UNIVERSIDADE D
COIMBRA

André Pinto Dias

MONITORIZAÇÃO DE INFRAESTRUTURA DE REDE E CONSCIENCIALIZAÇÃO PARA O PHISHING

Dissertação no âmbito do Mestrado em Segurança Informática orientada pela Professora Doutora Naghmeh Ivaki e apresentada ao Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2023

FACULDADE DE
CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D
COIMBRA
DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

André Pinto Dias

Monitorização de Infraestrutura de rede e consciencialização para o Phishing

Dissertação no âmbito do Mestrado em Segurança Informática orientada pela Professora Doutora Naghmeh Ivaki e apresentada ao Departamento de Engenharia Informática da Faculdade de Ciências e Tecnologia da Universidade de Coimbra.

Setembro de 2023

Agradecimentos

À minha família,

Aos meus orientadores, Professora Naghmeh Ivaki, Engº Sérgio Boticário e Engº Carlos Craveiro.

A todos aqueles que me apoiaram durante a realização do projeto.

Resumo

Nos últimos anos, a segurança da informação tem recebido muita atenção de diversas áreas de negócios, empresas, organizações e governos. O foco nesta área deve-se ao elevado aumento nas violações de segurança, levando a grandes perdas pelas empresas afetadas. Estas violações podem ser, de certa forma, combatidas através de tecnologias. Porém, o que não se consegue controlar com as tecnologias é a forma como cada um de nós lida com este tipo de ameaças. É, pois, fundamental treinar e consciencializar as pessoas de que elas são a primeira e mais crítica linha de defesa de uma organização.
Um dos principais fatores para o sucesso na gestão da segurança da informação é o cumprimento efetivo das políticas de segurança e a integração adequada das pessoas, processos e tecnologias.
No que diz respeito aos sistemas informáticos, devem ser realizadas análises de vulnerabilidades periódicas, por forma a avaliar as possíveis brechas de segurança que possam existir e que caso sejam exploradas, por agentes externos, podem culminar num ciberataque à organização em questão. Não obstante, nas pessoas, esta eficácia pode ser alcançada através de vários mecanismos, sendo um deles a consciencialização para as boas práticas de segurança.
A defesa de uma instituição passa, desta forma, por termos os sistemas informáticos devidamente atualizados e os colaboradores consciencializados para as diversas ameaças a que poderão estar sujeitas, mais concretamente para o phishing.
Este trabalho permitiu explorar os sistemas informáticos da Bluepharma na pesquisa de vulnerabilidades existentes, através da utilização da ferrementa OpenVas, para que fosse possível detetar e mitigar essas mesmas vulnerabilidades. De igual forma foram realizadas campanhas de phishing, através da ferramenta Gophish, com o intuito de avaliar o grau de consciencialização que os colaboradores da Bluepharma têm para a temática da segurança da informação.

Palavras-Chave

Segurança da informação, cibersegurança, pesquisa de vulnerabilidades, OpenVas, Gophish

Abstract

In recent years, information security has received a lot of attention from various business areas, companies, organizations, and governments. The focus in this area is due to the high increase in security breaches, leading to large losses for the affected companies. These breaches can, to a certain extent, be controlled through technology, but what technology cannot control is the way in which each of us deals with these types of threats. It is therefore essential to train and make people aware that they are the first and most critical line of defense in an organization.

One of the key factors for success in information security management is effective obedience to security policies and proper integration of people, processes and technology. With regard to computer systems, periodic vulnerability analyses should be performed in order to assess possible security breaches that may exist and that, if exploited by external agents, could culminate in a cyber-attack on the organization in question.

Nevertheless, with people, this effectiveness can be achieved through various mechanisms, one of them being awareness of good security practices. The defense of an institution is, therefore, to have the computer systems properly updated and employees aware of the various threats to which they may be subjected to, specifically phishing. This work allowed Bluepharma's computer systems to be explored in the search for existing vulnerabilities, through the use of the OpenVas tool, so that it was possible to detect and mitigate those vulnerabilities. Phishing campaigns were also carried out, using the Gophish tool, in order to assess the level of awareness of Bluepharma's employees regarding information security.

Keywords

Information security, security management, OpenVas, Gophish, Phishing

Índice

Acrónimos

GPL - General Public License
PCI - Payment Card Industry
CVSS - Common Vulnerability Scoring System
AI - Artificial Intelligence
EOP - Exchange Online Protection
CVE - Common Vulnerabilities and Exposures
SOX- Sarbanes-Oxley Act
HIPAA- Health Insurance Portability and Accountability Act
FISMA- Federal Information Security Management Act
NVT- Network Vulnerability Test
APWG - Anti-Phishing Working Group
GVMD - Greenbone Vulnerability Manager Daemon
GSA- Greenbone Security Assistant
GMP- Greenbone Management Protocol
NIST- National Institute of Standards and Technology

Lista de Figuras

Lista de Tabelas

Capítulo 1 Introdução

Devido ao constante desenvolvimento de novas técnicas de ciberataques, surge a necessidade de dotarmos as organizações de ferramentas automatizadas que possam avaliar o estado de proteção dos sistemas informáticos.

Em paralelo, abordagens de *Security Awareness Training* [1] têm sido cada vez mais utilizadas como forma de alerta, para com os colaboradores das organizações, para as diversas ameaças externas a que estes podem estar sujeitos e que consequentemente possam colocar em perigo a própria organização. Este tipo de abordagens tem como principal função educar os colaboradores para os problemas de Cibersegurança e como estes podem ser mitigados. Desta forma, é possível criar uma cultura de consciencialização para a segurança da informação dentro das organizações. De igual forma, educando os colaboradores para melhores práticas e ameaças mais comuns as empresas podem reduzir a probabilidade de incidentes de segurança, minimizando o impacto de qualquer acontecimento que possa ocorrer. É, pois, importante para as organizações assegurarem que o treino de consciencialização dos seus colaboradores está atualizado para o modelo de negócio das mesmas.

Desta forma surge o presente relatório, realizado no âmbito da unidade curricular de Dissertação/Estágio do 2º ano do Mestrado de Segurança Informática da Universidade de Coimbra (UC), no ano letivo de 2022/2023. Este relatório visa descrever o estágio realizado pelo aluno André Pinto Dias na empresa Bluepharma, tendo em conta as problemáticas acima referidas.

1.1 Entidade de acolhimento - Bluepharma

A Bluepharma é uma empresa da indústria farmacêutica que concentra os seus esforços no fabrico, investigação, desenvolvimento e comercialização de medicamentos [2]. A empresa foi fundada em fevereiro de 2001 e desenvolve a sua atividade em três áreas distintas:

- Produção de medicamentos próprios e para terceiros;
- Investigação, desenvolvimento e registo de medicamentos;
- Comercialização de medicamentos genéricos.

1.2 Contextualização do problema

Nos dias de hoje a temática da Cibersegurança nunca foi tão importante, visto que existem diariamente milhares de ciberataques a serem executados contra empresas/organizações, sendo até alguns destes financiados por governos de certos países com objetivo de criar constrangimentos numa determinada indústria ou também para roubar informações confidenciais.

Estas ciberameaças, caso não sejam acauteladas, podem resultar em perdas financeiras significativas e em certos casos levar ao encerramento do negócio das empresas afetadas.

É, pois, essencial garantir que temos os controlos implementamos nas organizações por forma a reduzir ao mínimo possível um ataque cibernético.

1.3 Definição do problema

Desde o início da pandemia do Covid-19, tem existido um elevado aumento no número de ciberataques contra o setor da saúde. Estes ataques têm como principais organizações de saúde hospitais e empresas de investigação, entre outras. Caso estes ciberataques sejam concretizados, podem criar disrupções em serviços críticos como por exemplo o comprometimento dos dados de pacientes ou o roubo de informações confidenciais de pesquisas realizadas, sobre um determinado tratamento.

Este projeto visa consciencializar os colaboradores da Bluepharma para os perigos que poderão chegar do exterior, através da execução de campanhas de *phishing* para colocar à prova as capacidades dos colaborares na identificação de um email fraudulento, por forma a que no futuro estejam mais capacitados, para se protegerem a eles e à organização.

Além disto, devido ao aumento dos ciberataques, não pode ser esquecida a própria infraestrutura de rede e as possíveis vulnerabilidades que nela possam existir, sendo por isso necessário implementar ferramentas automatizadas que nos ajudem a detetar e mitigar essas mesmas ameaças.

1.4 Objetivos do Trabalho

O presente estágio pretende atingir os seguintes objetivos no decorrer do trabalho:

- Levantamento do estado dos trabalhos, tecnologias e abordagens.
- Especificação e implementação dos componentes necessários para a implementação de uma ferramenta de análise de vulnerabilidades.
- Especificação e implementação dos componentes necessários para a configuração de uma ferramenta de campanha de *phishing*.
- Formação aos colaboradores sobre cuidados a ter para a segurança da informação.

1.5 Plano de Trabalhos

O plano de trabalhos a realizar durante o decorrer do estágio é dividido em duas partes. O primeiro referente ao 1ºSemestre (período entre setembro de 2022 e janeiro de 2023) e o segundo referente ao 2ºSemestre (período entre fevereiro e julho de 2023).

Semestre 1

O plano de escalonamento dos trabalhos pretendidos é dividido nos seguintes tópicos, referentes apenas ao 1ºsemestre:

- T1 - Levantamento do estado dos trabalhos, tecnologias e abordagens;
- T2 - Especificação de requisitos;
- T3 - (Contínuo) Elaboração do documento de Dissertação;.
- T4 - Implementação da aplicação de pesquisa de vulnerabilidades.

Semestre 2

O plano de escalonamento dos trabalhos pretendidos é dividido nos seguintes tópicos, referentes ao 2ºsemestre:

- T5 - Implementação da aplicação de Security Awareness Training;
- T6 - Execução das aplicações a nível produtivo;
- T7 - (Contínuo) Elaboração do Documento de Dissertação.

1.6 Estrutura do relatório

O presente relatório está dividido em 6 capítulos, os quais podem ser descritos da seguinte forma:

- Capítulo 1 – Introdução ao estágio curricular, apresentação da entidade acolhedora bem como contextualização do problema e os objetivos do estágio.
- Capítulo 2 – Contextualização dos temas para o desenvolvimento do projeto como a arquitetura dos *scanners* de vulnerabilidades, cuidados a ter na implementação dos mesmos.
- Capítulo 3 – Configuração e instalação da ferramenta de análise de vulnerabilidades bem como os resultados obtidos.
- Capítulo 4 – Descrição do trabalho realizado no âmbito da consciencialização para a cibersegurança.

- Capítulo 5 – Apresentação das conclusões retiradas após a realização do trabalho, bem como os passos futuros a realizar.

Capítulo 2 Estado da Arte

Nos dias de hoje existem diversos tipos de vulnerabilidades, tais como vulnerabilidades de software, erros de configuração, como por exemplo passwords fracas, sendo estas uma das portas de entrada para um atacante conseguir ganhar acesso à rede corporativa, afetando desta forma a confidencialidade, integridade e disponibilidade dos seus *assets*, roubando ou manipulando informações, podendo causar também incidentes de *Denial of Service*.
A gestão eficiente de vulnerabilidades é, por conseguinte, um esforço que todas as empresas modernas devem fazer, por forma a manter a sua infraestrutura de rede o mais robusta possível, contra possíveis ameaças, sejam elas internas ou externas.
Acompanhar todas as vulnerabilidades presentes nos sistemas e corrigi-las adequadamente é uma tarefa árdua, visto que as infraestruturas de rede das organizações estão cada vez maiores e mais complexas.
Felizmente, existem ferramentas destinadas a fornecer suporte automatizado para este processo, tais como a utilização de *scanners* de vulnerabilidades.
Um scanner de vulnerabilidades é um software usado para efetuar uma pesquisa na rede, que permite identificar vulnerabilidades e posteriormente indica as medidas corretivas que devem ser implementadas, por forma a mitigar as ameaças encontradas.
A pesquisa de vulnerabilidades em rede envolve a identificação dos *hosts* ativos, quais os sistemas operativos que estes tem instalados, bem como os serviços que se encontram em execução em cada um destes. Durante um *scan*, uma base de dados de assinaturas de vulnerabilidades conhecidas é comparada às informações obtidas na pesquisa de rede. Após a pesquisa, é possível extrair um relatório detalhado com uma listagem de vulnerabilidades das ameaças que estavam ativas.

A segurança de uma infraestrutura de IT está dependente maioritariamente dos seguintes pontos:

- Atacantes com experiência, equipamento e dinheiro suficiente para realizar o ataque.
- Acesso à infraestrutura de rede.
- Vulnerabilidades nos sistemas, causadas por erros em aplicações, sistemas operativos ou configurações incorretas.

Se todos estes três elementos se verificarem, é bem provável que ocorra um ataque bem-sucedido à infraestrutura de IT.
Porém, como a maioria das vulnerabilidades são conhecidas e podem ser corrigidas, a superfície de ataque pode ser reduzida usando *scanners* de vulnerabilidades. A gestão de vulnerabilidades envolve olhar para a infraestrutura de IT, do ponto de vista de um atacante, para tentar perceber a forma como estes poderão penetrar a rede informática.

De igual forma, nos últimos anos, o uso de computadores e da internet tornou-se indispensável para o desenvolvimento dos negócios das organizações. Este uso trouxe também alguns riscos

associados, tais como ataques cibernéticos, que podem colocar em risco informações confidênciais de uma determinada empresa. Esta ameaça é comum a qualquer organização, visto que irá existir sempre alguém com interesses na informação que a empresa possui, ou simplesmente pode querer ganhar vantagem de alguma forma.

Não existe uma solução tecnológica que resolva todos os riscos de segurança. Posto isto, as organizações devem garantir que não estão apenas a investir na tecnologia, mas também na criação de uma cultura de segurança no local de trabalho.

A chave para proteger os utilizadores é fazê-los perceber que estes são uma parte importante do plano de segurança de uma empresa, mostrando-lhes o que podem fazer, para se tornarem na primeira linha de defesa de uma organização.

Nos dias de hoje, uma organização não consegue proteger a confidencialidade, integridade e disponibilidade dos seus dados, sem garantir que todas as pessoas envolvidas na infraestrutura compreendam as suas funções e responsabilidades relacionadas com a missão, política, procedimentos e boas práticas de segurança da informação.

O âmbito desde projeto passa, numa primeira fase, por fazer a instalação e configuração de uma ferramenta de vulnerabilidades, com o intuito de reduzir a superficie de ataque da organização. Numa segunda fase, como é impossível proteger uma infraesturura sem o apoio de todas as pessoas que a utilizam, irá ser implementado um programa de treino e consciencialização para os colaboradores da organização, de forma a consciencializá-los para a necessidade de segurança da informação.

2.1 Scanners de vulnerabilidades

Nos dias de hoje, são descobertas novas vulnerabilidades diariamente. É, pois, necessário termos ferramentas que permitam detetar, localizar, priorizar e mitigar os possíveis riscos para o correto funcionamento do negócio de uma organização.

Estes scanners de vulnerabilidades ajudam-nos, em primeiro lugar, na deteção precoce de problemas de segurança, executando avaliações de segurança periódicas, sendo fácil identificar vulnerabilidades de segurança que possam estar presentes na rede, tanto numa perspetiva interna, como externa. Estes auxiliam-nos também na verificação do inventário de rede de uma organização. (tipo de dispositivo, versão do sistema operativo, configurações de hardware, entre outros).

Arquitetura

No geral, os scanners de vulnerabilidades são constituídos por quatro módulos principais, conforme inidcado na Figura 1.

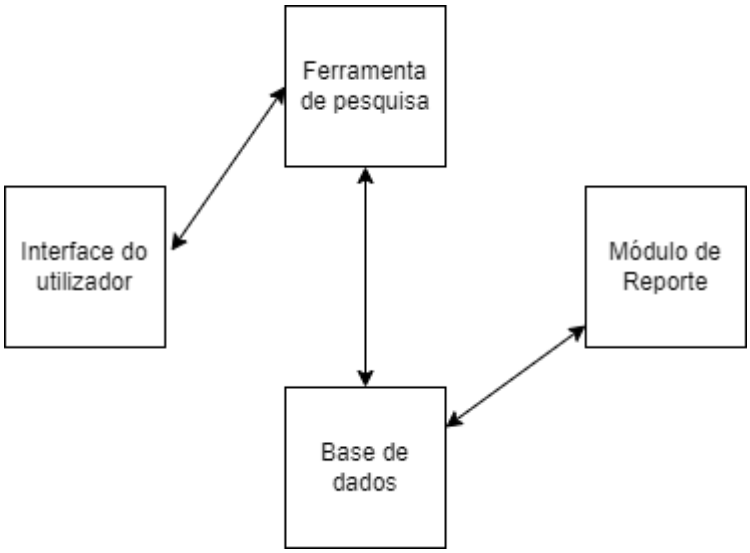

Figura 1- Arquitetura Scanner de Vulnerabilidades

- Interface do utilizador - Consola gráfica para o operador controlar o Scanner. Esta interface pode ser uma interface gráfica ou simplesmente uma linha de comandos.
- Ferramenta de pesquisa - Este módulo é responsável pela execução de validações de segurança, consoante os plug-ins instalados, recolhendo informações sobre o sistema, bem como possíveis vulnerabilidades.
- Base de dados - A base de dados guarda informação sobre as vulnerabilidades e resultados de pesquisas, entre outros. O número de plug-ins disponíveis, bem como a frequência da atualização, irá variar consoante o vendedor. Cada plug-in, em geral, contém o teste a executar, a descrição da vulnerabilidade, um identificador de CVE, bem como instruções para mitigar a vulnerabilidade encontrada.
- Módulo de Reporte - Este módulo é responsável por fornecer diferentes níveis de relatórios, como por exemplo relatórios detalhados para os administradores de sistemas, bem como relatórios gráficos, de alto nível, para os executivos de uma organização.

