos, redes e sistemas informáticos, quer seja para verificação de segurança, para aperfeiçoamento ou para praticar atos ilícitos, neste caso também é denominado de atacante, criminoso, pirata informático, intruso, invasor, espião ou agressor.

Hacking - refere-se ao uso indevido de dispositivos informáticos e redes para causar danos ou corromper sistemas, obter informação sobre utilizadores, roubar dados e/ou documentos ou interromper atividades relacionadas com dados.

Inteligência Artificial - é um conjunto diversificado de tecnologias e metodologias que colaboram para aperfeiçoar a capacidade que uma máquina tem de imitar a maneira como o cérebro humano processa as informações, utilizando algoritmos e regras para analisar conjuntos de dados extensos a fim

de identificar padrões que servem de base para os seus modelos de tomada de decisão.

JavaScript – é uma linguagem de programação que permite a criação de conteúdo que se atualiza dinamicamente, controla conteúdo multimédia, imagens animadas, etc.

Keyloggers - é um *software* de monitorização, criado para registar tudo o que a vítima escreve.

Machine learning – a aprendizagem máquina (ML) é um método de análise de dados que automatiza a construção de modelos analíticos. É um ramo da inteligência artificial baseado na ideia de que sistemas podem aprender com dados, identificar padrões e tomar decisões com o mínimo de intervenção humana.

Malware - é um termo geral para designar *software* malicioso, que é projetado para interromper ou obter dados de uma rede de computadores ou servidores. Alguns exemplos de *malware* são o *Ransomware*, o *Spyware*, os *Keyloggers*, os *Rootkits*, o *Adware*, os *Worms*, os *Trojans*, o *Scareware* e os Vírus.

Modus operandi - maneira de praticar uma operação ou de desenvolver determinada atividade.

Password – é uma senha combinando uma cadeia arbitrária de caracteres que pode incluir letras, números e caracteres especiais. É utilizada para confirmar a identidade do utilizador.

Plug-in - ou módulo de extensão é um programa de computador utilizado para adicionar funções a outros programas maiores, fornecendo funcionalidades especiais ou muito específicas.

Rootkits – é um *software* criado para facultar aos *hackers* o acesso a um dispositivo-alvo.

Router – é um dispositivo que estabelece a conexão entre duas ou mais redes IP ou sub-redes.

Script – é uma série de instruções que são executadas de maneira ordenada ou um conjunto de instruções que promovem a execução de uma determinada tarefa num *software*. A linguagem de *script* é utilizada para dar instruções a programas que estão em execução num computador.

SOC - *Security Operations Center* (Centro de Operações de Segurança), consiste numa equipa ou departamento dentro de uma organização responsável pela monitorização, análise e resposta a incidentes de segurança. O SOC é concebido para detetar, investigar e responder a ciberameaças e ataques em tempo real.

Software – é definido como os programas, dados e instruções que comandam o funcionamento de um computador, *smartphone*, *tablet* ou outro dispositivo eletrónico.

Spam – é definido como mensagens não solicitadas, geralmente enviadas em massa, que podem incluir e-mails, mensagens de texto ou postagens em redes sociais.

Spyware – é um programa espião.

Trojan - também conhecido como “Cavalo de Troia”, é um tipo de *malware* que, com o objetivo de enganar os utilizadores e induzi-los a instalá-lo nos seus sistemas, se disfarça como um *software* legítimo ou útil.

Wireless - esta rede é conhecida como rede sem fios, é uma forma de conexão entre 2 ou mais dispositivos sem a utilização de cabos.

WLAN – é a rede de área local sem fios, também conhecida por *Wi-fi* que é a marca que possui a maior classe de dispositivos certificados registados. Esta rede é maioritariamente utilizada para realizar conexões de *internet* via ondas de rádio. O seu alcance é de 60 metros, aproximadamente.

Capítulo 1 - INTRODUÇÃO

Nos últimos anos, Portugal tem registado um aumento significativo na complexidade e frequência dos ataques informáticos. Com o aparecimento da era digital e o aumento da dependência da tecnologia, as ameaças informáticas tornaram-se uma preocupação crescente para indivíduos, empresas e entidades governamentais em todo o país. Este fenómeno não reflete apenas a evolução do cenário tecnológico, mas também a crescente sofisticação e diversificação de atores maliciosos que operam no ciberespaço.

1.1 Enquadramento

O estudo dos ataques informáticos em Portugal apresenta-se como um campo de investigação crucial para compreender as ameaças atuais e futuras que o país enfrenta no âmbito digital. Desde invasões a sistemas governamentais e ataques a infraestruturas críticas a campanhas de *phishing* direcionadas a indivíduos e empresas, os ataques informáticos abrangem uma ampla gama de táticas e motivações. Estes incidentes não apenas representam riscos à segurança nacional e à estabilidade económica, mas também representam desafios significativos em termos de proteção de dados, privacidade e confiança *on-line*.

Além de analisar a natureza técnica das ameaças informáticas, também é fundamental entender os fatores socioeconómicos e geopolíticos que influenciam o cenário nacional de cibersegurança. Isto inclui examinar a infraestrutura de Tecnologias da Informação e Comunicação (TIC), políticas de segurança informática, parcerias público-privadas e consciencialização e educação em segurança informática.

1.2 Motivação

O que motivou a escolha do tema para esta dissertação de mestrado foi a importância da segurança informática, devido à grande necessidade de mitigar

os ataques informáticos, que a cada dia se vão tornando maiores em número e em especialização.

As empresas, principalmente as pequenas e médias empresas (PME), ainda estão muito céticas quanto à necessidade de investir em formação e aquisição de programas de cibersegurança. No entanto, quando se tornam vítimas de ataques informáticos, acabam por ter gastos avultados que podem ultrapassar o valor do investimento necessário em cibersegurança.

1.3 Objetivos

Nos dias de hoje, a segurança informática é uma preocupação crescente para empresas e indivíduos, devido ao aumento da frequência e sofisticação dos ataques informáticos. Este estudo tem como objetivo, explorar diversos aspetos relacionados com esses ataques, desde a sua classificação até aos danos reputacionais que estes podem causar.

É fundamental entender os diferentes tipos de ataques que podem ser perpetrados contra sistemas e redes, pois cada um deles possui características específicas e métodos de execução, o que torna essencial a sua classificação para a implementação de medidas de defesa adequadas. À medida que a tecnologia avança, também evoluem as técnicas utilizadas pelos *hackers* pelo que é crucial identificar e compreender as tendências emergentes para que as empresas possam estar preparadas e protegidas contra novas ameaças. A literatura sobre segurança informática aborda frequentemente os danos que podem resultar de um ataque informático. Os dados obtidos neste estudo sobre os ataques sofridos pelas empresas serão categorizados de modo a fornecer um melhor entendimento sobre os mesmos. A transparência é um aspeto importante na comunicação de incidentes de segurança e muitas empresas incluem informações sobre ataques nos seus relatórios anuais, detalhando a sua natureza, as medidas tomadas em resposta e as lições aprendidas: esta prática não apenas informa os *stakeholders*, mas também demonstra um compromisso

com a própria segurança das empresas. Pretende-se, com estas informações, perceber como as empresas estão preparadas para enfrentar os desafios da segurança informática. Serão analisados os ataques informáticos ocorridos em Portugal, no período de 2018 a 2023.

1.4 Metodologia

A realização deste trabalho consistiu em pesquisa *online*, onde foram analisados artigos, relatórios empresariais, relatórios de cibersegurança, notícias sobre os ataques e outros documentos onde se abordam as temáticas da cibersegurança e dos ataques informáticos

1.5 Contribuições

Com este trabalho pretende-se contribuir para o aumento da consciencialização de todos os possíveis interessados para este problema. Ele aborda os ataques informáticos a empresas, porém e atendendo a que qualquer pessoa pode ser vítima, a informação presente no estudo que aqui se detalha é útil, tanto como documento informativo quanto aos ataques informáticos mais comuns, como à forma como os mesmos podem ser evitados. O estudo efetuado também pode contribuir como ponto de partida para outros trabalhos, tais como investigação sobre os seguros informáticos que existem em Portugal e como estão a ser utilizados em PME e grandes empresas.

1.6 Estrutura da Dissertação de Mestrado

Esta dissertação encontra-se dividida em 5 capítulos, onde o primeiro consiste na introdução, onde se explica o contexto, o enquadramento, a motivação, a metodologia utilizada e as contribuições que este estudo facultará, permitindo desenvolver uma melhor compreensão do mesmo. No segundo faz-se a descrição do problema, os tipos de ataques informáticos mais conhecidos, o impacto das ameaças informáticas, e quais as tendências das técnicas aplicadas nesses ataques de forma a permitir uma melhor compreensão do tema

escolhido. No terceiro apresenta-se a metodologia de investigação. No quarto descreve-se o estudo documental e os resultados obtidos, assim como a análise e discussão dos mesmos. E no quinto está a conclusão que inclui as principais conclusões, contributos, limitações e proposta de trabalhos futuros.

Capítulo 2 - REVISÃO DE LITERATURA

2.1 Caracterização do Problema

O problema que este trabalho aborda é o aumento dos ataques informáticos nas empresas portuguesas, bem como os impactos financeiros e reputacionais que estes ataques informáticos provocam nestas empresas.

A *internet* e a tecnologia foram desenvolvidas com o objetivo de tornar mais fácil o desempenho de determinadas tarefas, no entanto, com o aumento da facilidade de utilização e o facto de se poder navegar de forma anónima na *internet*, tornou-se fácil cometer crimes informáticos.

O relatório "Riscos e Conflitos em Cibersegurança 2023" (Cibersegurança, 2023) do Centro Nacional de Cibersegurança, destaca uma evolução preocupante dos ataques informáticos em Portugal.

Em 2022, houve um aumento significativo de incidentes de segurança informática no país, refletindo uma tendência global de crescimento das ameaças informáticas. Os ataques informáticos em Portugal abrangeram uma variedade de técnicas, como *ransomware*, *phishing*, comprometimento de contas, engenharia social, sabotagem informática, distribuição de *malware*, espionagem informática e exploração de vulnerabilidades, como indicado na tabela 1.

Tabela 1 - Incidentes por tipo registados pelo CERT.PT, 2021 e 2022 - TOP 10

2021				2022				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Variação %	Lugar RK
1º	Phishing/Smishing	715	40	1º	Phishing/Smishing	742	37	+4	=
2º	Engenharia social	246	14	2º	Engenharia social	285	14	+16	=
3º	Distribuição de *malware*	226	13	3º	Distribuição de *malware*	214	11	-5	=
4º	Comprometimento de conta não privilegiada	114	6	4º	Utilização Ilegítima de nome de terceiros	126	6	+58	+
5º	Utilização Ilegítima de nome de terceiros	80	4	5º	Comprometimento de conta não privilegiada	115	6	+1	-
6º	Indeterminado (outro)	50	3	6º	Sistema infetado (*malware*)	84	4	+83	+
7º	Sistema infetado (*malware*)	46	3	7º	Comprometimento de aplicação	81	4	+125	+
8º	Sistema vulnerável (vulnerabilidade)	44	2	8º	Modificação não autorizada (69 *ransomware*)	74	4	+195	+
9º	Modificação não autorizada (35 *ransomware*)	38	2	9º	SPAM	62	3	+77	+
10º	Exploração de Vulnerabilidade (tent. Intrusão)	37	2	10º	Sistema vulnerável	48	2	+9	+

Fonte: CERT.PT

Segundo Murphy (2020), em 2014, uma pesquisa (apoiada pela *McAfee*) estimou que os danos anuais à economia mundial seriam de 445 mil milhões de dólares. Perto de 1,5 mil milhões de dólares foram roubados nos EUA (Estados Unidos da América) devido à apropriação indevida *online* de dados de cartões bancários (crédito e débito).

Em 2018, o Centro de Estudos Estratégicos e Internacionais (CSIS) e a *McAfee* publicaram um estudo que estimava que cerca de 1% do PIB global (aproximadamente 600 mil milhões de dólares) são perdidos anualmente devido ao crime informático (Murphy, 2020).

O Estado, as organizações e as empresas são muito dependentes das Tecnologias de Informação (TI) e das redes para a realização das suas atividades diárias, e para a execução dos seus negócios, esta grande dependência leva a um aumento significativo de incidentes de segurança informática o que causa grandes perdas e interrupções nas operações comerciais.

Segundo Kaddoura (2021), à medida que o mundo migra para dados eletrónicos *online*, as bases de dados tornam-se mais vulneráveis a ataques, especialmente quando contêm informações críticas. Com o número crescente de ataques, as medidas preventivas não podem ter sucesso por si só, portanto, as abordagens de avaliação e recuperação tornam-se mais importantes.

Para Esparza (2019), as credenciais roubadas mais utilizadas são as de *login* bancários e de redes sociais, seguidas pelos fornecedores de serviços de *e-mail* e *web* e as credencias utilizadas para comércio eletrónico. As credenciais obtidas de forma ilícita, podem ser utilizadas de várias maneiras. Uma das mais comuns é facilitar a violação de dados, aproveitando as contas empresariais utilizando-as para perpetrar intrusões graves. Outras formas incluem fazer-se passar por pessoas conhecidas (VIP – *Very Important Person*) nas redes sociais, ou *e-mail* para prejudicar a reputação da empresa ou instruir transações fraudulentas.

Os crimes informáticos consistem em dois tipos principais de atividades ilegais, que são a Pirataria na *Internet* e o *Hacking* de Computadores. A pirataria consiste na cópia e distribuição de conteúdo ilegal, com o objetivo de, na maioria das vezes, obter lucro com as transações, enquanto o *hacking* de computadores, consiste no ato de quebrar medidas de segurança para aceder a informações, que de outra forma seriam inacessíveis, com o objetivo de obter lucro ou apenas para mero entretenimento.

Os ataques informáticos consistem num conjunto de ações, direcionadas contra sistemas de informação, com o objetivo de obter informação confidencial, alterar, desativar ou destruir dados.

Nem sempre os *hackers* têm como objetivo a obtenção ilegal de dados informáticos: em alguns casos, apenas pretendem interromper o acesso aos sistemas de informação ou à infraestrutura de TI para abalar a empresa, transmitir uma mensagem de poder ou de protesto.

Os custos associados aos ataques informáticos podem ser significativos, para as organizações em particular e para a economia como um todo. Esses custos incluem não apenas os danos diretos causados pelos ataques, como perda de dados, interrupção de serviços e extorsão financeira, mas também os custos indiretos, como danos à reputação, custos de recuperação e possíveis penalizações legais.

2.2 Ataques informáticos

Os dados da tabela 2 mostram o número de ataques informáticos em Portugal, e a sua variação nos vários anos compreendidos entre 2018 e 2023.

Em 2018, ocorreram 599 ataques, em 2019, ocorreram 754, em 220 ocorreram 1252, em 2021 ocorreram 1781, em 2022 ocorreram 2023 e em 2023 ocorreram 2025 ataques.

Entre 2018 e 2019 verificou-se um crescimento de 25,9%, entre 2019 e 2020 o aumento foi de 66%, entre 2020 e 2021 o aumento foi de 42,3%, entre 2021 e 2022 o aumento foi de 13,6% e entre 2022 e 2023 o aumento foi de 0,1%.

Tabela 2 - Incidentes por tipo registados pelo CERT.PT por ano

Incidentes	2018	Var %	2019	Var %	2020	Var %	2021	Var %	2022	Var %	2023
Phishing/smishing	176	34,1%	236	159,7%	613	56,8%	961	6,9%	1027	-11,9%	905
Infeção (malware)	215	-17,2%	178	61,8%	288	7,6%	310	20,0%	372	-27,2%	271
Utilização ilegítima de nome de terceiros	69	-31,9%	47	-31,9%	32	150%	80	57,5%	126	-18,3%	103
Sistema vulnerável (vulnerabilidade)	59	28,8%	76	-46,1%	41	97,6%	81	-40,7%	48	39,6%	67
Compromisso de Conta/aplicação	46	230,4%	152	64,5%	250	-54,4%	114	71,9%	196	-8,7%	179
Outros não definidos	34	91,2%	65	-56,9%	28	739,3%	235	8,1%	254	96,9%	500
Total	599	25,9%	754	66,0%	1252	42,3%	1781	13,6%	2023	0,1%	2025

Fonte: Relatórios Cibersegurança em Portugal 2018-2023, CNCS. Elaboração Própria.

