Instituto Superior de Gestão e Administração de Santarém

Mestrado em Engenharia de Tecnologias e Sistemas Web

Dissertação

A cibersegurança aplicada no âmbito das PME's

Tomás Evaristo, a22100608

Santarém

Ano 2022/2023

Instituto Superior de Gestão e Administração de Santarém

Mestrado em Engenharia de Tecnologias e Sistemas Web

Dissertação

A cibersegurança aplicada no âmbito das PME's

Tomás Evaristo, a22100608

Dissertação submetida para satisfação parcial dos requisitos do grau de Mestre em Engenharia de Tecnologias e Sistemas Web sob a orientação do Professor Doutor Domingos Martinho

Santarém

Ano 2022/2023

Resumo

Introdução: A cibersegurança tem vindo a crescer nos últimos anos e é mais importante que nunca, tendo em conta a recente mudança de paradigma social e laboral em que o uso das redes sociais e da internet cresceu massivamente, tal como a abordagem ao teletrabalho pelas empresas cresceu significativamente. Esta dissertação tem como objetivo principal estudar um modelo de cibersegurança para atender às necessidades das Pequenas e Médias Empresas (PME's), complementado de ações e ferramentas que possam servir de "guia" de preparação a utilizar pelas empresas.
Método: Foi adaptado o modelo de cibersegurança proposto pelo NIST (National Institute os Standarts and Technology), que consiste em cinco fases: Identificar; Proteger; Detetar; Responder; Recuperar.
Implementação: Foi realizada uma implementação para cada uma das fases propostas pelo modelo, começando por um questionário utilizado como um dos instrumentos da fase identificar visando detetar as vulnerabilidades existentes na empresa, seguindo-se a utilização de ferramentas e técnicas apropriadas a cada uma das restantes fases, nomeadamente o Nmap, Nessus, Autopsy, VirusTotal, entre outras.
Discussão: Os resultados obtidos mostram que as ferramentas utilizadas melhoram, significamente, a proteção das empresas no âmbito da cibersegurança. Constatou-se ainda que as conclusões do presente estudo vão de encontro às conclusões de outros estudos sobre as mesmas temáticas.
Conclusão: Os resultados obtidos na implementação mostram que os métodos utilizados têm bastante impacto no que toca à cibersegurança e que é uma mais-valia quando aplicado nas empresas. Conclui-se também que existe um crescente interesse pela área da cibersegurança, apesar de se verificar que as PME's ainda demonstram um nível de maturidade e preparação abaixo do que seria considerado ideal para enfrentar as ameaças informáticas atuais. Espera-se que a metodologia proposta neste trabalho, se seguidas com rigor, possa contribuir para melhorar significativamente a postura das PME's em relação à cibersegurança, minimizando os riscos e aumentando a sua resiliência em relação a este tipo de ameaças.

Palavras-chave: Cibersegurança, Cibercrime, Hacking, Hackers, Malware, Ciberataques, PME's.

Abstract

Introduction: Cybersecurity has been growing in recent years and is more important than ever, considering the recent change in social and work paradigm in which the use of social networks and the internet has grown massively, as has the approach to teleworking by companies grew significantly. This dissertation's main objective is to study a cybersecurity model to meet the needs of Small and Medium-sized Enterprises (SMEs), complemented by actions and tools that can serve as a preparation "guide" to be used by companies.
Method: The cybersecurity model proposed by NIST (National Institute of Standards and Technology) was adapted, which consists of five phases: Identify; Protect; Detect; To respond; To recover.
Implementation: An implementation was carried out for each of the phases proposed by the model, starting with a questionnaire used as one of the instruments in the identify phase to detect existing vulnerabilities in the company, followed using appropriate tools and techniques for each of the remaining phases. phases, namely Nmap, Nessus, Autopsy, VirusTotal, among others.
Discussion: The results obtained show that the tools used significantly improve the protection of companies in the field of cybersecurity. It was also found that the conclusions of this study are in line with the conclusions of other studies on the same themes.
Conclusion: The results obtained in the implementation show that the method used has a significant impact in terms of cybersecurity and that it is an added value when applied in companies. It is also concluded that there is a growing interest in cybersecurity, even though SMEs still demonstrate a level of maturity and preparation below what would be considered ideal to face current IT threats. It is expected that the methodology proposed in this work, if followed rigorously, can contribute to

significantly improving the posture of SMEs in relation to cybersecurity, minimizing risks and increasing their resilience in relation to this type of threats.

Keywords: Cybersecurity, Cybercrime, Hacking, Hackers, Malware, Cyberattacks, SME's

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1 INTRODUÇÃO

Atualmente, continuamos com as mesmas barreiras que antigamente protegiam impérios, mas agora são virtualizadas e protegem empresas e os seus dados. Hackers denominados de black hats, tentam aceder a dados de terceiros, que por sua vez, estão protegidos por barreiras não físicas, as firewalls (Gaspar, 2018).

Seguindo a mesma linha de raciocínio, o conceito de ciberespaço também tem cada vez mais um papel determinante na forma como lidamos com os conflitos internacionais, por exemplo, a ciberguerra (Arquilla, J., & Ronfeldt, D., 1993).

As ações das empresas em relação à sua proteção em ambientes digitais, poder ser condicionada, positiva ou negativamente, por diversos fatores internos e externos: o conhecimento e a sensibilidade para o tema, os recursos financeiros, os meios técnicos e humanos disponíveis, entre outros (Matos, 2018).

De forma a evitar, e se não for possível evitar minimizar, estes constantes ataques devem-se em primeiro lugar compreender o inimigo, identificá-lo e analisar a forma como ele ataca. Em segundo lugar diminuir as vulnerabilidades existentes, melhorando constantemente as barreiras defensivas e em último e, em terceiro lugar, estar sempre pronto a tomar a iniciativa através de ações contraofensivas (Tzu, 2022).

1.1 Motivação

É importante destacar que os ciberataques se têm tornado cada vez mais frequentes e sofisticados ao longo dos últimos anos. O aumento significativo do número de ocorrências tem tornado o cibercrime uma realidade presente em diversos setores de atividade, desde universidades até entidades governamentais e empresas de diferentes áreas de atuação. Essa ameaça não pode mais ser vista como uma exceção, mas sim como um risco constante para as organizações no mundo inteiro.

Além disso, é importante destacar que os ciberataques podem causar graves prejuízos para as organizações, como a perda de dados sensíveis, interrupção de serviços e danos à sua reputação. Por isso, é fundamental que as empresas invistam em medidas de cibersegurança para mitigar esses riscos. Essas medidas podem incluir a implementação de firewalls, a realização de testes de vulnerabilidade e a adoção de políticas de segurança da informação.

Dois exemplos recentes de grandes ciberataques que chamaram a atenção de todo o mundo são o WannaCry e o NotPetya. Esses ataques são caracterizados pela escala e complexidade, e têm causado prejuízos significativos para as empresas afetadas. Portanto, é essencial que as organizações estejam preparadas para enfrentar esse tipo de ameaça, adotando medidas preventivas e de resposta em caso de incidentes de segurança (Morgan, 2017).

Tendo em conta a complexidade das situações que os ciberataques se podem revestir e os danos que os mesmos podem causar às organizações este trabalho tem por base motivações de ordem pessoal e profissional. Assim, pretendo estudar estes problemas de modo a dar um contributo para a segurança das organizações em geral e das empresas portuguesas em particular, posicionando-me como um elemento ativo no combate ao cibercrime.

1.2 Problema e questões de investigação

No mundo da cibersegurança, somos constantemente confrontados com novos produtos, novas ferramentas e novas técnicas de ataque. Somos levados diariamente em várias direções sobre o que proteger e como protegê-lo (Tanner, 2019).

Parece consensual que a cibersegurança não deve ser vista de forma individualizada, mas sim como um conjunto de sinergias entre os três fatores estruturais da organização: pessoas, processos e tecnologia (Raposo, 2016). Nesse sentido, a tecnologia só consegue proteger eficazmente uma organização se as pessoas tiverem conhecimento e competências tecnológicas e de cibersegurança. Logo, uma organização pode ter bons recursos tecnológicos para se defender de ciberataques, mas se uma das pessoas da organização não seguir as diretrizes e os processos estabelecidos pode comprometer toda a organização (ENISA, 2018).

Considerando a realidade das empresas portuguesas em que os três fatores referidos anteriormente nem sempre se encontram alinhados, surge a questão de partida que orienta esta investigação “Contribuir para a melhoria da resposta das PME’s aos desafios da cibersegurança.”

1.3 Objetivos, geral e específicos

Cada vez mais nos tempos que correm a segurança informática é um tema bastante abordado nas empresas. Atualmente as PME's a nível global têm dificuldade em estar aptas para se protegerem de ataques informáticos.

O objetivo geral deste trabalho consiste em fazer com que as PME's fiquem mais sensibilizadas com o âmbito da cibersegurança e dispondo de uma solução integrada para responder às questões que se lhes colocam.

O objetivo específico consiste em definir um modelo de abordagem às PME's, no âmbito à cibersegurança, organizado em diferentes fases, apresentando questões e respostas concretas para cada uma dessas fases, complementando o estudo com a identificação de ações e ferramentas concretas que se possam constituir como um "guia" de preparação a utilizar pelas empresas no âmbito da cibersegurança.

2 REVISÃO DA LITERATURA

2.1 PME'S

Não existe uma definição única de PME (Pequenas Médias Empresas). A Comissão Europeia desenvolveu critérios para classificar uma PME com base no número de empregados, no volume de negócios e nas estatísticas do balanço. De acordo com a Comissão Europeia, a categoria de micro, pequenas e médias empresas são constituídas por empresas que empregam menos de 250 pessoas, que têm um volume de negócios anual não superior a 50 milhões de euros e/ou um balanço anual total não superior a 43 milhões de euros. As PME podem ser classificadas entre si como médias, pequenas ou micro PME's com base no número de empregados, volume de negócios e balanço (Suchan, W. & Sobiesk, E, 2006) (Tabela 1).

Tabela 1 - Categorias das PME's com base nos trabalhadores, volume de negócios anual e balanço total anual

CATEGORIA DA EMPRESA	TRABALHADORES	VOLUME DE NEGÓCIOS ANUAL	BALANÇO TOTAL ANUAL
MÉDIA	< 250	≤ 50 MILHÕES DE EUROS	≤ 43 MILHÕES DE EUROS
PEQUENA	< 50	≤ 10 MILHÕES DE EUROS	≤ 10 MILHÕES DE EUROS
MICRO	< 10	≤ 2 MILHÕES DE EUROS	≤ 2 MILHÕES DE EUROS

Embora as PME's sejam comparáveis em tamanho, elas são muito diversificadas nas suas operações comerciais. A título de exemplo, apresentamos alguns cenários que permitem identificar diferentes categorias de PME's:

- Cenário 1. Uma pequena PME doméstica que vende bolos caseiros, onde o número de funcionários pode ser um ou dois e podem alcançar os clientes através de um site. Neste tipo de PME espera-se baixo capital e baixo orçamento de IT.

- Cenário 2. Uma oficina automóvel com 20 funcionários onde todos as transações/pagamentos aos clientes são administradas através de um site apesar de não haver nenhum funcionário com formação em IT pois é contratada uma empresa externa para essas funções.
- Cenário 3. Uma PME com 70 funcionários que vende software para outras empresas. Têm um próprio departamento de IT com um grande orçamento e funcionários para questões de segurança de IT.

Os cenários apresentados facilmente demonstram que no âmbito das PME´s existem especificidades que indiciam necessidades diferentes a todos os níveis e também ao nível da forma de encarar a cibersegurança.

2.2 PME's e a cibersegurança

É importante perceber o que é a cibersegurança. Assim, ao dividir a palavra em duas podemos obter: "ciber", associado ao conceito de ciberespaço, e segurança (Craigen, D., Diakun-Thibault, & Purse, 2014).

O conceito de ciberespaço pode ser explicado como sendo uma "rede global de infraestruturas de tecnologias de informação interligadas entre si", no entanto, de forma mais generalizada, o termo ciberespaço faz referência a algo que está ligado à internet direta ou indiretamente (Fernandes, 2012). O ciberespaço apresenta características como anonimato, a estabilidade e a inexistência de fronteiras, assim, estas fazem com que seja um espaço mais propício ao crime, quando comparado com ambientes tradicionais, o que faz com que a criminalidade online tenha aumento nos últimos anos (Santos, 2018).

Por outro lado, "segurança" é um termo muito abrangente e pode ser aplicado a diversas áreas. De forma generalizada, segurança é um conceito que refere a ausência de perigo ou ameaças (Craigen, D., Diakun-Thibault, & Purse, 2014).

Aprofundando um pouco mais o conceito, conclui-se que a cibersegurança consiste em "um conjunto de ferramentas, políticas, diretrizes, abordagens de gestão de risco, formação, boas práticas e tecnologias que podem ser utilizadas para proteger o ciberespaço" (ITU, 2008).

Com a tendência para a digitalização em todas as áreas da sociedade, temos de olhar para os aspetos positivos, mas, e principalmente, aos aspetos negativos que esta pode introduzir

na sociedade, em especial, nas empresas. Este foco é uma oportunidade para identificar fragilidades e encontrar as melhores soluções para uma tomada de decisão informada.