Tipos de Scanner de vulnerabilidades

As ferramentas de deteção de vulnerabilidades podem ser divididas em dois grupos: *network-based*, que analisam o tráfego que circula numa infraestrutura de rede e os scanners *host-based,* que analisam as configurações de uma determinada máquina.

Um scanner de rede é tipicamente instalado numa única máquina que faz a pesquisa em vários hosts, presentes na rede, auxiliando o administrador de rede a detetar possíveis vulnerabilidades, tais como configurações incorretas, serviços e software vulneráveis.

Um scanner de host é instalado na máquina que se pretende analisar, tendo este acesso a dados de baixo nível, como é o caso de serviços específicos que estão a correr no sistema operativo do host. Pode também detetar atempadamente possíveis atividades de risco, por parte do utilizador, como é o caso do uso de passwords fracas. Adicionalmente, pode detetar que o sistema pode ter sido comprometido , através da análise de determinados ficheiros de sistema.

Cuidados a ter na configuração destas ferramentas

Ao efetuarmos a instalação e configuração destas ferramentas de deteção de vulnerabilidades, devemos ter em consideração alguns aspetos, por forma a que a nossa análise seja o mais correta e eficiente possível:

- Localização do Scanner - Quando fazemos a configuração de um scanner temos de ter em atenção onde instalamos esta ferramenta, pois o resultado da análise de segurança terá um resultado diferente caso seja executada a partir da rede interna, ou realizada a partir do exterior. Se efetuarmos um scan da rede a partir do exterior, só iremos conseguir detetar serviços que estejam disponíveis para a internet e não nos será possível detetar vulnerabilidades internas, visto que, regra geral, a rede interna encontra-se protegida por uma firewall.
- Gestão de vulnerabilidades - Normalmente, o ciclo de um scan de vulnerabilidades incluí uma avaliação inicial, seguida da implementação de medidas corretivas e posteriormente de uma nova análise. Por forma a verificar que as correções implementadas foram bem sucedidas, é boa prática o armazenamento de logs de scans anteriores, para que seja possível comparar os resultados obtidos, com o histórico de resultados de análise já efetuados.
- Precauções - Ao efetuarmos uma pesquisa de vulnerabilidades, a própria pesquisa pode trazer riscos para a infraestrutura de IT, visto que poderão existir equipamentos de rede mais frágeis que não suportam a quantidade de tráfego gerado por estas ferramentas (ex: PLC´s).
- Armazenamento dos resultados obtidos - Após efetuada a análise de rede à infraestrutura de rede, a informação obtida deve ser armazenada de forma segura, pois traduz um risco elevado para a organização, caso seja obtida por pessoas não autorizadas, visto que contém as falhas de segurança encontradas durante a pesquisa. Caso esta análise seja efetuada por uma empresa externa, a organização deve-se assegurar que a entidade externa é de confiança e que não partilha com ninguém qualquer informação confidencial da organização, que venha a obter, após a análise à infraestrutura de rede da organização.

Considerações a ter na escolha de um scanner de vulnerabilidades

Existem, no mercado, diversas ferramentas de pesquisa de vulnerabilidades, algumas delas de utilização livre, enquanto outras são pagas. As organizações podem usar diferentes scanners de

vulnerabilidades, por forma a garantir uma melhor cobertura dos seus ativos, criando uma imagem completa dos possíveis vetores de ataque a que poderão estar expostas.

Adicionalmente, devemos terem em conta alguns fatores. aquando da escolha da ferramenta de vulnerabilidades a configurar. numa determinada organização:

- Frequência de atualizações – Normalmente, um scanner de vulnerabilidades não consegue identificar uma vulnerabilidade, caso o seu Plug-in correspondente não esteja disponível. Por conseguinte, quanto mais rápido um vendedor conseguir lançar um plug-in, mais rapidamente essa ferramenta poderá detetar estas novas falhas.
- Qualidade vs Quantidade de Vulnerabilidades detetadas - A eficácia com que as vulnerabilidades críticas são identificadas é mais importante do que o número de vezes que são executados testes de vulnerabilidades, visto que a mesma vulnerabilidade pode ser detetada, por mais do que uma vez, pela ferramenta.
- Qualidade dos relatórios gerados - Além da informação das ameaças que foram detetadas, a ferramenta deve ser capaz de providenciar bons relatórios, para que seja possível, ao administrador de rede, a identificação de medidas corretivas a implementar.

Nessus

O Nessus é um dos scanners de vulnerabilidades mais populares. Isto deveu-se ao facto de inicialmente, até 2005, ser um software Open Source, altura em que este apenas ficou disponível através de uma licença comercial [3]. Existe uma versão gratuita do Nessus (Nessus Essentials), porém apenas disponíve para uso pessoal. Tem, no entanto, algumas limitações, como é o caso de apenas permitir analisar 16 endereços IP.
O Nessus Professional é a versão paga, oferecendo todas as capacidades deste software. Esta versão permite-nos, de igual forma, estar de acordo com diversos padrões de segurança como o PCI [4], o FDCC [5] e NIST [6].
Este software tem vantagens, tais como:

- Pode ser instalado em sistemas operativos como Windows, Mac OS, Debian, Ubuntu, entre outros.
- Contém uma base de dados com mais de 72000 CVEs.
- Tem uma das taxas de falsos positivos mais baixa do setor.
- Disponibiliza mais de 100 novos *Plug-in´s* semanalmente [7].

OpenVas

O OpenVAS é um scanner de vulnerabilidades gratuito e OpenSource, que nasceu da versão GPL do Nessus, depois de esta se tornar proprietária em 2005.

Este software tem as seguintes vantagens:

- scanner de segurança acompanhado por um *feed* de *Network Vulnerability Tests* (NVTs) com mais de 50.000 testes. Os produtos OpenVAS são licenciados sobre a *General Public License* (GNU GPL) [8], de utilização livre;

- os plugins do OpenVas são escritos na linguagem Nessus Attack Scripting Language (NASL) [9];
- o *Greenbone Community Feed* é atualizado diariamente, oferecendo proteção contra vulnerabilidades importantes e conhecidas, como é o caso da *Supernova*, *BlueKeep* ou o *PrintNightmare*.

Ao contrário do Nessus, este software tem de ser instalado numa máquina com sistema operativo Linux.

beSecure

O beSecure é outra ferramenta de análise de segurança, criada pela empresa BeyondSecurity [10].

Caraterísticas deste software:

- Permite efetuar pesquisa entre 64 a 200000 endereços IP ativos.
- Possui uma base de dados com mais de 10000 vulnerabilidades identificadas.
- Atualiza a base de dados num tempo estimado de 1 hora, após ter sido descoberta uma vulnerabilidade.
- Não necessita de agentes instalados nas máquinas para efetuar a análise.

GFI LanGuard

O GFI LanGuard é outra framework de pesquisa de vulnerabilidades, que ajuda na gestão de uma infraestrutura de rede. Através desta ferramenta, podemos ter vários benefícios, tais como:

- Visão geral de todos os elementos presentes na rede, ajudando na identificação de possíveis vulnerabilidades ativas.
- Identificação de vulnerabilidades por corrigir, através da consulta de uma base de dados com mais de 60.000 ameaças conhecidas, bem como portos abertos e informações do sistema, diretorias partilhadas e serviços.
- Controlo nas atualizações que são instaladas que, em caso de problemas, possibilita que as mesmas sejam revertidas.
- Disponibilidade de relatórios de segurança automatizados, que cumprem as normas de padrões de segurança, tais como o PCI, HIPAA [11] e SOX [12].

TripWire IP360

O TripWire é uma solução de gestão de vulnerabilidades da empresa Helpsystems [13].

Vantagens desta ferramenta:

- Arquitetura modular, que pode ser extensível de acordo com as necessidades da organização, com pouco impacto na performance da rede e dos sistemas.

- Utiliza uma avaliação de risco inovadora de priorização das vulnerabilidades, através do uso de uma escala de 1 a 50000, permitindo identificar, inequivocamente, onde as vulnerabilidades mais críticas residem. O resultado é dado consoante a facilidade com que pode ser explorada a vulnerabilidade e o nível de privilégios que o atacante irá obter, após a execução do ataque, bem como o tempo em que vulnerabilidade já está ativa na máquina.
- Permite que as organizações ajam de acordo com diversos padrões de segurança, com são o caso do PCI DSS [14], FISMA [15] e SOX.
- Permite analisar infraestruturas de rede, quer estas estejam *on-premises* ou na *cloud.*

Comparação das ferramentas

Na Tabela 1 podemos visualizar um comparativo entre as diferentes ferramentas que foram analisadas. Podemos ver algumas das características mais importantes, como é o caso do número de CVE que constituem a base de dados de cada uma delas, os tipos de relatórios que é possível extrair, por forma a conseguirmos analisar mais facilmente os resultados obtidos, bem como o licenciamento que cada ferramenta necessita.

Tabela 1 - Comparativo de ferramentas

Ferramenta	**Plugin´s**	**CVE**	**Relatórios**	**Interface Web**	**Agente**	**Licença**	**Vantagens**
Nessus	> 130.000	> 50.000	HTLM, CSV, XML	Sim	Sim	Paga	Menor taxa de falsos postivos
OpenVas	Não tem	> 26.000	HTLM, CSV, PDF,TXT	Sim	Não	Gratuita	Mais de 50.000 testes disponíveis
beSecure	****	>10.000	*****	Sim	Não	Paga	****
GFI LanGuard	*****	>11.500	HTLM, CSV, PDF, XLSX	Sim	Não	Paga	Mais de 60.000 ameaças conhecidas
TripWire IP360	*****	****	******	Sim	Não	Paga	Score de vulnerabilidades inovador

Após o comparativo entre as ferramentas analisadas, para o propósito deste estágio, o principal objetivo passa pela escolha de uma ferramenta que seja *open source* e gratuita, visto que a organização onde a ferramenta irá ser implementada não tem recursos financeiros disponíveis,

de momento, para adquirir uma ferramenta que exiga licenciamento. Por conseguinte, devido à necessidade de implementação de uma ferramenta de licenciamento gratuito, optou-se pela ferramenta *OpenVas*. De salientar que, caso não existisse esta restrição, iria ser escolhida a ferramenta Nessus, já que esta ferramenta tem uma base de dados com um maior leque de CVE´s e ~~tem~~ uma taxa de falsos positivos mais baixa.

Capítulo 3 Ferramenta de gestão de vulnerabilidades

3.1 OpenVas

O *Greenbone Community Edition* foi originalmente construído como um projeto comunitário chamado "OpenVAS" e é principalmente desenvolvido pela *Greenbone Networks*. Consiste no *Greenbone Vulnerability* Manager Daemon (gvmd), o *Greenbone Security Assistant* (GSA), com o *deamon* [16] *Greenbone Security Assistant* (gsad), e a aplicação que executa testes de vulnerabilidade nos sistemas escolhidos.

O *Greenbone Community Edition* consiste numa ferramenta com diversos serviços, sendo desenvolvido como parte dos produtos *Greenbone Enterprise*.

Greenbone Vulnerability Manager Daemon (GVMD)

O *Greenbone Vulnerability Manager* é o serviço central que consolida a pesquisa de vulnerabilidades numa solução completa de gestão de vulnerabilidades. Este controla o scanner *OpenVAS* usando o Open Scanner Protocol (OSP). É baseado em Xml e não requer uma conexão permanente para comunicação [17].

O próprio serviço oferece o *Greenbone Management Protocol* (GMP) sem estado, baseado em Xml. O Gvmd controla igualmente uma base de dados SQL (PostgreSQL), onde todos os dados de configuração e resultados de pesquisa são armazenados centralmente. Além disso, o Gvmd é responsável pela gestão de utilizadores, incluindo o controlo de permissões com grupos e funções. Este serviço possui igualmente um sistema de tempo de execução interno para tarefas agendadas e outros eventos.

Assistente de Segurança Greenbone (GSA)

O *Greenbone Security Assistant (GSA*) é a interface web que o utilizador utiliza para gerir a ferramenta. É o principal ponto de contato do utilizador com esta. Este conecta-se ao gvmd através do servidor web Greenbone Security Assistant Daemon (gsad), que possui um serviço web, para efetuar a gestão da ferramenta, recorrendo ao *Greenbone Management Protocol (GMP)*.

Scanner OpenVAS

O *OpenVAS Scanner* é um mecanismo de pesquisa completo, que executa testes de vulnerabilidades sobre determinados *hosts*, usando *feeds* atualizados e completos tais como o *Greenbone Enterprise Feed* ou o Greenbone Community Feed (disponível gratuitamente).

O scanner consiste nos componentes ospd-openvas e openvas-scanner. O *scanner* OpenVAS é controlado através do protocolo *Open Scanner Protocol* (OSP). O OSP Daemon do OpenVAS Scanner comunica com o gvmd através do OSP. Os dados das vulnerabilidades são armazenados, as pesquisas são iniciadas/interrompidas e os resultados das pesquisas são transferidos para o gvmd via OSPD. Na Figura 2 podemos observar o funcionamento deste scanner.

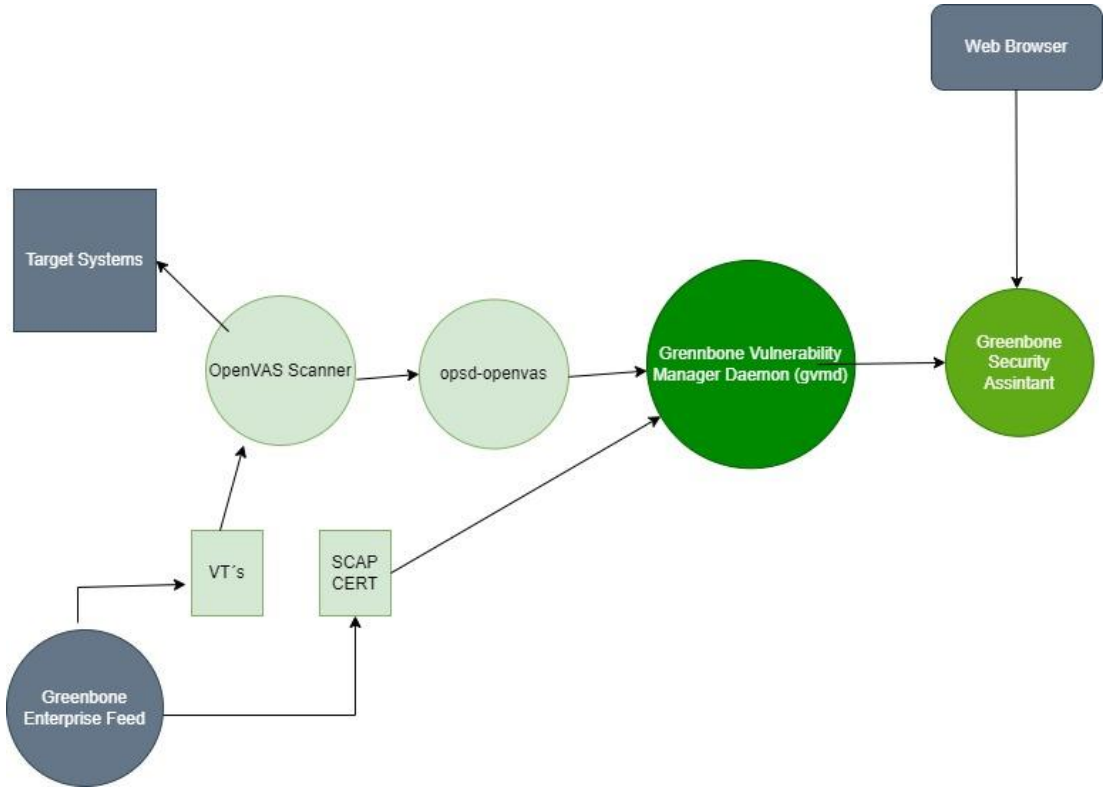

Figura 2 - Arquitetura Greenbone

Na próxima secção será descrita a metodologia usada para instalar e configurar a ferramenta de deteção de vulnerabilidades.

Instalação e configuração

Esta ferramenta foi instalada num computador com o sistema operativo Kali Linux.

Para fazer a instalação da ferramenta OpenVas, foi inicalmente feita uma atualização do sistema operativo, com recurso aos seguintes comandos:

- apt-get update;
- apt-get upgrade.

Após a atualização do Kali Linux, foi efeutada a instalação da ferramenta de deteção de vulnerabilidades, utlizando o comando indicado abaixo:

- apt-get install openvas

Finalizada a instalação da ferramente, foram atualizados os f*eed´*s, demonstrados na Figura 3, que contêm os testes de segurança e vulnerabilidades, que serão testados contra um determinado sistema, recorrendo ao comando abaixo demonstrado:

- gvm-feed-update

De salientar que estes devem ser regularmente atualizados, de modo a termos as vulnerabilidades mais recentes na base de dados da nossa ferramenta.