Observando a tabela 2 assim como o gráfico 1, em todos os anos o número de ataques aumentou. Tal como aconteceu a nível mundial, o maior aumento verificou-se durante o período de isolamento provocado pela pandemia COVID-19.

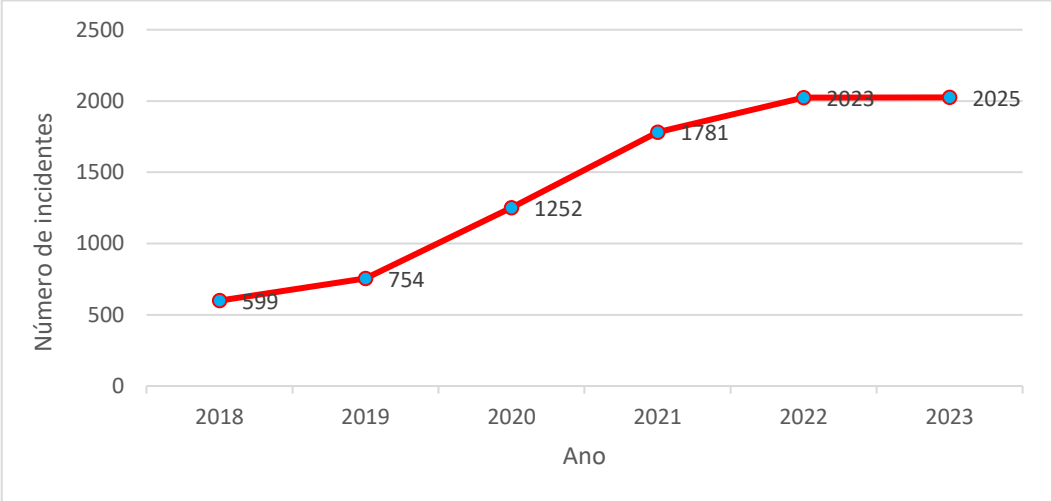

Gráfico 1 - Número de incidentes por ano

Fonte: Relatórios Cibersegurança em Portugal, CNC. Elaboração Própria.

Ao se compararem diretamente os anos de 2018 e 2023, o aumento foi de 238,1%, observa-se também que em todos os incidentes, houve um aumento do número de ataques, como se pode verificar na tabela 3.

Tabela 3 - Variação de Incidentes por tipo registados pelo CERT.PT entre 2018 e 2023

Incidentes	2018	Var %	2023
Phishing/smishing	176	414,2%	905
Infeção (*malware*)	215	26,0%	271
Utilização ilegítima de nome de terceiros	69	49,3%	103
Sistema vulnerável (vulnerabilidade)	59	13,6%	67
Compromisso de Conta / aplicação	46	289,1%	179
Outros não definidos	34	1379,6%	500
Total	599	238,1%	2025

Fonte: Relatórios Cibersegurança em Portugal, CNCS. Elaboração Própria.

A nível mundial, os incidentes informáticos também aumentaram de 8.886 milhões em 2015 para 22.072 milhões em 2022, o que se traduz num aumento de 148,38% (Dave *et al*., 2023).

Esta evolução deveu-se à combinação de vários fatores, tais como, a pandemia de COVID-19 - a qual acelerou a digitalização em muitos setores, o que levou a um aumento na utilização de serviços online, trabalho remoto e dependência das tecnologias digitais ampliando assim a superfície de ataque para os hackers - a evolução das técnicas de ataque e o aumento do número de dispositivos ligados à internet.

2.3 Tipos mais comuns de ataques informáticos

2.3.1 *Ransomware*

O *Ransomware* é um tipo de *malware* que se tem tornado cada vez mais comum e perigoso no mundo da cibersegurança. O seu *modus operandi*, consiste no acesso indevido aos dados da vítima, de seguida os mesmos são criptografados

nos seus próprios dispositivos informáticos e, posteriormente, ocorre a exigência de um resgate para que a vítima possa recuperar o acesso aos sistemas. O resgate é solicitado, geralmente, através de uma mensagem que surge no ecrã da vítima, conhecida como "nota de resgate", sendo a transação solicitada/exigida em criptomoedas como a *Bitcoin*, tal como indica a figura 1.

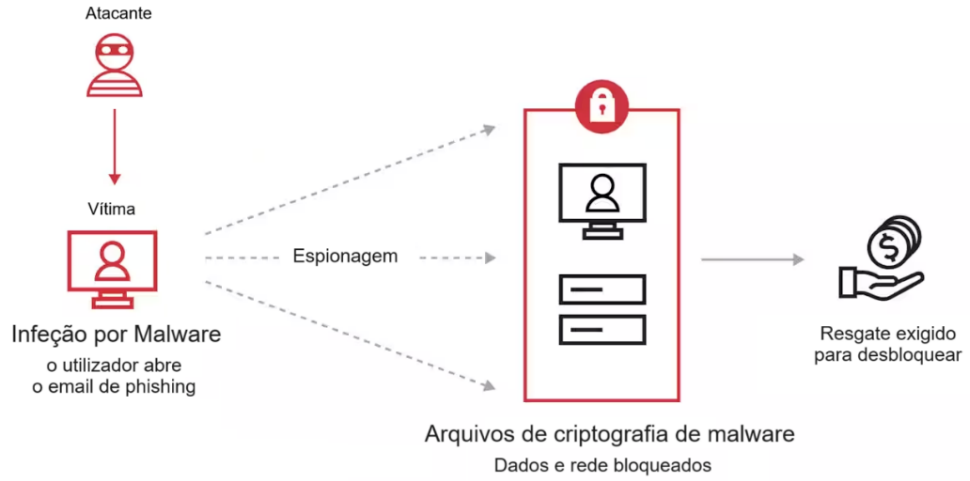

Figura 1 - Esquema de Ransomware

Fonte: (Akamai, 2023)

O *Ransomware* pode afetar sistemas através de vários vetores, como por exemplo: *e-mails* de *phishing*, *downloads* de *malware*, entre outros. Assim que se introduz no sistema, espalha-se rapidamente e começa a criptografar ficheiros com documentos, imagens, vídeos e áudio. Assim que os ficheiros são criptografados, tornam-se inacessíveis para o utilizador, o qual apenas poderá recuperar o seu acesso através do pagamento do resgate solicitado, o que lhe facultará o acesso à obtenção da chave de criptografia necessária para os desbloquear.

O *Ransomware* é um dos tipos de *malware* mais prejudiciais, podendo ter consequências devastadoras para indivíduos e organizações, incluindo a perda de dados críticos, a interrupção de operações de negócios e perdas financeiras significativas, para além de danos reputacionais. Os ataques de *Ransomware*

podem ser acompanhados por ameaças de violação de dados, em que os invasores ameaçam tornar públicos os dados, caso a vítima não pague o resgate (IBM, 2024c).

Como medidas preventivas, é fundamental implementar medidas de segurança proativas, devendo manter o *software* atualizado, utilizar soluções de segurança robustas, fazer *backups* dos dados regularmente e formar os colaboradores sobre as melhores práticas de segurança informática. Além disso, é essencial ter um plano de resposta a incidentes que possua procedimentos para a deteção, contenção e recuperação dos dados.

2.3.2 *Phishing*

O termo *phishing* provém das palavras em inglês "*phrase*" e "*fishing*" que significa "pescar palavras".

Os ataques de *phishing* ocorrem quando alguém mal-intencionado envia um *e-mail* (*phishing)*, texto (*smishing*) ou realiza uma chamada telefónica de voz (*vishing*). Estas mensagens parecem vir de entidades conhecidas e confiáveis, na tentativa de obter acesso às informações confidenciais da vítima, como indicado na figura 2.

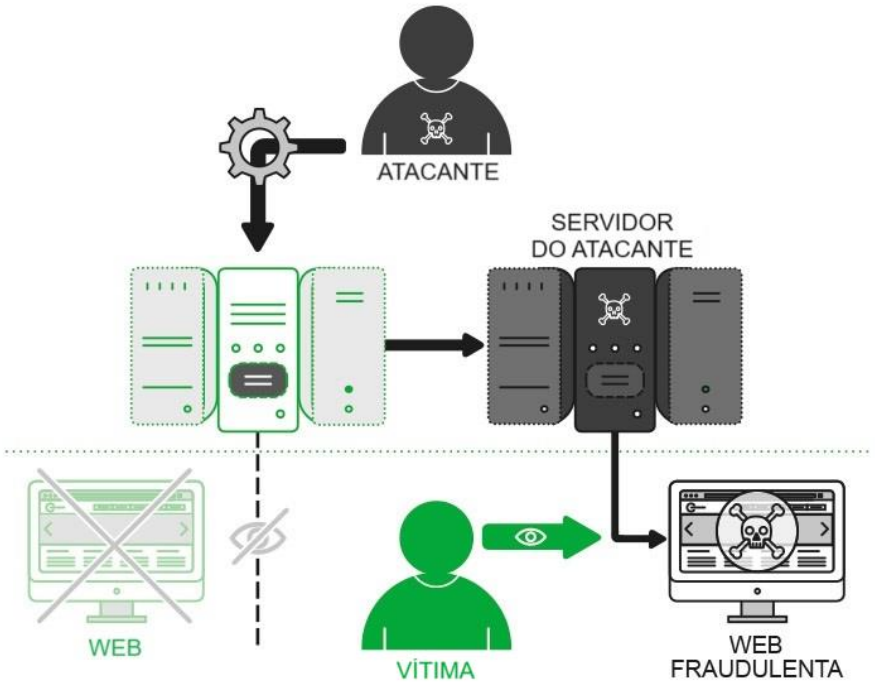

Figura 2 - Esquema de Phishing

Fonte: (Corchado, 2023)

Apesar de haver tipos de *phishing* em que os *hackers* pedem os dados diretamente por resposta ao *e-mail*, na maior parte dos casos estes ataques direcionam a vítima para um novo *website*, com imagem semelhante à que a vítima identifica como sendo verdadeira, onde ela é incitada a validar os seus dados pessoais, preenchendo os campos com os seus dados, dados esses que, logo de seguida, são acedidos indevidamente, sendo os dados de contas bancárias, contas *online* ou outra informação confidencial aqueles que geram mais interesse (IBM, 2024b).

Os tipos de ataque *de phishing* podem ser classificados como *Spear-phishing*, *Smishing*, *Vishing*, *Whaling* e *Angler phishing*. O procedimento em todos é o mesmo, mudando apenas o tipo de conteúdo manipulado ou o veículo do ataque.

2.3.3 *Man-in-the-middle* (MitM)

Os ataques *man-in-the-middle* (homem do meio) ocorrem quando o *hacker* se coloca entre duas partes numa comunicação. Normalmente ele coloca-se entre a vítima e *site*s importantes, tais como *site*s de bancos ou contas de *e-mail*, intercetando dados ou comprometendo a rede para espiar. Ao fim de algum tempo a intercetar a comunicação, o espião faz-se passar pela pessoa com quem a vítima estava a conversar (IBM, 2024a).

Estes ataques são especialmente comuns ao utilizar redes *Wi-Fi* públicas, como estas redes não são protegidas por *password*, podem ser facilmente "hackeadas" / comprometidas. Para esse efeito, o *hacker* configura o próprio computador, ou outro dispositivo *wireless*, para funcionar como ponto de *Wi-Fi*, nomeando-o com o mesmo nome da rede pública existente no local. consequentemente, quando a vítima se liga ao "falso *router"* e navega em *site*s importantes, tais como bancos ou realizando compras e pagamentos ou outros acessos relevantes, o agressor consegue aceder indevidamente às credenciais de acesso da vítima. O mais comum é *session hijacking,* que consiste num ataque de sequestro de sessão, correspondendo a um tipo de ataque no qual o pirata informático invade e assume o controlo de uma sessão entre um cliente e o servidor, enquanto a vítima verifica, por exemplo, o saldo bancário, ou efetua pagamentos ou realiza compras *online*, como indicado na figura 3.

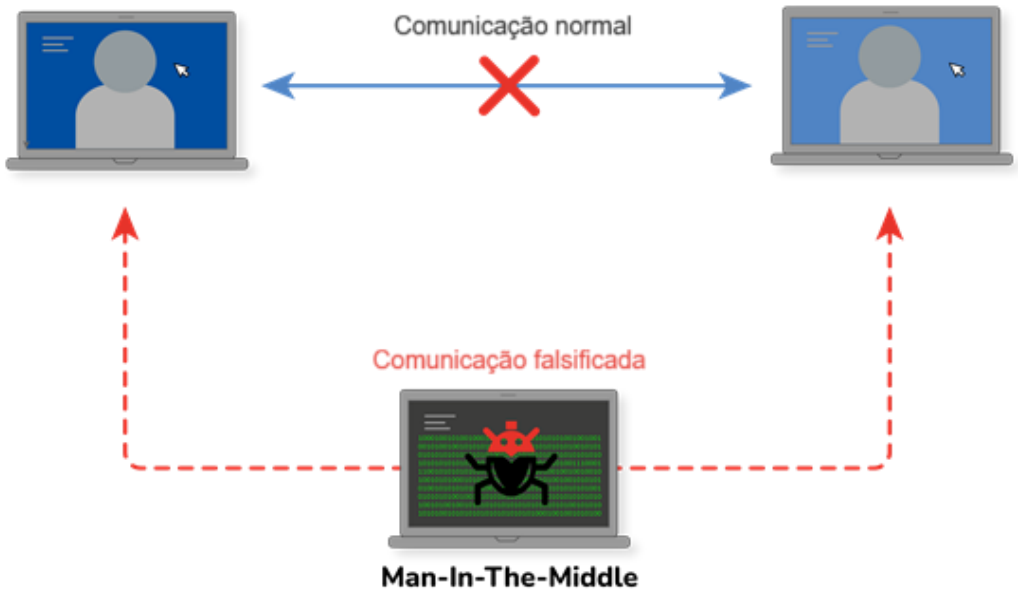

Figura 3 - Esquema de ataque MITM

Fonte: (Ichi, 2023)

As consequências mais graves do sequestro de sessão são:

- Roubo monetário – neste caso o agressor consegue obter as credenciais de acesso à conta bancária da vítima e realiza transferências ou compras em seu nome.
- Roubo de identidade – neste caso o criminoso consegue obter acesso não autorizado a informações pessoais e confidenciais da vítima e utiliza-as para cometer crimes usando a identidade da mesma.
- Roubo de dados – neste caso o invasor consegue obter acesso a dados confidenciais e utiliza-os para prejudicar a vítima.

2.3.4 *Cross-site scripting attacks*

Num ataque de *cross-site scripting* (ataques de *script* entre *site*s (XSS)), o *hacker* aproveita-se de *site*s vulneráveis e instala *scripts* maliciosos no código de aplicações ou *site*s confiáveis. A seguir, o código é iniciado, fazendo correr o *script* malicioso permitindo assim ao atacante, conseguir obter acesso não

autorizado a informações confidenciais, ou até mesmo conseguir fazer-se passar pela vítima (Robinson, 2015), como ilustrado na figura 4.

Figura 4 - Esquema de ataque XSS

Fonte: (Rutledge, 2019)

Os ataques baseados no XSS incluem, normalmente, a transmissão de dados privados tais como *cookies* ou outras informações importantes para o *hacker*, redirecionando a vítima para conteúdo da *web* controlado ou executando outras operações maliciosas na máquina da vítima.