Nos últimos 15 anos, as organizações têm gastado biliões de euros para construir fortes defesas para proteger os seus dados de hackers (Steele, S., & Wargo, C., 2007). As consequências de uma violação de segurança têm implicações negativas para a privacidade dos clientes, perda de lucros dos investidores e distorção da competitividade na indústria (Hiller, J. S., & Russel, R. S., 2013). Um único incidente de violação de bases de dados pode levar a milhões de dólares em custos de recuperação e afetar a confiança das partes interessadas e dos clientes (Steele, S., & Wargo, C., 2007).

Com o aumento exponencial da atividade humana assente na utilização de plataformas digitais, e essencialmente online, o fenómeno do cibercrime tem, nos últimos anos, tomado proporções astronómicas. Transformando-se mesmo, em Portugal, na única tipologia de crime com crescimento de incidência desde 2019 (Sistema de Segurança Interna, 2020).

As PME's representam 99% das empresas na Europa, logo, se a essa evidencia, acrescentarmos o facto de que em cada ano que passa, não só aumenta o volume de ameaças, como também o cenário de ameaças se torna mais diversificado, partindo do pressuposto de que as PME são mais vulneráveis, podemos concluir que as PME´s dificilmente estarão cientes de como se podem proteger dos riscos a que estão expostas. Constata-se assim que as PME´s se tornaram um alvo preferencial de atacantes por disporem de menos recursos para se defenderem quando comparadas com as empresas grandes (Symantec, 2016).

Com o aumento exponencial da atividade humana assente na utilização de plataformas digitais, e essencialmente online, o fenómeno do cibercrime tem, nos últimos anos, tomado proporções astronómicas. Transformando-se mesmo, em Portugal, na única tipologia de crime com crescimento de incidência desde 2019 (Sistema de Segurança Interna, 2020). As ameaças às PME's estão a aumentar, logo aumentam as vulnerabilidades dos meios de IT.

As tendências mais comuns são a colaboração social, aumento do uso de dispositivos móveis, a transferência dos dados para a nuvem, a digitalização de documentos confidenciais e a migração para tecnologias *Smart Grids*[1] (US State of Cybercrime Survey, 2013).

Estes pressupostos aparentam contrariar a ideia de que são as grandes empresas que são alvo de ataques informáticos, visto que, as mesmas dispõem de mais recursos financeiros e sofrerão maiores prejuízos na eventualidade de um ataque. No entanto, ao longo dos anos, tem-se verificado uma tendência nos aumentos dos ataques a empresas de menor dimensão. Com base em Toesland (2016), para esse aumento podem concorrer razões como:

- Uma menor preparação para fazer face a ataques dada a diferença na prioridade atribuída à segurança digital em relação à prioridade que habitualmente se encontra nas grandes empresas;
- A maior capacidade que as pequenas empresas vão tendo para armazenar dados e estes poderem representar grande valor económico;
- E também as ligações e relações que se estabelecem entre empresas e mercados, podendo fazer das pequenas empresas portas de entrada para perpetrar ataques em grandes empresas.

2.3 Comportamentos Humanos

Na cibersegurança é fundamental ter em conta os comportamentos humanos, sabendo-se que existem quatro tipos principais de incidentes devido aos comportamentos das pessoas nas empresas (Baptista, 2017).

Em primeiro lugar, a divulgação acidental de informação sensível é um dos principais incidentes. Acontece quando os colaboradores publicam ou partilham informações confidenciais sem intenção de cometer esse erro. Os comportamentos que podem levar a este tipo de incidente são o facto de os colaboradores não eliminarem informações dos seus dispositivos, mesmo quando estes não são necessários no futuro ou o acesso a redes sociais para fins pessoais no trabalho (CERT, 2013).

[1] As *Smart Grids* são plataformas tecnológicas capazes de monitorar e otimizar de forma autónoma e automática os fluxos do fornecimento de energia nas redes elétricas

Em segundo lugar, a perda ou o roubo de dispositivos como computadores, telemóveis, tablets e componentes de armazenamento podem colocar em causa a segurança das organizações.

Uma terceira fonte de problemas pode ocorrer devido ao facto de os dispositivos serem deixamos não protegidos e inseguros, sem supervisão na ausência do proprietário e em alguns casos desbloqueados (Ponemon Institute, 2012).

Por fim, o código malicioso como por exemplo vírus e spyware, é também identificado como um incidente relaciona com o comportamento humano. As ações dos colaboradores que aumentam substancialmente a probabilidade deste tipo de incidentes são as ligações a Wi-Fi inseguras, conexão de dispositivos próprios à rede da empresa, não atualização dos softwares antivírus e anti-malware, utilização de serviços *cloud* sem permissão da organização, etc. (CERT, 2013).

Adicionalmente, as *passwords* representam outro grande problema, onde as pessoas nem sempre seguem as melhores práticas. Exemplo disso é o facto de partilharem *passwords* com terceiros, utilizarem a mesma *password* para diferentes contas e não haver uma alteração das passwords com regularidade (Ponemon Institute, 2012).

2.4 Normas e Regulamentações relacionadas à cibersegurança

2.4.1 GDPR

A GDPR (General Data Protection Regulation) é uma regulamentação da União Europeia que entrou em vigor em maio de 2018 e tem como objetivo proteger a privacidade e os dados pessoais dos cidadãos da UE. As PME's também são afetadas pela GDPR e precisam de cumprir as suas exigências (Calder & Khalid, 2018). A regulamentação visa garantir que os indivíduos tenham controlo sobre os seus dados pessoais e que as empresas façam o processamento desses dados de maneira justa, transparente e segura (Calder & Khalid, 2018).

Segundo, Calder & Khalid (2018) a GDPR define "dados pessoais" como qualquer informação que possa ser usada para identificar uma pessoa, incluindo nome, morada, número de identificação, dados de localização, entre outros. A regulamentação também exige que as empresas obtenham consentimento explícito dos utilizadores para aceder, armazenar e processar os seus dados pessoais, e forneçam informações claras e precisas

sobre como os dados serão usados. Além disso, a GDPR exige que as empresas implementem medidas de segurança adequadas para proteger os dados pessoais dos utilizadores contra o acesso não autorizado, roubo, perda ou danos.

A implementação da GDPR pode ser um desafio para as PME's, uma vez que podem ter menos recursos e capacidade para cumprir os requisitos da regulamentação. No entanto, é importante que as PME's estejam em conformidade com a GDPR para proteger a privacidade e os dados pessoais dos indivíduos envolvidos nos seus negócios.

Para garantir a conformidade com a GDPR, as PME's podem adotar várias práticas. É obrigatório nomear um responsável pela proteção de dados (Data Protection Officer - DPO) para supervisionar a conformidade com a regulamentação. Além disso, é importante que as PME's realizem avaliações de risco e análises de impacto à privacidade para identificar e mitigar potenciais problemas relacionados com a privacidade dos dados. Outra prática importante é garantir que todos os funcionários estejam cientes das políticas e procedimentos de proteção de dados e que recebam o treino adequado para garantir que cumprem com as exigências da GDPR. As empresas também devem implementar técnicas de segurança de dados, como criptografia, backups regulares e controlos de acesso, para garantir a proteção dos dados pessoais (Kosa, 2019).

Por fim, as PME's devem manter registos precisos e atualizados de todas as atividades de processamento de dados para garantir a conformidade com a GDPR. Manter registos precisos pode ajudar as PME's a responder rapidamente a solicitações de indivíduos em relação a seus dados pessoais, bem como detetar e relatar violações de dados a tempo (Information Commissioner's Office, 2017).

Em resumo, as PME's podem enfrentar desafios ao implementar a GDPR, mas isso não deve impedi-las de proteger a privacidade e os dados pessoais dos indivíduos envolvidos nos seus negócios. Adotar práticas como nomear um DPO, realizar avaliações de risco, garantir que os funcionários estejam cientes das políticas de proteção de dados, implementar medidas de segurança e manter registos precisos pode ajudar as PME's a garantir a conformidade com a regulamentação.

2.4.2 ISSO 27001

A ISO 27001 ajuda as empresas a implementar uma estrutura de segurança da informação que identifica, avalia e faz a gestão dos riscos de segurança da informação. A norma define

uma série de controlos de segurança da informação, que podem ser adaptados às necessidades específicas de cada empresa (Watkins, 2019).

Segundo, Watking (2019), para as PME's, a implementação da ISO 27001 pode parecer um desafio, uma vez que elas podem ter menos recursos e capacidade para cumprir os requisitos da norma. No entanto, as PME's podem adotar várias práticas para implementar com sucesso um SGSI, incluindo:

- Realizar uma avaliação de riscos de segurança da informação;
- Identificar ativos de informação e definir medidas de segurança adequadas para protegê-los;
- Implementar controlos de segurança da informação, como políticas de segurança, gestão de acessos, monitoramento e controlo da rede;
- Manter registos atualizados de todas as atividades de segurança da informação;
- Realizar auditorias regulares para garantir a conformidade contínua com a norma.

2.5 Red and Blue Team

O exercício Red/Blue Team não é um conceito novo. Foi introduzido há muito tempo durante a Primeira Guerra Mundial e, como muitos termos usados em segurança das informações, teve origem nas forcas armadas. A ideia geral era demonstrar a eficácia de um ataque por meio de simulações, como podemos observar na figura 1 (Diogenes & Ozkaya, 2018).

Red team vs. Blue team é um termo usado em cibersegurança para referir-se a dois grupos diferentes que simulam ataques e mecanismos de defesa para testar a segurança da infraestrutura de uma organização. A equipa vermelha é a força atacante que tenta infiltrar-se num sistema, enquanto a equipa azul é a força defensiva que tenta prevenir e responder aos ataques. Neste tópico, vamos aprofundar as funções e responsabilidades de cada equipa e como elas trabalham juntas para melhorar a cibersegurança (NIST, 2018).

A Red Team descreve uma variedade de técnicas de simulação e avaliação usadas pelas comunidades de negócios, militares, inteligência e aplicação de lei. Por um lado, pretendem simular as ações de prováveis adversários quando se trata de avaliar a eficácia de planos e procedimentos ou em situações de jogo em que a Blue Team procura testar conceitos, capacidades, táticas ou operações contra um adversário. oponente fictício. Por outro lado, os

Red Teams são constituídos para servir como uma espécie de "advogado do diabo" para encontrar pontos fracos em conceitos, estratégias e sistemas de segurança que podem ser explorados por determinados oponentes. Quando usado como substantivo, o termo Red Team sugere que alguém está a desempenhar o papel de oponente ou competidor; quando usado como verbo, sugere que está em andamento uma avaliação critica de estratégias ou conceitos (Zenko, 2015).

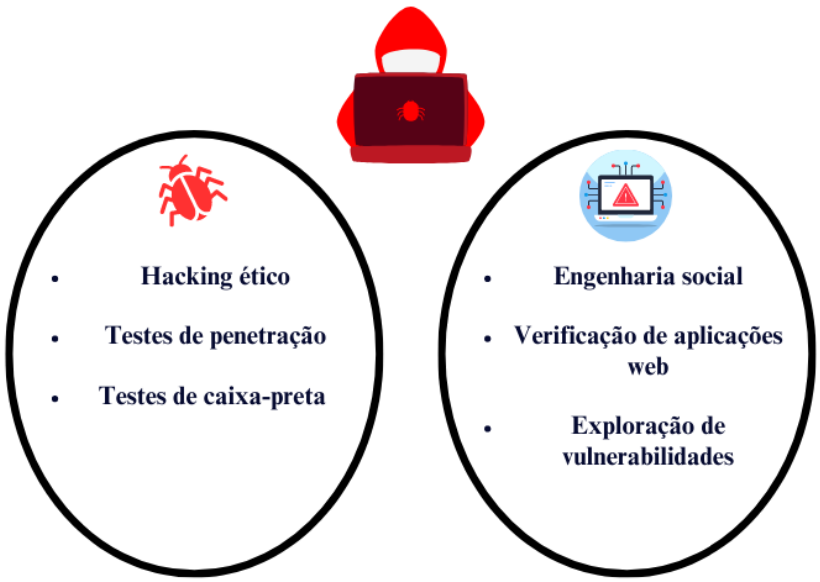


Figura 1 - Red Team

Adaptado de (Climer & Khan, s.d.)

A Blue Team, ao nível macro, é toda a organização, incluindo os utilizadores e clientes, isto porque os mesmo serão os primeiros a perceber quando algo estiver errado do ponto de vista da segurança. Ao nível micro, a equipa azul é composta pelas pessoas diretamente responsáveis por monitorizar, defender e responder a incidentes (J. Carey & Jin, 2020).

A Blue Team desempenha um papel crucial na cibersegurança de uma organização. São responsáveis pela manutenção dos sistemas e redes da organização, que são componentes essenciais para as operações da empresa. A função da Blue Team consiste em implementar controlos de segurança e monitorar o ambiente para procurar atividades suspeitas. Esse monitoramento ajuda a prevenir e a responder a ataques informáticos. Normalmente é composta por analistas de segurança que trabalham juntos para detetar e responder a incidentes de segurança. Esses profissionais possuem formação especializada em cibersegurança e são qualificados em vários aspetos da gestão de segurança, são também

responsáveis por manter os sistemas e redes da organização seguros e garantir que os dados e outras informações confidenciais sejam protegidos (SANS, 2021).