Podemos, de igual forma, atualizar cada um destes individualmente, caso assim se pretenda, recorrendo aos comandos indicados:

- greenbone-feed-sync --type GVMD_DATA
- greenbone-feed-sync --type SCAP
- greenbone-feed-sync --type CERT
- greenbone-nvt-sync

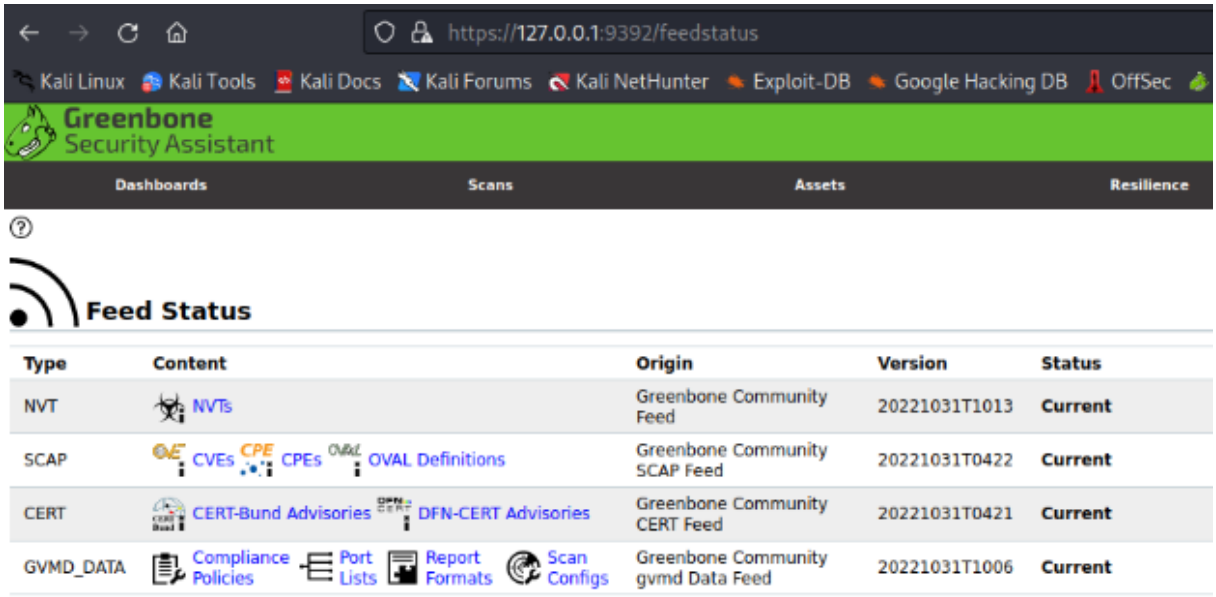

Figura 3 - Feed´s OpenVas

Na Figura 3 podemos realçar o uso dos NVT e das CVE.

Os network vulnerability tests (NVT) são testes de rotina usados pelo *Greenbone Security Manager* (GSM). Estes fazem parte do *Greenbone Security Feed* (GSF), que é atualizado regularmente. Os NVT incluem informação sobre a data de desenvolvimento, sistemas afetados, impacto das vulnerabilidades, bem como a forma de mitigação das mesmas.

A *Common Vulnerabilities and Exposures* (CVE) é uma base de dados que identifica, de forma unívoca, uma determinada vulnerabilidade. Cada CVE contém o número de identificação, uma breve descrição da ameaça, bem como as recomendações necessárias, por forma a mitigar a mesma.

Seguidamente, foi inicializada a ferramenta propriamente dita, com recurso ao comando "gvm-start". Na Figura 4, podemos visualizar o referido serviço em execução.

Figura 4 - OpenVas em execução

Após execução do serviço, disponível no porto 9392 da máquina, é possível aceder à consola gráfica da ferramenta de gestão de vulnerabilidades, conforme demonstrado na Figura 5.

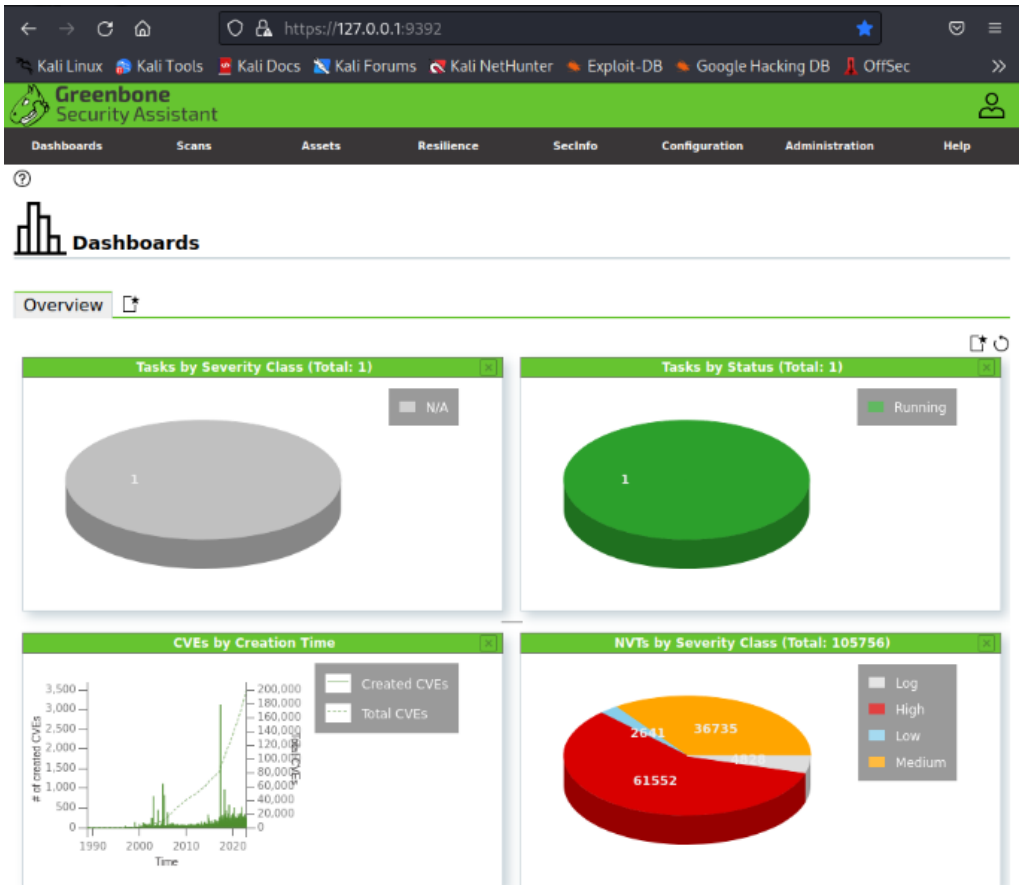

Figura 5 - Consola gráfica OpenVas

3.2 Análise de rede

Por forma a fazermos uma pesquisa de vulnerabilidades mais eficiente, foram realizados os seguintes passos:

- Primeiramente devem ser obtidas informações relacionadas com o sistema, tais como o hardware, software, interfaces e topologia, recorrendo a ferramentas como o NMAP [18].
- Seguidamente, tentam-se identificar possíveis vulnerabilidades existentes nas diferentes máquinas que constituem a rede, por forma a explorar as mesmas.
- Após a descoberta das vulnerabilidades, deve ser feita uma análise das mesmas, para perceber quais são as que poderão ter um maior impacto, no negócio de uma organização, caso sejam exploradas, recorrendo ao CVSS [19].
- Finalizado o processo de priorização das ameaças, devem ser implementados controlos, por forma a minimizar o risco apresentado por cada uma das ameaças identificadas.

- Posteriormente, devem ser efetuadas verificações de segurança periódicas, para garantir o correto funcionamento das medidas corretivas implementadas, bem como a possível descoberta de novas ameaças.

Através do NMAP, foram realizadas diferentes pesquisas nas sub-redes existentes, com objetivo de identificar os equipamentos ativos, que iriam ser analisados.

Após a pesquisa, foram identificadas nove subredes com endereços ativos, conforme demonstrado na Figura 6.

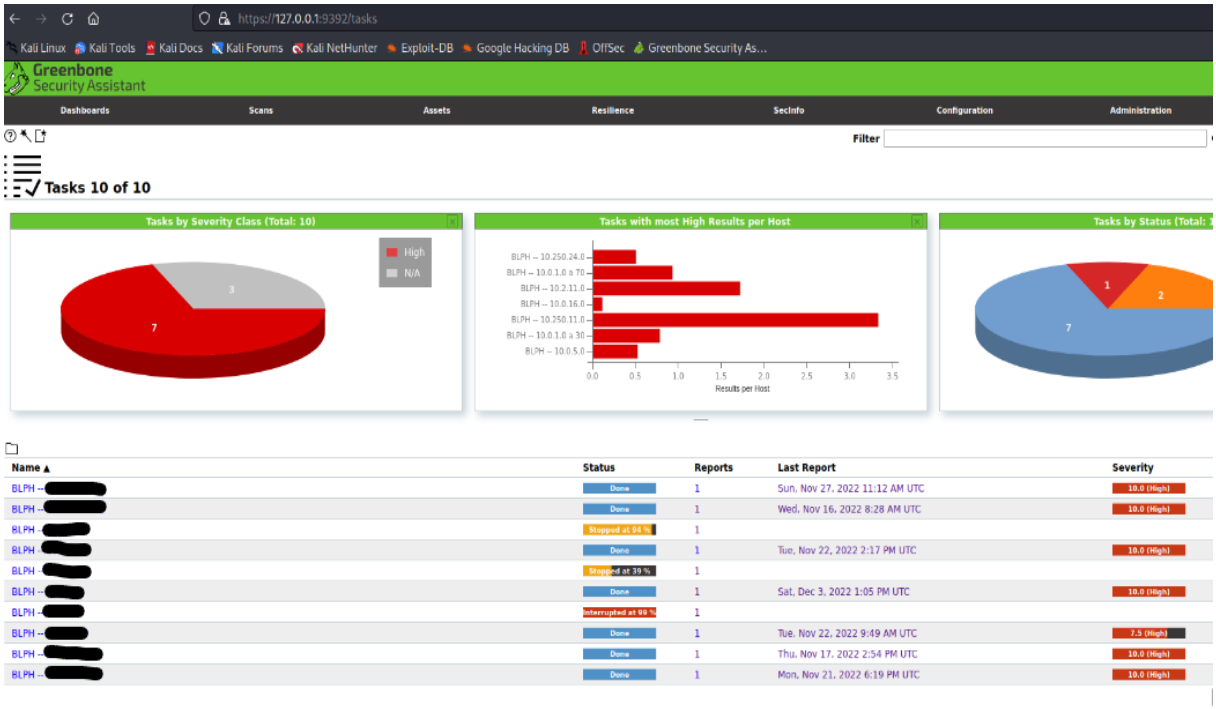

Figura 6 - Redes analisadas

A **Error! Not a valid bookmark self-reference.** identifica as vulnerabilidades identificadas, de acordo com o *Common Vulnerability Scoring System*, para cada uma das sub-redes.

De salientar que somente estão apresentados os números das vulnerabilidades descobertas, não sendo descritos os nomes das vulnerabilidades bem como os endereços ip das máquinas, por forma a proteger a organização.

Tabela 2 - Vulnerabilidades (Fase 1)

	Vulnerabilidades		
Sub-Rede	Alta	Média	Baixa
1	21	98	30
2	15	39	23
3	26	152	64
4	35	47	11
5	10	57	4
6	2	87	60
7	12	9	4
8	236	487	60
9	3	21	1

3.3 Correção de Vulnerabilidades

Após a identificação de vulnerabilidades foi iniciado um plano para correção das mesmas, começando por aquelas que apresentavam um maior nível de ameaça para a organização (CVSS mais elevado).

Após a correção de algumas destas vulnerabilidades, foram realizados novos *scans* a cada uma das sub-redes, em que foram implementadas medidas corretivas.

Os controlos implementadas nesta primeira fase passaram essencialmente pela correção de vulnerabilidades ao nível atualizações de versões de sistemas, nos computadores dos colaboradores, bem como correções de segurança no que se refere a login´s por omissão. Os resultados obtidos podem ser visualizados na Tabela 3.

Tabela 3 - Vulnerabilidades (Fase 2)

	Vulnerabilidades		
Sub-Rede	Alta	Média	Baixa
4	22	47	11
5	2	55	4

De referir que o plano de correção de algumas destas vulnerabilidades é um plano a médio prazo, visto que determinadas correções implicam a paragem dos sistemas produtivos da empresa.

Capítulo 4 Consciencialização para a Cibersegurança

De acordo com o *Anti-Phishing Working Group*, o número de ataques de phishing atingiu um novo recorde no terceiro trimestre de 2022, como um total de 1.270.883 ataques identificados [20].
A consciencialização dos utilizadores é, por isso, considerada uma das abordagens mais importantes e utilizadas na luta contra este tipo de ataques. Por conseguinte, as organizações devem levar a cabo campanhas de sensibilização, por forma a educar os trabalhadores sobre o que são os ataques de phishing e como se podem detetar ~~estes ataques~~.

4.1 Conceitos

Antes de iniciar o processo de *phishing* é importante relembrarmos alguns conceitos importantes, tais como o que é a segurança da informação e o *phishing* propriamente dito.

Segurança da informação

O termo "segurança da informação" significa proteger a informação e os sistemas de informação contra o acesso, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer integridade, confidencialidade e disponibilidade dos dados [21].

A segurança da Informação é construída em torno de três grandes objetivos, conhecidos como Confidencialidade, Integridade e Disponibilidade (CIA).

- A confidencialidade é a parte que garante que as informações não são divulgadas a indivíduos, entidades ou processos não autorizados.
- A integridade é o meio que garante que os dados não podem ser editados de forma não autorizada.
- A disponibilidade tem como função garantir que a informação está disponível, sempre que necessária.

De igual forma, existe também um príncipio que protege os programas de segurança da informação, denominado não repúdio. Este tem como objetivo garantir que uma determinada parte não possa negar que fez uma determinada ação.

4.2 Componentes

Um programa de segurança da informação deve consistir em três fases [22]:

- Desenvolvimento de políticas de segurança, que reflitam as necessidades do negócio, perante os riscos conhecidos.
- Informação dos utilizadores sobre as suas responsabildades na segurança da infraestrutura informática, conforme documentado nas politicas de segurança da organização.
- Criação de processos para monitorização e revisão do programa.

A consciencialização e o treino devem ser focados em todos os índividuos da organização, desde o trabalhador comum, ao executivo da organização.

Um programa efetivo de consciencialização e treino deve explicar as regras e procedimentos para o uso correto dos sistemas informáticos implementados na organização.

Esta secção descreve a relação entre estas três componentes: consciencialização, treino e educação.

Consciencialização

Os esforços na consciencialização para a segurança informática são realizados com o objetivo de criar a mudança de comportamento dos utilizadores e o reforço das boas práticas de segurança.

De salientar que a consciencialização não é um treino, mas sim um alerta para os utilizadores sobre as necessidades de segurança.

Um exemplo de um tópico que poderia ser abordado numa campanha de consciencialização seria a proteção contra vírus infomáticos. Nesta ação podia ser explicado aos utilizadores o que é um vírus, o que pode acontecer caso um vírus seja executado numa máquina, e o que um utilizador deve fazer caso detete que o seu computador ficou infetado.

Estas campanhas podem incluir vários formatos de comunicação tais como:

- Emails – através do email podem ser enviados alertas de segurança regulares para que os utilizadores fiquem a par das comunicações de segurança.
- Posters – colocação de posters em espaços partilhados, por forma a relembrar os utilizadores das boas práticas de segurança da informação.
- Workshops – através de workshops podem ser explicados os diversos tipos de *phishing*, como também podem ser feitas sessões de esclarecimentos.
- Cursos online – através da realização de cursos online podem ser visualizados vídeos formativos, bem como realizar questionários sobre os mesmos, verificando assim o nível de aptidão do indivíduo para a cibersegurança.

De salientar que é importante utilizar uma variedade de canais de comunicação de forma a assegurar que a mensagem chega a todos os colaboradores da organização. Adicionalmente, o conteúdo deve ser específico para o público em questão e deve ser apresentado de forma a que seja de fácil compreensão.
Usando os meios de comunicação apropriados, as organizações podem melhorar a consciencialização de cibersegurança entre os indivíduos, reduzindo o risco de um possível incidente de segurança.

Treino

O treino, segundo o *National Institute of Standards and Technology* (NIST), tem como objetivo dotar os índividuos de competências para a segurança da informação [22].

A maior diferença entre o treino e a consciencialização é que o treino tem como função dar competências aos indivíduos, o que permite a uma pessoa efetuar uma determinada ação, enquanto que a consciencialização pretende focar a atenção de uma pessoa para um problema ou um conjunto de problemas. As competências adquiridas durante o treino são construídas após já se ter consciencialização para tal.

Um exemplo de um treino é um curso de segurança de infomática para os administradores de sistema, que devem englobar controlos (gestão, operação e técnicos). Controlos de gestão incluem políticas de gestão de risco e programas de gestão de segurança de IT. Controlos operacionais incluem questões com os utilizadores, planos de contigência, atuar em caso de existir algum incidente, consciencialização e treino, bem como suporte aos computadores. Controlos técnicos incluem identificação e autenticação, controlos de acessos lógicos, auditorias e criptografia.

Educação

Nos dias de hoje, à medida que as organizações expandem a utilização das mais diversas tecnologias, os hackers estão a aproveitar esse facto com o objetivo de entrar nos sistemas informáticos das instituições, tendo como alvo preferêncial os utilizadores.

A educação das pessoas é, por isso, vital para que estas possam ficar dotadas de capacidades e competências de segurança nas várias especialidades funcionais.

Adiconalmente, esta educação tem como objetivo capacitar os especialistas de segurança informática para que possam dar respostas proativas aos diversos problemas que poderão encontrar.

Um exemplo de educação é um curso num instituto / universidade, em que as pessoas completam o curso com o objetivo de adquirir conhecimentos, numa matéria em particular.

4.3 Análise de ferramentas

Após o comparativo entre as ferramentas analisadas, para o propósito deste estágio, tal como aconteceu na escolha da ferramenta de gestão de vulnerabilidades, o objetivo passa pela escolha de uma ferramenta gratuita, visto que a organização não tem recursos financeiros disponíveis, de momento, para adquirir uma ferramenta que requer licenciamento. Por conseguinte, devido à necessidade de implementação de uma ferramenta sem licenciamento, optou-se pela ferramenta Gophish.

4.4 O que é *phishing*

O *phishing* é um tipo de ciberataque que utiliza técnicas de engenharia social com o objetivo de aceder a informação sensível/confidencial dos utilizadores [23].
Este começa com a criação de um site falso, idêntico a um site de uma organização legítima, mas com um endereço URL ligeiramente diferente. Em seguida, é enviado um e-mail a milhares de utilizadores da Internet, que solicita que estes acedam ao site falso, para alterarem os seus registos, pedindo que introduzam os seus dados pessoais.
Quando o utilizador introduz as suas informações pessoais, no website falso, as informações pessoais são enviadas para o atacante, sendo a vítima posteriormente redirecionada para o site legítimo, de modo a encobrir a tentativa de fraude.

Na Figura 7 podemos visualizar todo este processo.