Este tipo de ataque aproveita a entrada em fóruns, *blogs* e outros *site*s que permitem aos utilizadores inserir conteúdo, sendo estes os locais mais suscetíveis.

Os ataques XSS dividem-se em 3 categorias:

1. **Ataques XSS refletidos** – são a forma mais habitual e simples de ataque XSS. Este ataque consiste em orientar a vítima a fazer uma solicitação ao servidor *web*, e em seguida o *malware* é "refletido" na resposta HTTP do servidor *web* para o utilizador.

No ataque refletido, o *script* injetado apresenta-se como sendo uma mensagem de erro resultante de uma pesquisa efetuada através de um *link* mal-intencionado.

Quando esse *link* é clicado, dá início à execução do *script* permitindo que o código infetado seja transferido para o *site* e "reflita" de volta para o utilizador. A partir daí, o *script* pode executar qualquer ação disponível para o utilizador nessa sessão, assim como, capturar os dados transmitidos pelo utilizador (Rutledge, 2019).

2. **Ataques XSS armazenados** – também conhecidos como ataques XSS persistentes, ocorrem quando uma aplicação *web* compartilha dados de uma fonte não confiável ou não verificada em respostas HTTP subsequentes.

   No ataque XSS armazenado, o *script* injetado é salvo de forma permanente nos servidores de destino, tais como bancos de dados, campos de comentários ou outros locais.

   Se o *site* não tiver verificação dos dados enviados pelos utilizadores, o *hacker* pode facilmente inserir conteúdo que inclua um *script* mal-intencionado e assim infetar os outros utilizadores. A vítima acede ao *script* malicioso do servidor, quando solicita as informações armazenadas (Rutledge, 2019).

3. **Ataques XSS baseado em DOM** (*Document Object Model*) – neste ataque, existe a exploração de vulnerabilidades de segurança no código do lado da vítima ou do navegador (*browser*). Este ataque ocorre quando uma aplicação *web* processa dados *JavaScript* de uma fonte não confiável de forma insegura. Os ataques DOM XSS ocorrem em *JavaScript*, uma vez que *Java* é a única linguagem que todos os navegadores (*browsers*) entendem (Rutledge, 2019).

2.3.5 *Cryptojacking*

A criptomineração maliciosa envolve a utilização não autorizada dos recursos de dispositivos pessoais, tais como, computadores, *smartphones* ou *tablets*, por *hackers* para a mineração de criptomoedas. Este ataque tem como único objetivo a obtenção de lucro e é projetado para ser invisível para a vítima.

O invasor compromete um *site* e assim que os utilizadores se ligam a este *site*, o *script* de criptomineração é automaticamente executado. A partir deste momento, as vítimas começam a minerar criptomoedas para o atacante, permitindo assim, que ele receba uma recompensa em criptomoedas por cada bloco adicionado com sucesso à *blockchain*, como exemplificado na figura 5.

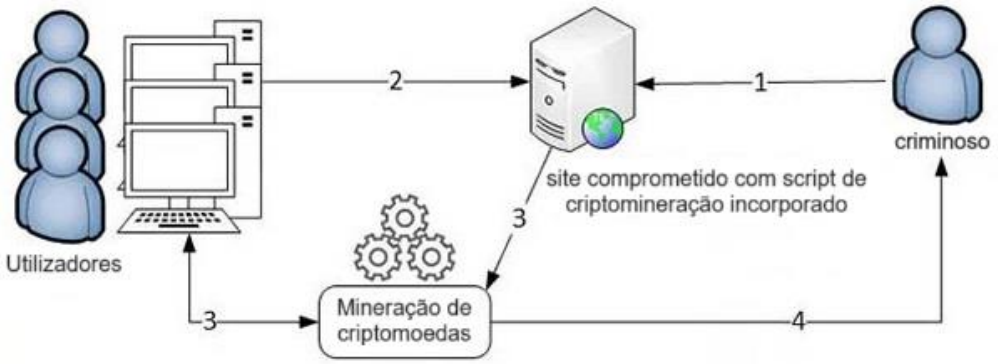

Figura 5 - Esquema de Cryptojacking

Fonte: (GoldSparrow, 2023)

Neste ataque, os criminosos procuram obter os benefícios da mineração de criptomoedas, sem terem os elevados custos que este processo inclui. Nestes casos, o intruso invade o dispositivo alvo e instala *software* de criptografia maliciosa. Este *software* funciona em segundo plano, minerando criptomoedas ou apoderando-se indevidamente de carteiras de criptomoedas (Malwarebytes, 2024).

Este ataque consegue ser invisível, sendo que as vítimas apesar de notarem que os seus dispositivos estão mais lentos e com menor desempenho que antes,

continuam a utilizá-los sem se aperceberem que estes estão também a ser utilizados por terceiros.

2.3.6 *Denial of Service* (DOS) e *Distributed Denial of Service* (DDoS)

Um ataque de negação de serviço (DoS, *Denial of Service*) ocorre, quando os *hackers* utilizam solicitações e tráfego falsos para sobrecarregar um sistema, de modo que este não responda às solicitações, como esquematizado na figura 6.

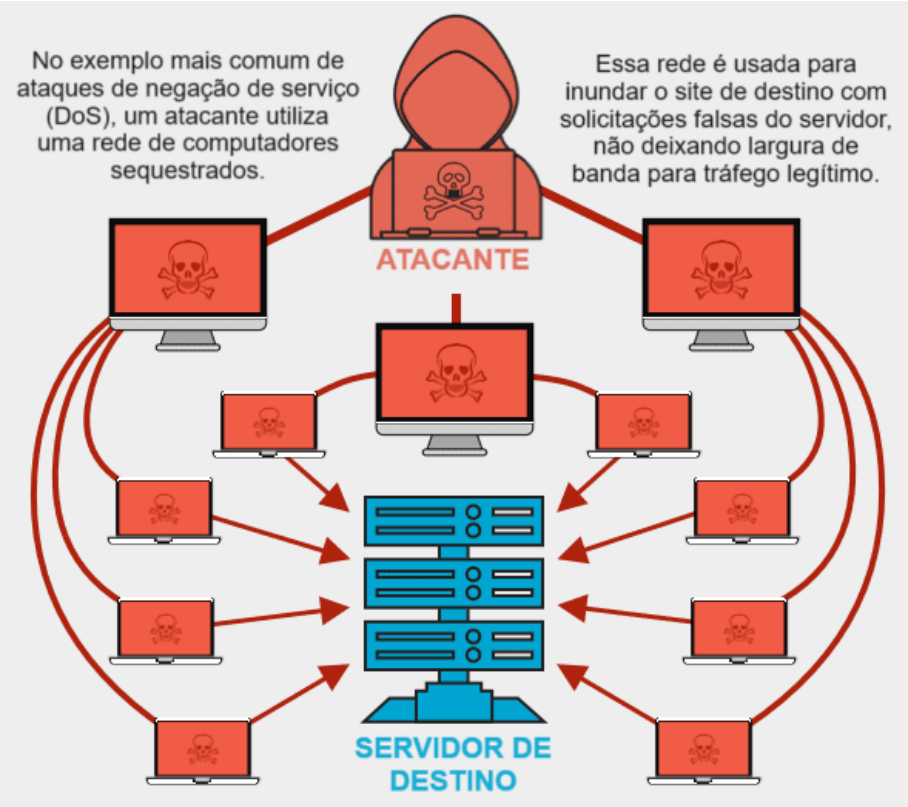

Figura 6 - Esquema de Denial os Service

Fonte: (Oza, 2023)

Um ataque distribuído de negação de serviço (DDoS, *Distributed Denial of Service*) é o mesmo tipo de ataque do DoS, embora, no caso de DDoS, o invasor utilize, ao mesmo tempo, diversos dispositivos comprometidos, recorrendo a um computador mestre para gerir um grupo de computadores denominados de "zombies".

O agressor invade um computador "mestre" e através deste escraviza várias máquinas tornando-as Zombies, ordenando-lhes que acedam a um determinado recurso num servidor, todos ao mesmo tempo. Ao acederem concomitantemente e ininterruptamente ao mesmo recurso do servidor, acabam por o sobrecarregar e este deixa de responder.

Este ataque não invade o sistema e nem tem acesso a nenhum dos seus dados internos.

O objetivo deste ataque é sobrecarregar um sistema informático, para que os recursos do sistema fiquem indisponíveis conseguindo assim, apenas denegrir a imagem da instituição vítima, ou praticar *Ransomware* exigindo o pagamento em troca da reposição do serviço, ou praticar concorrência desleal aproveitando-se da indisponibilidade do sistema para oferecer o mesmo tipo de serviço e assim conseguir apropriar-se dos clientes da vítima (Cloudflare, 2024).

2.3.7 DNS *spoofing or "poisoning"*

O envenenamento de cache de DNS (*Domain Name System*) consiste na falsificação do Sistema de Nomes de Domínio (DNS) que permite que os *hackers* enviem tráfego *online* para um *site* falsificado.

Estes *site*s, conforme exemplificado na figura 7, parecem idênticos aos originais e capturam qualquer informação que a vítima insira ou partilhe, enviando-a diretamente para os *hackers*, dando-lhes acesso às suas contas (Sudipto, 2023).

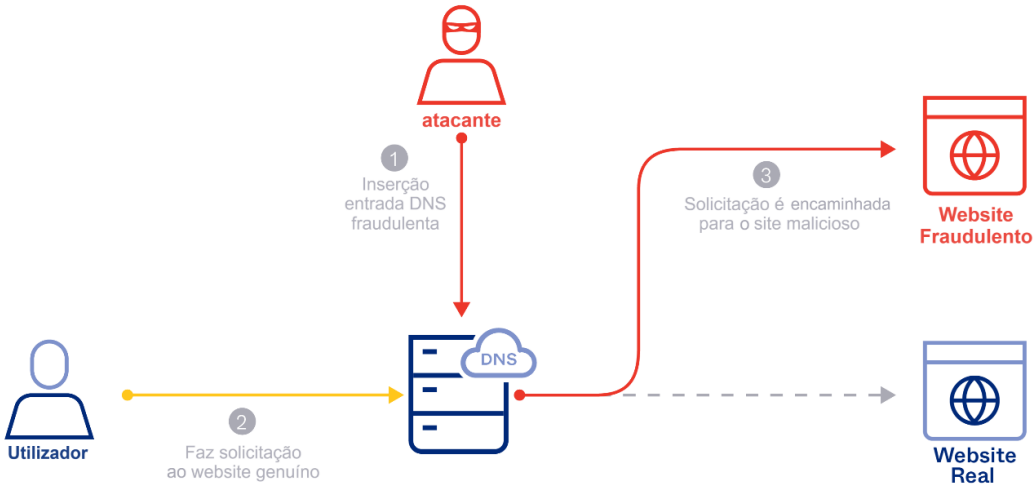

Figura 7 – Esquema de envenenamento de DNS

Fonte: (Okta, 2024)

2.3.8 DNS *tunneling*

O túnel / encapsulamento DNS é um tipo de ataque informático em que os invasores contornam os sistemas de segurança tradicionais, como *firewalls*, para obter acesso a sistemas e redes.

Este ataque, encaminha solicitações DNS para o servidor invasor, fornecendo ao *hacker* um canal secreto de comando e controlo e um caminho de exfiltração de dados (CheckPoint, 2024), tal como esquematizado na figura 8.

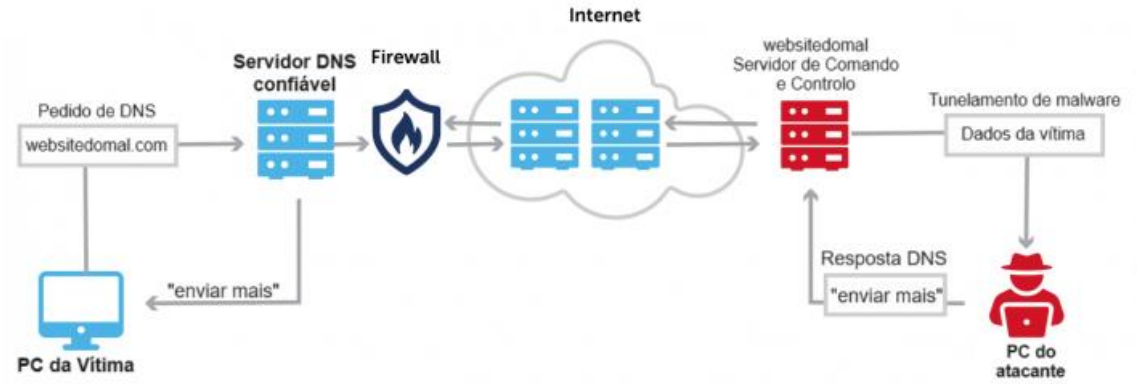

Figura 8 - Esquema DNS tunneling

Fonte: (Pawar, 2022)

2.3.9 Drive-by Download Attacks

Os *hackers* aproveitam as vulnerabilidades existentes nos *plug-ins*, *web browsers* e aplicações, para instalar *malware* no dispositivo da vítima sem o seu conhecimento, tal como indicado na figura 9.

Figura 9 - Esquema Drive-by download

Fonte: (Mitra, 2017)

Estes ataques podem ser efetuados de 2 formas:

1. *Downloads* autorizados – estes *downloads* são apresentados à vítima através de ataques de *phishing*, onde a vítima é incitada a clicar num *link* ou *site* malicioso sem que perceba quais são as implicações, normalmente é atraída a clicar num anúncio que se encontra no *site*. Este ataque necessita que seja a vítima a iniciar o *download*.
2. *Downloads* não autorizados – estes *downloads* aparecem dissimulados em *site*s comprometidos, e iniciam-se automaticamente sem que a vítima receba qualquer aviso ou notificação. Este ataque não depende da vítima para iniciar o *download*.

2.3.10 *Inside threats*

As ameaças internas ocorrem quando um colaborador da empresa, com acesso autorizado às redes ou sistemas, faculta o acesso a esses dados e sistemas a pessoal não autorizado ou promove intencionalmente a exposição de palavras-passe.

As ameaças internas podem ser, tal como apresentado na figura 10:

- **Intencionais** – a ameaça interna é intencional quando o colaborador (infiltrado mal-intencionado), causa danos à organização de forma propositada.
- **Involuntárias** – a ameaça interna é involuntária quando por erro ou negligência do colaborador (infiltrado negligente), há o roubo ou perda de dados.

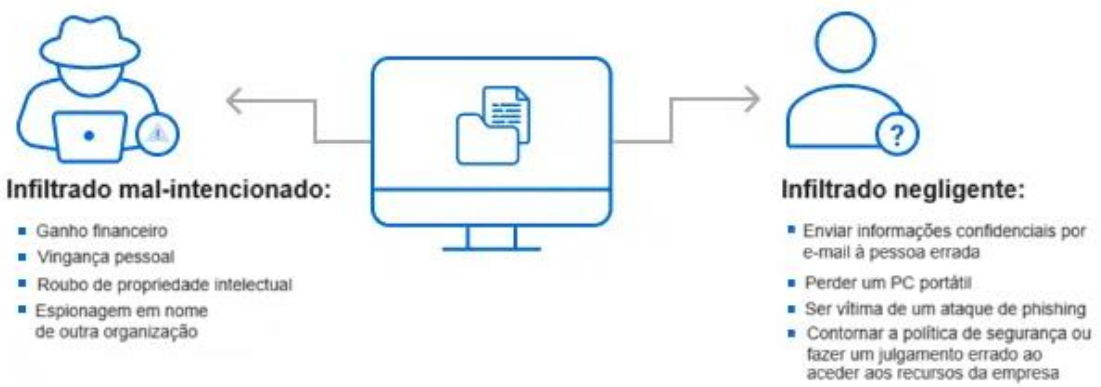

Figura 10 – Ameaças internas

Fonte: (Gamboa, 2023)

2.3.11 *Internet of Things (IoT) attacks*

Um ataque de IoT ocorre, quando os atacantes se apropriam indevidamente de dados de um dispositivo IoT ou juntam vários dispositivos IoT numa *botnet* utilizando-os para ataques DDoS, tal como se apresenta na figura 11.