Além disso, o objetivo principal da Blue Team é evitar que os ataques aconteçam em primeiro lugar, conseguem isso implementando várias medidas de segurança, como firewalls, sistemas de deteção de intrusão e controlos de acesso. Essas medidas de segurança destinam-se a criar várias camadas de proteção que ajudam a impedir o acesso não autorizado aos sistemas e dados da organização. (Zeller, 2019)

A Blue Team monitoriza continuamente o ambiente para procurar atividades suspeitas usando ferramentas avançadas de gestão de eventos e informações de segurança (SIEM) e outras ferramentas de monitoramento de segurança. Esse monitoramento contínuo ajuda a garantir que os sistemas e redes da organização estejam seguros e fornece alertas em tempo real se alguma atividade suspeita for detetada. Essas informações são então analisadas pela equipa, que trabalha em conjunto para responder a qualquer possível incidente de segurança de maneira oportuna e eficaz (Pennington, 2019).

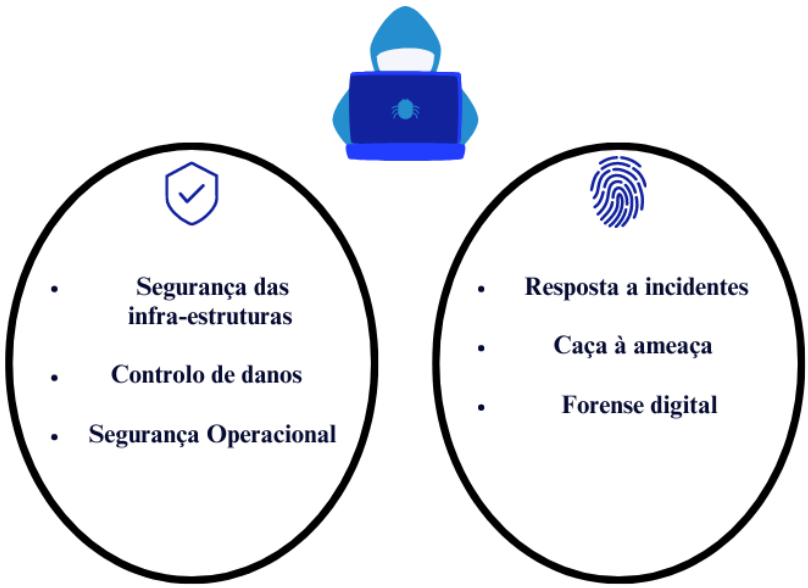


Figura 2 - Blue Team

Adaptado de (Climer & Khan, s.d.)

A Red Team e a Blue Team trabalham juntas para melhorar a segurança de uma organização. A Red Team identifica vulnerabilidades que precisam de ser corrigidas, enquanto a Blue Team implementa controlos de segurança para evitar que essas vulnerabilidades sejam exploradas. A Blue Team também usa as informações coletadas pela

Red Team para melhorar os recursos de monitoramento de segurança e resposta a incidentes. A colaboração entre as equipas é um aspeto crucial da estratégia geral de segurança de uma organização. Ao simular ataques do mundo real e testar defesas, as organizações podem identificar pontos fracos e resolvê-los antes que ocorra um ataque real. O processo de testar e melhorar as defesas é conhecido como "teste de penetração" (Haight, 2018).

Concluindo, o conceito de Red Team vs. Blue Team constitui uma parte essencial da cibersegurança. A Red Team simula ataques para identificar vulnerabilidades, enquanto a Blue Team implementa controlos para prevenir e responder a esses ataques. A colaboração entre as duas equipas é fundamental para melhorar a postura de segurança de uma organização e prevenir ataques no mundo real. Ao trabalharem juntas, as organizações podem garantir que estão preparadas para enfrentar o cenário de ameaças em constante evolução e proteger seus ativos contra criminosos informáticos (Isik, 2019).

2.6 Ferramentas

2.6.1 VMware

A VMware, Inc., é uma empresa líder no mercado da virtualização e das infraestruturas cloud, tem sido pioneira em fornecer soluções inovadoras para otimizar o uso de recursos de computação em ambientes empresariais e de data centers (VMware, Inc., 2019).

Entre as suas características mais notáveis está o VMware vSphere, que introduziu o revolucionário conceito de virtualização de servidores. Isso permite que múltiplas máquinas virtuais operem num único servidor físico, maximizando a utilização dos recursos e reduzindo significativamente os custos operacionais. (VMware, Inc., 2019).

Mas a inovação da VMware vai além da virtualização de servidores, a empresa também desenvolveu ferramentas integradas numa plataforma unificada para a gestão de redes, armazenamento, segurança e mobilidade. Com o ESXi, um hypervisor tipo 1, a VMware possibilita a execução de várias máquinas virtuais num único hardware físico. O vCenter Server auxilia na gestão centralizada das infraestruturas virtuais, simplificando processos como o fornecimento, a monitorização e a otimização de recursos. A vSAN é uma inovadora solução de armazenamento definido por software que permite a integração de armazenamento físico num cluster compartilhado. A NSX, uma plataforma de virtualização de rede, facilita a criação de redes virtuais complexas, otimizando a segurança e o

desempenho. E o Workspace ONE oferece uma plataforma especializada para a gestão de mobilidade empresarial, melhorando a entrega e a gestão de aplicações em dispositivos móveis. A abordagem integrada e inovadora da VMware revolucionou o mercado de IT, promovendo maior eficiência, flexibilidade e escalabilidade em ambientes de IT modernos (Marshall, N., & Baldwin, G., 2018)

2.6.2 Nmap

O Nmap é uma ferramenta de rede de código aberto que é utilizada para mapeamento de rede e exploração de vulnerabilidades. Foi criado por Gordon Lyon em 1997 e é suportado por uma grande comunidade de desenvolvedores e utilizadores (The Nmap Project, 2022).

A principal função do Nmap é verificar quais as portas de um determinado host que estão abertas e quais os serviços que estão sendo executados nesses hosts. Isto pode ajudar a identificar vulnerabilidades de segurança que podem ser exploradas por invasores mal-intencionados. O Nmap também pode ser usado para descobrir hosts na rede e para identificar o sistema operativo em execução em cada host. (Lyon, G. , 2009)

O Nmap é executado numa variedade de sistemas operativos, incluindo Linux, Windows, macOS e BSD, e pode ser executado a partir da linha de comando ou de uma interface gráfica do utilizador. Suporta uma ampla variedade de opções de procuras na rede, incluindo scans TCP SYN, scans UDP, scans de reconhecimento de versão e scans de deteção de sistemas operativos. Além disso, o Nmap suporta scripts personalizados que podem ser usados para automatizar tarefas de varredura, como detetar vulnerabilidades específicas e identificar sistemas para executar software desatualizado. Esses scripts são escritos numa linguagem de script personalizada chamada Nmap Scripting Engine (NSE) (The Nmap Project, 2022).

O Nmap também inclui recursos avançados de filtragem e classificação que permitem aos utilizadores limitar o alcance dos scans e exibir resultados de maneira organizada e fácil de entender. Também pode ser integrado com outras ferramentas de segurança, como o Metasploit Framework, para facilitar a exploração de vulnerabilidades (Kottler, B., 2020).

No entanto, é importante notar que o Nmap pode ser usado para fins maliciosos se não for usado com responsabilidade. Por essa razão, é importante que os utilizadores tenham uma compreensão completa das leis e regulamentações locais antes de usar o Nmap em qualquer sistema que não seja de sua propriedade (Kottler, B., 2020).

2.6.3 Nessus

O Nessus, criado pela Tenable Network Security, é um produto na área da segurança informática, que atua como uma ferramenta de avaliação de vulnerabilidades. Originalmente lançado como um projeto de código aberto em 1998, passou por várias iterações até tornar-se um produto comercial em 2005. Tem a capacidade de efetuar *scans* detalhados em sistemas e redes, e tem sido essencial para inúmeras organizações, permitindo-lhes identificar vulnerabilidades antes de serem exploradas por utilizadores mal-intencionados (Nessus, 2018).

Um dos pontos fortes do Nessus é a grande biblioteca de *plugins* que tem ao seu dispor, que são atualizados frequentemente para refletir novas descobertas de vulnerabilidades em *softwares* e sistemas. Estes *plugins* permitem ao Nessus detetar uma ampla gama de falhas de segurança, desde problemas em configurações até falhas *zero-day*. Adicionalmente, a ferramenta pode avaliar o grau de conformidade de um sistema com determinadas normas de segurança, facilitando para as empresas a manutenção de padrões elevados de segurança e conformidade regulamentar (Skoudis, E., & Liston, T., 2014).

Outro recurso do Nessus é a capacidade de integração com outras ferramentas e plataformas. Isso é particularmente útil em ambientes empresariais complexos, onde a coordenação entre diferentes soluções de segurança é crucial. Além disso, com uma interface intuitiva e relatórios detalhados, os profissionais de segurança podem tomar decisões informadas e prioritárias sobre quais vulnerabilidades corrigir primeiro, com base no risco potencial associado (Skoudis, E., & Liston, T., 2014).

Em termos de aplicabilidade, o Nessus é utilizado numa variedade de cenários, incluindo testes de penetração, avaliações de segurança de rotina e em auditorias de segurança. A sua flexibilidade e poder tornam-no adequado tanto para pequenas ou grandes empresas e entidades governamentais (Nessus, 2018).

2.6.4 FTK Imager

O FTK Imager, desenvolvido pela AccessData, é uma ferramenta forense que facilita a aquisição reservada de imagens digitais de diversos dispositivos de armazenamento, como discos rígidos, dispositivos USB, CDs e DVDs (AccessData, 2020).

Esta capacidade garante que os profissionais de investigação digital possam recolher dados sem alterar as informações originais. Para além da sua capacidade de aquisição, o FTK Imager oferece a possibilidade de visualizar e analisar os dados contidos nessas imagens, abrangendo desde a estrutura de arquivos e pastas até metadados e conteúdos específicos (AccessData, 2020).

Uma das suas maiores vantagens é que a integridade dos dados é mantida durante todo o processo, evitando qualquer modificação nos originais. O programa suporta vários formatos de imagem, incluindo RAW, E01 (formato EnCase) e AFF, e ainda permite uma análise detalhada, que inclui até mesmo arquivos que foram previamente eliminados. Adicionalmente, a sua portabilidade é notável, já que pode ser operado diretamente de uma unidade USB, facilitando a colheita de evidências em locais específicos. Os investigadores também têm a opção de exportar dados, metadados e outras informações relevantes conforme necessário (Nelson, B., Phillips, A., & Steuart, C., 2015).

2.6.5 Autopsy

O Autopsy é uma plataforma de análise forense digital de código aberto, frequentemente utilizada por investigadores para conduzir exames em dispositivos digitais e ajudar na identificação de evidências em potencial. Desenvolvida como uma interface gráfica para a ferramenta de linha de comando Sleuth Kit, a mesma oferece uma abordagem intuitiva num ambiente unificado para realizar tarefas forenses, desde a recuperação de arquivos eliminados até à análise de atividades suspeitas (Casey, E., Ferraro, M., & Nguyen, L., 2009).

Uma das maiores vantagens do Autopsy é sua modularidade. Possui uma variedade de módulos internos que permitem aos utilizadores identificar dados específicos, como históricos de navegação na web, conexões ou registos de geolocalização. Além disso, graças à sua natureza de código aberto, a comunidade forense pode desenvolver e compartilhar os seus próprios módulos, ampliando ainda mais as capacidades da ferramenta (Richardson, R., & Marjie, T., 2018).

Segundo Richardson, R., & Marjie, T. (2018) o autopsy também é conhecido pela sua capacidade de realizar análises temporais, permitindo aos investigadores visualizar eventos numa linha do tempo. Isso é fundamental para entender a sequência de atividades num dispositivo e identificar padrões ou ações suspeitas. Outra característica significativa é a

funcionalidade de pesquisa por palavras-chave, que facilita a identificação rápida de informações relevantes.

A combinação de robustez, adaptabilidade e custo zero torna o Autopsy uma das melhores escolhas entre os profissionais de forense digital, tanto no setor público quanto no privado. Em ambientes acadêmicos, também é frequentemente utilizado como uma ferramenta educativa devido à sua capacidade de fornecer insights práticos sobre os processos forenses digitais.

2.6.6 VirusTotal

VirusTotal é uma ferramenta online que desempenha um papel crucial na análise de arquivos e URLs suspeitos, fornecendo um serviço que agrega os resultados de múltiplos motores antivírus e scans de ameaças. Lançado inicialmente em 2004 por Hispasec Sistemas, foi posteriormente adquirido pela Google em 2012, tornando-se parte da Chronicle, uma subsidiária da Alphabet focada em cibersegurança (Guarnizo, J.D., Buitrago, S.O., Gharib, M.A., Ochoa, M., & Tippenhauer, N.O., 2018).

A principal utilidade do VirusTotal é oferecer um panorama abrangente da deteção de potenciais ameaças. Ao submeter um arquivo ou um URL, o serviço faz um scan usando diversos motores antivírus, oferecendo assim uma visão consolidada que ajuda a determinar se um arquivo ou URL é malicioso. Além disso, fornece detalhes técnicos sobre os arquivos analisados, incluindo relações com outros arquivos, comunicações de rede, e até mesmo comportamentos observados quando executados em ambientes isolados (Chronicle., 2019).