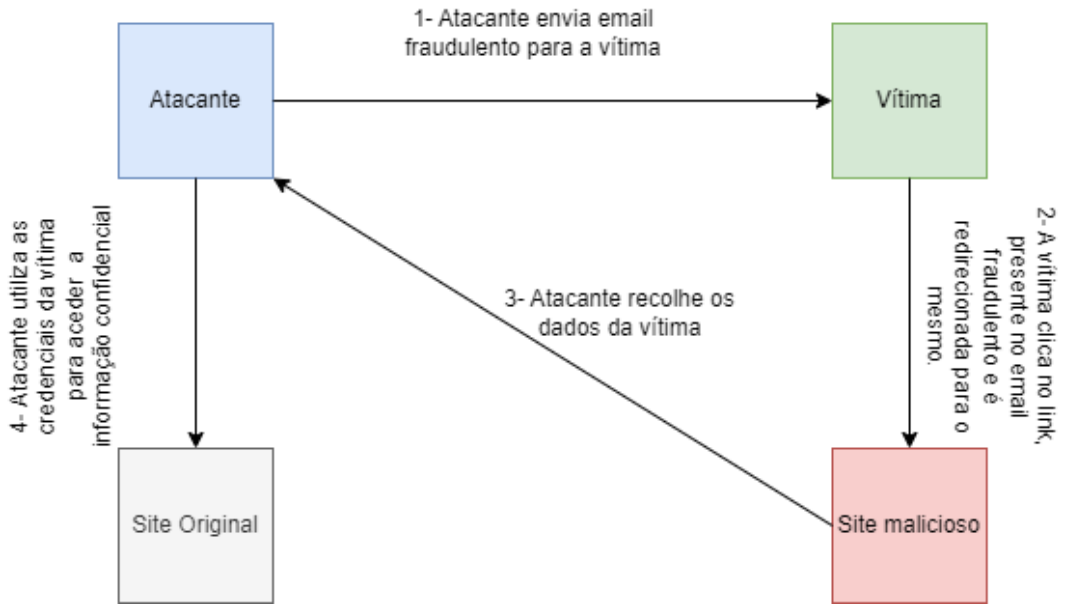

Figura 7 - Como funciona o Phishing

Adicionalmente, o *phishing* foi declarado como sendo o método principal usado pelos atacantes para explorarem a privacidade dos utilizadores na Internet [24].
Os ataques de *phishing* já não são recentes, porém, a cada ano que passa, têm-se tornando um problema cada vez maior para os utilizadores da Internet, já que os atacantes utilizam técnicas inovadoras, para ultrapassar a segurança dos sistemas informáticos.

4.5 Técnicas de *phishing*

- *Email Spoofing*
    - Neste tipo de ataques, os atores maliciosos enviam um email fraudulento às vítimas, fingindo pertencerem a uma determinada organização, de forma a ganhar a confiança destas, com o intuito de que elas introduzam credências, no site fraudulento.
- *Vishing*
    - Neste tipo de ataque, os hackers efetuam uma chamada telefónica para a vítima, fazendo-se passar por uma determinada organização, solicitando dados pessoais. Podem também, por outro lado, levar as pessoas a executar ações maliciosas (redireccionamento para sites maliciosos, transferência de dinheiro para a conta do atacante, entre outros).

- *Malvertising*
    - Este é um tipo de ataque onde é injetado código malicioso em anúncios legítimos nos websites, redirecionado as vítimas para sites maliciosos. O modo de funcionamento deste ataque está descrito na Figura 8.
        1. O atacante cria inicialmente um anúncio falso.
        2. O anúncio é submetido numa cadeia legitima de partilha de anúncios, que é depois distribuída por vários websites.
        3. Quando o utilizador clica no anúncio, é feito o download do *malware* para o computador da vítima.
        4. Após este ser instalado, o atacante fica com uma porta de entrada para controlar o computador da vítima.

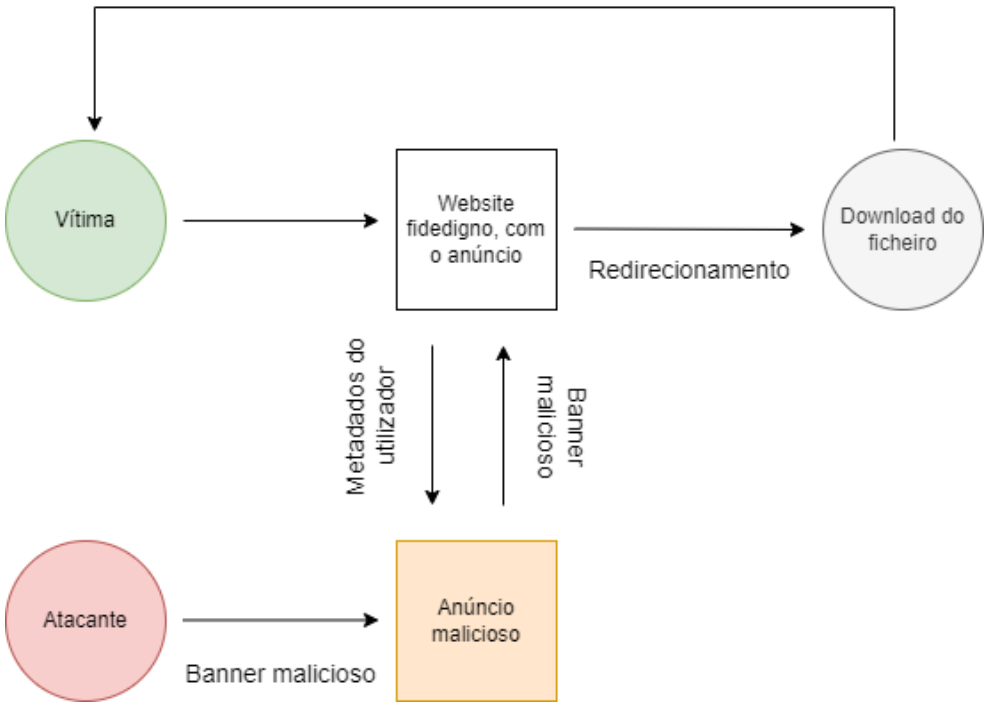

Figura 8 - Funcionamento Malvertising

- *Browser Vulnerabilities*
  - Neste ataque, os atores maliciosos utilizam vulnerabilidades dos browsers [25], levando as vítimas a aceder a sites fraudulentos, fingindo que estes pareçam fidedignos.

- *Clickjacking*
  - Este é um ciberataque em que o atacante tenta enganar o utilizador clicar num botão/link num website. Isto é conseguido através da sobreposição de uma janela "transparente" que está sobre o botão legítimo do website.
    - Na Figura 9 encontra-se detalhado o modo de funcionamento do ataque.
      1. O atacante cria o site falso e envia o link para a vítima através de email ou SMS.
      2. Seguidamente o ator malicioso coloca, sobre o botão do site, uma janela, com o anúncio malicioso.
      3. Quando a vítima clica, no que parece ser o botão real do site, ela está a clicar na janela maliciosa.
      4. Seguidamente é efetuado o download do *malware* para o computador, permitindo ao atacante obter o controlo da máquina infetada.

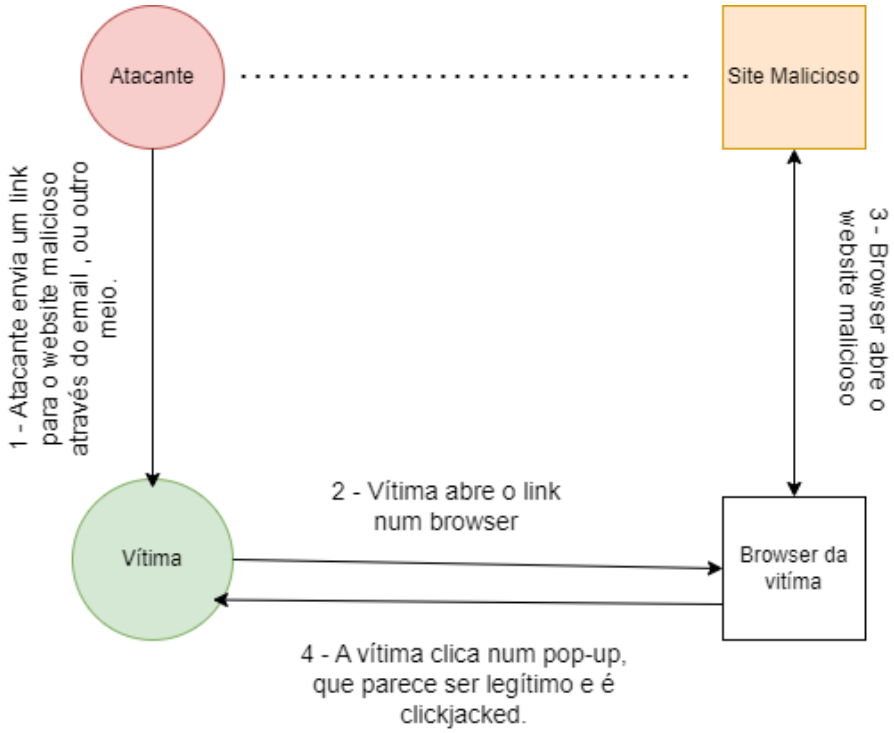

Figura 9 - Funcionamento Clickjacking

- *Smishing*
  - Neste tipo de ataque, a vítima recebe uma mensagem de texto (SMS) parecendo vir de uma instituição legítima, solicitando a introdução dos seus dados pessoais.

- *Whaling*
  - Neste caso, o atacante faz-se passar por uma pessoa de alto cargo na organização (administrador, diretor de departamento), com o objetivo de pedir informação sensível aos restantes colaboradores.

- *Typosquatting*
  - Neste tipo de ataque, o atacante regista domínios que são semelhantes aos domínios legítimos (google.com), porém contêm erros tipográficos (gogle.com). Posteriormente, este tenta ludibriar as vítimas para que estas acedam aos websites fraudulentos [26].

4.6 Ferramentas de *phishing*

Existem no mercado diversas ferramentas para envio de campanhas de *phishing*, sendo algumas delas gratuitas e outras que exigem licenciamento.

Ferramentas Licenciadas:

- InfosecIQ [27]
    - Vantagens:
        - Permite realizar diversos ataques de *phishing* tais como:
            - *Drive-by* (envio de email com elevada urgência, de forma a criar interesse da vítima, para que a mesma clique no *link*).
            - *Data entry* (ataque que redireciona a vítima para uma página fraudulenta, esperando que esta coloque as suas credenciais).
            - *Spearphishing* (ataque realizado a uma pessoa específica, usando emails pré-preenchidos)
            - *Malware attachments* (permite a anexação de emails com *malware*, ao computador).
            - USB (Permite carregar ficheiros com macros, em dispositivos amovíveis, com o objetivo de educar os colaboradores sobre os cuidados a ter aquando da ligação destes dispositivos ao computador.
    - Desvantagens:
        - Custo 15€ por *asset*

- Lucy Security [28]
    - Vantagens:
        - Configurações de dispositivos amovíveis com ficheiros executáveis.
        - Execução de várias campanhas em simultâneo.
        - Envio de campanhas de *smishing.*
        - Criação de sites falsos para uso nas campanhas de phishing.
        - Ataques baseados em aplicações Java.
        - Diversos *templates*, disponíveis em várias línguas.
    - Desvantagens:
        - Custo- 11€ por asset.

- KnowBe4 [29]
    - Vantagens:
        - Execução de várias campanhas em simultâneo.

        - Disponibilização de diversos *templates*, de emails de *phishing* disponíveis em várias línguas.
        - Download de relatórios com informações detalhadas sobre os utilizadores.
        - Plataforma com vídeos educativos para formar os trabalhadores sobre necessidades de Cibersegurança.
    - Desvantagens:
        - Ferramenta paga (9€/utilizador).

- Goldphish [30]
    - Vantagens:
        - Execução de várias campanhas em simultâneo.
        - Monitorização de atividade dos utilizadores.
        - Plataforma com vídeos educativos para formar os colaboradores sobre necessidades de Cibersegurança.
    - Desvantagens:
        - Custo de 6€ /colaborador.

Ferramentas Gratuitas

- Gophish [31]
    - Benefícios:
        - Execução de várias campanhas em simultâneo.
        - Software open-source e gratuito.
        - Instalação fácil e intuitiva, bastando para tal efetuar o download da ferramenta e executá-la de seguida.
        - Recolha de credenciais das vítimas.
    - Desvantagens:
        - Relatórios das campanhas realizadas com poucos detalhes.
        - Requer configuração manual de *templates* de email.

- King Phisher
    - Vantagens:
        - Execução de várias campanhas de *phishing* em simultâneo.
        - Geolocalização das vítimas.
        - Recolha de credenciais das vítimas.
    - Desvantagens:
        - Layout pouco intuitivo.
        - Ferramenta deixou de sofrer atualizações desde 2019.

Na Tabela 4 podemos visualizar as diferentes ferramentas de *phishing*, bem como as técnicas que estas permitem executar.

Tabela 4 - Técnicas de phishing usadas pelas ferramentas de phishing

Ferramentas	Email Spoofing	Vishing	Malvertising	Browser Vulnerabilities	Clickjacking	Smishing	Whaling
KnowBe4	x	-	-	-	-	-	x
InfosecIQ	x	-	-	-	-	-	x
Lucy Security	x	x	-	-	-	x	x
Gophish	x	-	-	-	-	-	x
King Phisher	x	-	-	-	-	-	x
Goldphish	x	-	-	-	-	-	x

Após o comparativo entre as ferramentas analisadas, para o propósito deste estágio, tal como aconteceu na escolha da ferramenta de gestão de vulnerabilidades, o objetivo passa pela escolha de uma ferramenta gratuita, visto que a organização não tem recursos financeiros disponíveis, de momento, para adquirir uma ferramenta que exiga licenciamento. Atendendo a estas necessidades foi escolhida a ferramenta Gophish.

4.7 Técnicas de Anti-Phishing

O *anti-phishing* refere-se ao método usado para detetar e prevenir ataques de *phishing*. Algumas técnicas funcionam em e-mails, outras funcionam em atributos de sites da web e algumas em URL de sites. Estas técnicas têm como objetivo ajudar o utilizador a reconhecer e filtrar vários tipos de ataques de phishing.
Em geral, o *anti-phishing* pode ser conseguido através da implementação das seguintes técnicas: [32].

1. *Content-filtering* - Nesta técnica é utilizada inteligência artificial para filtrar emails fidedignos de emails de phishing.
2. *Multi Factor Authentication* - Esta técnica usa dois ou mais mecanismos distintos (SMS, chamada telefónica, autenticação via aplicação) aquando da autenticação do utilizador num determinado sistema.
3. *Black listing* - Nesta técnica são identificados diversos tipos de sites fraudulentos, sendo estes colocados numa plataforma pública para consulta dos utilizadores.
4. *Machine Learning* - Esta técnica utiliza inteligência artificial, analisando os processos do sistema operativo.

5. *Greylisting* - Técnica usada para bloquear temporariamente a receção de emails, de emissores desconhecidos [33].
6. *Sender Policy Framework* (SPF) - Protocolo que permite verificar se o remetente do email vem de uma máquina que está autorizada a enviar emails de um determinado domínio.
7. *URL scanning* - Técnica que analisa os links presentes no email, para verificar se os mesmos são considerados maliciosos ou não.
8. *Email Alias* - Técnica que permite aos utilizadores enviarem e receberem emails sem partilhar o seu verdadeiro email. Usando este mecanismo os utilizadores podem proteger o seu email original, impedindo-o de receber comunicações de spam.

O desenvolvimento deste tipo de mecanismos tem crescido, em grande parte devido à necessidade de combater o aumento do número de ataques de *phishing* em todo o mundo.
O objetivo dos ataques passa por assegurar que a vítima não detete o ataque até que seja tarde de mais. Estes tipos de técnicas/algoritmos, recorrem à inteligência artificial, com o objetivo de ajudar a detetar o ataque, enquanto este está a acontecer. Na Figura 10 encontra-se representado o modo de funcionamento deste tipo de tecnologia.

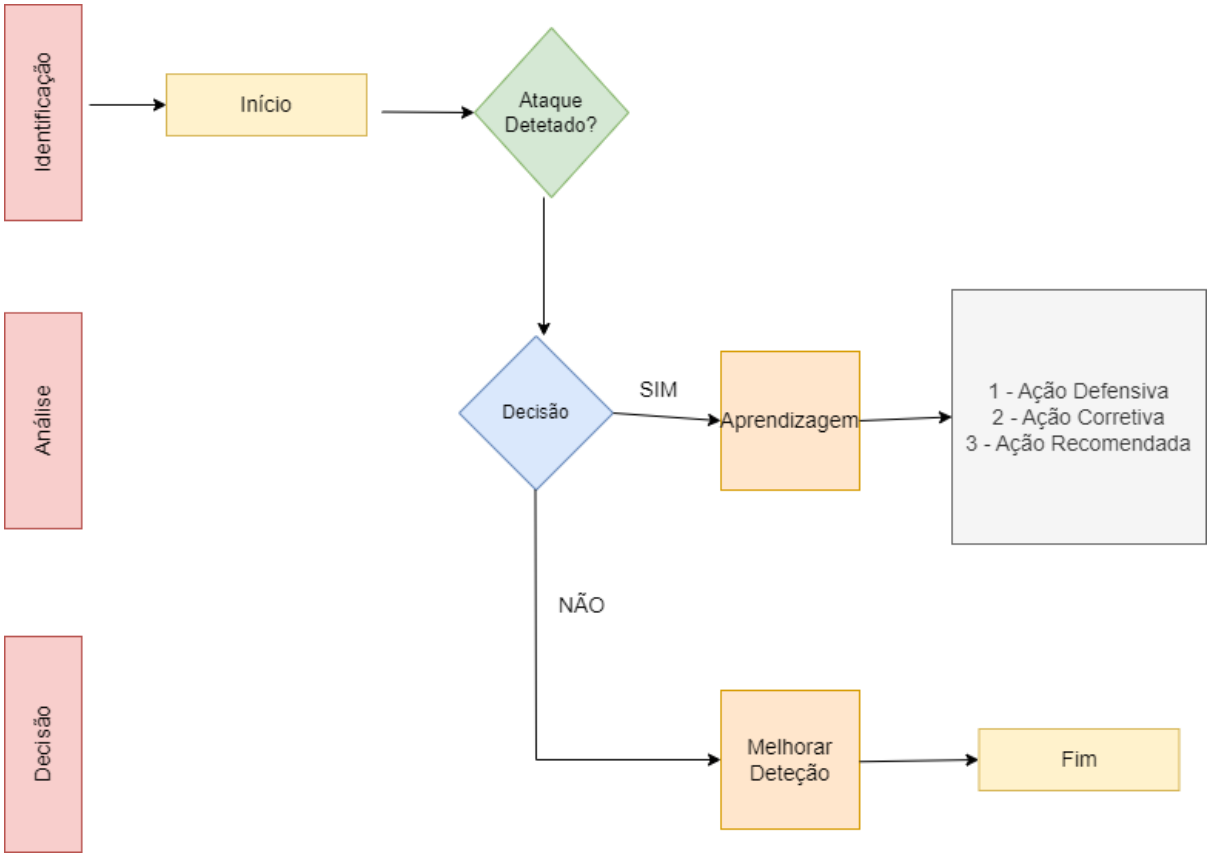

Figura 10 - Funcionamento de algoritmo de IA

Nesta imagem podemos verificar que é inicialmente efetuada uma validação do email, em que é analisada a existência de um ataque. Caso seja detetado o ataque, é tomada uma decisão sobre o que fazer. Caso o mesmo não seja detetado, deve ser verificado o que falhou, por forma a melhorar a deteção.