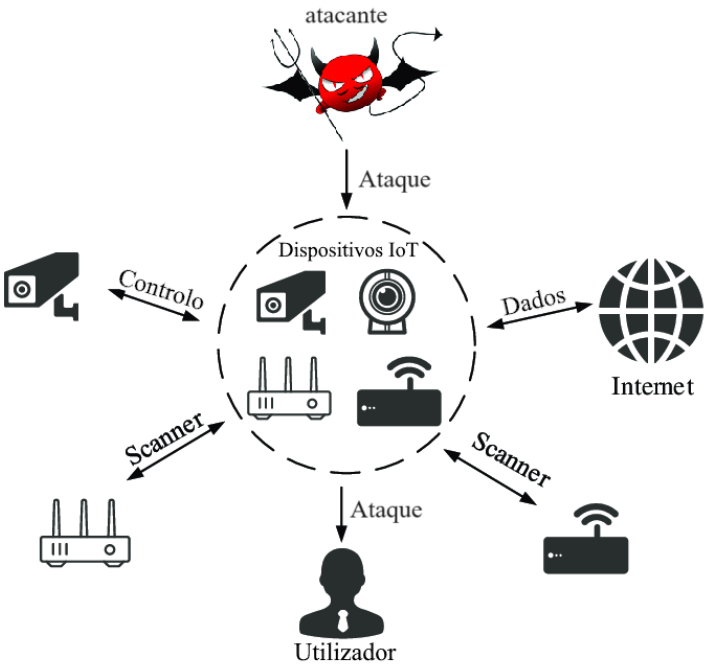

Figura 11 - Esquema ataque IoT

Fonte: (Zheng, 2020)

Os dispositivos IoT podem ser sensores de diversos tipos, controladores de voz, fechaduras inteligentes, detetores de fumo, sistemas de iluminação, rastreadores de *fitness*, implantes corporais integrados, entre outros (Fortinet, 2024).

2.3.12 Password attacks

Os ataques de senha incluem quaisquer ataques informáticos, nos quais os *hackers* tentam adivinhar, ou obter à força, as senhas, ou enganando a vítima para que a mesma desista delas, tal como esquematizado na figura 12.

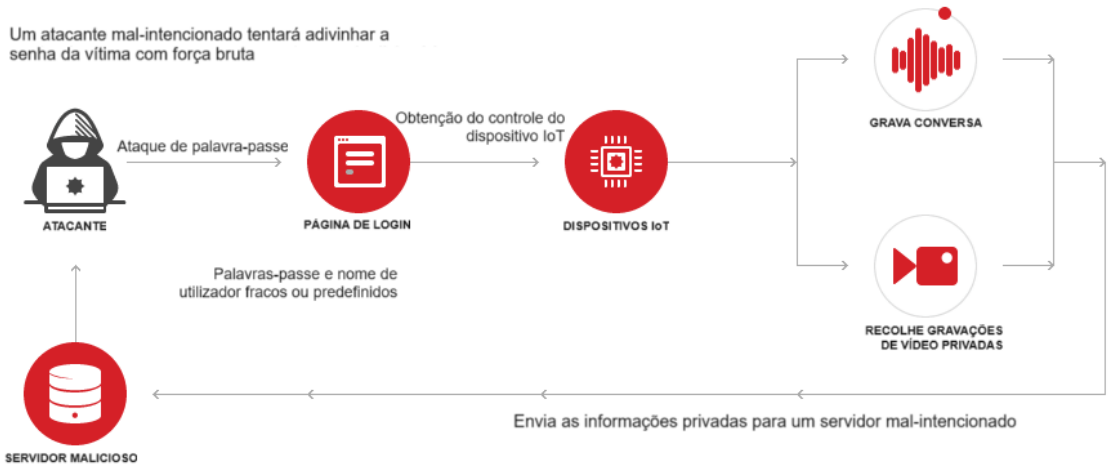

Figura 12 - Esquema de ataque de password

Fonte: (Heimdal, 2023)

Os ataques de senha envolvem a exploração de vulnerabilidades de autorização quebradas no sistema, combinada com ferramentas de ataque automático de senhas que aceleram o processo de descoberta e a quebra de senhas.

Os tipos de *Password attacks* são:

- *Password spraying* – na pulverização de senhas, o atacante adquire uma lista de nomes de utilizadores e tenta fazer *login* em todos utilizando a mesma senha. Assim, vai repetindo o mesmo processo tentando novas

senhas até que consiga violar o sistema de autenticação e obtenha acesso à conta e aos sistemas.

- *Brute force* – nos ataques de força bruta, o *hacker* utiliza a abordagem de tentativa e erro para adivinhar sistematicamente informações de *login*, credenciais e chaves de criptografia recorrendo à automatização de *scripts* para adivinhar senhas, conseguindo, através deste método tentar até biliões de senhas por segundo.

  No ataque reverso de força bruta, o *hacker* começa com uma senha conhecida e tenta encontrar o nome de utilizador ou número de conta correspondente.

- *Social engineering* – estes ataques utilizam táticas psicológicas para manipular as vítimas e levá-las a fornecer informações confidenciais. Esta manipulação funciona porque as pessoas são compelidas a agir por motivações como dinheiro, amor e medo, jogando com essas características, oferecendo falsas oportunidades para que as vítimas possam realizar esses desejos.

2.3.13 SQL *injection attacks*

A maioria dos *site*s utiliza bases de dados e linguagem SQL para armazenar informação confidencial, os *hackers* realizam um ataque de injeção de SQL que consiste na inserção ou "injeção" de uma consulta SQL maliciosa através dos dados de entrada do cliente para a aplicação.

Tal como esquematizado na figura 13, o atacante identifica os *site*s vulneráveis e injeta consultas SQL maliciosas, através de dados de entrada. Esta consulta SQL mal-intencionada é validada e o comando é executado pela base de dados, como se se tratasse de um comando legítimo e inofensivo. De seguida o agressor recebe acesso para visualizar e alterar registos, ou potencialmente agir como administrador do banco de dados.

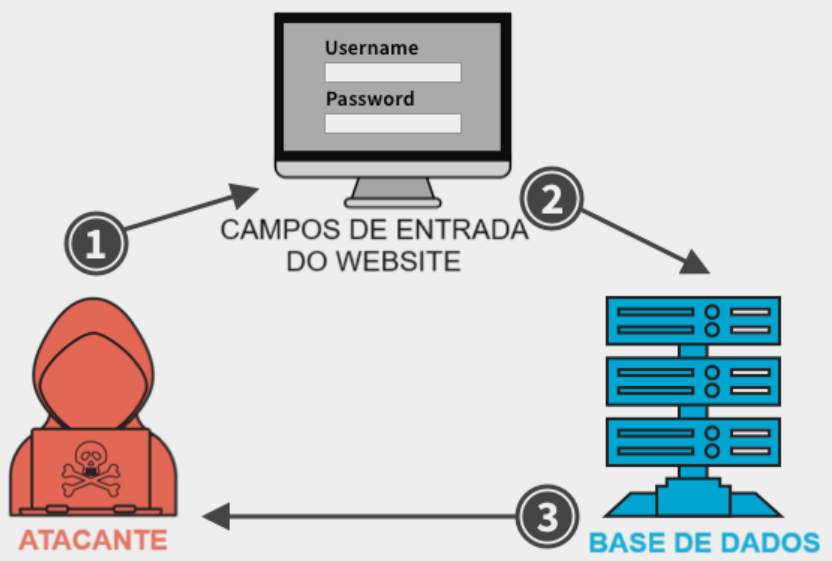

Figura 13 - Esquema de ataque SQL injection

Fonte: (Leonard, 2019)

Estes ataques permitem que os piratas informáticos falsifiquem identidade, adulterem dados, anulem transações, alterem saldos, permitam a divulgação completa de todos os dados no sistema, destruam dados ou os tornem inacessíveis e se tornem administradores do servidor de base de dados.

2.3.14 Manipulação de URL

A manipulação de URL ocorre quando os *hackers* alteram os parâmetros num endereço URL para o redirecionar para um *site* de *phishing* ou provocar a transferência automática de *malware*.

2.3.15 *Zero-day exploits and attacks*

Explorações de “dia zero” são vulnerabilidades de segurança informática que existem num *software* ou rede sem que o fabricante tenha conhecimento. Um ataque de “dia zero” ocorre, quando são utilizadas essas vulnerabilidades para entrar num sistema, com o objetivo de aceder indevidamente a dados ou causar danos, como ilustrado na figura 14.

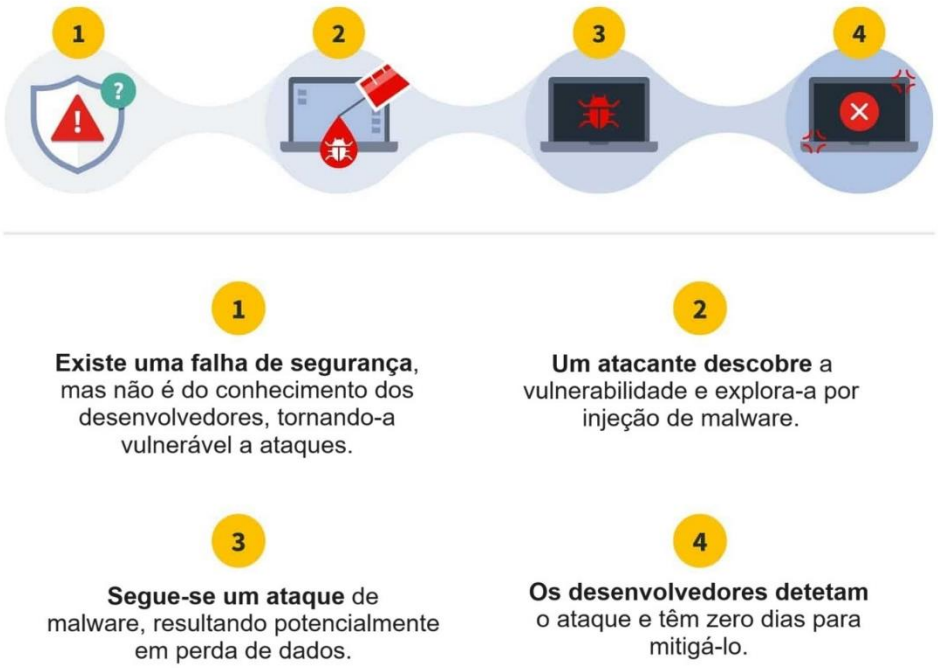

Figura 14 - Esquema de ataque Zero-day exploits

Fonte: (Ravoof, 2024)

O termo “dia zero” refere-se ao facto de que o fornecedor ou desenvolvedor acabou de saber da falha, e tem “zero dias” para a corrigir, é sabendo dessa falha que os criminosos aproveitam para atacar antes que a mesma possa ser resolvida.

2.4 Impacto das ameaças informáticas

As empresas que não garantirem a devida proteção das informações dos seus clientes enfrentam a possibilidade de sofrer danos, tanto financeiros, como à sua reputação, que podem ser extremamente prejudiciais (Toma et al., 2023).

As ameaças informáticas podem surgir de várias fontes, como grupos criminosos, *hackers*, terroristas, pessoas dentro das organizações e países estrangeiros envolvidos em atividades criminosas, ativismo político, espionagem

e guerra de informações. Estas ameaças podem ser intencionais ou acidentais, com diferentes motivações, incluindo obter dinheiro ou vantagens políticas. Por isso, é essencial proteger os sistemas contra essas ameaças para evitar consequências negativas para a segurança nacional, económica e pública (Wilshusen, 2012).

2.5 Cibersegurança

A segurança informática consiste na prevenção de acesso não autorizado, divulgação, interrupção, modificação e destruição de sistemas de computadores, redes e dados. Inclui a implementação de procedimentos robustos para identificar e impedir ataques informáticos.

O aumento exponencial dos ataques informáticos, motivou a um aumento de forma igual da importância da segurança digital.

A segurança informática inclui a proteção de *hardware*, redes e dados, em conjunto com a formação dos utilizadores, a aplicação de políticas de segurança e a manutenção de planos de resposta a incidentes para cenários de ataques informáticos (Dave et al., 2023).

A proteção das informações pessoais é uma das principais razões pelas quais, a defesa cibernética é tão primordial na era digital dos dias hoje, onde praticamente todas as pessoas têm presença *online* através de diversas atividades, tais como, redes sociais, serviços bancários *online* e compras, colocando constantemente os dados em risco de serem alvo de cibercriminosos (Dave et al., 2023). A proteção de dados tem por objetivo, garantir a disponibilidade, a confidencialidade e a integridade dos dados e sistemas (Dave et al., 2023).

A segurança da informação é fundamental para a promoção da confiança na economia digital, os consumidores devem-se sentir seguros de que os seus

dados permanecem seguros, promovendo o envolvimento *online* e apoiando o crescimento económico e a inovação (Dave et al., 2023).

Segundo Cram & D'Arcy (2023), é importante que os gestores garantam que as iniciativas de segurança informática sejam percebidas como justas e razoáveis pelos colaboradores, uma vez que as ameaças internas também devem ser tidas em consideração.

A importância da defesa cibernética está em ascensão na sociedade devido à transição digital em vários setores. Com a crescente integração das tecnologias de informação e comunicação, surgem também os perigos de interferência eletrónica e as suas consequências nas atividades e relações sociais. Para lidar com esses desafios, muitos países têm implementado estratégias direcionadas para proteger o ciberespaço e assegurar a segurança das redes e sistemas de informação.

Portugal possui uma estratégia nacional de segurança cibernética desde 2015, que foi atualizada em 2019 para a Estratégia Nacional para a Segurança do Ciberespaço 2019-2023 (Cncs, 2019). O Centro Nacional de Cibersegurança Português (CNCS) desempenha o papel de Autoridade Nacional de Cibersegurança, enquanto o CERT.PT atua como o CSIRT - *Computer Security Incident Response Team Nacional*, integrado no CNCS. Além disso, o CNCS é responsável por coordenar a elaboração, execução e revisão do Plano de Ação da Estratégia Nacional para a Segurança do Ciberespaço 2019-2023, em estreita colaboração com todas as entidades envolvidas na segurança informática.

A implementação desta estratégia visa fortalecer Portugal como um país mais seguro e próspero, por meio de ações inovadoras, inclusivas e resilientes, que preservem os valores essenciais do Estado de Direito.

Em 22 de janeiro de 2024 foi aprovado o Aviso nº 1517/2024, que estabelece critérios e requisitos de segurança para as entidades da Administração Pública

em relação à redes e sistemas de informação. Este documento baseia-se na Lei nº 46/2018, que constitui o Regime Jurídico da Segurança do Ciberespaço, e no decreto-Lei nº 65/2021, que detalha as medidas técnicas organizativas necessárias para a gestão de riscos de segurança informática. Este regulamento é uma resposta às crescentes ameaças informáticas e à necessidade de proteger dados sensíveis e de garantir a continuidade dos serviços públicos.

A continuidade dos negócios e a recuperação de ataques informáticos está intimamente relacionada com o planeamento e a preparação avançada, que incluem a implementação de medidas de segurança robustas, a realização de testes regulares de resiliência, e a formação contínua de colaboradores para reconhecer e responder a potenciais ameaças.

As equipas de gestão da continuidade de negócios e de gestão de incidentes devem ser o principal suporte, e a primeira linha de defesa para gerir os ataques informáticos, criando planos de resposta para os incidentes que provoquem interrupção nos negócios.

As credenciais roubadas raramente são utilizadas em tempo real, porque os cibercriminosos necessitam de tempo para analisar os dados que capturam. Quanto mais rapidamente uma organização detetar credenciais roubadas melhor, pois assim podem minimizar grandemente o risco de um ataque ou, pelo menos, limitar os danos.