O VirusTotal não deve ser usado como a única ferramenta de avaliação de segurança ou substituto de uma solução antivírus dedicada, mas sim como um recurso complementar. A sua abordagem baseada na comunidade também incentiva os utilizadores a fornecer feedback e informações adicionais sobre as ameaças, tornando-se uma plataforma colaborativa na luta contra o malware e outros tipos de software malicioso (Chronicle., 2019).

O uso extensivo do VirusTotal em investigações de cibersegurança, pesquisa de ameaças e análise de malware destaca sua a importância e confiabilidade como ferramenta no campo da segurança da informação (Pfeffer, K., Eckert, C., & Holz, T. , 2017).

2.6.7 Avira AntiVirus

O Avira Antivirus é uma solução de segurança amplamente reconhecida que foi desenvolvida pela empresa alemã Avira Operations GmbH & Co. KG. Desde o seu lançamento, o Avira ganhou popularidade devido à sua eficácia na deteção e remoção de malware e à sua versão gratuita, que atraiu uma base considerável de utilizadores individuais. Com uma combinação de assinaturas tradicionais, heurísticas e tecnologias baseadas em nuvem, o Avira oferece proteção contra uma variedade de ameaças, desde vírus até *ransomware* e *phishing* (Avira Operations GmbH & Co. KG., 2019).

Uma das principais características do Avira é o seu mecanismo de deteção "AHeAD" (Advanced Heuristic Analysis and Detection), que utiliza técnicas heurísticas para detetar código malicioso desconhecido ou variantes de malware já conhecidas. Ao longo dos anos, o Avira expandiu o seu portfólio de produtos para incluir não apenas proteção antivírus, mas também soluções de VPN, otimização de sistema e proteção de identidade.

A interface do utilizador do Avira é delineada para ser intuitiva, tornando-o acessível para utilizadores não técnicos, enquanto oferece opções avançadas para aqueles que desejam um controlo mais fragmentado sobre as configurações de segurança (Avira, 2019).

Nas avaliações independentes, o Avira, frequentemente, está entre os principais antivírus em termos de taxa de deteção, demonstrando a sua competência em manter os dispositivos dos utilizadores seguros.

2.6.8 ClamAV

O ClamAV é um software antivírus de código aberto de ampla utilização, especialmente conhecido pela sua integração em *gateways* de e-mail para fazer o *scan* de anexos que contenham malware. Desenvolvido inicialmente por Tomasz Kojm em 2001, o ClamAV cresceu e evoluiu, tornando-se um padrão na comunidade de software livre e código aberto (FOSS) para deteção de malware (ClamAV Team., 2020)

Segundo a ClamAV Team (2020) uma das características notáveis do seu programa é sua versatilidade. O programa pode ser usado tanto em ambientes Linux quanto Windows, e a sua natureza modular permite que ele seja integrado em várias aplicações e serviços. Opera principalmente através da linha de comando, o que facilita a sua utilização em scripts e outras ferramentas automatizadas.

O ClamAV é atualizado regularmente com definições de vírus e também suporta a deteção heurística, permitindo que detete novas variantes de malware. Dado que é de código aberto, o ClamAV possui uma comunidade ativa que contribui tanto para as definições de vírus, quanto para o próprio desenvolvimento do software (Marpillero, S., Laskov, P., & Düssel, P. , 2008).

Além da sua capacidade de detetar malware, o ClamAV também é conhecido por identificar outros tipos de conteúdos potencialmente indesejados, como arquivos PDF que contêm links suspeitos.

2.7 Trabalhos Relacionados

Fator Humano da Cibersegurança nas Organizações

Neste trabalho Gonçalves (2019) investiga como o elemento humano afeta a cibersegurança nas empresas, identificando as particularidades e atitudes humanas que influenciam a cibersegurança, o seu efeito nos graus de cibersegurança atingidos, e as soluções apropriadas para essas atitudes.

Para a realização do mesmo foram realizadas entrevistas individuais a peritos e investigadores em cibersegurança, que permitiram concluir que as pessoas têm realmente uma grande influência e, consequentemente, importância, na cibersegurança das organizações.

O trabalho foi realizado com a finalidade de contribuir tanto tecnicamente como de maneira prática. Tecnicamente, o foco foi aprofundar a análise do elemento humano na cibersegurança das empresas, expondo conceitos teóricos e o panorama atual desta área, apoiado em fontes bibliográficas confiáveis e entrevistas com especialistas e pesquisadores.

No que diz respeito ao lado prático, o autor espera que o trabalho possa difundir conhecimento e consciencializar a sociedade sobre a relevância da cibersegurança, incentivando uma alteração de atitudes e pensamentos em favor de uma cultura de cibersegurança robusta.

O Impacto da Segurança Informática nas PME

Este trabalho de Arim (2014) procura ser um estudo inicial para a execução de uma pesquisa empírica, que envolve questionar PME's europeias sobre seus métodos de segurança e atitudes face às correntes inovações tecnológicas. Um questionário foi elaborado

para alcançar os objetivos. Foram realizadas entrevistas a 16 PME's com diferentes atividades de negócio sediadas na Europa, focando nas abordagens recentes à segurança da informação, exposição ao cibercrime e estratégias de prevenção do mesmo.

Risco calculado? Uma ferramenta de avaliação de cibersegurança para PME's

Benz e Chatterjee (2020) descrevem uma metodologia desenvolvida usando a framework de cibersegurança do *National Institute of Standards and Technology's* (NIST) como ponto de partida. O NIST cibersecurity framework não atende a todas as necessidades TI das PME, mas oferece uma base sólida para uma metodologia útil de avaliação e recomendação.

No estudo propôs-se uma ferramenta de avaliação de segurança informática para PME's que consiste numa pesquisa on-line de 35 perguntas a ser respondida por líderes de TI para autoavaliar a maturidade dentro das cinco categorias da estrutura NIST: identificar, proteger, detetar, responder e recuperar. Descreveu-se esta abordagem à gestão de riscos de segurança informática antes de discutir a sua eficácia e implicações para os profissionais.

Segurança informática e hacking ético para PME's

Neste trabalho foi abordado por Berger e Jones (2016) o tema do Hacking Ético, onde hackers com permissão tentam invadir sistemas e redes de uma empresa a pedido dos donos para identificar lacunas de segurança. No entanto, estas ações têm custos elevados e muitas PME's carecem do know-how e dos meios para as realizar. Com um caso prático de uma PME, foi mostrado perspetivas sobre como o Hacking Ético, através de testes de penetração com ferramentas open-source gratuitas, pode ser uma solução para PME's melhorarem a segurança das suas redes e operações.

Utilizando Nmap, Google Hacking, Nessus e Brutus, foram encontradas 232 falhas de rede. Posteriormente, adotaram-se estratégias para corrigir essas fragilidades e resguardar o caso de estudo de futuros riscos informáticos. Embora as PME's frequentemente usem medidas básicas como firewalls robustos, encriptação de dados e antivírus, medidas de segurança mais avançadas são geralmente negligenciadas. Reconhece-se que tais medidas de segurança têm custos elevados e muitas PME's não têm meios para implementá-las.

3 METODOLOGIA

Neste capítulo, descreve-se a metodologia desenvolvida para permitir um melhor entendimento do processo de desenvolvimento do estudo. Este estudo surge como rum contributo para ultrapassar as dificuldades e falta de preparação que as pequenas e médias empresas (PME's) têm em relação à cibersegurança e à proteção da sua empresa no mundo digital.

Para tornar possível a criação de um guia de preparação capaz de ajudar as PME's a ambientarem-se com o tema da cibersegurança e tornarem-se mais seguras, é necessário um trabalho minucioso que contemple todas as funções cruciais da cibersegurança numa PME, desde a identificação de uma ameaça até à recuperação da empresa em caso de ataque.

Este estudo baseia-se na metodologia NIST que fornece orientações específicas para a gestão e segurança da informação de organizações, incluindo as PME's. Além disso, para uma melhor experiência e análise da realidade das PME's na deteção de ameaças, serão utilizadas ferramentas para analisar o tráfego de rede nas mesmas, recorrendo-se a simulações desenvolvidas com a ajuda da criação de máquinas virtuais.

É importante destacar que a cibersegurança é um assunto complexo e em constante evolução, por isso, além do guia de preparação, a metodologia incluirá também um plano de treino para as equipas de IT das PME's, com o objetivo de garantir que as medidas de cibersegurança sejam implementadas corretamente e atualizadas constantemente.

Em suma, esta metodologia visa fornecer uma abordagem completa e eficaz para a implementação de medidas de cibersegurança nas PME's, ajudando-as a compreender melhor os riscos associados à sua atividade e a tomar medidas preventivas apropriadas.

3.1 Modelo Concetual

A metodologia seguida para o desenvolvimento deste projeto consiste na adaptação da NIST – Cybersecurity Framework (Mahn, Marron, Quinn, & Topper, 2021) ao contexto das PME portuguesas.

De acordo com o U.S Department of Commerce o NIST pode ajudar uma organização a iniciar ou melhorar o seu programa de cibersegurança, e está organizada em cinco funções principais – Identificar, Proteger, Detetar, Responder e Recuperar. Estes cinco passos,

quando considerados em conjunto, fornecem uma visão abrangente para a gestão do risco de segurança informática ao longo do tempo (Mahn, Marron, Quinn, & Topper, 2021) (Fig.3).

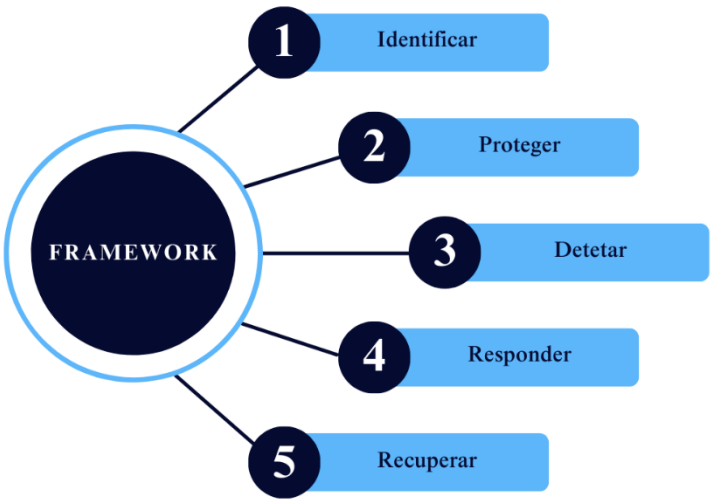


Figura 3. NIST Framework

Adaptado de (Mahn, Marron, Quinn, & Topper, 2021)

3.1.1 Identificar

A função identificar apresenta a importância da cibersegurança e destaca duas funções fundamentais para garantir a proteção adequada das informações das empresas: estabelecer políticas de cibersegurança que incluam funções e responsabilidades; e identificar ameaças, vulnerabilidades e riscos (Mahn, Marron, Quinn, & Topper, 2021).

A primeira função, estabelecer políticas de cibersegurança que incluam funções e responsabilidades, é fundamental para garantir que as expectativas em relação à cibersegurança sejam claramente definidas e que todos os envolvidos saibam as propostas de modelo para as políticas. Essas políticas devem descrever claramente os procedimentos e expectativas que ajudarão a proteger as informações da empresa.

Já a segunda função, identificar ameaças, vulnerabilidades e riscos, é importante para que as empresas possam fazer a gestão adequada das ameaças internas e externas. As empresas devem estabelecer processos de gestão de riscos que permitam identificar, avaliar e documentar todas as ameaças, vulnerabilidades e riscos. Isso ajudará a garantir que as

medidas de segurança adequadas sejam tomadas para proteger as informações das empresas. (Whitman, M. E., & Mattord, H. J. , 2018)

Em resumo, a implementação dessas duas funções é crucial para garantir a segurança das informações das empresas e prevenir possíveis ataques informáticos e violações de dados.

Segundo o NIST (2018), para entender melhor as políticas de segurança de uma empresa, é importante questioná-la diretamente. Uma forma de fazer isso de maneira organizada e estruturada é realizar um questionário. As políticas propostas para esta fase são as seguintes:

- Política de atualização de software
- Política de passwords
- Política de backups
- Política de partilha de ficheiros
- Política de controlo de conta do utilizador
- Política de Antivírus e Firewall
- Política de Logs de Auditoria

As políticas de atualização de software são diretrizes estabelecidas por uma organização para garantir que todo o software usado nos seus sistemas seja mantido atualizado. Isso é vital para a segurança informática, pois muitas ameaças exploram vulnerabilidades em versões desatualizadas de software. Esta política tem como diretrizes a programação regular de atualizações, a instalação obrigatória de atualizações de segurança, testar atualizações, atualizações de versões descontinuadas e auditoria e conformidade (Microsoft, 2020).

As políticas de password, são diretrizes estabelecidas por uma organização para garantir que os utilizadores alterem as suas senhas regularmente, ajudando assim a manter a segurança da informação. Algumas diretrizes são a frequência de alteração, histórico de senhas, complexidade da senha e o bloqueio da conta (NIST, 2017).