4.8 Ferramentas Anti-Phishing

Exchange Online Protection

O EOP [34] é um serviço *cloud*, da Microsoft, que tem como objetivo a proteção das organizações contra emails de spam, *malware* e outras ameaças.
O modo de funcionamento desta ferramenta é descrito na Figura 11.

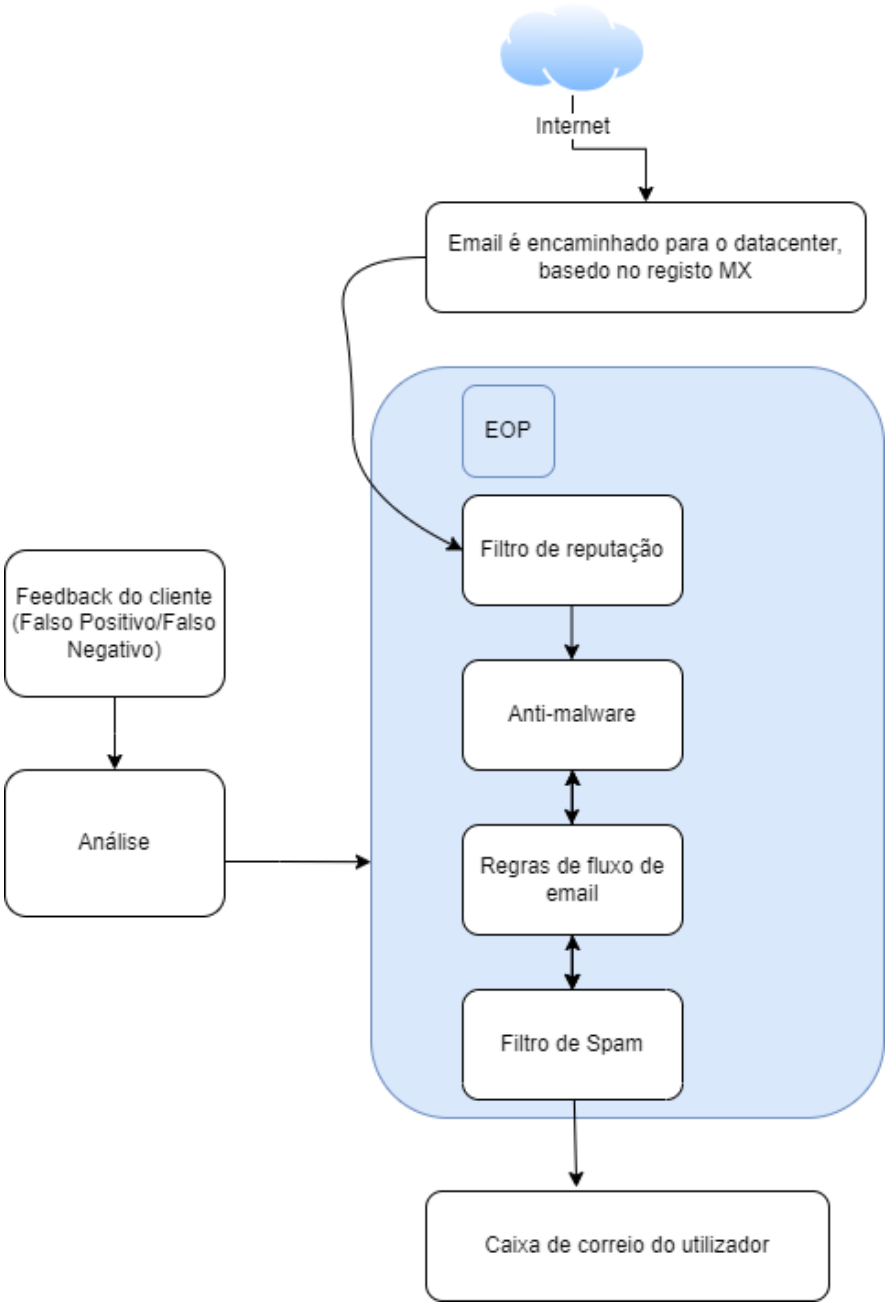

Figura 11 - Funcionamento da ferramenta EOP

1. Quando um email chega ao EOP, passa inicialmente no filtro de reputação, que avalia a cotação do emissor da mensagem.
2. Seguidamente, o email é analisado, para ver se é detetado *malware*. Caso seja descoberto, (quer seja no email em si, ou nos anexos a ele associados) o mesmo é encaminhado para a quarentena.

3. Posteriormente, o email passa por mais filtros, onde é avaliado perante as regras de fluxo de emails existentes (ex: notificação ao administrador de rede quando um email, de um determinado domínio, chega ao servidor de email).
4. Finalmente, o email passa por um filtro de spam, onde as mensagens são identificadas como *spam*, *high confidence spam*, *phishing* e *high confidence phishing*. Caso o email cumpra todos os requisitos associados, o mesmo é entregue na caixa de email do colaborador.

TensorFlow

O *TensorFlow* é uma biblioteca *open source*, desenvolvida pela Google, com o intuito de criar e treinar modelos de inteligência artificial (IA). Funciona definindo um gráfico computacional que representa as operações matemáticas envolvidas num modelo de IA [35].
Na criação de um modelo *TensorFlow*, são definidas séries de operações que transformam os dados de entrada numa previsão de saída. Essas operações podem incluir operações matemáticas como a adição e multiplicação, bem como operações complexas, como é o caso da *Convolution* [36].
Este modelo fornece uma variedade de ferramentas e *Application Programming Interface*s (API) para criar e treinar modelos de inteligência artificial, incluindo APIs de alto nível, como é o caso do Keras [37], permitindo a criação de modelos de forma fácil e rápida, como também APIs de baixo nível (TensorFlow Core API, TensorFlow Graphs, TensorFlow Sessions) para ajustar modelos e otimizar o desempenho, contudo este tipo de API´s de baixo nível requer mais competências de programação.

Icloud Mail

O *Icloud Mail* é o serviço de email da empresa Apple. Este utiliza diversas técnicas por forma a detetar e bloquear emails de Spam [38].

1. Filtros de análise de conteúdo
    a. Através deste filtro é possível analisar o conteúdo dos emails procurando por frases, palavras ou padrões que poderão indicar a presença de um email de *phishing*.

2. Reputação do emissor do email
    a. Esta técnica avalia a reputação do email, endereço IP e domínio do emissor do email.

3. Análises de links (URL)
    a. Este serviço analisa os links contidos no email, por forma a determinar se estes redirecionam para sites de *phishing* conhecidos.

4. Inteligência artificial
    a. São usados algoritmos de inteligência artificial para identificar padrões e anomalias que possam indicar a presença de um email de *phishing*.

5. Feedback dos utilizadores
    a. Este serviço permite aos utilizadores reportarem emails que consideram suspeitos. Caso um email seja reportado como suspeito por múltiplos utilizadores, irá ativar mecanismos de proteção (alertas/filtros).

Barracuda Email Security

O Barracuda Email Security é um serviço cloud [39] que fornece proteção contra diversas ameaças como spam, vírus e ataques de phishing. Este serviço usa múltiplas camadas de segurança, (filtragem de emails, proteção *anti-spoofing*, *advanced thread protection*, com recurso a IA) por forma a detetar e bloquear ameaças, antes que estas cheguem às caixas de correio dos utilizadores.
Na Tabela 5 encontram-se demonstradas as técnicas de *anti-phishing* utilizadas pelas diferentes ferramentas.

Tabela 5 Técnicas Anti-Phishing usadas pelas ferramentas

	Ferramentas			
	Exchange Online Protection	Google Spam Filter	iCloud Mail Filter	Barracuda Email Security
Content-filtering	x	x	x	x
Multi-Factor Authentication	x	x	x	-
Black listing	x	x	x	x
Machine Learning	x	x	-	x
Greylisting	x	-	-	-
Sender Policy Framework (SPF)	x	x	x	x
URL scanning	x	x	x	x
Email Alias	-	-	x	-

Após a comparação das diferentes ferramentas de *anti-phishing* e as técnicas que estas utilizam por forma a prevenir o *phishing*, é importante salientar que nenhuma destas consegue providenciar proteção total contra este tipo de ataques. As combinações destas técnicas, juntamente com a formação dos colaboradores e atualizações constantes dos sistemas informáticos, podem ajudar na redução de um possível ataque de *phishing* e melhorar a segurança da organização.

4.9 Plano de Ação da Campanha

O propósito deste capítulo é delinear o que as organizações devem considerar, aquando da realização de campanhas de *phishing*. Este capítulo descreve todos os passos numa experiência deste gênero, incluindo considerações éticas e legais, escolha da plataforma, informação aos colaboradores, lançamento da campanha e análise de resultados.

Antes de lançar uma campanha de phishing

Propósito das campanhas de phishing

A realização de campanhas de *phishing* têm como objetivo verificar e aumentar a consciencialização para as necessidades de cibersegurança na organização, visto que um ataque bem-sucedido à organização poderá levar a perdas monetárias, bem como grandes danos de reputação. Adicionalmente, existe a necessidade de cumprir com regulamentos. Exemplificando, a política da empresa ou os contratos que esta estabelece com outros podem indicar a necessidade de executar testes de segurança periódicos mensais ou anuais.

Considerações éticas

As avaliações de phishing devem ser realizadas por forma a que não causem transtornos psicológicos aos utilizadores visados. Exemplificando, o conteúdo do email enviado não deve conter conteúdo ofensivo e a privacidade de cada indivíduo deve ser mantida.

Tipos de utilizadores

É importante referir que os utilizadores, sendo seres humanos, têm noções diferentes dos perigos associados aos meios informáticos. Exemplificando, na Bluepharma existem diversos tipos de colaboradores com diferentes noções de segurança, podendo dividir os utilizadores em dois grupos.

1. Utilizadores ativos – Utilizadores com noções do modo de funcionamento de um computador e que utilizam frequentemente o serviço de e-mail.
2. Utilizadores passivos - Utilizadores que têm pouca experiência (têm vagas noções do modo de funcionamento de um computador) e utilizam o e-mail só quando necessário.

Planeamento da campanha de phishing

A criação de uma campanha deste gênero requer preparação e planeamento antes da execução da mesma. Antes do lançamento desta devem ser tidos em consideração os seguintes aspetos:

1. Como irá ser anunciada a campanha de phishing aos colaboradores da organização?
2. Como poderão os colaboradores reportar a existência do email de phishing?

3. Qual o tema que a campanha de *phishing* irá ter?
4. Como irá ser efetuada a monitorização dos colaboradores que abriram os emails, os que clicaram no link, os que submeteram credenciais, bem como aqueles que reportaram a presença do mesmo?
5. Como irão ser apresentados os resultados obtidos e o que irá ser feito com esses resultados, por forma a assegurar melhoras práticas no futuro?
6. Periodicidade na realização de campanhas de *phishing*?

4.10 Lançamento da campanha de phishing

Com objetivo de estudar a vulnerabilidade dos utilizadores a possíveis ataques de *phishing*, foi enviada uma campanha, sem conhecimento prévio dos colaboradores da organização, por forma a obter um número mais concreto das necessidades de segurança da organização.

O tema da primeira campanha foi a pandemia de Covid-19. Nesta campanha, foi configurado um website idêntico ao site da Bluepharma, que era acedido aquando do preenchimento de assuntos relacionados com o tema do Covid-19. Seguidamente, foi configurado um email, em que nos fizemos passar pelo departamento de Ambiente e Segurança, pedindo aos colaboradores que preenchessem um questionário sobre o tema.

Para esta campanha foi utilizada a ferramenta *Gophish*, como forma de disseminação do email. Após o envio do email, os colaboradores poderiam reportar o email fraudulento através da plataforma *Servicedesk*, plataforma essa que já se encontrava em funcionamento, com o intuito de reportar problemas relacionados com a área informática.

De realçar que o único objetivo da campanha foi a identificação de potenciais vítimas, não sendo reveladas quaisquer credenciais obtidas. O site falso ficou online durante uma semana. Após esse período, foi enviado um comunicado geral para a organização indicando que o departamento de informática tinha sido o responsável pelo envio deste email.

Depois da recolha dos resultados, os mesmos foram apresentados, numa reunião com o conselho de administração, expondo os resultados obtidos, identificando os utilizadores que submeteram credenciais, exaltando a necessidade de serem executadas periodicamente estes tipos de campanhas de sensibilização aos colaboradores. Nessa mesma reunião, ficou definido que iriam ser ministradas formações de Cibersegurança, para que fosse possível consciencializar os colaboradores para a temática da segurança da informação.

Instalação e configuração Gophish

Para a instalação da ferramenta, foi utilizada uma máquina virtual, configurada no Microsoft Azure, com as seguintes características:

- Windows 10
- 4GB de RAM
- Processador Intel Xeon 8272 CL
- Disco de 120GB

Instalação

Para fazer a instalação e configuração da ferramenta em questão foi usada uma máquina virtual. Seguidamente, foi efetuada a instalação da ferramenta propriamente dita. Para tal, bastou executar a aplicação propriamente dita, para podermos visualizar o serviço em execução no porto 1724 da máquina, conforme demonstrado na Figura 12

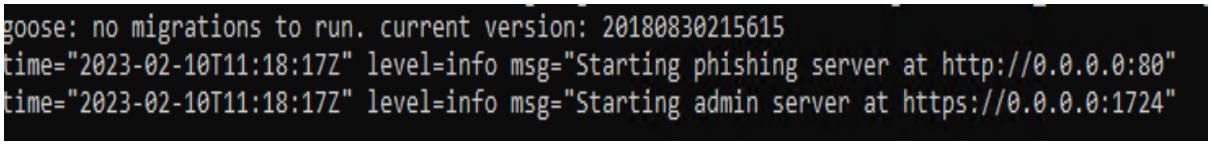

Figura 12 - Execução do Gophish

Configuração

Email Templates

Por forma a executar a campanha de *phishing*, o primeiro passo foi configurar o email que iria ser enviado aos colaboradores da organização. Estes podem ser importados de *templates* existentes ou podem ser criados de raiz.
Na Figura 13 encontra-se demostrado o *template* que foi utilizado como base, para o envio da campanha.
Para a sua configuração foi importado um email do departamento de Ambiente e Segurança. Neste sugeríamos o preenchimento de um formulário relacionado com a pandemia da Covid-19. Como podemos visualizar igualmente na Figura 13, o email continha um link que iria redirecionar os colaboradores para a página web suspeita.

06/04/2022 **INFORMAÇÃO COVID-19** **Ref. SST_Covid 51/2022**

Caros Colaboradores,

Agradecemos com alguma urgência que preencham o seguinte formulário relativamente a pandemia Covid-19!

Disponível em Sustentabilidade/Sistema de Gestão Integrado/ Covid-19 Plano de Contingência

A PANDEMIA NÃO TERMINOU!
VAMOS CONTINUAR A CUIDAR UNS DOS OUTROS!

Qualquer sintoma, suspeita de situação de risco, isolamento profilático (independentemente da causa e do regime de trabalho do colaborador), deve ser de imediato reportado à equipa ASST, para que seja dado o devido acompanhamento a cada situação.

Atentamente,
A Equipa de Ambiente e Segurança

with eyes set on the future www.bluepharmagroup.com

Figura 13 - Template de email

Landing Pages

O Gophish permite a criação de "*landing pages"*. Estas são páginas para onde os utilizadores são redirecionados após estes clicarem no link, que recebem através do email de phishing, configurado no Email Templates.
Na Figura 14, abaixo, encontra-se demonstrada a *Landing Page*, para onde os colaboradores eram redirecionados, quando clicavam no link, contido no email.