Compreender o ciclo de vida de uma credencial roubada é fundamental, para proteger as organizações contra danos causados pelo roubo.

As diferentes fases do ciclo de vida do roubo de credenciais são a recolha, a filtragem e extração, a validação e o lucro. Na fase 1 - recolha, o atacante identifica os alvos vulneráveis e recolhe as informações necessárias sobre os mesmos, na fase 2 - filtragem e extração, o *hacker* acede aos dados do sistema atacado, na fase 3 – validação, o pirata informático verifica a qualidade e

utilidade dos dados obtidos e na fase 4 – lucro, o *hacker* procura obter lucro com o ataque, como esquematizado na figura 15.

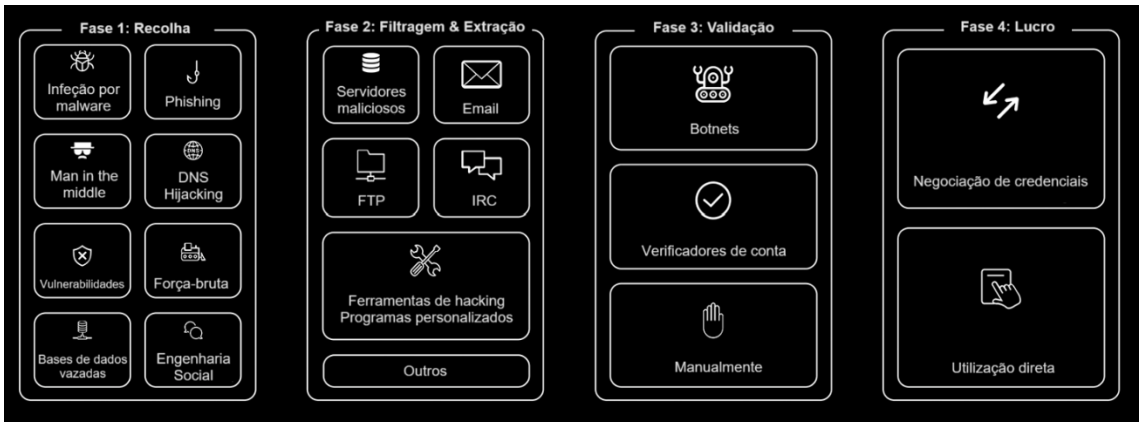

Figura 15 - O ciclo de vida do roubo de credenciais.

Fonte: (Esparza, 2019)

Segundo Piccirilli (2022) a segurança informática é vista como um mal necessário e não como um canal para o sucesso. Quando a atenção dos gestores se centra noutros objetivos de desempenho, o foco na segurança *online* pode diminuir.

Desde sempre, esta área e os investimentos relacionados recebem menos atenção por parte da gestão e, por isso, as empresas têm mais dificuldade em corresponder às iniciativas de proteção informática e em fornecer apoio para a sua conclusão com sucesso em relação a outras iniciativas propostas.

Para Pandya (2024), a aplicação de técnicas de aprendizagem máquina é essencial, para a deteção precoce de ataques informáticos em sistemas físicos. À medida que os métodos de ataque evoluem, torna-se cada vez mais urgente a necessidade de novos sistemas de deteção. A adoção do método de aprendizagem de máquina (ML), é vista como uma solução promissora para enfrentar os desafios da segurança informática.

Arroyabe (2023) defende que a gestão de riscos digitais surge nas organizações como um elemento-chave para garantir a resiliência das empresas, permitindo o desenvolvimento das suas atividades sem afetar a sua operacionalidade.

Em comparação com as grandes empresas, as PME enfrentam desafios substanciais em termos de capacidade para gerir estes desafios, tais como falta de conhecimento, de competências e de recursos financeiros para planear e implementar a segurança e a transformação digital.

Muitas PME consideram a proteção digital como algo sem importância, acreditando que é improvável serem alvo de ataques informáticos, no entanto, estas empresas são de facto alvo, quer de ataques automatizados, quer de ataques deliberados e podem servir como porta de entrada para ataques à segurança digital na cadeia de abastecimento de grandes empresas (Senapati, 2024).

A perceção da segurança da informação que existe entre as PME leva a uma falta de atenção por parte da gestão, resultando no aumento das vulnerabilidades e do potencial risco de problemas operacionais nestas empresas (Senapati, 2024).

A criação de sistemas de segurança informática envolve o desenvolvimento e implementação de medidas operacionais. Implica também decisões organizacionais e estratégicas relativas à proteção de dados, desde a atribuição de equipamentos para a gestão da segurança da informação, desenvolvimento de políticas e sistemas de avaliação de riscos de proteção informática, incluindo questões de defesa cibernética nas reuniões de dirigentes das empresas. Estas medidas têm como objetivo desenvolver procedimentos e rotinas que permitam o correto funcionamento das empresas e dos seus colaboradores, reduzindo as vulnerabilidades de segurança informática (Senapati, 2024).

As organizações devem envolver os gestores a todos os níveis, na atualização sobre as questões de gestão de riscos digitais.

A utilização quase exclusiva do mecanismo de controlo não é suficiente, visto que uma elevada percentagem de incidentes e vulnerabilidades provêm da inadequada utilização das políticas e procedimentos por parte dos colaboradores (Senapati, 2024).

Para melhorar a conformidade dos funcionários com as políticas de gestão de riscos digitais, os gestores podem adotar várias estratégias, tais como, investir em programas de formação contínua para quadros superiores, de forma a garantir a sua participação ativa na gestão de riscos digitais e para funcionários, informando-os sobre as ameaças informáticas e a importância de seguir as políticas de segurança. Assegurar que as políticas de segurança são comunicadas de forma clara e compreensível, evitando termos técnicos que possam confundir os colaboradores. Encorajar um ambiente onde os funcionários possam dar *feedback* sobre as políticas de segurança e discutir abertamente quaisquer preocupações ou sugestões. Utilizar reforço positivo, como recompensas ou reconhecimento, para incentivar a conformidade com as políticas de segurança. Simplificar os processos de segurança sempre que possível para reduzir a inconveniência para os funcionários, aumentando assim a probabilidade de adesão (Senapati, 2024).

Os líderes devem demonstrar a importância da segurança informática através do seu próprio comportamento, cumprindo as políticas e promovendo uma cultura de segurança, avaliado regularmente a eficácia das políticas de segurança e promovendo atualizações, conforme necessário, para antecipar novas ameaças ou mudanças no ambiente de trabalho. Implementando estas estratégias, os gestores podem construir uma cultura de segurança informática mais robusta e aumentar e garantir a conformidade dos funcionários com essas políticas.

Todas as empresas devem investir em bons programas de segurança informática, utilizar sempre a tecnologia “Rede Privada Virtual” (VPN) e promover formação adequada de todos os colaboradores.

As empresas com meios económicos devem investir numa equipa de TI e também devem subscrever um seguro específico para esta área (Seguro Informático), por forma a mitigar os custos com os ataques informáticos.

2.6 Tendências emergentes das técnicas aplicadas nos ataques informáticos

As novas tecnologias, como por exemplo a Inteligência Artificial (IA), trazem várias oportunidades e desafios para as organizações, e a IA pode ser utilizada tanto para o bem como para o mal, dependendo da maneira como é programada. Assim como é uma importante ferramenta para a defesa das organizações, também o é para quem as ataca.

Os cibercriminosos estão a aproveitar as tecnologias de IA para desenvolver programas inteligentes de *malware* e executar ataques cada vez mais furtivos e destrutivos.

Na visão de Cândido (2021), as ameaças estão bem presentes, em constante mudança e são cada vez mais diversificadas. Os ataques de *machine-to-machine* (M2M), ataques silenciosos e altamente personalizados, estão a dificultar a atuação das abordagens tradicionais de segurança, as quais não conseguem responder de forma eficaz, mostrando-se lentas e incapazes de se adaptar a estas novas ameaças.

De acordo com a perspetiva de Nunes (2021), os ataques informáticos muitas vezes exploram a heterogeneidade das redes e dos sistemas de informação, onde coexistem múltiplas gerações de *hardware* (o legado dos diversos sistemas) e diferentes versões de *software*.

Devido a condicionantes operacionais, orçamento insuficiente ou outras razões que provoquem o atraso na sua substituição, os sistemas introduzem múltiplas vulnerabilidades e fornecem uma área de ataque alargada, fazendo com que se torne cada vez mais difícil a gestão dos riscos daí decorrentes.

Empresas, indivíduos e até mesmo o Setor Público enfrentam, atualmente, os desafios de um mundo cada vez mais em rede, incerto, complexo, volátil e ambíguo (VICA – Volátil, Incerto, Completo e Ambíguo) onde as ameaças assumem um carácter cada vez mais multiforme e híbrido.

Pela citação de Cândido (2021), o *ransomware* está cada vez mais evoluído e incorpora técnicas avançadas de evasão à deteção, conseguindo comprometer na sua totalidade, em poucos minutos, o parque informático das organizações.

O *ransomware* continua a evoluir com novas técnicas e tecnologias que surgem constantemente: em 2021 eram utilizadas, entre outras, a "dupla extorsão" (os operadores de *ransomware* não apenas criptografam os dados, como também os publicam na *internet*), em 2022 esta técnica evoluiu para "extorsão quádrupla", ou seja, coação das empresas vítimas para pagamentos de grandes somas de dinheiro, negando o acesso a dados críticos, retendo o acesso às máquinas de produção e contactando diretamente os clientes e as partes interessadas.

De acordo com Nunes (2021), o acesso à quantidade de recursos disponíveis *online*, *kits* de *ransomware*, de *phishing*, que qualquer um, mesmo com pouca experiência pode comprar por menos de 60€, facilita a programação e endereçamento deste tipo de ataques.

Os ataques de *ransomware* tornaram-se mais sofisticados devido à especialização: já não existe apenas o atacante isolado, mas sim um grupo que trata de enviar os *e-mails* e fazer a implantação do *ransomware* e, outros grupos especializados em dar acesso como um serviço, por fim, existe quem se dedica à gestão destes processos. A sofisticação e tornar isto num modelo de negócio leva à especialização, o que os torna mais difíceis de combater. Além da IA, o *ransomware* também já recorre à técnica de *machine learning* (ML).

Conforme Carreiro (2022), os ataques DDoS continuam a revelar-se eficazes e os *hackers* que utilizam este método estão a tornar-se mais prolíficos e agressivos.

Como mencionado por Gáldon (2022), apesar dos avanços nas ferramentas de segurança, os cibercriminosos continuam a explorar vulnerabilidades humanas e a utilizar métodos sofisticados para realizar ataques. Estes ataques muitas vezes começam com a exploração do elemento humano nas organizações: mesmo os ataques mais tecnológicos, têm uma componente significativa que depende da manipulação de pessoas utilizando engenharia social e técnicas de *deepfakes*.

À luz do que diz Carreiro (2023), com a evolução das técnicas de *hacking*, especialmente os modelos de linguagem avançados, como o *ChatGPT* , podem ser utilizados para criar mensagens de *phishing* mais convincentes e personalizadas, aumentando a eficácia dos ataques de engenharia social.

Como afirma Castro (2024), com a utilização da IA, os ataques de *phishing* e *spear phishing* tornaram-se mais credíveis, sem erros gramaticais, automatizados, permitindo que os criminosos realizem campanhas em larga escala, mas com personalização dinâmica para cada vítima, o que aumenta a sua taxa de sucesso.

Com base em Leviathan (2024), o surgimento de uma nova técnica para ultrapassar sistemas de VPN chamada *TunnelVision*, permite aos cibercriminosos espiar o tráfego das vítimas, em qualquer sistema que deveria ser protegido pela VPN, invalidando assim a sua proteção.

Capítulo 3 - METODOLOGIA DE INVESTIGAÇÃO

Para se poder classificar e conhecer os tipos de ataques mais comuns, bem como identificar as tendências emergentes relativamente às técnicas aplicadas nos ataques informáticos, realizaram-se pesquisas na web e em literatura profissional e académica, de modo a proceder à identificação dos principais ataques e ao seu modo de funcionamento, sendo apresentados na Revisão da Literatura.

Para efetuar a revisão da literatura necessária à realização deste trabalho, o método escolhido foi a Metodologia de Revisão Sistemática da Literatura com PRISMA 2020 *(Preferred Reporting Items for Systematic reviews and Meta-Analyses).*

Com esta metodologia, recolheu-se, avaliou-se e sintetizou-se a literatura existente sobre o tema a estudar, com o objetivo de se conseguir obter conclusões gerais, mas confiáveis sobre o mesmo. Por esse motivo, escolheram-se bases de dados com reputação e credibilidade, amplamente reconhecidas e utilizadas por académicos, pesquisadores e instituições de ensino em todo o mundo e já anteriormente identificadas. A sua reputação indica que oferecem conteúdo de qualidade, que é frequentemente atualizado garantindo que os utilizadores têm acesso às pesquisas mais recentes e relevantes, onde especialistas na área avaliam a qualidade e a validade da pesquisa antes da publicação.

Para conhecer a forma como são identificados na literatura os danos reputacionais, formas de prevenir ataques informáticos e mitigar os riscos da presença das empresas *online*, realizaram-se pesquisas, onde se utilizou como frase de pesquisa seguinte e o intervalo dos anos de publicação de 2018 a 2024

(“*reputational impact*” OR ”impacto reputacional”) AND (“*cyber attack*” OR “cyber crime” OR “ciberataque” OR “ataque informático” OR “crime informático”)

Com esta pesquisa na base de dados EBSCO obtiveram-se 10 resultados, na base de dados GOOGLE SCHOLAR obtiveram-se 230 resultados, na base de dados DOAJ obtiveram-se 1629 resultados, na base de dados JSTOR obtiveram-se 7 resultados, na base de dados *Proquest ebook* central obtiveram-se 2189 resultados, na base de dados *ScienceDirect* obtiveram-se 25 resultados e na base de dados SCOPUS obtiveram-se 13 resultados.

Com o objetivo de analisar os ataques informáticos perpetrados em Portugal nos anos de 2018 a 2023, efetuou-se um estudo documental, pesquisando em notícias na *web* e também nos relatórios do Centro Nacional de Cibersegurança de Portugal, quais as empresas que foram alvo de ataques informáticos nos últimos 6 anos (2018-2024) e centrou-se o presente este estudo nestas empresas.

No que respeita ao estudo documental referente aos relatórios das empresas vítimas de ataques, nos relatórios e contas das empresas pesquisou-se por dados relacionados com os ataques informáticos, utilizando-se as seguintes palavras-chave:

"crime(s) informático(s)", "ciberataque(s)", "cibersegurança", "segurança informática", "ataque(s) informático(s)", "*cybersecurity*", "*cyberattack*", "*cyber risk*".

Capítulo 4 - ESTUDO DOCUMENTAL

Com o objetivo de analisar os ataques informáticos perpetrados em Portugal nos anos de 2018 a 2023, efetuou-se um estudo documental, pesquisando em notícias na *web* e também nos relatórios do Centro Nacional de Cibersegurança de Portugal, quais as empresas que foram alvo de ataques informáticos nos últimos 6 anos (2018-2024) e orientou-se para estas empresas este estudo.

Para categorizar as notícias da imprensa sobre os ataques sofridos pelas empresas, recorreu-se à função de resumo do *ChatGPT* como auxílio na procura do tipo de ataques sofridos. Desta forma, foi possível conhecer a forma como as empresas colocam nos relatórios de divulgação os ataques de que foram alvo.

De forma a conhecer como as empresas indicam, nos seus relatórios de divulgação, a mitigação dos riscos e desafios associados aos ataques informáticos e prevenir as ameaças, pesquisou-se nos seus Relatórios e Contas e recorreu-se à função de resumo do *ChatGPT* como ferramenta auxiliar.

Com o objetivo de identificar os danos reputacionais que surgiram na sequência dos ataques informáticos, pesquisou-se nos seus Relatórios e Contas dos anos (2019-2023) e recorrendo à ajuda do *ChatGPT*.