As políticas de backups, ou políticas de cópia de segurança, são diretrizes criadas para garantir que os dados importantes sejam regularmente copiados e armazenados de maneira segura. Estas políticas são cruciais para a cibersegurança, pois permitem a recuperação de dados em caso de um incidente de segurança, como um ataque ransomware, ou num caso de falha de hardware ou erro humano. Algumas das diretrizes são, frequência de backups, tipo de backups, dados a serem incluídos, armazenamento de backups e criptografia (SANS Institute, 2014).

Segundo o SANS Institute (2014), as políticas de partilha de ficheiros são um conjunto de diretrizes que uma organização implementa para controlar a forma como as informações são compartilhadas e transferidas entre os utilizadores, tanto internamente quanto externamente. A partilha de ficheiros é uma necessidade comum nos negócios de hoje, mas também apresenta riscos significativos de segurança. Portanto, uma política de partilha de ficheiros é essencial para proteger as informações sensíveis da organização. Algumas das diretrizes são, quais as informações que podem ser compartilhadas e com quem, como é que os ficheiros devem ser partilhados, autenticação e permissão, criptografia, e auditoria e monitorização.

Ao questionar a empresa sobre as suas políticas de segurança, é possível avaliar a eficácia dessas políticas e identificar possíveis lacunas ou vulnerabilidades que precisam de ser abordadas. Além disso, também pode ser uma oportunidade para sugerir melhorias e ajudar a empresa a fortalecer a sua postura de cibersegurança.

3.1.2 Proteger

Este tópico traz informações relevantes sobre a função proteger, que é fundamental para garantir a segurança dos dados e dispositivos de uma empresa.

Para gerir o acesso aos ativos e proteger os dispositivos, é necessário criar contas exclusivas para cada funcionário e garantir que os utilizadores tenham acesso apenas às informações, computadores e aplicações necessárias para cada um. Além disso, a instalação de firewalls baseadas em host e outras proteções, como produtos de segurança de endpoint, pode ajudar a proteger os dispositivos e evitar ataques informáticos (Whitman, M. E., & Mattord, H. J. , 2018).

De acordo com as diretrizes publicadas pelo National Institute of Standards and Technology (NIST) no ano de 2018, uma outra medida crucial para a gestão de segurança da informação é a proteção rigorosa de dados confidenciais. Esta proteção deve ser executada através do emprego de mecanismos de criptografia, não apenas durante o período em que os dados se encontram armazenados em sistemas computacionais, mas também durante o processo de transmissão dessas informações para outras entidades ou partes interessadas. A aplicação deste método de segurança oferece uma garantia robusta no que diz respeito à preservação da privacidade e à integridade das informações em questão

Realizar backups também é uma medida essencial para garantir a segurança dos dados. Muitos softwares possuem o recurso de realizar backups integrados, mas também estão disponíveis soluções de software em nuvem que podem automatizar o processo de backup. Desta forma, é possível evitar a perda de dados em caso de falhas de hardware ou ataques informáticos. (National Institute of Standards and Technology, 2018)

Por fim, treinar os colaboradores é uma medida importante para garantir que eles estejam a par das políticas e procedimentos de cibersegurança da empresa e das suas funções. Esta ação deve ser feita regularmente para manter todos atualizados sobre as práticas de segurança.

Com estas medidas, as empresas podem aumentar a segurança dos seus ativos e dispositivos, proteger dados confidenciais e evitar perdas de dados. É fundamental que as empresas estejam sempre atentas às novas ameaças informáticas e implementem novas medidas de segurança conforme necessário para garantir a proteção contínua dos seus dados e dispositivos. (Whitman, M. E., & Mattord, H. J. , 2018)

Nesta fase "Proteger", no âmbito da cibersegurança, as Políticas de Grupo desempenham um papel crucial. Estas políticas permitem implementar medidas proativas e preventivas para proteger os sistemas contra várias ameaças informáticas, sendo uma componente fundamental na construção de uma infraestrutura de IT segura (Desmond, B. , 2020).

As Políticas de Grupo, são uma característica do Microsoft Windows que permite aos administradores de sistemas controlarem o ambiente de trabalho de utilizadores e computadores. Usando as *group policies*, podemos definir regras para o comportamento do sistema, como direitos de acesso, privilégios, configurações de software, etc (Moskowitz, J. D., & Barber, M., 2019).

No âmbito da cibersegurança, as *group policies* são uma ferramenta essencial. Elas permitem aos administradores aplicar políticas de segurança na rede, como restrições de software, configurações de firewall, atualizações automáticas, controlo do utilizador e outros recursos. Isso pode ajudar a prevenir ciberataques, como malware, phishing e ataques de força bruta (Moskowitz, J. D., & Barber, M., 2019).

As políticas a melhorar podem incluir a criação de *Group Policies* como as que estão demonstradas na tabela 2 (Microsoft, 2021).

Tabela 2 - Group Policies

POLÍTICA	DESCRIÇÃO	CONFIGURAÇÃO
Autenticação do Utilizador	Exigir que os utilizadores autentiquem-se antes de aceder a rede.	Ativar
Password Mínima	Definir o comprimento mínimo da password.	Definir como 8 caracteres
Complexidade da Password	Exigir que as passwords contenham pelo menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.	Ativar
Expiração da Password	Definir o período máximo antes de uma password precisar de ser alterada.	Definir como 90 dias
Bloqueio da Conta	Bloqueiar a conta após um número específico de tentativas de login falhadas.	Definir como 5 tentativas
Forçar Logout	Força o logout do utilizador após um período de inatividade.	Definir como 15 minutos
Antivírus	Assegurar que todos os sistemas possuem software de antivírus e estejam atualizados.	Ativar
Firewall	Ativar a firewall em todos os sistemas.	Ativar
UAC (Controle de Conta de Utilizador)	Exigir permissão do administrador para alterações importantes no sistema.	Ativar
Atualizações Automáticas	Forçar todos os sistemas a instalar atualizações de segurança.	Ativar
Acesso a Pastas partilhadas	Definir os níveis de permissão para pastas partilhadas.	Configurar de acordo com o papel do utilizador
Logs de Auditoria	Habilitar e configurar a auditoria de eventos de segurança.	Ativar

Após saber qual o estado da empresa, o passo seguinte é aplicar as group policies que estão em falta para protegermos a mesma.

Começando pela autenticação do utilizador, é essencial para qualquer sistema de segurança informática. Requer que cada utilizador forneça credenciais válidas, geralmente um nome de utilizador e uma senha, antes de ter permissão para aceder à rede da empresa.

Esta política serve como a primeira barreira contra intrusões, garantindo que apenas os indivíduos autorizados possam aceder à rede (Microsoft, 2022).

A política de password mínima é uma medida de segurança que determina que todas as passwords dos utilizadores da empresa devem ter pelo menos um determinado número de caracteres. Neste exemplo, a política exige um mínimo de 8 caracteres. Senhas mais longas são tipicamente mais seguras e mais difíceis de serem descobertas por atacantes (Moskowitz, J. D., & Barber, M., 2019).

No mesmo âmbito temos a política de complexidade da password que aumenta a segurança exigida, segundo Moskowitz, J. D., & Barber, M. (2019) as senhas têm de conter uma combinação de letras maiúsculas, letras minúsculas, números e caracteres especiais. Ao impor esta complexidade, a política torna as senhas mais resistentes a ataques de força bruta e mais difíceis de serem adivinhadas. Junto a isso, a política de expiração da password define um prazo para a alteração regular das senhas, neste exemplo, a cada 90 dias. Esta política ajuda a mitigar o risco de acesso não autorizado, especialmente se uma senha for comprometida sem o conhecimento do utilizador.

A política de bloqueio da conta que serve para proteger as contas de utilizadores de tentativas repetidas de acesso não autorizado. Neste caso, uma conta é bloqueada após cinco tentativas de login falhadas. Esta política é uma medida de segurança eficaz contra os ataques de força bruta (Moskowitz, J. D., & Barber, M., 2019).

A política de forçar log out é concebida para minimizar o risco de acesso não autorizado quando um utilizador deixa o computador sem vigilância. Esta política encerra automaticamente a sessão do utilizador após um período de inatividade, que neste exemplo é de 15 minutos (Stanek, W. R., 2018).

Para assegurar que todos os sistemas da empresa possuem um software de antivírus instalado e devidamente atualizado temos de criar uma política de antivírus. O software antivírus é um dos mecanismos mais fundamentais de segurança para proteger contra uma ampla gama de ameaças maliciosas, incluindo vírus, worms, trojans, ransomware, entre outros. (Microsoft, 2022)

A política de firewall exige que uma firewall esteja ativa em todos os sistemas. Os firewalls ajudam a proteger a rede e os sistemas da empresa contra os ataques externos,

bloqueando o tráfego indesejado ou potencialmente prejudicial (Tulloch, M., Northrup, T., & Honeycutt, J., 2019).

O UAC (Controlo de Conta de Utilizador) exige a permissão de um administrador para qualquer alteração significativa no sistema, como a instalação de um novo software. Esta política ajuda a prevenir alterações não autorizadas no sistema que podem comprometer a segurança (Moskowitz, J. D., & Barber, M., 2019).

As atualizações automáticas são uma parte essencial de qualquer política de segurança. Esta política exige que todos os sistemas sejam configurados para instalar automaticamente as atualizações de segurança. Manter o software atualizado é uma das formas mais eficazes de proteger a empresa contra novas vulnerabilidades e ameaças (Tulloch, M., Northrup, T., & Honeycutt, J., 2019).

A política de acesso a pastas partilhadas especifica quem pode aceder a quais pastas partilhadas na rede da empresa. As permissões de acesso devem ser estritamente controladas e adequadas ao papel de cada utilizador na organização, de forma a minimizar o risco de acesso não autorizado a dados sensíveis (Stanek, W. R., 2018).

Por último, mas não menos importante, a política de logs de auditoria exigem a gravação de eventos de segurança. Estes logs são cruciais para identificar a fonte de um problema de segurança ou para detetar padrões de comportamento suspeitos (Microsoft, Group Policy for Beginners., 2022).

3.1.3 Detetar

Segundo o NIST, a função detetar, é uma das principais funções de cibersegurança numa empresa. A função detetar é responsável por monitorar logs e realizar testes e atualizações de processos de deteção para identificar anomalias nos computadores e softwares da empresa, bem como entidades e ações não autorizadas nas redes e no ambiente físico. Ao monitorizar logs, a equipa de segurança pode identificar atividades suspeitas, como tentativas de acesso não autorizado, uso indevido de dados ou comportamentos incomuns. Essas anomalias podem ser exploradas para descobrir possíveis vulnerabilidades e agir rapidamente para corrigi-las e prevenir incidentes de segurança maiores.

Além disso, a equipa de cibersegurança deve desenvolver e testar processos e procedimentos para a deteção de entidades e ações não autorizadas. Isso pode incluir a

criação de listas de comportamentos suspeitos, testes de penetração e simulações de ataques informáticos. A equipa deve estar ciente de suas funções e responsabilidades para a deteção e relatórios relacionados, tanto dentro de sua organização quanto para autoridades legais (Mahn, Marron, Quinn, & Topper, 2021).

Em resumo, a função detetar é fundamental para a cibersegurança de uma empresa, pois ajuda a identificar e corrigir possíveis vulnerabilidades e ações maliciosas. É importante que a equipa de segurança informática esteja atualizada e treinada em relação aos processos e procedimentos de deteção, bem como estar atenta a anomalias nos logs e outras fontes de dados para evitar possíveis incidentes de segurança.

Nesta fase, propõe-se a utilização de duas ferramentas para monitorar os logs da empresa: o Nessus e o Nmap. O Nessus tem a capacidade de efetuar *scans* detalhados em sistemas e redes, enquanto o Nmap é uma ferramenta de código aberto que permite a descoberta de dispositivos e serviços numa rede. Além disso, a análise de logs pode fornecer informações cruciais para a segurança da empresa, como potenciais ameaças de cibersegurança ou falhas no sistema. Portanto, é fundamental realizar uma análise detalhada dos logs para garantir a proteção dos dados e sistemas da empresa.

3.1.4 Responder

Um aspeto crucial para garantir uma segurança informática eficaz dentro de uma organização é o desenvolvimento e a manutenção de um plano de resposta. O plano de resposta descreve as etapas que precisam de ser tomadas no caso de um incidente de cibersegurança, desde a identificação do incidente até à contenção, erradicação e recuperação dele. (Mahn, Marron, Quinn, & Topper, 2021)

No entanto, ter um plano de resposta em vigor não é suficiente. É igualmente importante testar e atualizar o plano regularmente para garantir que ele ainda seja relevante e eficaz. É aqui que entra a função de "Responder", que é responsável por certificar que os planos de resposta são testados e atualizados. Testar o plano de resposta ajuda a identificar quaisquer lacunas ou pontos fracos no plano antes que ocorra um incidente real. Também oferece uma oportunidade de treinar os funcionários sobre suas funções e responsabilidades durante um incidente, o que pode aumentar a probabilidade de uma resposta bem-sucedida. (ENISA, 2018)

A atualização do plano de resposta também é crucial, pois as ameaças à cibersegurança estão em constante evolução e o plano de resposta precisa de acompanhar essas mudanças. Por exemplo, se surgirem novos tipos de ameaças informáticas ou se houver mudanças na infraestrutura de TI da organização, o plano de resposta precisa de ser atualizado de acordo. (National Institute of Standards and Technology, 2018)

Portanto, a função de "Responder" desempenha um papel crítico para garantir que a organização esteja preparada para responder com eficácia a incidentes de cibersegurança. Ao certificar que os planos de resposta são testados e atualizados, a função ajuda a minimizar o impacto de incidentes de cibersegurança e a proteger os ativos e a reputação da organização.