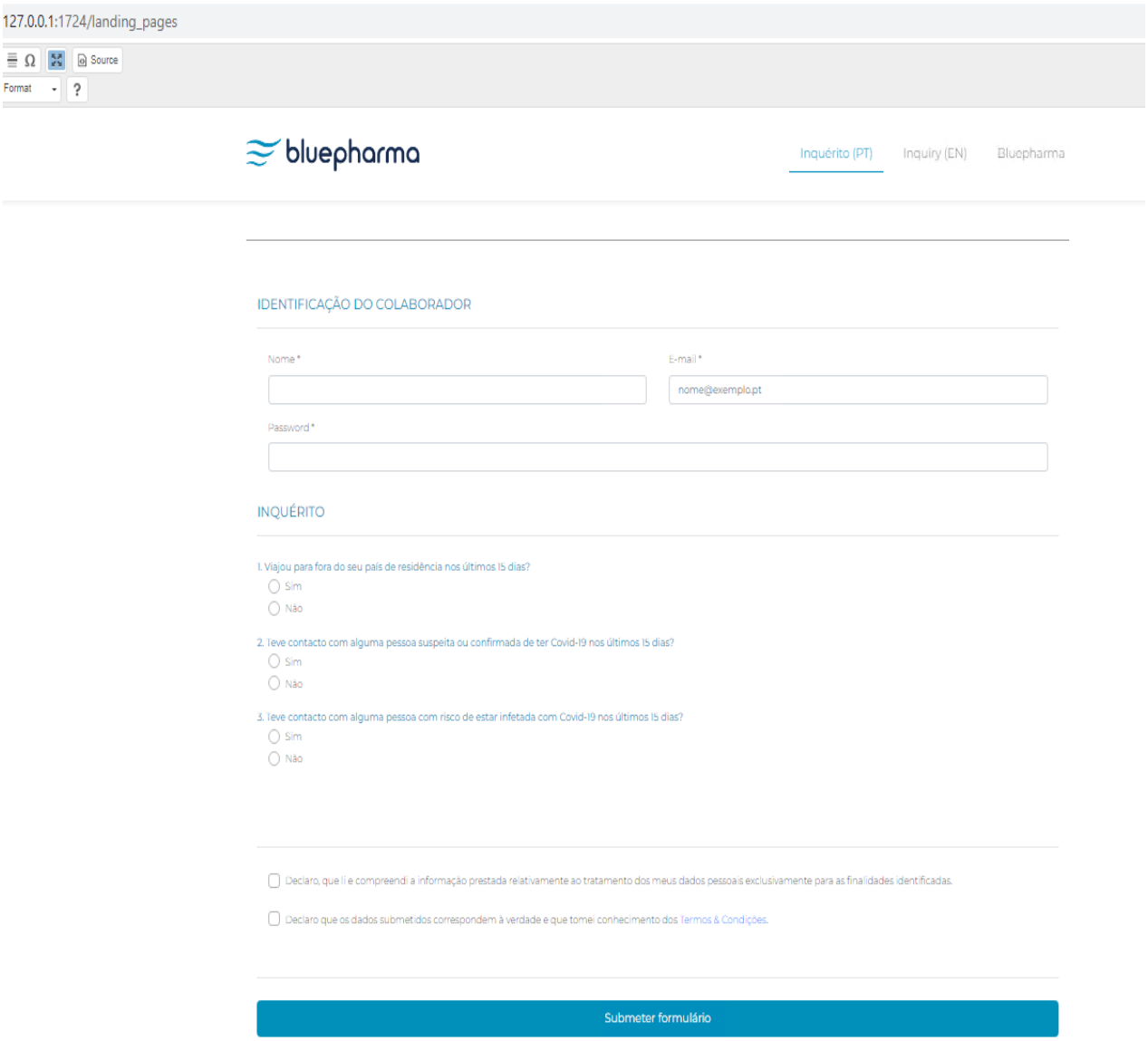

Figura 14 - Landing Page

Após a submissão das credenciais, os colaboradores foram redirecionados para o site original da Bluepharma, de forma a mascarar a tentativa de phishing a que tinham sido sujeitos.

Sending Profiles

Para enviarmos a campanha para os diferentes utilizadores, o Gophish requer a configuração de um servidor SMTP [40].
Na Figura 15 encontra-se demonstrada a configuração do referido servidor de SMTP.
De salientar que foi criado o endereço de email *ambiente.segurança@gmail.com* para ser o emissor da mensagem de correio eletrónico.

Finalmente, por forma a conseguirmos enviar o email, teve de ser desativada a opção de "*Less secure apps*" [41] da conta Gmail.

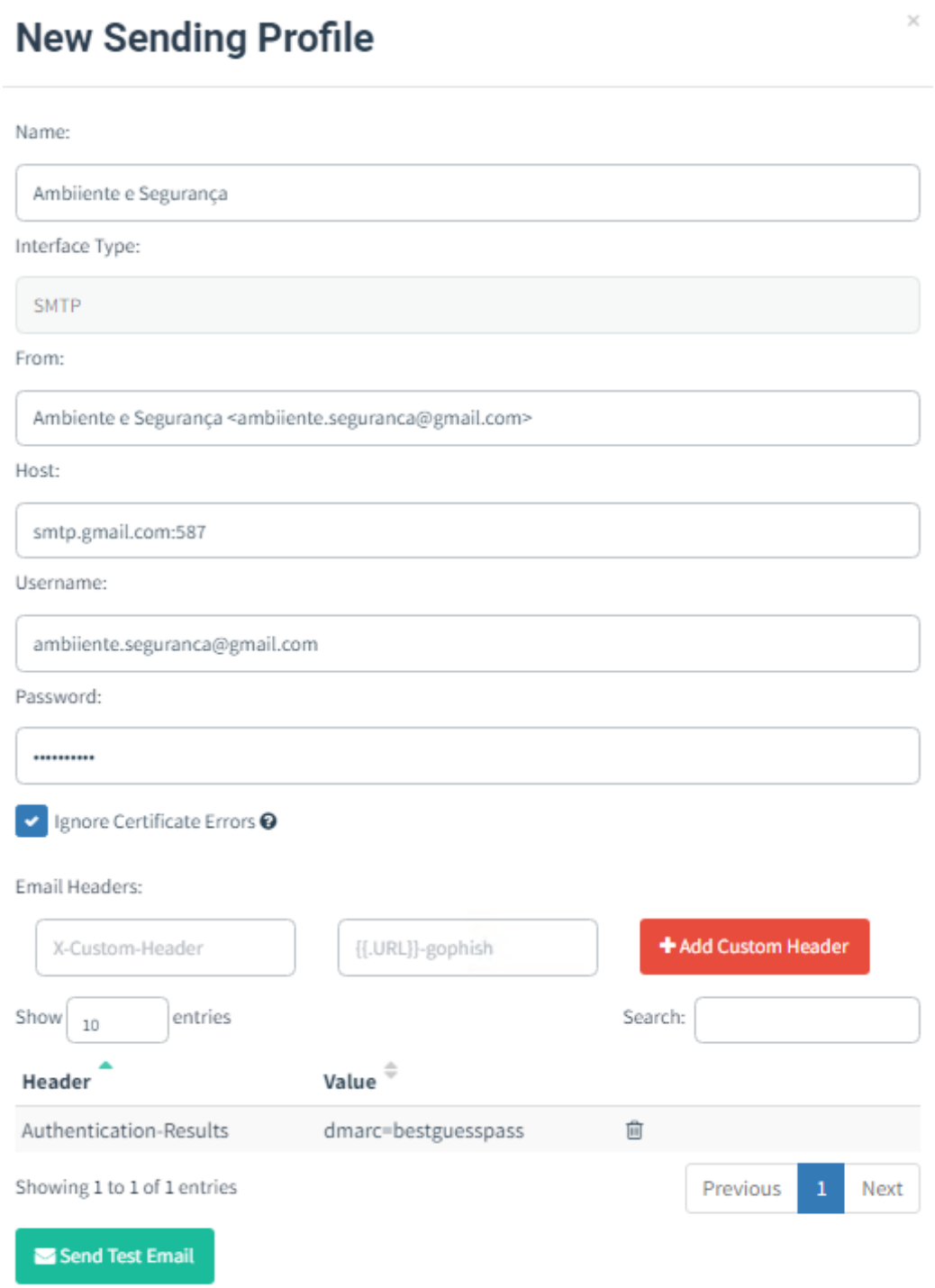

Figura 15 - Configuração Servidor Email

Utilizadores e Grupos

Para fazer o envio do email de phishing para os colaboradores da empresa foram criados quinze grupos, onde foram inseridos os diferentes colaboradores.
Os utilizadores foram carregados para a aplicação através de um ficheiro de texto, tendo este de estar configurado no formato (*First Name*, *Last Name*, *Email*, *Position*), conforme demonstrado na Figura 16.

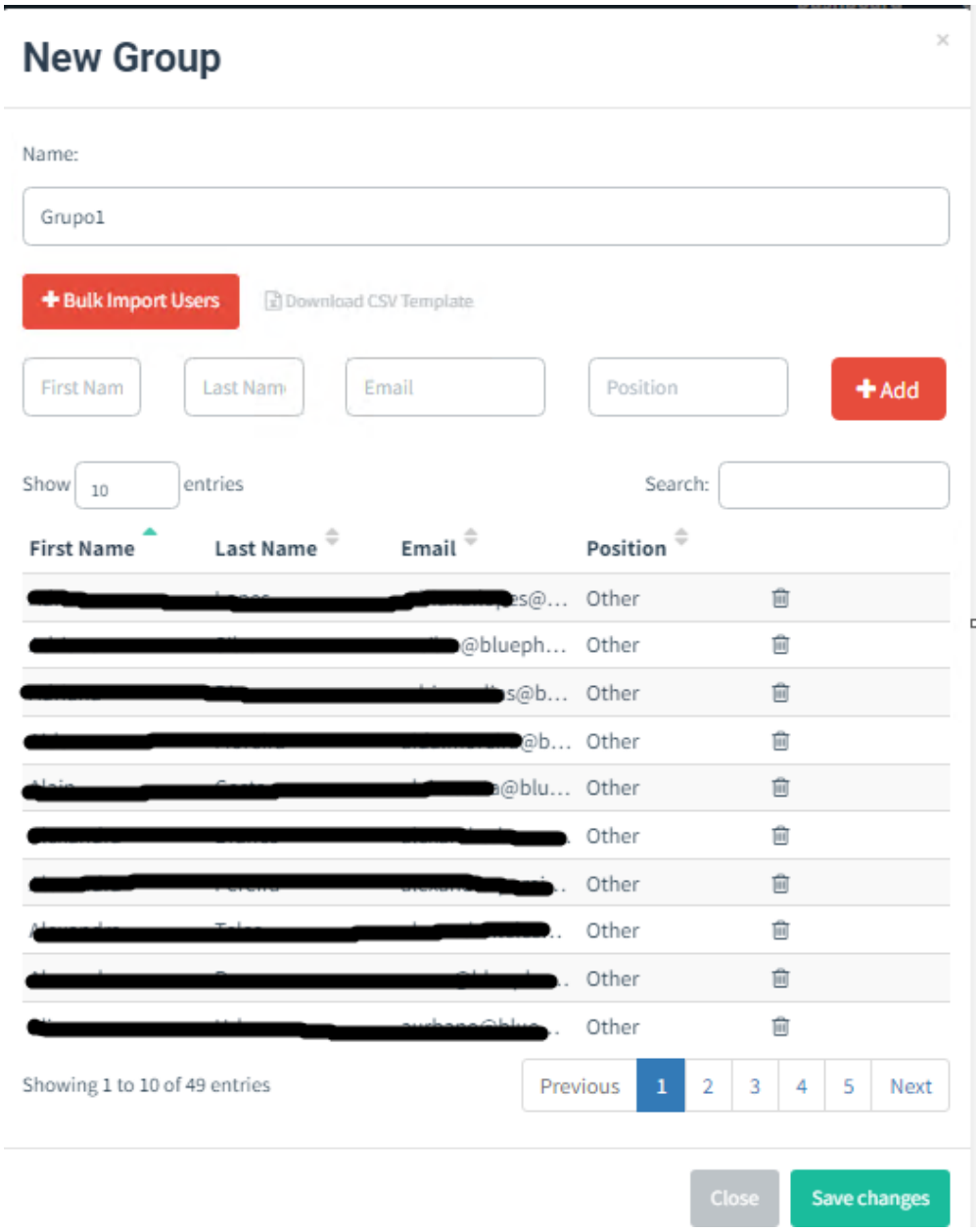

Figura 16 - Grupos de utilizadores

Campanha

Por forma a enviar o email para todos os colaboradores, foram criados quinze grupos, para fazer o envio faseado.
Na Figura 17 encontra-se demonstrada a configuração de uma campanha. Nas campanhas seguintes, apenas foi alterado o grupo para o qual era enviada a campanha.

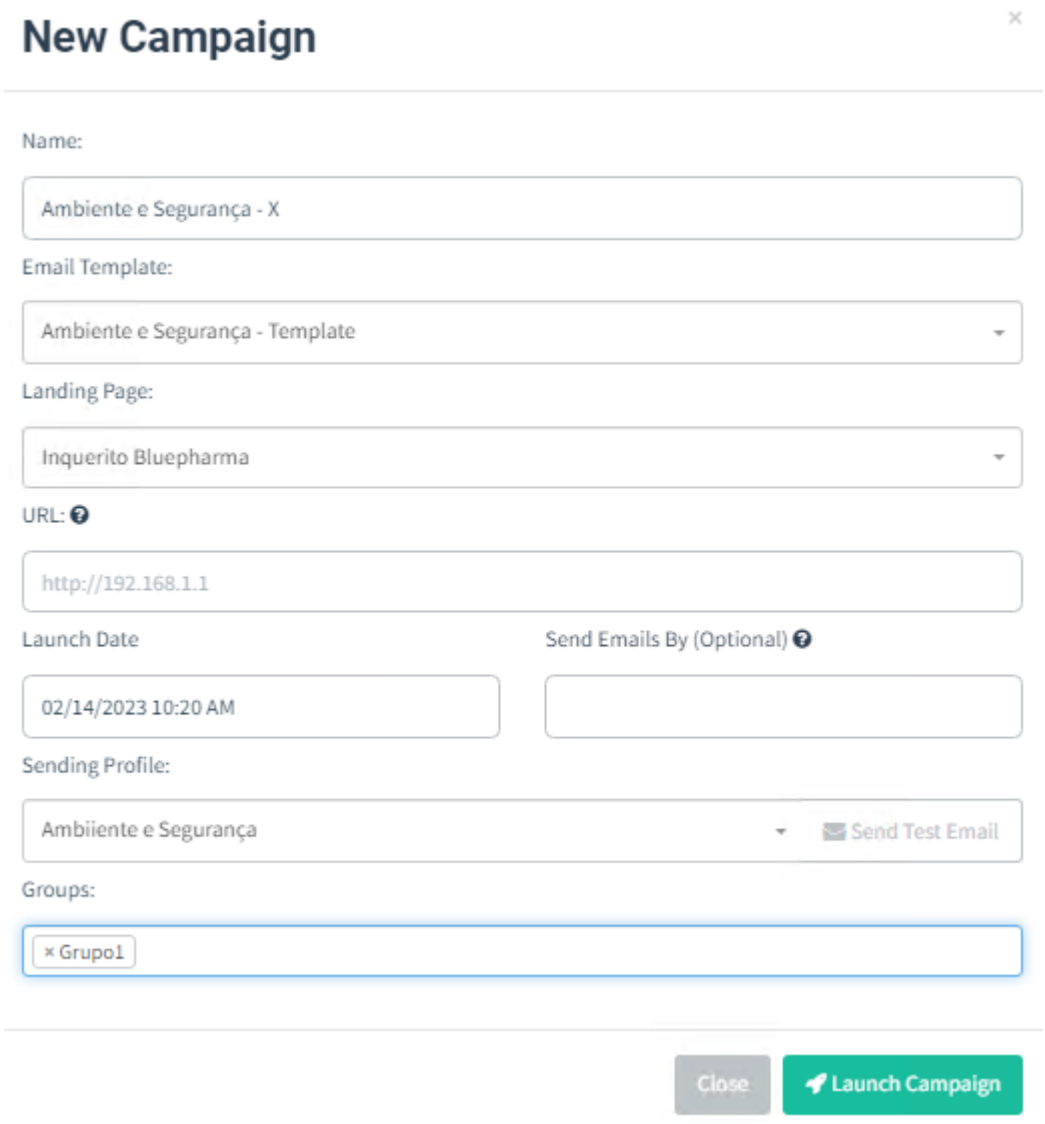

Figura 17 - Configuração da Campanha

Resultados da campanha

Após o envio das diversas campanhas de phishing, os resultados obtidos encontram-se detalhados na Figura 18.

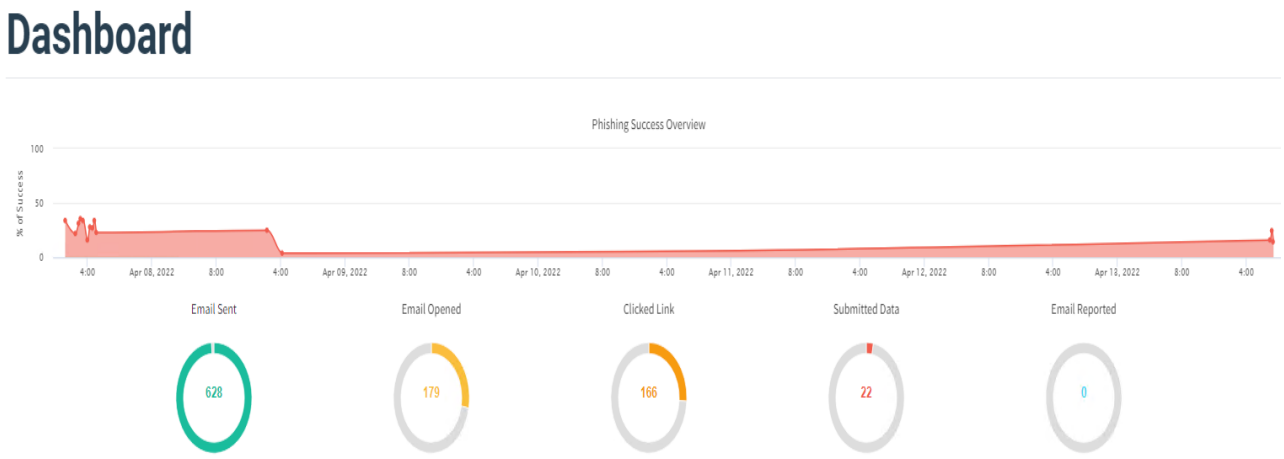

Figura 18 - Resultados da campanha

De um total de 628 emails enviados, 181 colaboradores abriram o email. Desses 181 colaboradores que abriram o email, 168 clicaram no link, que redirecionava para a página maliciosa. Adicionalmente, dos colaboradores que abriram o link contido no email, 22 submeteram credenciais. Através da análise dos resultados podemos verificar que existem colaboradores que não sabem distinguir um email legítimo de um email fraudulento. É, pois, fundamental educar os colaboradores para os cuidados a ter quando recebem estes tipos de emails.
De salientar que houve colaboradores "passivos" que submeteram credenciais, o que demonstra que estes estão menos consciencializados para a segurança da informação. Na Tabela 6 podemos observar esses mesmos resultados.