4.1 Resultados

Neste subcapítulo apresentam-se os resultados obtidos, a partir da análise dos dados recolhidos durante a pesquisa. A apresentação dos resultados será acompanhada de tabelas que contêm as principais informações, facilitando a interpretação e a discussão subsequente. A tabela 4 está ordenada por data do ataque e contém o nome da empresa, a data do ataque, o tipo de ataque sofrido, se a empresa reportou esse ataque nos seus relatórios ou não, qual foi a duração das disrupções provocadas, qual o valor do prejuízo causado e a fonte de onde foi obtida a notícia da ocorrência do ataque.

O ataque à CUF ocorreu a 3 de agosto de 2018, foi um ataque de *ransomware.* A CUF mencionou a ocorrência deste ataque no seu Relatório Integrado de 2018, na página 49, este ataque teve como objetivo impedir a utilização dos sistemas, impedindo assim o cesso a informações clínicas e não clínicas. A CUF deu prioridade à recuperação dos dados invadidos e o evento foi comunicado aos clientes, à Comissão Nacional de Proteção de Dados (CNPD) e à Polícia Judiciária (PJ) (CUF, 2018).

O ataque à Fundação Champalimaud foi um ataque de *ransomware* e ocorreu no dia 1 de julho de 2019. Este ataque não se encontra reportado em nenhum dos seus relatórios, a sua duração foi de 2 dias. O ataque à EDP ocorreu a 13 de abril de 2020. O ataque ocorrido foi de *ransomware* e foi pedido um valor de resgate de 10.000.000€, no entanto este ataque não foi mencionado em nenhum dos seus relatórios. O ataque à Altice ocorreu no dia 16 de abril de 2020, foi um ataque de *ransomware* e a Altice não referiu em nenhum dos seus relatórios este ataque. O ataque ao Hospital Divino Espírito Santo ocorreu no dia 24 de junho de 2021. Foi um ataque de *ransomware*, cujas disrupções duraram 30 dias, no entanto não foi mencionado em nenhum dos seus relatórios.

O ataque ao Grupo Impresa aconteceu no dia 24 de janeiro de 2022. Foi um ataque de *ransomware* e na página 7 do Relatório e Contas 2022 é referido um aumento de 9,5% dos custos operacionais motivados por este ataque, pela Guerra na Ucrânia, pelo aumento dos custos energéticos e pelo aumento do preço do papel do jornal impresso. Com este ataque informático o grupo teve alguns constrangimentos nas suas comunicações, tendo sido criado um endereço de *e-mail* alternativo do atendimento, a fim de garantir a manutenção do contacto permanente e a resposta aos telespetadores. O ataque foi comunicado à Comissão Nacional de Proteção de Dados. As disrupções provocadas tiveram uma duração de 20 dias (Impresa, 2022).

O ataque ao Website da Assembleia da República ocorreu a 30 de janeiro de 2022, foi um ataque de *ransomware*.

O ataque à Vodafone ocorreu no dia 6 de fevereiro de 2022, foi um ataque de *ransomware*, as disrupções provocadas duraram 2 dias. A Vodafone referiu o ataque informático na página 6 do seu Relatório & Contas de abril 2022 a março 2023 (Vodafone, 2022).

O Grupo Cofina sofreu o ataque informático *ransomware* a 6 de fevereiro de 2022, não havendo referência a ele nos seus relatórios. O Grupo Visão sofreu o ataque de *ransomware* a 9 de fevereiro de 2022. O Grupo Germano de Sousa sofreu o ataque de ransomware a 10 de fevereiro de 2022, as disrupções provocadas tiveram a duração de 5 dias.

O Grupo Sonae sofreu um ataque de *ransomware* a 30 de março de 2022. O ataque informático foi reportado na página 96 do Relatório Anual Integrado 2022 (Sonae, 2022).

O Hospital Garcia de Orta sofreu um ataque de *ransomware* a 26 de abril de 2022. As disrupções provocadas duraram 2 dias, este ataque impossibilitou o acesso aos sistemas de informação clínicos e administrativos, levando à necessidade de retornar ao uso de registos em papel. Só em dezembro de 2022 é que a normalidade da situação foi alcançada (HGO, 2022). Este ataque foi referido na página 3 do Relatório e Contas 2022.

Os SMTUC foram alvo de um ataque de *ransomware* a 2 de maio de 2022. Durante esse ano verificaram-se múltiplas tentativas de ataques informáticos, que evidenciaram a vulnerabilidade dos seus sistemas de segurança informática. Os SMTUC referiram este ataque na página 42 do Relatório de Gestão e Contas 2022 (SMTUC, 2022).

A Agência Lusa foi vítima de ataques DDoS em maio e junho de 2022. As disrupções provocadas pelos ataques tiveram uma duração de 4 dias, a Agência Lusa investiu cerca de 538.000 €, sobretudo na aquisição de soluções de equipamentos de cibersegurança das infraestruturas de rede e sistemas de informação, com a adjudicação de serviços à Altice e a aquisição de 4 *firewalls*

dedicadas (A. Lusa, 2022). A Agência Lusa fez referência aos ataques na página 5 do seu Relatório e Contas 2022.

A Eletricidade dos Açores foi vítima de um ataque informático a 16 de maio de 2022. O Grupo Newsplex foi vítima de um ataque de *ransomware* a 29 de junho de 2022. As disrupções provocadas pelos ataques tiveram uma duração de 2 dias, o ataque não foi mencionado nos seus relatórios.

A TAP sofreu um ataque de *ransomware* a 25 de agosto de 2022. A Tap referiu este ataque na página 25 do seu Relatório de Gestão e Contas Consolidadas. Por este ataque foram pedidos 5,7 milhões de euros de resgate (TAP, 2022b).

Os Websites do Sporting Clube de Portugal e do Futebol Clube do Porto foram vítimas de um ataque DDoS a 15 de setembro de 2022. A Câmara Municipal de Loures foi vítima de um ataque de *ransomware* a 23 de setembro de 2022. O Banco Comercial Português foi vítima de um ataque DDoS a 3 de outubro de 2022. A Rede do Estado Maior das Forças Armadas sofreu um ataque de *ransomware* nos dias 8 e 27 de setembro de 2022.

Ao analisar os relatórios destas empresas, verificou-se que apenas 34,8% divulgaram nos seus relatórios que tinham sido vítimas de ciberataque, 21,7% apresentam medidas de segurança implementadas ou a implementar, 21,7% não fazem qualquer referência, nem a medidas de segurança *online* nem a ataques informáticos sofridos, e os restantes 21,7% não disponibilizaram os seus relatórios para acesso *online*.

Nota: As empresas assinaladas com (*) na tabela 4 não reportaram os ataques nos seus relatórios e contas, mas fizeram referências a medidas de segurança da informação.

Tabela 4 - Tabela identificativa de ataques

Nome da empresa vítima	**Data do ataque**	**Tipo de ataque sofrido**	**A empresa reportou o ataque no relatório anual de contas? (sim/não)**	**Quantos dias durou o ataque?**	**Valor do prejuízo causado (€) / valor investido em cibersegurança (€)**	**Fonte**
CUF	03/08/2018	*Ransomware*	Sim	nd	nd	(CUF)
Fundação Champalimaud	01/07/2019	*Ransomware*	Não	2 dias		(FC)
EDP	13/04/2020	*Ransomware*	Não (*)	nd	Pedido de resgate de 10M €	(EDP)
Altice	16/04/2020	*Ransomware*	Não (*)	nd	nd	(ALTICE)
Hospital Divino Espírito Santo, em Ponta Delgada.	24/06/2021	*Ransomware*	Não	30 dias		(HDES)
Grupo Impresa	02/01/2022	*Ransomware*	Sim	De 2 a 20 dias		(GI)
Web*site* da Assembleia da República	30/01/2022	*Ransomware*	-	nd	nd	(AR)
Vodafone	06/02/2022	*Ransomware*	Sim	2 dias		(VODAFONE)
Grupo Cofina	06/02/2022	*Ransomware*	Não (*)	nd	nd	(GC)
Trust in News - Visão	09/02/2022	*Ransomware*	-	nd	nd	(TIN)
Grupo Germano de Sousa	10/02/2022	*Ransomware*	-	5 dias		(GGS)
Sonae	30/03/2022	*Ransomware*	Sim	nd	nd	(SONAE)
Hospital Garcia de Orta	26/04/2022	*Ransomware*	Sim	8 meses		(HGO)
SMTUC	02/05/2022	*Ransomware*	Sim	nd	nd	(SMTUC)
Agência Lusa	12/05/2022	DDoS	Sim	4 dias	538.000 €	(AL)
Eletricidade dos Açores	16/05/2022		Não (*)	nd	nd	(EDA)
Grupo Newsplex	29/06/2022	*Ransomware*	-	2 dias		(GN)
TAP	25/08/2022	*Ransomware*	Sim	nd	5,7 M €	(TAP)
Web*sites* Sporting CP	15/09/2022	DDoS	Não	nd	nd	(SCP)
Web*sites* FC Porto	15/09/2022	DDoS	-	nd	nd	(FCP)
Câmara Municipal de Loures	23/09/2022	*Ransomware*	Não	nd	nd	(CML)
BCP	03/10/2022	DDoS	Não (*)	nd	nd	(BCP)
Rede do Estado Maior General das Forças Armadas	08/09/2022 e 27/09/2022	*Ransomware*	Não	nd	nd	(REMGFA)

Fonte: Elaboração Própria

Após o ataque sofrido, as empresas acrescentaram medidas de segurança informática às que já possuíam (tabela 5).

A CUF deu prioridade à recuperação dos dados afetados e implementou ações corretivas, como o robustecimento da segurança das infraestruturas de informação, aumento da segmentação da rede, reforço dos *backups*, melhorias nas firewalls e implementação de melhorias nas cópias de segurança. Além disso, a José de Mello Saúde tem uma Direção de Auditoria Interna que avalia os sistemas de controle interno, contribuindo para o desenvolvimento e robustez do processo de gestão de risco. Em 2018, foram consolidados os processos de planeamento e execução das auditorias nas áreas de risco crítico, incluindo o *follow-up* das recomendações, como parte das medidas de segurança e controle da organização (CUF, 2018; REMGFA, 2022).

A EDP reforçou as medidas de mitigação como o *cyber-range*, aquisição dos serviços do Centro de Operações de Segurança - SOC, seguro de riscos informáticos e sessões de formação e sensibilização, bem como a implementação de boas práticas de gestão de crises e continuidade de negócio. Para além disso, a EDP dispõe de uma apólice de seguros abrangente para danos patrimoniais, responsabilidade civil e riscos ambientais, gerida pela Unidade de Riscos Seguráveis. Existe ainda um comité de Prevenção e Segurança que coordena as melhores práticas de operação, inspeção e manutenção preventiva e estabelece planos de gestão de crises e de continuidade de negócio (EDP, 2020).

A Altice Portugal disponibilizou no seu site institucional dicas e informações sobre como as pessoas se podem proteger de ataques de cibersegurança, adotando algumas regras simples no seu dia a dia (Altice, 2020).

O Grupo Impresa implementou várias medidas de segurança, como o aumento das políticas e controlos de segurança física e o reforço dos mecanismos de encriptação de dados, *firewalls* e autenticação multifator. As políticas e

procedimentos do Grupo Impresa abrangem áreas como a proteção de dados, a gestão de riscos e sustentabilidade e a conformidade com os normativos legais. A empresa dispõe ainda de um regulamento para a comunicação de irregularidades e de um programa de proteção da propriedade intelectual (Impresa, 2022).

No relatório o Grupo Cofina menciona iniciativas relacionadas com a formação de funcionários em cibersegurança, a implementação de autenticação multifactor para acesso remoto a sistemas e a utilização de soluções como *Cisco Secure Endpoint*, *Cisco Umbrella* e *Veeam backup* para mitigar riscos e garantir a continuidade das operações face aos desafios da transformação digital (Cofina, 2022).

O Grupo Sonae após a deteção do incidente, ativou a equipa de gestão de crise que se focou na análise e caracterização do mesmo, bem como na implementação de ações de contenção, mitigação e recuperação (Sonae, 2022).

O Hospital Garcia de Orta implementou iniciativas para melhorar a segurança. Estas medidas incluíram ações imediatas e outras a implementar a médio ou longo prazo, com o objetivo de minimizar o risco de futuros ataques informáticos. As iniciativas assentaram em três pilares principais, nomeadamente no reforço da segurança no repositório de *backups* e imagens, no investimento em equipamentos e formação para melhorar a segurança e na implementação de medidas para melhorar a segurança global da infraestrutura informática do hospital (HGO, 2022).

De modo a minimizar os efeitos colaterais dos ataques informáticos, os SMTUC recorreram ao apoio de uma empresa especializada em Cibersegurança de forma a adotar medidas corretivas e diversas outras ações (SMTUC, 2022).

A Lusa lançou medidas para um plano de Cibersegurança mais eficaz para as suas infraestruturas, clientes e colaboradores, e finalizou o projeto *Contrafake*, que desenvolveu um protótipo baseado em Inteligência Artificial para analisar a

credibilidade de conteúdos informativos ao nível do conteúdo e do contexto Efetuou também testes de intrusão, como uma medida sistemática, por uma empresa externa, testes de *phishing* e testes à nova infraestrutura de centros de dados (A. Lusa, 2022).

A empresa Eletricidade dos Açores para melhorar a sua segurança, optou pelo cumprimento dos requisitos legais na área da cibersegurança para a rede de comunicações e sistemas de informação (EDA, 2022).

A TAP promove a monitorização da segurança informática numa base contínua, tendo por isso adotado e implementado mais medidas para reforçar a segurança dos sistemas de informação, tais como ferramentas tecnológicas para prevenir e responder rapidamente a ataques informáticos. Também adaptaram os processos a cenários de risco em mudança e promoveram formações de sensibilização regulares (TAP, 2022b).

Como medidas de cibersegurança o BCP investiu na manutenção de *hardware* e *software*, implantou uma nova infraestrutura tecnológica que inclui a atualização da plataforma *cloud* e a utilização de componentes de TI modulares que permitem desenvolver competências de topo ao nível da escalabilidade, resiliência e eficiência em custo (BCP, 2022).