Nesta fase, é essencial criar um plano de resposta completo que inclua todo o processo de resposta a um ciberataque. O plano de resposta passa por detalhar todos os passos de resposta a incidentes, de acordo com a Microsoft (2023) são:

- Preparação
- Identificação de ameaças
- Contenção de ameaças
- Eliminação de ameaças
- Recuperação e restauro
- Feedback e refinamento

Antes de qualquer eventual incidente de segurança ocorrer, é de suma importância que as organizações tomem medidas proativas na fase de preparação para minimizar suas vulnerabilidades. Neste estágio, torna-se imperativo para as entidades corporativas efetuar uma rigorosa avaliação de risco, com o objetivo de identificar pontos fracos e, consequentemente, alocar os recursos disponíveis de maneira otimizada.

Este processo abrangente envolve não somente o desenvolvimento, mas também o contínuo aprimoramento de políticas e procedimentos de segurança, além da clara definição de papéis e responsabilidades dentro da organização. Adicionalmente, é crucial manter os sistemas atualizados com o intuito de mitigar os riscos associados. É uma prática comum e altamente recomendada que as organizações revisitem e refinem regularmente esta fase de preparação (Fig.4). Esse ciclo de revisão e melhoria contínua se torna especialmente

relevante à medida que novas lições são aprendidas e as tecnologias subjacentes passam por evoluções. (Microsoft, 2023).

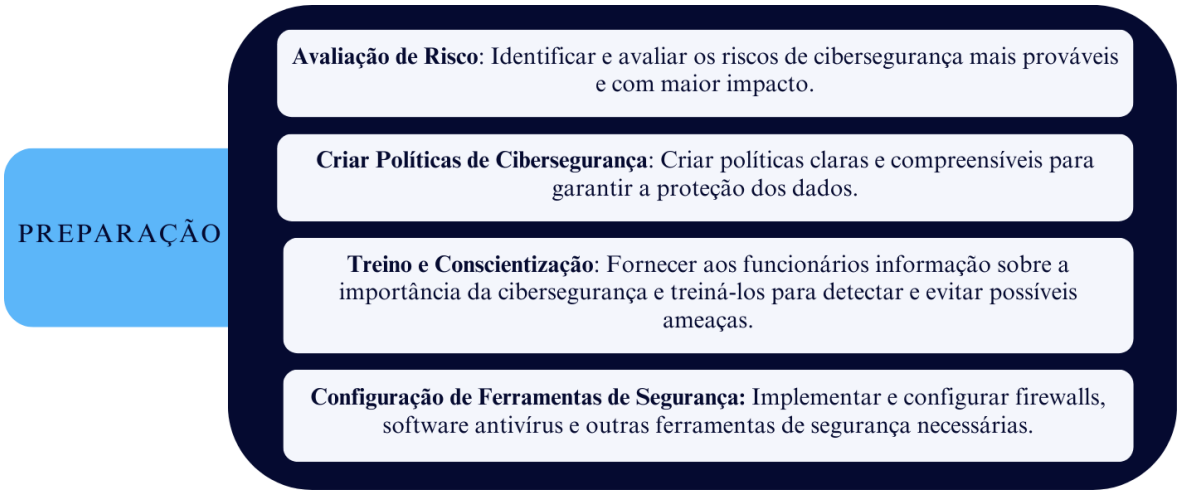


Figura 4 - Fase Responder: Preparação

No processo de identificação de ameaças (Fig.5), as equipas de segurança são responsáveis por avaliar diariamente uma grande quantidade de alertas relacionados a atividades suspeitas. No entanto, muitos desses alertas podem ser falsos positivos ou não necessariamente indicar um incidente de segurança real. Quando um incidente é identificado, a equipa de segurança começa a investigar a raiz do problema, incluindo a origem da falha de segurança, o tipo de ataque que foi realizado e quais eram os objetivos do atacante. Além disso, a equipa precisa informar os envolvidos e comunicar os próximos passos a serem tomados. É importante destacar que a eficácia da equipa de segurança na identificação de incidentes e na comunicação dos resultados pode ter um impacto significativo na capacidade de uma organização para prevenir, detetar e responder a ameaças

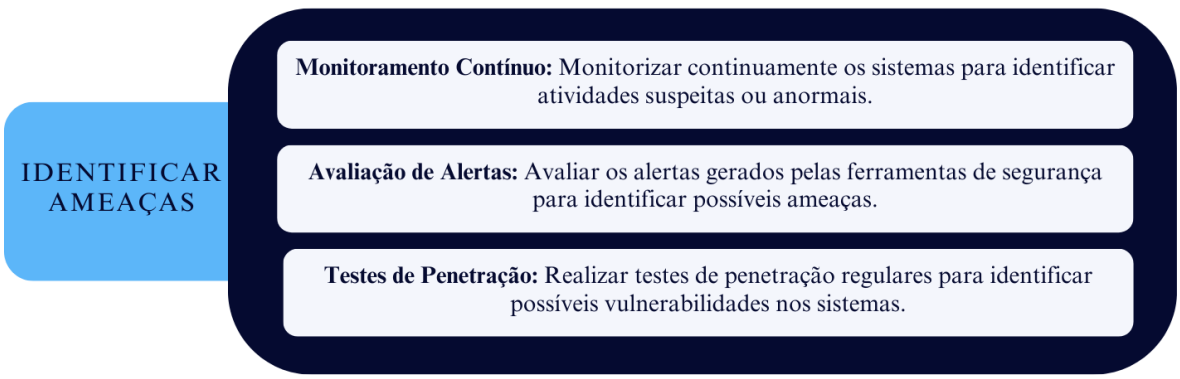


Figura 5 - Fase Responder: Identificação de Ameaças

Uma vez identificada uma ameaça, é fundamental que a equipa de segurança trabalhe rapidamente para conter a ameaça (Fig.6). Quanto mais tempo a ameaça permanecer ativa, maior será o potencial de danos que ela pode causar. Para isso, a equipa de cibersegurança precisa de isolar quaisquer sistemas ou aplicações afetadas das outras redes da empresa, evitando que os atacantes acedam a outras partes da rede. Este processo de contenção de ameaças é crucial para minimizar o impacto de um incidente de segurança e pode ajudar a evitar que a ameaça se espalhe para outros sistemas ou dispositivos (Kim, D. K., Chung, K. H., & Kim, J. H., 2019)

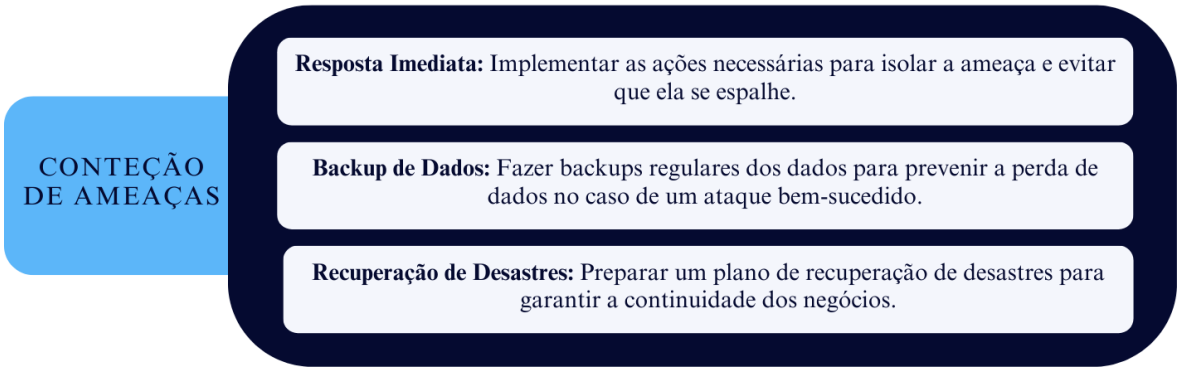


Figura 6 - Fase Responder: Contenção de Ameaças

Depois da equipa de segurança conter a ameaça, o próximo passo é eliminar o atacante e todo o malware dos sistemas e recursos afetados (Fig.7). Esta etapa pode envolver a desativação temporária dos sistemas, a limpeza dos dados infetados e a instalação de atualizações ou patches de segurança para garantir que os sistemas estejam protegidos contra futuros ataques. Durante este processo, a equipa mantém os intervenientes informados sobre o progresso da eliminação de ameaças e as próximas etapas a serem tomadas para garantir que os sistemas sejam totalmente restaurados. O objetivo final é garantir que a empresa esteja segura e protegida contra futuros ataques informáticos (Peltier, T. R., Peltier, J. W., & Blackley, J. A., 2018).

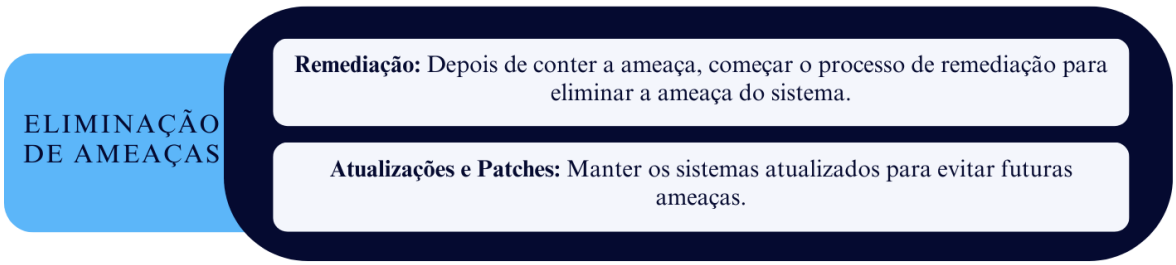


Figura 7 - Fase Responder: Eliminação de Ameaças

A recuperação e restauro dos sistemas e dados afetados (Fig.8) pode levar algumas horas para ser concluído. A equipa tem de realizar uma verificação completa do sistema, reinstalar o software necessário e restaurar dados a partir dos backups. Depois disso, fazem a monitorização cuidadosamente do ambiente para garantir que o atacante não tenha voltado e tomam medidas para reforçar a segurança, se necessário. O objetivo final é trazer a empresa de volta à sua operação normal o mais rápido possível (Doherty, 2018).

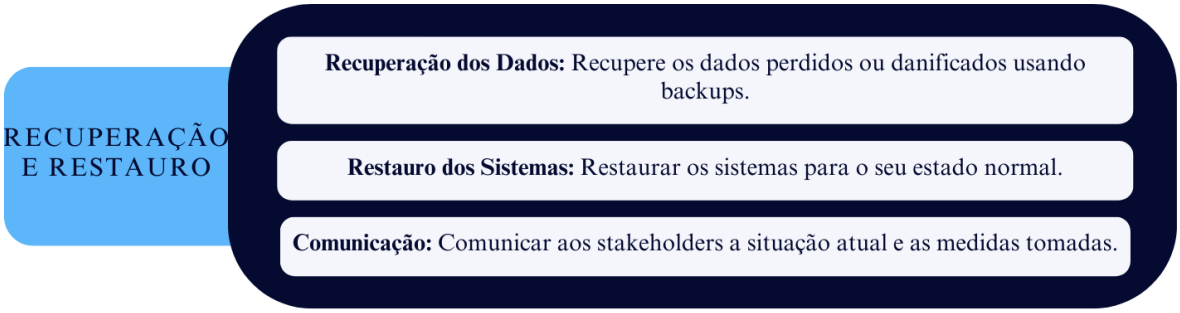


Figura 8 - Fase Responder: Recuperação e Restauro

Por último, a equipa de segurança inspeciona cuidadosamente o que aconteceu e procura identificar pontos que possam ser melhorados no processo (Fig.9). Analisando as etapas do ataque, a equipa procura entender onde é que as defesas da organização falharam e onde podem ser fortalecidas. A equipa usa essas informações para criar planos de ação e aprimorar o processo de resposta a ataques, garantindo que estejam mais bem preparados para lidar com futuras ameaças de segurança (NIST, 2018).

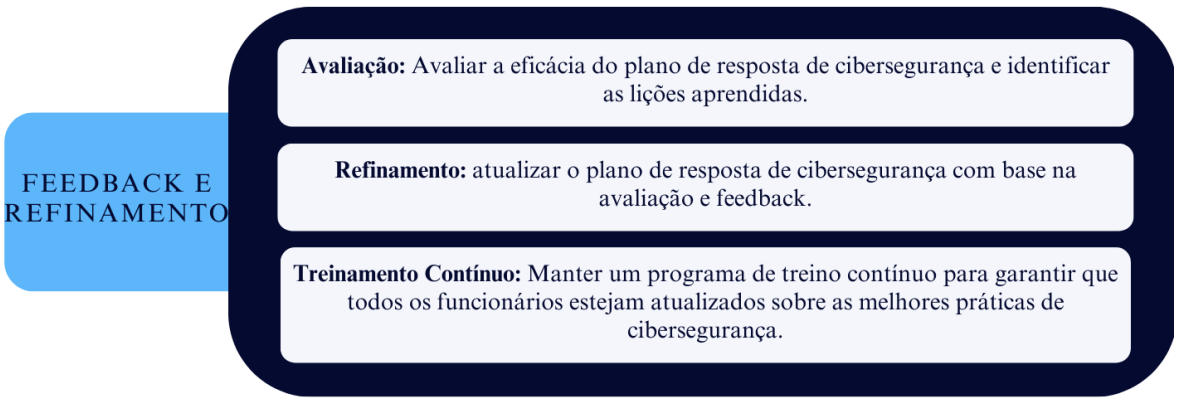


Figura 9 - Fase Responder: Feedback e Refinamento

Na implementação desta fase proteger vai ser realizado um teste de conceito do plano de resposta onde um utilizador recebe um email que, à primeira vista, parece ser legítimo. Este email contém um link que, quando clicado, direciona o utilizador para um site ou recurso malicioso. Imediatamente, um software malicioso é descarregado e instalado no computador do utilizador (Fig.10).