Tabela 6 - Comparação de submissão de credenciais dos diferentes tipos de colaboradores

Tipo de colaborador	Nº de credenciais submetidas
Ativo	9
Passivo	13

Na Figura 19 podemos visualizar os resultados obtidos para um grupo de utilizadores.

Figura 19 - Resultados campanha (grupo)

De forma a extrair os dados inseridos pelo utilizador, bastava aceder aos detalhes do referido utilizador e verficar o campo *Content Body Password* e *Content Body Email*, conforme demonstrado na Figura 20.

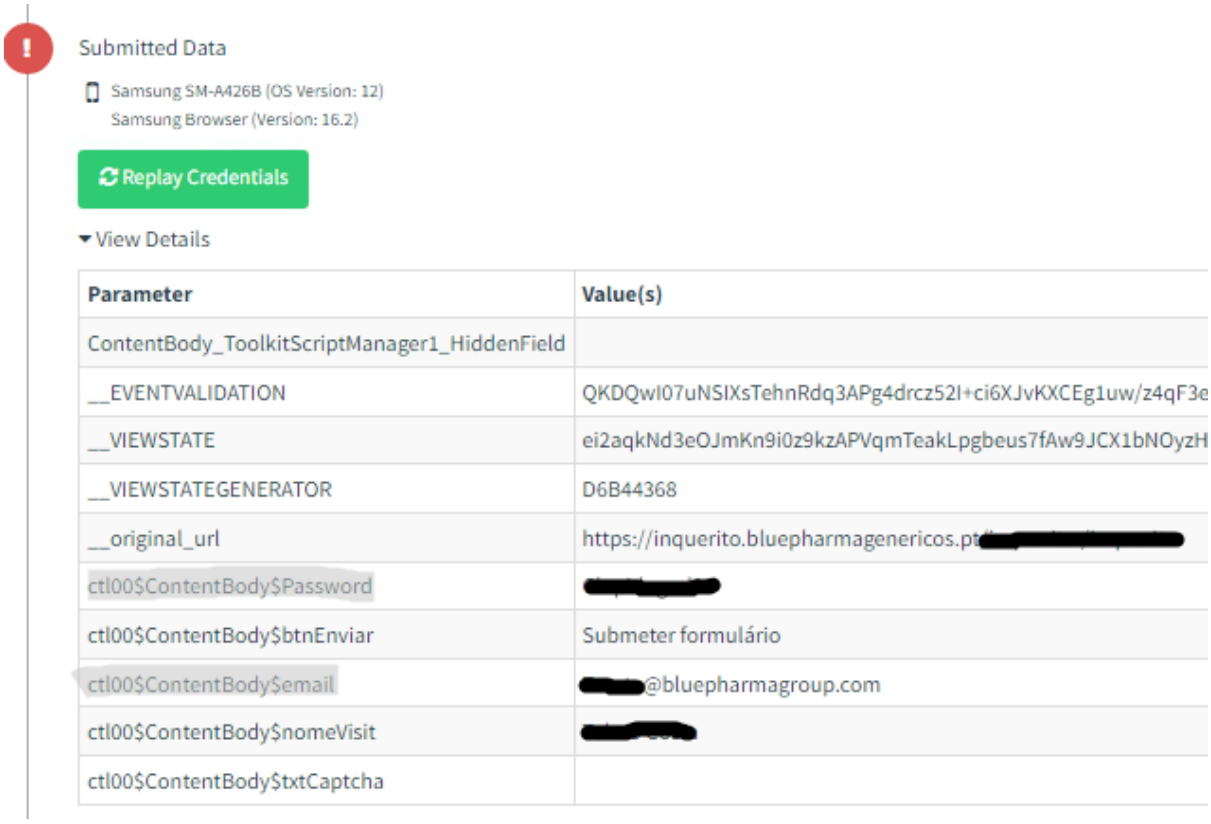

Figura 20 - Obtenção de credenciais

Na próxima secção iram ser descritas as medidas que foram tomadas, por forma a conscienciализar os colaboradores, para as necessidades de Cibersegurança.

4.11 Implementação de medidas preventivas

Após a realização da campanha de *phishing*, os resultados obtidos foram apresentados aos administradores da organização.
Nessa reunião, foram definidas medidas que iriam ser implementadas, com objetivo de consciencializar os colaboradores da organização para a temática da segurança da informação. Essas medidas passaram inicialmente pela realização de um workshop a todos os colaboradores da organização, começando por aqueles que inseriram credenciais na campanha de *phishing* efetuada, sendo depois ministrado aos restantes colaboradores nos meses seguintes.
No referido workshop foram abordados os seguintes tópicos:

- O que é o *phishing*?
- Tipos/formas de *phishing* (*vishing*, *smishing*, email).
- Mecanismos para detetar um possível email de *phishing* (neste caso foram mostrados diversos emails aos colaboradores, para que estes identificassem se o email era fraudulento ou fidedigno).
- Explicação aos colaboradores de como fazer uso do add-in *Report Message* [42], na aplicação Outlook.
- Indicação aos colaboradores de como procederem em caso de receção de email suspeito (abrir pedido na plataforma *ServiceDesk* e aguardar validação dos técnicos de informática sobre se o email é, ou não, fidedigno).

Segunda campanha de phishing

Por forma a avaliar se a consciencialização dos colaboradores para a Cibersegurança melhorou, após a implementação das medidas preventivas, foi lançada uma nova campanha de *phishing*, sem o conhecimento dos colaboradores.
Para o lançamento desta campanha foram estudados diferentes tópicos para o envio do email, tais como:

- Questionário de satisfação da cantina
- Autorização para estacionar no parque da empresa
- Mensagens por ler na quarentena
- Computador que não cumpre com políticas de segurança da empresa

Após o estudo destas possíveis alternativas, optei pelo tema do questionário da cantina, uma vez que este tópico abrange todos os colaboradores, já que todos a usam, para almoçar ou jantar. Relativamente ao tema do estacionamento no parque interno na empresa, os colaboradores já saberiam à partida que não haveria lugar para todas as pessoas, podendo levar a que alguns desconsiderassem o email. No que respeita às mensagens por ler na quarentena, alguns colaboradores poderiam considerar que o email seria spam, por terem de ir diretamente para a quarentena e não teriam interesse em abrir o link. Em relação ao tema do não cumprimento das políticas de segurança do computador, existem diversos colaboradores que utilizam computadores partilhados e que poderiam desconsiderar este tipo de email.

Após o envio do email, os colaboradores, tal como acontecia na campanha anterior, podiam reportar o email fraudulento através da plataforma *Servicedesk*.

Configuração de Gophish

Para a configuração da segunda campanha, foi configurado um email do departamento dos Recursos Humanos.

Template do email

Na Figura 21 podemos visualizar o *template* usado na segunda campanha realizada.

bluepharma

COMUNICAÇÃO INTERNA
Recursos Humanos

10/03/2023 **Questionário - Gertal** **04-23-RH**

Estimados colaboradores,

Informamos que se encontra disponível no link abaixo um questionário sobre a qualidade do serviço prestado pela Gertal.

Questionario

Agradecemos o preenchimento do inquérito de forma a melhorar a qualidade do serviço prestado.

Bom trabalho,

A Equipa de Recursos Humanos

Figura 21 - Template de email

Landing Page

No que respeita à página para a qual os utilizadores iriam ser redirecionados, aquando do clique no link presente no email enviado, foi configurada a página demonstrada na Figura 22.

Figura 22 - Página de autenticação

Esta página é apresentada aquando da autenticação no portal interno na organização, tendo sido por isso escolhida como forma de "isco", com o intuito de verificar se os colaboradores conseguiam distinguir o que era uma página falsa, tendo, para isso, de analisar o link da página web que lhes era apresentada.

Sending Profile

Para fazer o envio da campanha de *phishing* foi utilizado um servidor externo à organização, para não comprometer os servidores internos da empresa, visto que, ao enviar emails em massa, o servidor de email poderia ficar marcado como spam.
Neste caso, foi utilizado um servidor de email da Microsoft. Adicionalmente, foi criada a conta de email (rh@blue-pharma.pt) para servir de remetente da campanha de *phishing*. Foi igualmente necessário fazer *whitelisting* do domínio (blue-pharma.pt), para que este email não ficasse retido na quarentena. De igual modo foi desabilitado o *banner,* que aparece nos emails quando estes são recebidos de um domínio externo à Bluepharma. Na Figura 23 e na Figura 24 podem ser visualizadas as referidas configurações.

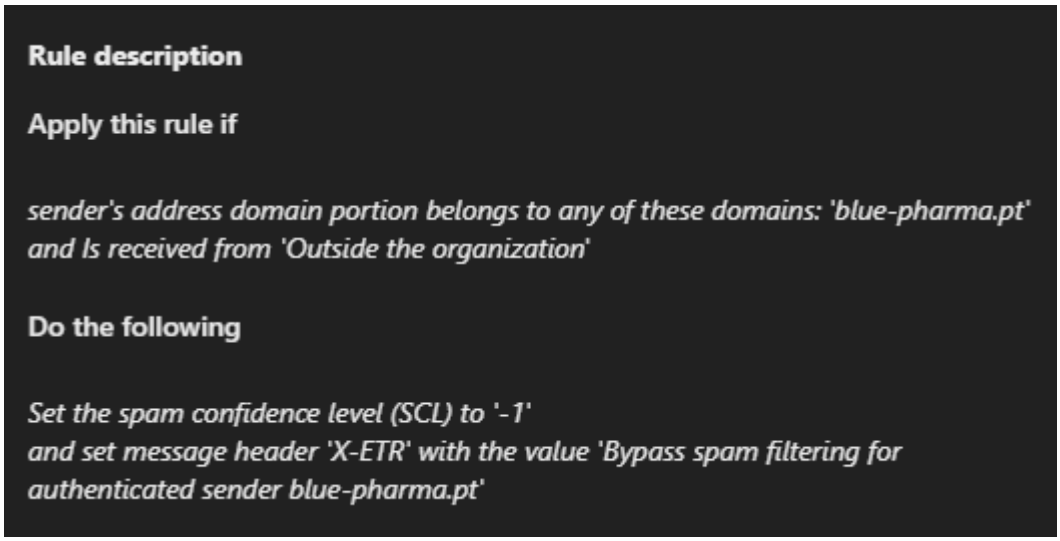

Figura 23 - Regra para bypass do filtro de spam

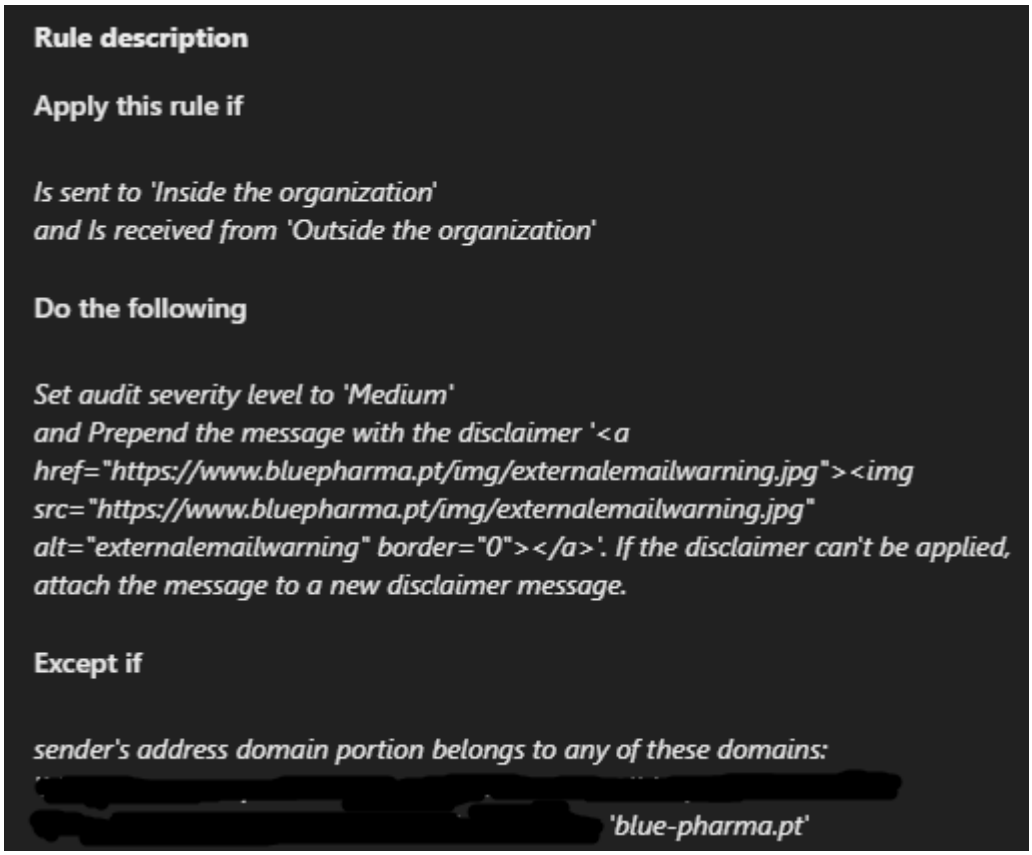

Figura 24 - Regra para remoção de Banner

Seguidamente foi configurado, no *Gophish*, o perfil do email, conforme ilustrado na Figura 25.

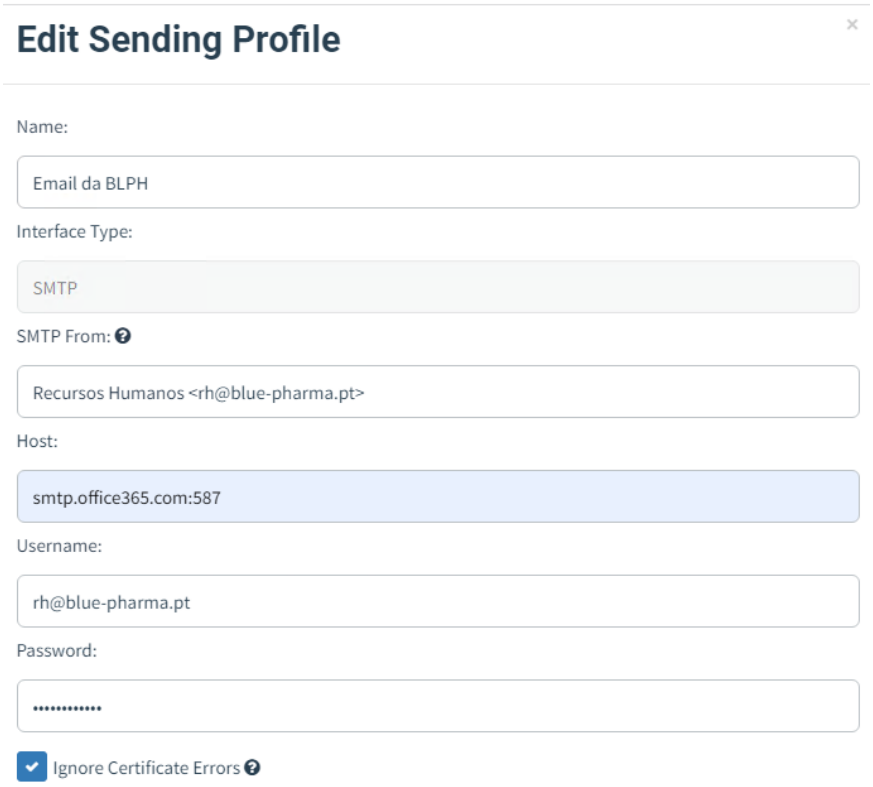

Figura 25 - Perfil de Email

Dificuldades durante a configuração da campanha

De forma a tornar esta campanha de phishing o mais real possível, estava pensado gerar um certificado SSL, para o site onde os utilizadores iriam ser redirecionados, por forma a não gerar o aviso de "site inseguro", aquando da abertura do link, visto que o browser não conseguia validar o certificado, o que poderia demover alguns utilizadores de introduzir as suas credenciais.
Para tal, foi gerado um certificado na plataforma *ZeroSSL*, conforme está demonstrado na Figura 26.