Tabela 5 - Medidas de segurança / cibersegurança implementadas após os ataques informáticos

Nome da empresa vítima	**Data do ataque**	**Medidas de segurança / cibersegurança implementadas**	**Título do relatório**
CUF	03/08/2018	- Recuperação dos dados afetados; - Implementação de ações corretivas; - Aumento da segmentação da rede; - Reforço dos *backups*; - Melhorias nas *firewalls;* - Implementação de melhorias nas cópias de segurança.	CUF - Relatório Integrado 2018

Nome da empresa vítima	**Data do ataque**	**Medidas de segurança / cibersegurança implementadas**	**Título do relatório**
EDP	13/04/2020	- Reforço de medidas de mitigação como o *cyber-range*, Centro de Operações de Segurança (SOC), seguro de riscos informáticos e sessões de formação e sensibilização; - Implementação de boas práticas de gestão de crises e continuidade de negócio; - Apólice de seguros abrangente para danos patrimoniais, responsabilidade civil e riscos ambientais; - Comité de Prevenção e Segurança que coordena as melhores práticas de operação, inspeção e manutenção preventiva.	EDP - Relatório Integrado 2020
Altice	16/04/2020	- Dicas e informações sobre como as pessoas se podem proteger de ataques de cibersegurança.	Altice - relatório sustentabilidade 2020
Grupo Impresa	02/01/2022	- Aumento das políticas e controlos de segurança física; - Reforço dos mecanismos de encriptação de dados, *firewalls* e autenticação multifator; - Regulamento para a comunicação de irregularidades; - Programa de proteção da propriedade intelectual.	Grupo Impresa - Relatório de Sustentabilidade 2022
Grupo Cofina	06/02/2022	- Formação de funcionários em cibersegurança; - Implementação de autenticação multifactor para acesso remoto a sistemas; - Utilização de soluções como *Cisco Secure Endpoint*, *Cisco Umbrella e Veeam backup*.	COFINA - Relatório contas 2022
Sonae	30/03/2022	- Equipa de gestão de crise; - Implementação de ações de contenção, mitigação e recuperação.	MC SONAE – Relatório anual 2022
Hospital Garcia de Orta	26/04/2022	- Reforço da segurança no repositório de *backups* e imagens; - Investimento em equipamentos; - Formação para melhorar a segurança; - Implementação de medidas para melhorar a segurança global da infraestrutura informática do hospital.	Hospital Garcia de Orta – Relatório e Contas 2022
SMTUC	02/05/2022	- Empresa especializada em Cibersegurança.	SMTUC – Relatório Gestão 2022
Agência Lusa	12/05/2022	- Medidas para um plano de Cibersegurança mais eficaz para as suas infraestruturas, clientes e colaboradores; - Protótipo baseado em Inteligência Artificial para analisar a credibilidade de conteúdos informativos ao nível do conteúdo e do contexto.	LUSA – Relatório e Contas 2022
Eletricidade dos Açores	16/05/2022	- Cumprimento dos requisitos legais na área da cibersegurança para a rede de comunicações e sistemas de informação.	EDA - Relatório Sumário Contas Reguladas 2022

Nome da empresa vítima	Data do ataque	Medidas de segurança / cibersegurança implementadas	Título do relatório
TAP	25/08/2022	- Monitorização da segurança informática numa base contínua; - Reforço da segurança dos sistemas de informação; - Adaptação dos processos a cenários de risco em mudança; - Promoção de formações de sensibilização regulares.	TAP - Relatório de Gestão e Contas Consolidadas 2022
BCP	03/10/2022	- Manutenção de *hardware* e *software*; - Implantação de uma nova infraestrutura tecnológica.	BCP - Relatório contas 2022

Fonte: Elaboração Própria

As medidas de cibersegurança implementadas pelas empresas analisadas, refletem uma abordagem proativa e abrangente para lidar com os desafios crescentes de cibersegurança. O reforço da segurança das infraestruturas de informação, a segmentação da rede, o *backup* robusto de dados, a melhoria das *firewalls* e a implementação de boas práticas de gestão de crises e continuidade de negócio são estratégias essenciais para proteger os ativos digitais, e garantir a resiliência contra possíveis ataques informáticos.

Além disso, a oferta de dicas de proteção contra ataques informáticos, e o investimento em formação de funcionários em cibersegurança demonstram um compromisso com a consciencialização e a capacitação dos colaboradores, para lidar com ameaças digitais. A utilização de soluções tecnológicas avançadas, como "*Cisco Secure Endpoint*", "*Cisco Umbrella*" e "*Veeam backup*", a importância de adotar ferramentas especializadas para mitigar riscos e garantir a continuidade das operações num ambiente digital cada vez mais complexo.

Essas iniciativas refletem a crescente consciencialização das organizações, sobre a importância da segurança informática e a necessidade de implementar medidas proativas para proteger os seus sistemas e dados, contra potenciais ameaças.

Analisando os relatórios e contas das empresas que foram atacadas durante os anos de 2018 a 2023, observa-se que entre aquelas que fazem referência à implementação de medidas de cibersegurança, 83% já tinham essas medidas em vigor, enquanto 17% começaram a implementá-las após experimentar ataques informáticos.

Tabela 6 - Análise dos relatórios período de 2018-2023

Nome da empresa vítima	**Data do ataque**	**As medidas de segurança / cibersegurança foram implementadas antes ou depois dos ataques**	**Quais relatórios incluem referências a medidas de cibersegurança**
CUF	03/08/2018	As medidas de cibersegurança foram implementadas após o ataque.	2018, 2019, 2020, 2021, 2022 e 2023
EDP	13/04/2020	As medidas de cibersegurança já estavam implementadas antes do ataque.	2018, 2019, 2021, 2022 e 2023
Altice	16/04/2020	As medidas de cibersegurança já estavam implementadas antes do ataque.	2019, 2020, 2021, 2022 e 2023
Grupo Impresa	02/01/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2020, 2021, 2022 e 2023
Grupo Cofina	06/02/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2021 e 2022
Sonae	30/03/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2019, 2020, 2021, 2022 e 2023
Hospital Garcia de Orta	26/04/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2020, 2021 e 2022
SMTUC	02/05/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2020, 2021, 2022 e 2023
Agência Lusa	12/05/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2018, 2019, 2020, 2021, 2022 e 2023
Eletricidade dos Açores	16/05/2022	As medidas de cibersegurança foram implementadas após o ataque.	2022
TAP	25/08/2022	Antes do ataque de 2022 já faziam referência a medidas de segurança da informação nos seus relatórios e contas anuas, no entanto só depois do ataque foi criado um Plano de Prevenção de Riscos de Corrupção e Infrações Conexas.	2018, 2019, 2020, 2021 e 2022
BCP	03/10/2022	As medidas de cibersegurança já estavam implementadas antes do ataque.	2021, 2022 e 2023

Fonte: Elaboração própria

4.2 Análise e Discussão dos Resultados

Os dados obrigatórios que devem constar dos relatórios anuais das empresas de acordo com o Código das Sociedades Comerciais (CSC), são o balanço, a demonstração dos resultados por naturezas, a demonstração das alterações no capital próprio, a demonstração dos fluxos de caixa, os anexos (princípios contabilísticos, detalhe das principais rubricas e outras informações relevantes) e o relatório de gestão que analisa a evolução da empresa, descreve a atividade desenvolvida e apresenta a situação financeira e os resultados obtidos.

Não é obrigatório que a informação sobre ataques informáticos constar nos relatórios, ficando assim a critério de cada gestor. No entanto, tanto a inclusão como a exclusão da informação sobre estes acontecimentos, podem ter várias consequências económicas pois, a transparência sobre um ataque informático pode afetar a confiança dos *stackholders*, mas a falta de comunicação, pode levar a uma perda de credibilidade e, consequentemente, a uma diminuição nas vendas e valorização da empresa. Dependendo das consequências que a perda dos dados origina aos clientes, as empresas podem ser responsabilizadas por não protegerem devidamente os seus dados e, inclusive, ter penalizações legais e multas. Ao não reportar o ataque, a empresa pode enfrentar custos adicionais para remediar a situação, incluindo custos com recuperação de dados e possíveis ações judiciais, assim como pode também afetar a cobertura de seguros informáticos causando dificuldades na reivindicação de compensações, aspetos que podem ter também várias consequências na gestão.

A transparência permite que a empresa implemente um plano de resposta a incidentes, minimizando assim os danos e, restaurando a confiança rapidamente. A comunicação de um ataque publicamente, pode levar a um fortalecimento das políticas de segurança informática, ajudando a prevenir incidentes futuros, e promove uma maior consciencialização sobre a cibersegurança entre os funcionários. Esta tende a ser a abordagem mais adequada, pois ajuda a mitigar tanto os riscos económicos, como os riscos de

gestão, além de promover uma cultura de responsabilidade e segurança dentro das organizações.

Os resultados mostram que as informações dos incidentes de cibersegurança são limitados assim como o conhecimento do impacto que estes tiveram em termos económicos e de gestão.

Capítulo 5 - CONCLUSÃO

Deste estudo, pode-se concluir que, com a crescente dependência de meios tecnológicos, as empresas tornaram-se mais vulneráveis, aumentando assim o risco de serem alvo de ataques informáticos. É evidente que o aumento do uso da *internet* e a ocorrência de ataques informáticos são diretamente proporcionais: quanto mais as empresas dependem e utilizam a *Internet*, maior é o número de ataques informáticos perpetrados contra elas. Além disso, é claro que a segurança informática é de extrema importância. É imperativo que as empresas invistam em medidas de segurança informática para prevenir ataques. No entanto, nos casos em que os ataques não podem ser totalmente evitados, estas empresas dispõem de ferramentas para ajudar a minimizar os danos incorridos.

Sabe-se agora que as empresas analisadas já previam diversas práticas quanto a proteção contra potenciais ataques, são os casos da CUF, EDP, Altice, Impresa, Sonae, Hospital Garcia de Orta, Agência Lusa e BCP.

Antes de sofrer os ataques em análise, a CUF já tinha implementado controlos de gestão de acesso, equipas de gestão especializadas para gerir os projetos de tecnologia da informação, implementação da política de continuidade das operações em caso de incidentes de segurança e adoção de medidas para garantir a conformidade como RGPD. A EDP já possuía controlos de manutenção do nível de exposição e medidas de mitigação, tais como, *cyber-range*, SOC, seguro de *cyber-riscos*, formações e sessões de sensibilização. A Altice desenvolveu campanhas de informação sobre *phishing* para aumentar a consciencialização dos seus colaboradores, colabora com o CNCS e a EUROPOL e possui uma equipa dedicada, que coordena incidentes de segurança informática e dissemina alertas. O Grupo Impresa adquiriu *software* da *Microsoft* MFA (autenticação multifator), promove a execução e gestão de *backups*, a gestão das atualizações de *software* e gestão de acessos. O Grupo Sonae criou equipas dedicadas de cibersegurança, efetuou programas de

sensibilização de cibersegurança, implementou procedimentos de gestão de incidentes, perímetro de segurança da rede, gestão de acesso e identidade, encriptação de informação crítica, antivírus, *anti-spam* e deteção de *malware*. O Hospital Garcia de Orta realizou um *upgrade* com servidores mais robustos e a realização de *backups*. A Agência Lusa investiu na atualização e reforço das infraestruturas de TI, na formação e sensibilização de colaboradores, na implementação de sistemas de monitorização contínua para detetar e responder a possíveis ameaças cibernéticas em tempo real. O BCP investiu em políticas adequadas de avaliação e controle do risco operacional e tecnológico, com destaque para sistemas de segurança da informação e nas linhas de defesa dos bancos.

Assim sendo, a maioria das empresas analisadas já havia investido em medidas de segurança informática, o que lhes permitiu lidar melhor com os danos pelos ataques sofridos. Outras procuraram implementar as medidas adicionais constantes na tabela 5. A CUF implementou ações corretivas, reforçou os *backups*, melhorou as *firewalls* e implementou melhorias nas cópias de segurança. A EDP reforçou as medidas de mitigação e adquiriu o seguro de riscos informáticos. O Grupo Impresa reforçou os mecanismos de encriptação de dados, *firewalls* e autenticação multifator. O Grupo Sonae ativou a equipa de gestão de crise e implementou ações de contenção, mitigação e recuperação. Os SMTUC recorreram ao apoio de uma empresa especializada em Cibersegurança de forma a adotar medidas corretivas. A TAP promove a monitorização da segurança informática numa base contínua, tendo por isso adotado e implementado mais medidas para reforçar a segurança dos sistemas de informação.

5.1 Principais contributos

Este trabalho contribui para melhorar o conhecimento sobre a crescente prevalência de ataques informáticos, identificando os tipos mais comuns de ataques informáticos e recomendando medidas de segurança informática

adequadas para preveni-los. Discute também alguns dos ataques que atingiram empresas portuguesas entre 2018 e 2023, analisando os seus relatórios financeiros.

O objetivo é fornecer informações, que possam ajudar outras empresas a compreender a importância da implementação de medidas de segurança informática. Embora estas medidas possam não impedir completamente os ataques, podem certamente ajudar a mitigar os danos incorridos.

5.2 Limitações

Uma das limitações ao realizar este trabalho, foi a dificuldade em encontrar todas as empresas que foram alvo de ataques informáticos, por isso a amostra é restrita. Também quanto aos dados que são reportados nos relatórios e contas, a expectativa era de que fossem encontradas mais evidências.

5.3 Proposta de trabalhos futuros

Como proposta para trabalhos futuros, considera-se realizar um estudo comparativo sobre como os diferentes países da União Europeia abordam a cibersegurança e a divulgação de ataques informáticos nos relatórios empresariais. Quais as medidas de cibersegurança que têm implementadas e quais implementam depois de serem vítimas de um ataque informático.

REFERÊNCIAS BIBLIOGRÁFICAS

A, B. M. (2022). Ciberataque EDP e Altice. https://cnnportugal.iol.pt/mario-vaz/ataque-informatico/vodafone-e-a-mais-recente-vitima-em-seis-anos-de-ciberataques/20500208/62028bd00cf21847f0a9ddfa

Açores, G. d. (2021). Ciberataque Hospital Divino Espírito Santo. https://portal.azores.gov.pt/web/comunicacao/news-detail?id=3838578

Agência, L. (2022). *Relatório e Contas*. https://www.lusa.pt/Files/lusamaterial/PDFs/Lusa_Relatorio_e_Contas2022.pdf

Akamai. (2023). Esquema Ransomware. https://www.akamai.com/glossary/what-is-ransomware

Altice. (2020). *Relatório sustentabilidade*. https://conteudos.altice.pt/institucional/documentos/pt/sustentabilidade/relatorio-sustentabilidade-2020.pdf

Andrade, F. (2022a). Ciberataque à Agência Lusa. https://tek.sapo.pt/noticias/internet/artigos/agencia-lusa-reune-esforcos-para-reforcar-seguranca-apos-ataque-informatico

Andrade, F. (2022b). Ciberataque Hospital Garcia de Orta. https://tek.sapo.pt/noticias/internet/artigos/cibertaque-condiciona-sistemas-informaticos-no-hospital-garcia-de-orta

BCP. (2021). *Relatório e Contas*. https://ind.millenniumbcp.pt/pt/Institucional/investidores/Documents/RelatorioContas/2021/RCBCP2021_29032022.pdf

BCP. (2022). *Relatório e contas*. https://ind.millenniumbcp.pt/pt/Institucional/investidores/Documents/RelatorioContas/2022/Relatorio-Grupo-BCP-2022.pdf

BCP. (2023). *Relatório e Contas*. https://ind.millenniumbcp.pt/pt/Institucional/investidores/Documents/RelatorioContas/2023/RCBCP2023PT_27032024.pdf

Bma. (2022a). Ciberataque à Cofina. *Agência Lusa*. https://cnnportugal.iol.pt/mario-vaz/ataque-informatico/vodafone-e-a-mais-recente-vitima-em-seis-anos-de-ciberataques/20500208/62028bd00cf21847f0a9ddfa

Bma. (2022b). Ciberataque ao Grupo Impresa. https://cnnportugal.iol.pt/mario-vaz/ataque-informatico/vodafone-e-a-mais-recente-vitima-em-seis-anos-de-ciberataques/20500208/62028bd00cf21847f0a9ddfa

Bma. (2022c). Ciberataque Vodafone. *Agência Lusa*, *2024*. https://cnnportugal.iol.pt/cibercrime/ciberataque/aceder-a-informacao-

politica-e-economica-ultimo-relatorio-de-seguranca-interna-alertava-para-ataques/20500208/620294e90cf21847f0a9df7c

CheckPoint. (2024). DNS tunneling. https://www.checkpoint.com/cyber-hub/network-security/what-is-dns-tunneling/

Cibersegurança, C. N. d. (2020). *Relatório Cibersegurança em Portugal*. https://www.cncs.gov.pt/pt/observatorio/#relatorios

Cibersegurança, C. N. d. (2021). *Relatório Cibersegurança em Portugal*. https://www.cncs.gov.pt/pt/observatorio/#relatorios

Cibersegurança, C. N. d. (2022). *Relatório Cibersegurança em Portugal*. https://www.cncs.gov.pt/pt/observatorio/#relatorios

Cibersegurança, C. N. d. (2023). *Relatório Cibersegurança em Portugal*. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

Cibersegurança, C. N. d. (2024). *Relatório Cibersegurança em Portugal*. https://www.cncs.gov.pt/pt/observatorio/#relatorios

Cloudflare. (2024). DoS. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Cncs. (2019). Estratégia Nacional de Segurança do Ciberespaço. https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