Esse software, em particular, foi projetado para explorar uma vulnerabilidade específica no sistema do utilizador, uma vulnerabilidade que ainda não foi corrigida ou para a qual não existe um patch de segurança. Ao explorar essa falha, o atacante consegue ter acesso e copiar dados sensíveis do computador do cliente. Estes dados, que podem incluir informações pessoais, financeiras ou quaisquer outros detalhes privados, são então transferidos para o computador ou servidor do atacante. Em seguida, o atacante publica ou disponibiliza esses dados na internet, seja para venda, chantagem ou simplesmente por maldade.

A presença destes dados na web é eventualmente detetada por especialistas em segurança ou pelas próprias vítimas, levando a uma reação e resposta ao ataque, com esforços para mitigar os danos e identificar os responsáveis.

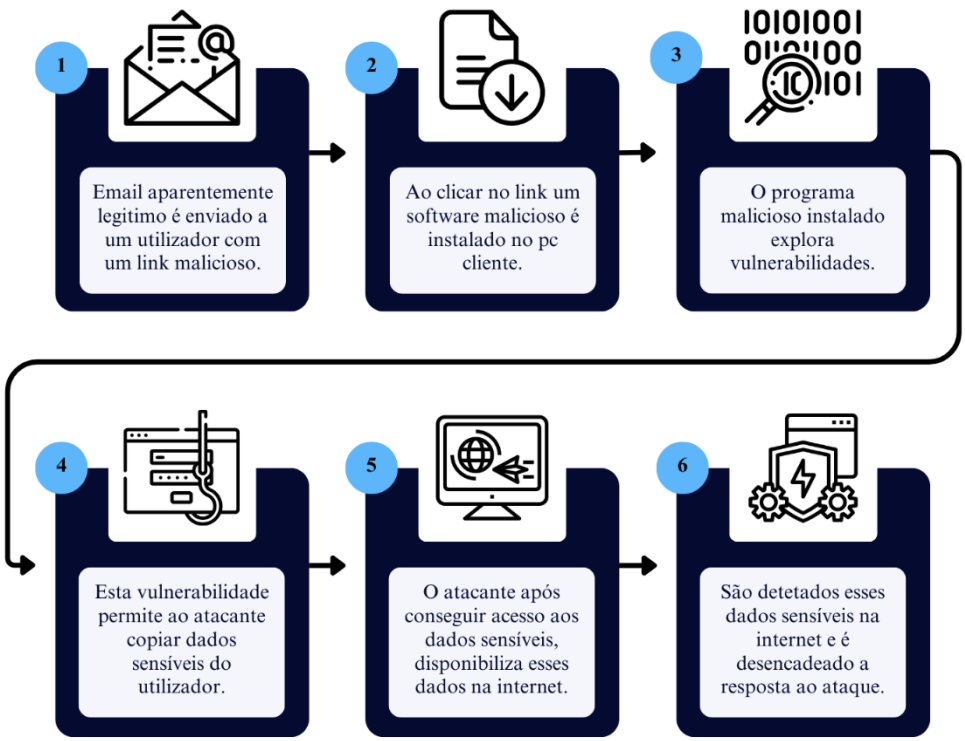


Figura 10 - Teste de conceito do plano de resposta

3.1.5 Recuperar

No contexto da cibersegurança, a função recuperar também é crítica, especialmente após uma violação de dados ou outro incidente de segurança. Durante o processo de recuperação, é essencial comunicar com as partes interessadas internas e externas para mantê-las informadas sobre a situação e quaisquer medidas tomadas para mitigar o impacto do incidente (Mahn, Marron, Quinn, & Topper, 2021).

Internamente, os funcionários devem ser informados sobre quaisquer alterações nos protocolos ou procedimentos de segurança e instruídos sobre as melhores práticas para prevenir futuros incidentes. As partes interessadas externas, como clientes e parceiros, também devem ser mantidas informadas sobre o incidente, incluindo quaisquer riscos ou impactos potenciais em seus dados ou operações. Além da comunicação, a gestão das relações-públicas e da reputação da empresa também é essencial após um incidente de cibersegurança. As empresas devem agir rapidamente para lidar com qualquer publicidade negativa e garantir aos clientes que seus dados estão seguros. Ao ser transparente sobre o ataque e tomar medidas rápidas para mitigar o impacto, as empresas podem ajudar a reconstruir a confiança dos clientes e proteger sua reputação (Doherty, 2018).

No geral, os princípios de gestão de comunicação e reputação são tão críticos no contexto dos esforços de recuperação de segurança informática quanto nas outras áreas de negócios. A comunicação eficaz e a gestão da reputação podem ajudar a minimizar o impacto de um incidente de segurança, manter a confiança do cliente e proteger a marca e a reputação de uma empresa (ENISA, 2018).

Na sequência de um ataque informático, a empresa deve seguir várias etapas para uma recuperação eficaz (Fig.11), conforme delineado por (Checkpoint, 2023):

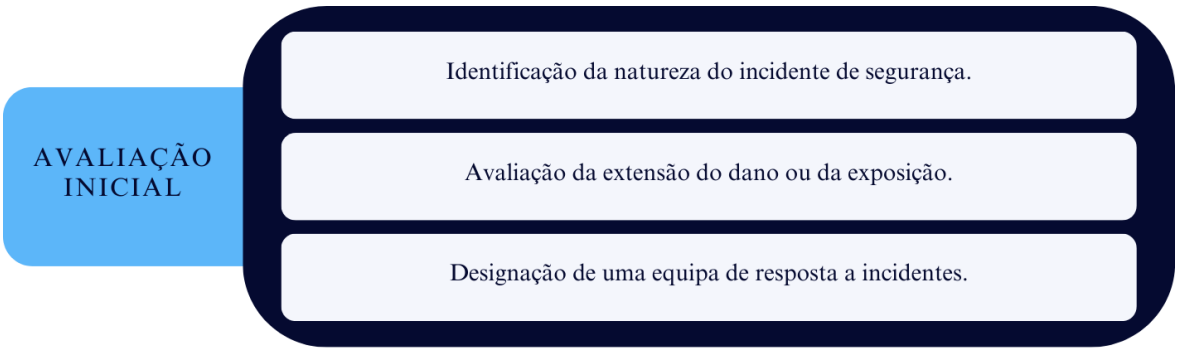


Figura 11 - Fase Recuperar: Avaliação Inicial

Manter a continuidade dos negócios dada a potencial duração da recuperação completa após um incidente de cibersegurança e o custo associado a uma paralisação, é crucial ter estratégias de continuidade de negócios incorporadas no plano de recuperação (Fig.12).

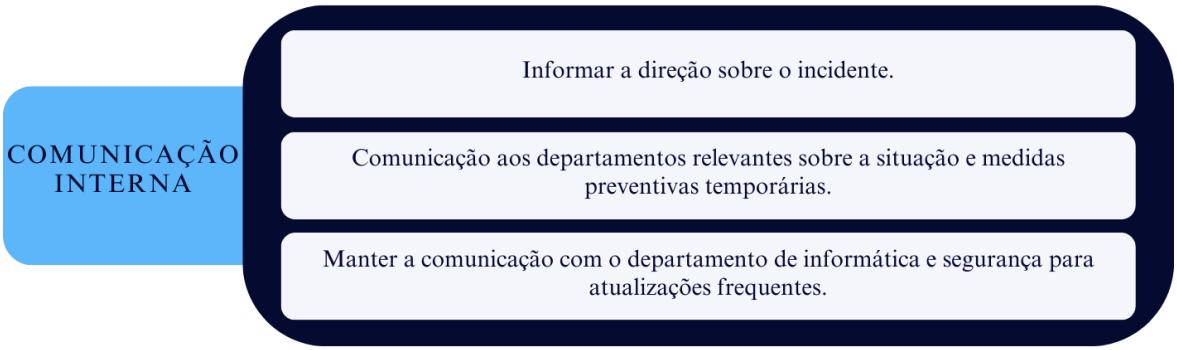


Figura 12 - Fase Recuperar: Comunicação Interna

Proteger dados confidenciais, sejam eles corporativos ou de clientes, podem aumentar drasticamente a gravidade e o custo de um incidente de cibersegurança. A proteção desses dados durante o incidente é fundamental para a segurança da empresa e dos seus clientes (Fig.13).

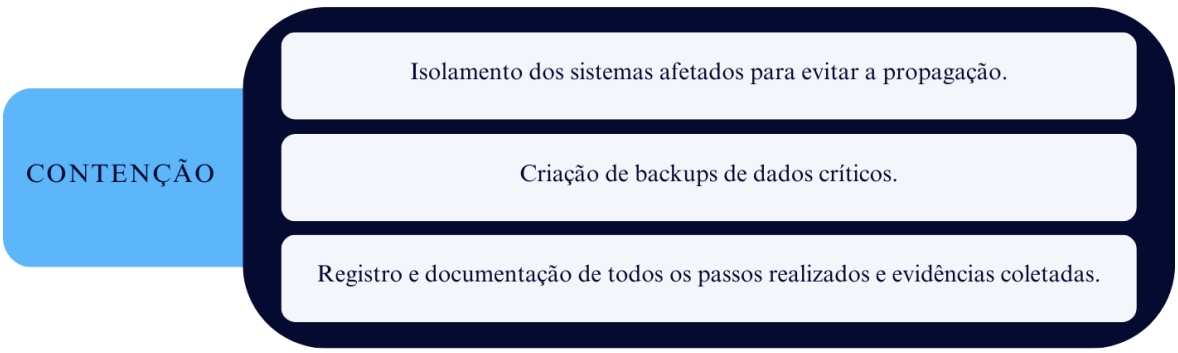


Figura 13 - Fase Recuperar: Contenção

dispendiosos e, sem uma gestão adequada, podem até levar uma empresa à falência. E essencial que os planos de recuperação de desastres incluam estratégias para minimizar os danos e perdas, como a manutenção das operações, proteção de ativos críticos e contenção do incidente (Fig.14 e 15).

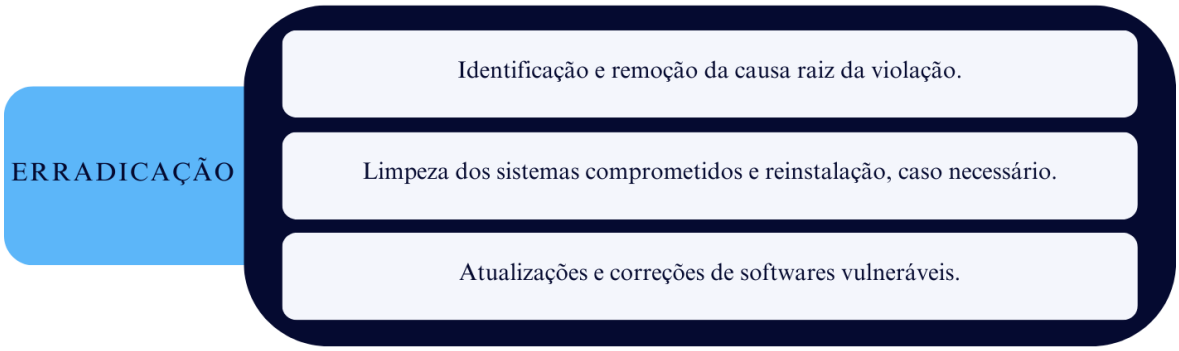


Figura 14 - Fase Recuperar: Contenção

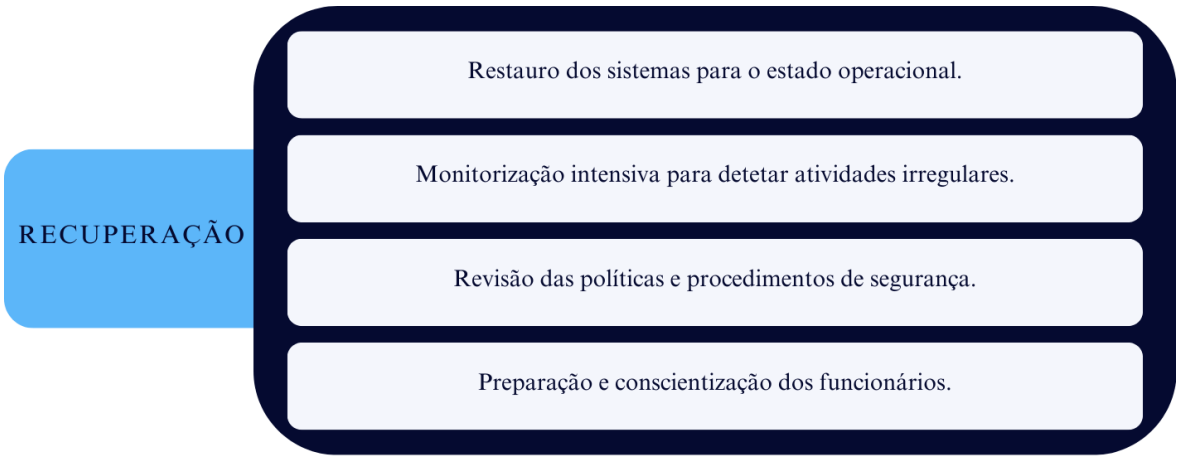


Figura 15 - Fase Recuperar: Recuperação

Comunicar com os Stakeholders é uma fase muito importante pois a ocorrência de um incidente de cibersegurança exige que as partes interessadas, tanto internas como externas à organização (como a equipa de resposta a incidentes, liderança, reguladores e clientes) sejam informadas adequadamente. Definir canais de comunicação claros e eficientes é crucial para uma gestão de incidentes efetiva e para cumprir com os prazos legais e regulatórios (Fig.16).