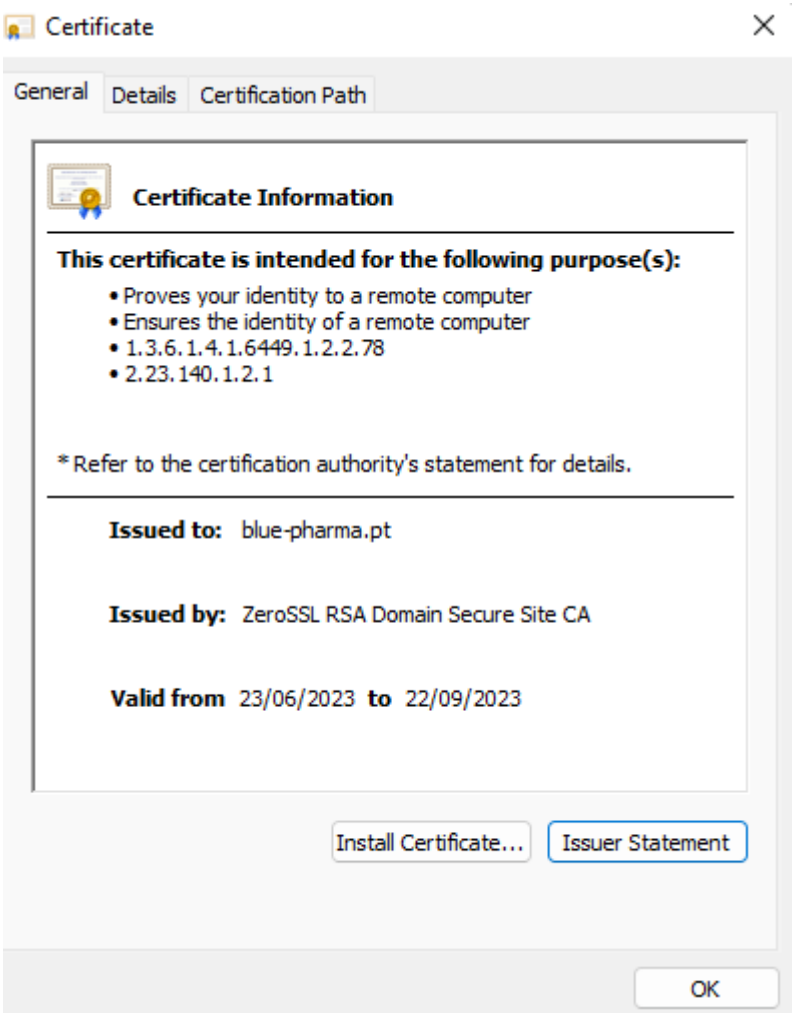

Figura 26 - Certificado Blue-pharma.pt

Seguidamente o certificado foi carregado na pasta do *Gophish* conforme descrito na Figura 27.

config.json - Notepad

File Edit Format View Help

```
{
        "admin_server": {
                "listen_url": "127.0.0.1:3333",
                "use_tls": true,
                "cert_path": "certificate.crt",
                "key_path": "certificate.key",
                "trusted_origins": []
        },
        "phish_server": {
                "listen_url": "0.0.0.0:443",
                "use_tls": true,
                "cert_path": "certificate.crt",
                "key_path": "certificate.key"
        },
        "db_name": "sqlite3",
        "db_path": "gophish.db",
        "migrations_prefix": "db/db_",
        "contact_address": "",
        "logging": {
                "filename": "",
                "level": ""
        }
}
```

Figura 27 - Configuração do Gophish

Após diversas tentativas de configurar o certificado na máquina do *Gophish*, não foi possível corrigir o problema do certificado, visto que não estava a ser resolvido o nome da máquina em questão, conforme ilustra a Figura 28, tendo, desta forma, sido enviada a campanha de *phishing* sem o certificado SSL instalado no site.

Outro ponto importante de referir, após a realização da segunda campanha de *phishing*, prende-se com o facto de que estes tipos de campanhas não devem ser realizadas em meses em que possa existir muitos colaboradores de férias, visto que o email pode ficar "esquecido" na *mailbox* dos utilizadores ou estes partilharem uns com os outros que houve uma tentativa de *phishing*, o que poderá reduzir o número dos dados introduzidos.

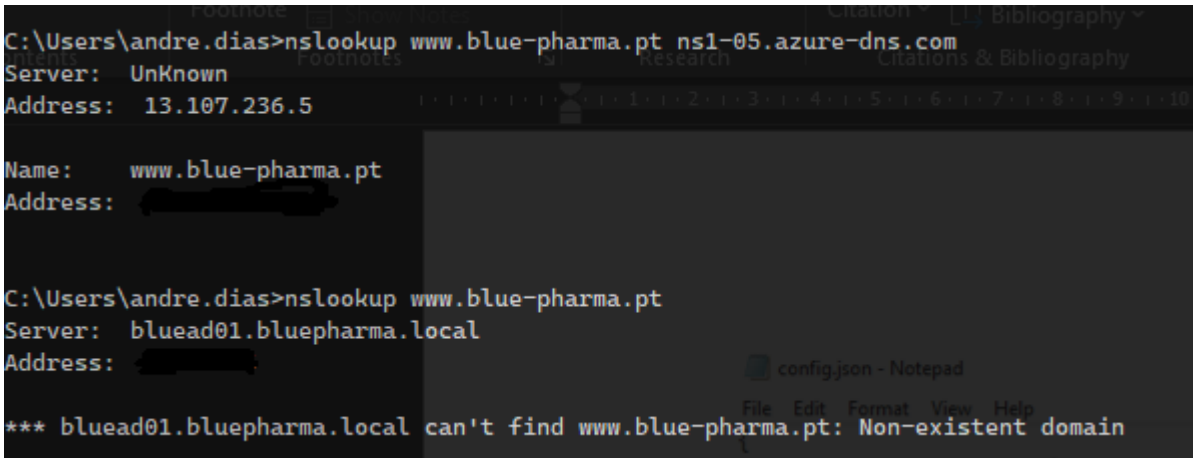

Figura 28 - Problema na resolução do DNS

Resultados da segunda campanha

Nesta campanha foram enviados 622 emails. Desses 622 emails, 9 colaboradores abriram o email, tendo 1 destes submetido credenciais.

Comparativamente com a primeira campanha de *phishing*, podemos observar que nesta segunda houve uma redução do número de colaboradores que foram vítimas desta ação, o que demonstra uma maior consciencialização para esta temática, após toda a formação realizada entre a primeira e segunda campanhas.

É importante salientar alguns aspetos que podem ser melhorados numa futura campanha, após a análise dos resultados obtidos nesta:

- A execução destas campanhas deve ser realizada fora de épocas festivas (Verão, Natal, Páscoa), visto que o menor número de pessoas que estão presentes na organização pode condicionar os resultados obtidos.
- Aquando do lançamento de uma campanha interna na organização, de forma a conseguirmos que o email se propague o melhor possível, podemos criar grupos por departamentos. Desta forma, conseguimos enviar o email de *phishing* em último lugar para os colaboradores do departamento visado. Assim conseguimos "esconder" o email de *phishing* o maior tempo possível, pois é provável que um colaborador desse departamento ao receber o email, o ache estranho, porque conhece melhor que os restantes colaboradores o que se passa no seu departamento e levante um alerta, o que comprometerá a campanha de *phishing* realizada em toda a organização.

Questionário sobre phishing

Foi igualmente criado um questionário, por forma a perceber o estado de consciencialização dos colaboradores da empresa.

No referido questionário são abordadas questões sobre o conhecimento dos colaboradores relativamente a esta temática, bem como se estes já foram alvo, ou mesmo vítimas, deste tipo de ataque informático.
Adicionalmente, neste questionário foram abordadas questões como o cargo dos colaboradores, visto que quanto mais alto é o cargo, maior é a probabilidade de terem acesso a informação confidencial.
De salientar que o referido questionário, antes de ser distribuído dentro da organização, foi partilhado com pessoas externas à empresa, por forma a obter feedback das mesmas, com objetivo de perceber se as perguntas estavam percetíveis e adequadas à temática do questionário.

Resultados

Após a partilha do questionário, de um total de 67 colaboradores, que participaram no seu preenchimento:

- 54% indicou que sabe identificar um email de *phishing*
- 80% refere que verifica o remetente dos emails
- 83% indicaram que foram alvos de *phishing*, sendo o e-mail, o meio preferencial para o envio do *phishing*.
- 97% referiram que nunca foram vítima de phishing

Após a obtenção destes dados, estes mesmos dados foram cruzados com os resultados da 2ª segunda campanha de *phishing*, de forma a conseguir perceber se os colaboradores que indicavam, no questionário, que tinham dificuldades na identificação de emails fraudulentos, eram os mesmos que submeteram credencias na campanha de *phishing*.
Fazendo esta análise comparativa, o colaborador que inseriu credenciais, indicou no questionário, que tinha algumas noções do que era o *phishing*, o que demonstra que não está totalmente consciencializado para esta temática.

Capítulo 5 Conclusões e trabalho futuro

O presente capítulo sintetiza as conclusões retiradas do trabalho realizado. Além disto, é apresentado o trabalho futuro, como forma de dar seguimento ao trabalho apresentado neste documento.

5.1 Conclusões

A temática da cibersegurança tem ganhado destaque a nível mundial. Isto deve-se ao facto de existirem cada vez mais ataques cibernéticos contra as organizações. A pesquisa por potenciais vulnerabilidades na infraestrutura de rede de uma organização, bem como a formação dos colaboradores para a segurança da informação, são pontos fulcrais, para qualquer empresa, caso estas queiram estar protegidas contra potenciais ciberataques.

O contributo do trabalho aqui documentado permitiu analisar a infraestrutura de rede da organização, detetando algumas vulnerabilidades, que posteriormente foram corrigidas. De igual forma, este trabalho permitiu também dar formação aos colaboradores da organização, para que estes estejam mais cientes das necessidades da segurança da informação.

Assim, o trabalho apresenta e documenta os resultados obtidos das vulnerabilidades descobertas na organização, bem como os resultados das campanhas de *phishing* realizadas, antes e após a formação dos colaboradores.

Em suma, o trabalho correu conforme o expectável, apesar de terem existido alguns constrangimentos no decorrer do mesmo, mas que, com empenho e dedicação, foram ultrapassados.

5.2 Trabalho Futuro

No seguimento do trabalho documentado, como trabalho futuro, serão realizadas ações de formação, através de *workshops* de segurança, com o intuito de manter alerta os colaboradores da organização das boas práticas da segurança da informação. Além disto, serão realizadas monitorizações periódicas das vulnerabilidades existentes, para reduzir ao máximo a superfície de ataque a que a empresa se encontra exposta. Adicionalmente, há o objetivo de alargar estas monitorizações aos Sistemas de Controlo Industriais, visto serem sistemas que cada vez mais são alvos dos *hackers* [43].

Capítulo 6 Referências

[1] M. K. Pratt, “security awareness training,” dezembro 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/security-awareness-training. [Acedido em janeiro 2023].

[2] “Quem somos,” 2022. [Online]. Available: https://www.bluepharma.pt/about-us.php.

[3] S. COOPER, “Nessus Vulnerability Scanner Review,” 10 outubro 2022. [Online]. Available: https://www.comparitech.com/net-admin/nessus-vulnerability-scanner-review/#:~:text=The\%20Nessus\%20\%system\%20was\%20developed,in20IT20during20the20day.

[4] “PCI FAQs,” 2023. [Online]. Available: https://www.pcicomplianceguide.org/faq/#1.

[5] “Federal Desktop Core Configuration (FDCC),” 18 agosto 2011. [Online]. Available: https://www.techopedia.com/definition/14204/federal-desktop-core-configuration-fdcc.

[6] N. Lord, “What is NIST Compliance?,” 24 agosto 2015. [Online]. Available: https://digitalguardian.com/blog/what-nist-compliance#:~:text=NIST20standards20are20based20on,programs20requiring20stringent20security20measures..

[7] tenable, “About Nessus Plugins,” 2023. [Online]. Available: https://docs.tenable.com/nessus/Content/AboutNessusPlugins.htm#:~:text=Plugins\%20contain\%20vulnerability\%20information\%2C\%20a,v2\%20and\%20v3\%20values\%20simultaneously..

[8] K. T. Hanna, “GNU General Public License (GNU GPL or GPL),” dezembro 2021. [Online]. Available: https://www.techtarget.com/searchdatacenter/definition/GNU-General-Public-License-GNU-GPL-or-simply-GPL.

[9] R. Deraison, “The Nessus Attack Scripting Language Reference Guide,” 13 setembro 1999. [Online]. Available: http://student.ing-steen.se/java/javacoding/toys/more_toys/nessus/txtfilez/nasl.html.

[10] beyondsecurity, “beSECURE FAQ,” beyondsecurity, [Online]. Available: https://www.beyondsecurity.com/besecure-faq.

[11] CompliancyGroup, “What is HIPAA Compliance?,” CompliancyGroup, [Online]. Available: https://compliancy-group.com/what-is-hipaa-compliance/.

[11] J. Coggins, “What is SOX Compliance and What Are the Requirements?,” 14 dezembro 2022. [Online]. Available: https://www.lepide.com/blog/what-is-sox-compliance-and-what-are-the-requirements/#:~:text=SOX%20compliance%20refers%20to%20annual,both%20financially%20and%20in%20IT..

[13] “Tripwire Integrity Management,” Fortra, [Online]. Available: https://www.tripwire.com/products/tripwire-ip360.

[14] AuditBoard, “The 12 PCI DSS Compliance Requirements: What You Need to Know,” 11 fevereiro 2022. [Online]. Available: https://www.auditboard.com/blog/pci-dss-requirements/.

[15] “What are FISMA Compliance Requirements?,” [Online]. Available: https://www.solarwinds.com/federal-government/solution/fisma-compliance-requirements.

[16] P. Brans, “daemon,” agosto 2022. [Online]. Available: https://www.techtarget.com/whatis/definition/daemon. [Acedido em 9 janeiro 2023].

[17] Greenbone, “Greenbone Enterprise Appliance,” [Online]. Available: https://docs.greenbone.net/GSM-Manual/gos-22.04/en/GSM-Manual-GOS-22.04-en.pdf. [Acedido em Dezembro 2022].

[18] “Nmap: Discover your network,” [Online]. Available: https://nmap.org/.

[19] FIRST, “Common Vulnerability Scoring System SIG,” 2022. [Online]. Available: https://www.first.org/cvss/.

[20] I. Anti-Phishing Working Group, “PHISHING ACTIVITY TRENDS REPORT,” 2022. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf. [Acedido em 20 Março 2023].

[21] "What is Information Security?," 22 junho 2022. [Online]. Available: https://www.geeksforgeeks.org/what-is-information-security/. [Acedido em 16 janeiro 2023].

[22] M. W. a. J. Hash, "Building an Information Technology Security Awareness and Training Program," Outubro 2003. [Online]. Available: https://profsite.um.ac.ir/kashmiri/nist/new/NIST-SP800-50.pdf. [Acedido em 14 janeiro 2023].

[23] Webroot, "What is Social Engineering?," 2023. [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering. [Acedido em 7 fevereiro 2022].

[24] M. Z. X. L. A. R. J. Z. J. &. K. K. Abdul Basit, "A comprehensive survey of AI-enabled phishing attacks detection techniques," 23 outubro 2020. [Online]. Available: https://link.springer.com/article/10.1007/s11235-020-00733-2.

[25] I. STAFF, "Top Five VUlnerabilities Attackers Use Against Browsers," 12 Janeiro 2022. [Online]. Available: https://www.itbusinessedge.com/security/top-five-vulnerabilities-attackers-use-against-browsers/#plugin-exploits. [Acedido em 12 Fevereiro 2023].

[26] kaspersky, "What is Typosquatting? – Definition and Explanation," kaspersky, 2023. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting. [Acedido em 5 Março 2023].

[27] I. Infosec Institute, "Prepare every employee with phishing simulations & training," 2023. [Online]. Available: https://www.infosecinstitute.com/iq/phishing-simulations/. [Acedido em dezembro 2022].

[28] Lucy, "Train Employees," 2022. [Online]. Available: https://lucysecurity.com/cyber-security-awareness-training/. [Acedido em 24 dezembro 2022].

[29] KnowBe4, "KnowBe4 Security Awareness Training," 2023. [Online]. Available: https://www.knowbe4.com/pricing-kevin-mitnick-security-awareness-training. [Acedido em 6 fevereiro 2023].

[30] GOLDPHISH, "CYBER SAVVY MADE SIMPLE," GOLDPHISH, 2023. [Online]. Available: https://www.goldphish.com/. [Acedido em 13 fevereiro 2023].

[31] Gophish, “Open-Source Phishing Framework,” 2022. [Online]. Available: https://getgophish.com/. [Acedido em 25 setembro 2022].

[32] A. U. R. S. J. T. M. A. J. A. S. M. A. Ayesha Arshad, “A Systematic Literature Review on Phishing and Anti-Phishing Techniques,” 2 abril 2021. [Online]. Available: https://arxiv.org/abs/2104.01255.

[33] “What is Greylisting and Anti-Greylisting Technology?,” clearout, 2023. [Online]. Available: https://clearout.io/blog/2020/12/16/what-is-greylisting-and-anti-greylisting-technology/. [Acedido em 2 Março 2023].

[34] Microsoft, “Exchange Online Protection overview,” 24 fevereiro 2023. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide. [Acedido em 28 feverireo 2023].

[35] Google, “TensorFlow is an end-to-end open source platform for machine learning,” [Online]. Available: https://www.tensorflow.org/overview. [Acedido em 2 Março 2023].

[36] “Convolution,” Fevereiro 2023. [Online]. Available: https://en.wikipedia.org/wiki/Convolution. [Acedido em 2 Março 2023].

[37] Keras, “About Keras,” [Online]. Available: https://keras.io/about/. [Acedido em 2 Março 2023].

[38] Apple, “Report and reduce spam in iCloud Mail,” 6 janeiro 2023. [Online]. Available: https://support.apple.com/en-gb/HT202315. [Acedido em 4 Março 2023].

[39] Barracuda, “Stop Advanced Threats that Evade Traditional Detection Techniques,” Barracuda, 2022. [Online]. Available: https://www.barracuda.com/solutions/advanced-threat-protection. [Acedido em 8 Março 2023].

[40] Cloudflare, “What is the Simple Mail Transfer Protocol (SMTP)?,” Cloudflare, 2023. [Online]. Available: https://www.cloudflare.com/learning/email-security/what-is-smtp/. [Acedido em 13 fevereiro 2023].

[41] Google, “Less secure apps & your Google Account,” 2023. [Online]. Available: https://support.google.com/accounts/answer/6010255?hl=en. [Acedido em 13 fevereiro 2023].

[42] Microsoft, “Use the Report Message add-in,” Microsoft, [Online]. Available: https://support.microsoft.com/en-us/office/use-the-report-message-add-in-b5caa9f1-cdf3-4443-af8c-ff724ea719d2. [Acedido em 7 Março 2023].

[43] Dragos, “ICS/OT CYBERSECURITY,” 2022. [Online]. [Acedido em 26 março 2023].

Apêndices