Cofina. (2021). *Relatório e Contas*. http://www.cofina.pt/investors/reports/2021.aspx?sc_lang=pt-pt

Cofina. (2022). *Relatório e Contas*. http://www.cofina.pt/investors/reports/2022.aspx?sc_lang=pt-pt

Corchado, B. (2023). Esquema Phishing. https://es.godaddy.com/blog/wp-content/uploads/esquema-pharming-dns-phishing.jpg

Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy. *Information Systems Journal*, *33*(6), 1396-1422. https://doi.org/10.1111/isj.12460

CUF. (2018). *Relatório Integrado*. https://www.cuf.pt/sobre-nos/investidores/cuf-sa/apresentacoes-e-relatorios

CUF. (2019). *Relatório Integrado*. https://www.cuf.pt/sobre-nos/investidores/cuf-sa/apresentacoes-e-relatorios

CUF. (2020). *Relatorio Integrado*. https://www.cuf.pt/sobre-nos/investidores/cuf-sa/apresentacoes-e-relatorios

CUF. (2021). Relatorio Integrado. https://www.cuf.pt/sobre-nos/investidores/cuf-sa/apresentacoes-e-relatorios

CUF. (2022). *Relatorio Integrado*. https://www.cuf.pt/sobre-nos/investidores/cuf-sa/apresentacoes-e-relatorios

CUF. (2023). *Relatorio Integrado*. https://www.cuf.pt/sobre-nos/investidores/cuf-sa/apresentacoes-e-relatorios

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). *The New Frontier of Cybersecurity: Emerging Threats and Innovations* Proceedings - ICT 2023 - 29th International Conference on Telecommunications: Next-Generation Telecommunications for Digital Inclusion and Universal Access, https://ieeexplore.ieee.org/document/10374044/

EDA. (2022). *Relatório e contas*. https://www.eda.pt/Mediateca/Publicacoes/Paginas/Relatorios.aspx#

EDP. (2018). *Relatório Integrado*. https://www.edp.com/sites/default/files/rc_edp_2018.pdf

EDP. (2019). *Relatório Integrado*. https://www.edp.com/sites/default/files/2020-03/R%26C_2019_PT.pdf

EDP. (2020). *Relatório Integrado*. https://www.edp.com/sites/default/files/2021-03/210x297_RC20_EDP_PT.pdf

EDP. (2021). *Relatório Integrado*. https://www.edp.com/sites/default/files/2022-03/RC_EDP_PT_vers%C3%A3o%20n%C3%A3o%20oficial%20-%20n%C3%A3o%20auditada.pdf

EDP. (2022). *Relatório Integrado*. https://www.edp.com/pt-pt/relatorio-anual-integrado-2022

EDP. (2023). *Relatório Integrado*. https://www.edp.com/pt-pt/relatorio-anual-integrado-2023

Esparza, J. M. (2019). Understanding the credential theft lifecycle. *Computer Fraud & Security*, *2019*(2), 6-9. https://doi.org/10.1016/S1361-3723(19)30018-1

Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. A. (2023). Cybersecurity Resilience in SMEs. A Machine Learning Approach. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2023.2248925

Ferreira, C. (2022). Ciberataque à Sonae. https://tek.sapo.pt/noticias/internet/artigos/grupo-sonae-confirma-ataque-informatico-esta-madrugada

Flávio, N. (2022). Ciberataque Website Assembleia da República. https://eco.sapo.pt/2022/02/09/wannacry-notpetya-estes-foram-alguns-dos-ciberataques-mais-mediaticos-dos-ultimos-anos-em-portugal/

Fortinet. (2024). IoT. https://www.fortinet.com/resources/cyberglossary/iot-security

Gabinete Nacional de, S. (2024). *Aviso n.º 1517/2024*. https://files.diariodarepublica.pt/1s/2018/08/15500/0403104037.pdf

Gamboa, F. (2023). Inside threats. https://blog.netwrix.com/2021/06/23/insider-threat/

GoldSparrow. (2023). Esquema de Cryptojacking. https://www.enigmasoftware.com/how-hackers-use-cryptojacking-malware-take-over-computers-mine-cryptocurrency/

Heimdal. (2023). Esquema Password attacks. https://heimdalsecurity.com/blog/iot-security-for-business/

HGO. (2020). *Relatório e Contas*. https://www.hgo.min-saude.pt/wp-content/uploads/sites/18/2020/09/RELATORIO-E-CONTAS-2020_RCA-27-de-maio_Assinado-CA-compactado_compressed-compactado.pdf

HGO. (2021). *Relatório e Contas*. https://www.hgo.min-saude.pt/wp-content/uploads/sites/18/2020/09/Relatorio-e-Contas-2021_rubricado.pdf

HGO. (2022). *Relatório e Contas*. https://www.hgo.min-saude.pt/wp-content/uploads/sites/18/2020/09/RELAT%C3%93RIO-E-CONTAS-2022_signed.pdf

IBM. (2024a). MITM. https://www.ibm.com/think/topics/man-in-the-middle?mhsrc=ibmsearch_a&mhq=Man-in-the-middle

IBM. (2024b). Phishing. https://www.ibm.com/topics/phishing?mhsrc=ibmsearch_a&mhq=phishing

IBM. (2024c). Ransomware. https://www.ibm.com/br-pt/topics/ransomware

Ichi. (2023). Esquema MITM. https://ichi.pro/es/detras-de-los-ataques-man-in-the-middle-para-autos-conectados-intercepcion-en-la-vida-real-del-trafico-de-red-143256135821644

Impresa. (2020). *Relatório anual*. https://sdistribution.impresa.pt/data/content/binaries/1b2/c9e/7404a29b-cc4a-4584-bd25-e12af2e96304/Relatorio-e-Contas-2020.pdf

Impresa. (2021). *Relatório e Contas*. https://sdistribution.impresa.pt/data/content/binaries/7e9/a46/d8a36363-9b62-4bfd-a52a-ee3618af3732/Rel-e-Contas-Anuais-IMPRESA-2021_NESEF_PT.pdf

Impresa. (2022). *Relatório e Contas*. https://sdistribution.impresa.pt/data/content/binaries/7e9/a46/d8a36363-9b62-4bfd-a52a-ee3618af3732/Rel-e-Contas-Anuais-IMPRESA-2021_NESEF_PT.pdf

Impresa. (2023). *Relatório e Contas*. https://sdistribution.impresa.pt/data/content/binaries/b2c/c39/b0d3ee4e-e434-44b9-b226-fccb56d91b20/RelatorioContas-IMPRESA--2023_N-ESEF_CMVM.pdf

Kaddoura, S., Haraty, R. A., Kontar, K. A., & Alfandi, O. (2021). A Parallelized Database Damage Assessment Approach after Cyberattack for Healthcare Systems. *Future Internet*, *13*(4), 90-90. https://doi.org/10.3390/fi13040090

Leonard, J. (2019). Esquema SQL injection attacks. https://www.business2community.com/cybersecurity/sql-injection-attacks-sqli-web-based-application-security-part-4-02223254

Lusa. (2022). Ciberataque à Trust in News - Visão. https://tek.sapo.pt/noticias/internet/artigos/dona-da-visao-alvo-de-tentativa-de-ataque-informatico-esta-madrugada

Lusa, A. (2022). *Relatório e Contas*. https://www.lusa.pt/Files/lusamaterial/PDFs/Lusa_Relatorio_e_Contas2022.pdf

Malwarebytes. (2024). Criptojacking. https://pt.malwarebytes.com/cryptojacking/

Mandeiro, N. (2022a). Ciberataque à CUF. https://cnnportugal.iol.pt/ciberseguranca/cibercrime/ciberataques-na-saude-ataques-a-cuf-champalimaud-e-garcia-de-orta-ja-tinham-disparado-alertas/20220211/620530e30cf2c7ea0f1847f6

Mandeiro, N. (2022b). Ciberataque à Fundação Champalimaud. https://cnnportugal.iol.pt/ciberseguranca/cibercrime/ciberataques-na-saude-ataques-a-cuf-champalimaud-e-garcia-de-orta-ja-tinham-disparado-alertas/20220211/620530e30cf2c7ea0f1847f6

Ministros, P. d. C. d. (2021). *Decreto-Lei n.º 65/2021*. https://files.diariodarepublica.pt/1s/2021/07/14700/0000800021.pdf

Mitra, A. (2017). Esquema Drive-by download. https://www.thesecuritybuddy.com/malware-prevention/what-is-drive-by-download-and-how-to-prevent-it/

Murphy, I. P. (2020). The chair of NSA's cybersecurity workcgroup talks about emerging cyber crimes,investigation, and data protection. *SHERIFF & DEPUTY*.

Ndc. (2022). Ciberataque SMTUC. https://www.noticiasdecoimbra.pt/piratas-dao-oito-dias-aos-smtuc-para-recuperar-dados-alegadamente-roubados/

Okta. (2024). Esquema DNS poisoning. https://www.okta.com/identity-101/dns-poisoning/.

Oza, S. (2023). Esquema de Denial of Service. https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/

Pandya, D., , Jadeja, A., , Bhuptani, M., , Patel, V., , Mehta, K., , Brahmbhatt, D., & (2024). Machine Learning: Enhancing Cybersecurity through Attack Detection and Identification. In (Vol. 65, pp. 03010): EDP Sciences.

Pawar, R. (2022). Esquema DNS tunneling. https://blogs.quickheal.com/introduction-of-dns-tunneling-and-how-attackers-use-it/

Piccirilli, C., & Tzabbar, D. (2022). Management attention and cyber risk position. *Organizational Dynamics*, *51*(3), 100867-100867. https://doi.org/10.1016/J.ORGDYN.2021.100867

Ravoof, S. (2024). Esquema de ataque Zero-day exploits. https://kinsta.com/blog/zero-day-exploit/

REMGFA. (2022). *Relatório e Contas*. https://www.tcontas.pt/pt-pt/ProdutosTC/Relatorios/relatorios-oac/Documents/2022/rel-oac002-2022-2s.pdf

República, A. d. (2018). *Lei n.º 46/2018*. Retrieved from https://files.diariodarepublica.pt/1s/2018/08/15500/0403104037.pdf

República, P. (1986). *Código das Sociedades Comerciais - CSC - Título I | DR*. Retrieved from https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1986-34443975-45996675

Robinson, R. M. R. (2015). Cross-site scripting.

Rutledge, B. (2019). Esquema XSS ataque. https://securityboulevard.com/2019/05/cross-site-scripting-xss-web-based-application-security-part-3/

SapoTek. (2022a). Ciberataque à EDA - Eletricidade dos Açores. https://tek.sapo.pt/noticias/internet/artigos/eletricidade-dos-acores-alvo-de-ataque-informatico-impacto-ainda-esta-a-ser-analisado

SapoTek. (2022b). Ciberataque ao BCP. In.

SapoTek. (2022c). Ciberataque ao Grupo Germano de Sousa. https://tek.sapo.pt/noticias/computadores/artigos/laboratorios-germano-de-sousa-alvo-de-ataque-informatico

SapoTek. (2022d). Ciberataque ao Grupo Newsplex. https://tek.sapo.pt/noticias/internet/artigos/ataque-informatico-ao-i-e-nascer-do-sol-impede-saida-do-diario-esta-quinta-feira

SapoTek. (2022e). Ciberataque aos Websites do Sporting e FC Porto. https://tek.sapo.pt/noticias/internet/artigos/websites-do-sporting-e-porto-indisponiveis-devido-a-ataques-ddos

SapoTek. (2022f). Ciberataque Câmara Municipal de Loures. https://tek.sapo.pt/noticias/computadores/artigos/camara-de-loures-alvo-de-ciberataque-malicioso-e-deliberado

Security, I. T. (2021a). *IT-Security - #01 JUNHO 2021*. https://www.itsecurity.pt/edicoes/it-security-n1-junho-2021

Security, I. T. (2021b). *IT-Security - #02 SETEMBRO 2021*. https://www.itsecurity.pt/edicoes/it-security-n2-setembro-2021

Security, I. T. (2021c). *IT-Security - #03 DEZEMBRO 2021*. https://www.itsecurity.pt/edicoes/it-security-n3-dezembro-2021

Security, I. T. (2022a). *IT-Security - #04 FEVEREIRO 2022*. https://www.itsecurity.pt/edicoes/it-security-n4-fevereiro-2022

Security, I. T. (2022b). *IT-Security - #06 JUNHO 2022*. https://www.itsecurity.pt/edicoes/it-security-n6-junho-2022

Security, I. T. (2023). *IT-Security - #10 FEVEREIRO 2023*. https://www.itsecurity.pt/edicoes/it-security-n10-fevereiro-2023

Security, I. T. (2024a). *IT-Security - #17 ABRIL 2024*. https://www.itsecurity.pt/edicoes/it-security-n17-abril-2024

Security, I. T. (2024b). *IT-Security - #18 JUNHO 2024*. https://www.itsecurity.pt/edicoes/it-security-n18-junho-2024

Senapati, P. (2024). The Importance of Cybersecurity for Small Businesses. *The Business Innovations*. https://thebusinessinnovations.com/business/the-importance-of-cybersecurity-for-small-businesses/

files/23/the-importance-of-cybersecurity-for-small-businesses.html

SMTUC. (2020). *Relatório de Gestão e Contas*. https://www.smtuc.pt/wp-content/uploads/2021/08/relatorio_gestao_2020.pdf

SMTUC. (2021). *Relatório de Gestão e Contas*. https://www.smtuc.pt/wp-content/uploads/2022/06/RELATORIO-DE-GESTAO-2021.pdf

SMTUC. (2022). *Relatório de Gestão e Contas*. https://www.smtuc.pt/wp-content/uploads/2023/06/Relatorio-Gestao-2022.pdf

SMTUC. (2023). *Relatório de Gestão e Contas*. https://www.smtuc.pt/wp-content/uploads/2024/05/RELATORIO-DE-GESTAO-2023.pdf

Sonae. (2019). *Relatório e Contas*. https://www.sonae.pt/fotos/dados_fin/r_c_pt2019_8781059015ed53af598239.pdf

Sonae. (2020). *Relatório e Contas*. https://www.sonae.pt/fotos/dados_fin/rc2020pt_740705753608c4f98c0794.pdf

Sonae. (2021). *Relatório Integrado*. https://www.sonae.pt/fotos/dados_fin/rc2021ptnaoesef_1660120231626b7f3c77f35.pdf

Sonae. (2022). *Relatório Integrado*. https://www.sonae.pt/fotos/dados_fin/relatoriointegrado_2022_pt_1277178973642cbcbfd0004.pdf

Sonae. (2023). *Relatório Integrado*. https://www.sonae.pt/fotos/dados_fin/rc2023pornaoesef.pdf

Sudipto, P. (2023). Esquema DNS poisoning. https://www.g2.com/articles/dns-spoofing

Tap. (2018). *Relatório de Gestão*. https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais

Tap. (2019). *Relatório de Gestão*. https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais

Tap. (2020). *Relatório de Gestão*. https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais

Tap. (2021). *Relatório de Gestão*. https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais

Tap. (2022a). *Relatório de Gestão*. https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais

TAP. (2022b). *Relatório de Gestão e Contas Consolidadas*. https://www.tapairportugal.com/pt/sobre-nos/relatorios-anuais

Toma, T., Décary-Hétu, D., & Dupont, B. (2023). The benefits of a cyber-resilience posture on negative public reaction following data theft. *Journal of Criminology*, *56(4)*, 470-493. https://doi.org/10.1177/26338076231161898

Vodafone. (2022). *Relatório e Contas*. https://www.vodafone.pt/a-vodafone/quem-somos/relatorios.html

Wilshusen, G. C. (2012). *CYBERSECURITY: Threats Impacting the Nation*. https://apps.dtic.mil/sti/pdfs/AD1153781.pdf

Zheng, D. (2020). Esquema Internet of Things attacks. https://www.mdpi.com/1424-8220/20/6/1706