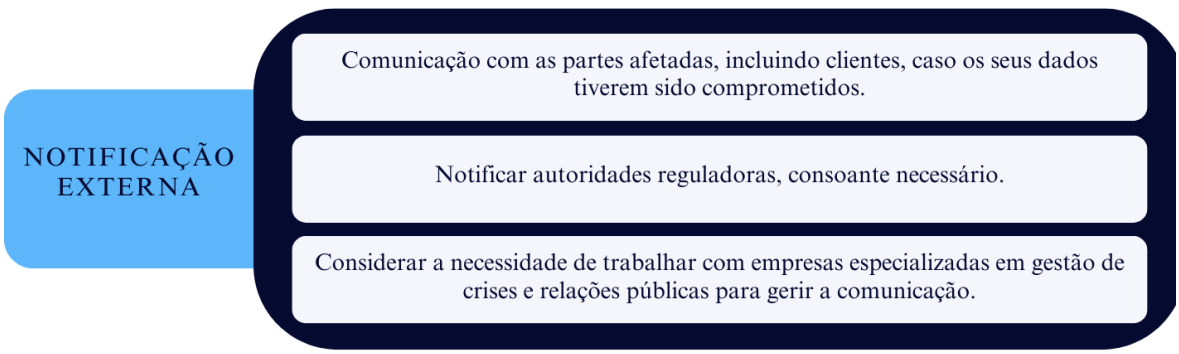


Figura 16 - Fase Recuperar: Notificação Externa

O Retorno à Normalidade é o objetivo final de qualquer plano de recuperação. O plano de recuperação de desastres informáticos deve detalhar o processo de transição da continuidade dos negócios até a total recuperação (Fig.17 e 18).

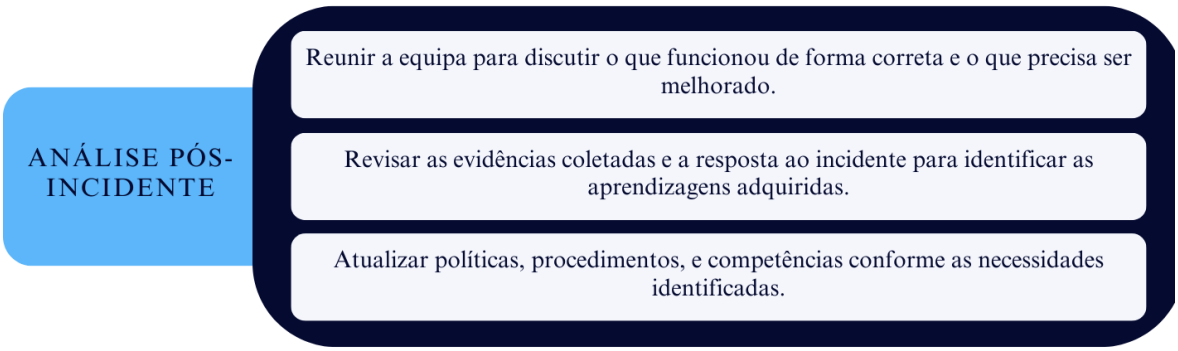


Figura 17 - Fase Recuperar: Análise Pós-incidente

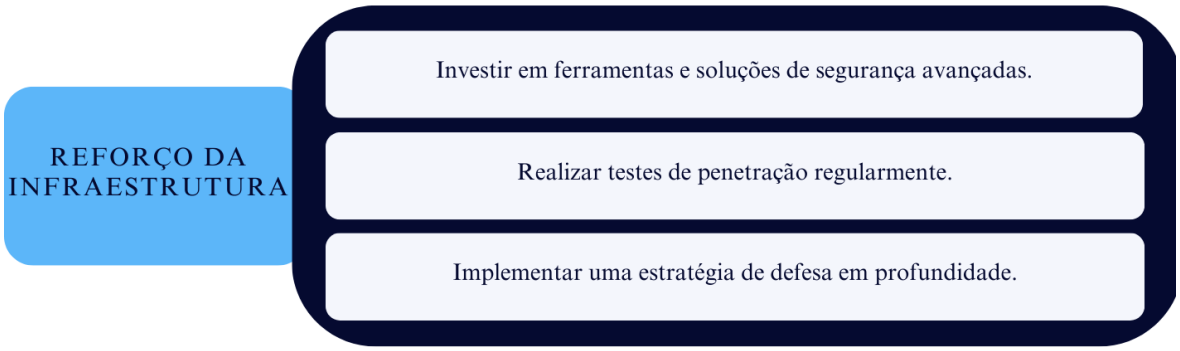


Figura 18 - Fase Recuperar: Reforço da Infraestrutura

Aprendizagem e Aperfeiçoamento, ao longo de todo o processo de recuperação de desastres, a equipa deve manter um registo detalhado de todas as suas ações, informações sobre o incidente e como ele foi gerido. Esses registos e métricas podem ser usados retrospetivamente para melhorar as estratégias de prevenção de acidentes e agilizar os procedimentos de recuperação futuros (Fig.19).

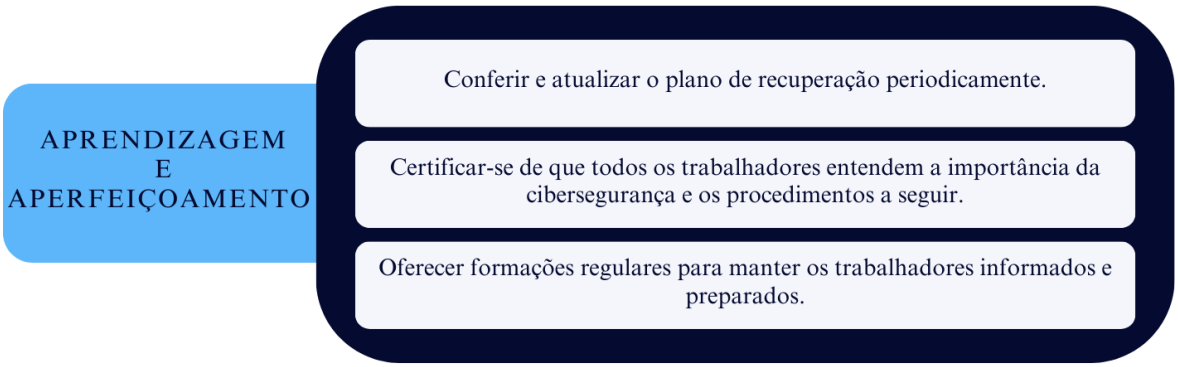


Figura 19 - Fase Recuperar: Aprendizagem e Aperfeiçoamento

4 IMPLEMENTAÇÃO

Neste capítulo serão expostos e detalhadamente analisados os resultados que emergiram de todas as etapas e fases investigativas delineadas na metodologia.

A análise abordará não só os processos operacionais e os procedimentos que são indispensáveis para estabelecer e manter um nível adequado de cibersegurança nas organizações, mas também os padrões de comportamento, atitudes e práticas tanto a nível individual como organizacional que podem exercer uma influência significativa, seja ela positiva ou negativa, na eficácia das medidas de segurança implementadas.

4.1 Fase Identificar

4.1.1 Cenário

A principal proposta deste estudo centra-se na elaboração e implementação de um questionário meticulosamente concebido, destinado especificamente às empresas, com o intuito de permitir que estas realizem uma avaliação autónoma e precisa do seu nível de preparação e maturidade em relação à cibersegurança. Este instrumento de pesquisa, que consta de um total de 16 perguntas criteriosamente elaboradas, foi desenvolvido e disponibilizado através da plataforma Microsoft Forms.

O principal objetivo desta abordagem é tornar o processo de autoavaliação tão intuitivo e descomplicado quanto possível, sem comprometer a sua eficácia em fornecer insights valiosos. Por meio deste questionário, pretende-se identificar de forma clara e precisa quaisquer lacunas, vulnerabilidades ou áreas que possam necessitar de intervenção imediata ou de um aprimoramento contínuo nos procedimentos e políticas de cibersegurança da organização em questão.

Nesta fase inicial, designada como 'Identificar', o questionário será aplicado numa Pequena e Média Empresa fictícia. As respostas obtidas servirão não apenas como um caso de estudo, mas também como um ponto de partida para a implementação das fases subsequentes deste projeto. Através da análise dos resultados, poderemos ajustar o questionário para que seja mais eficaz e, ao mesmo tempo, elaborar estratégias concretas para abordar os pontos fracos identificados.

4.1.2 Perguntas

- Questão 1: A empresa tem uma política de cibersegurança formal e documentada?

- Questão 2: Esta política é comunicada a todos os funcionários quando são contratados e regularmente depois disso?

- Questão 3: Existem protocolos definidos para manter a política de cibersegurança atualizada?

- Questão 4: Quais são as principais ameaças de cibersegurança que a empresa considera como parte da sua avaliação de riscos?

- Questão 5: Como é que a empresa gere as funções de cibersegurança?

- Questão 6: Existe uma política de monitoramento da rede e dos sistemas para detetar possíveis violações de cibersegurança?

- Questão 7: Existem procedimentos definidos em caso de violação da cibersegurança?

- Questão 8: Existe uma política de backup e recuperação de dados em caso de um incidente de cibersegurança?

- Questão 9: A empresa realiza auditorias regulares às políticas e práticas de cibersegurança?

- Questão 10: Existe um plano de formação regular sobre cibersegurança para todos os funcionários?

- Questão 11: A empresa utiliza algum tipo de software ou ferramenta para proteger os sistemas contra ameaças de cibersegurança?

- Questão 12: **(Se a resposta à questão 11 for positiva)** Se sim, qual?

- Questão 13: Existem políticas em vigor para o uso seguro de dispositivos móveis e trabalho remoto?

- Questão 14: A empresa utiliza algum tipo de sistema de autenticação de dois fatores para o acesso aos sistemas e redes?

- Questão 15: A empresa possui alguma política de password para todos os utilizadores da rede?

- Questão 16: A sua empresa aplica as regras RGPD para lidar com os dados dos clientes e tem um encarregado para a proteção de dados devidamente registado na comissão nacional de proteção de dados?

4.1.3 Resultados da avaliação do estado da cibersegurança numa visão técnica

Após uma avaliação meticulosa das respostas que a empresa forneceu ao questionário especializado em cibersegurança, tornaram-se evidentes várias falhas consideráveis na forma como a organização aborda a segurança informática. O facto de que as respostas para as três primeiras perguntas foram negativas sugere fortemente que, mesmo que haja algumas medidas rudimentares de segurança em prática, estas não se encontram formalmente estruturadas, devidamente documentadas ou disseminadas de forma eficiente entre os colaboradores da empresa.

Ao nível das ameaças informáticas, a organização identificou o Phishing e o Malware como os maiores perigos potenciais para as suas operações. No entanto, embora conte com uma equipa externa de Resposta a Incidentes de Segurança de Computadores (SCIRT), a falta de políticas de segurança formalmente estabelecidas e documentadas pode comprometer gravemente a eficácia deste mecanismo de resposta.

No que diz respeito à gestão de dados, a empresa assinalou que possui políticas específicas para backups e procedimentos de recuperação de dados, o que representa um aspeto positivo. Contudo, as respostas dadas às perguntas 9 e 10 revelaram que não existem auditorias de segurança realizadas de forma regular, nem um plano estruturado de formação em cibersegurança para os seus colaboradores.

A empresa também indicou o uso exclusivo de software antivírus e de uma Rede Privada Virtual (VPN) para proteção dos seus sistemas. Embora isto possa ser considerado um avanço positivo, fica aquém do que seria necessário para assegurar uma proteção verdadeiramente abrangente.

No contexto da rede da empresa, a ausência de um sistema de autenticação de dois fatores e de uma política bem definida de gestão de palavras-passe representa uma vulnerabilidade adicional, incrementando o risco de serem alvo de ataques informáticos bem-sucedidos.

Por fim, a empresa fez menção à sua conformidade com o Regulamento Geral de Proteção de Dados (RGPD) no que respeita à gestão de dados de clientes. Embora isso seja

indiscutivelmente um ponto forte, é imperativo que este aspeto seja integrado numa estratégia de cibersegurança mais abrangente e robusta para a organização como um todo.

4.1.4 Conclusão

A análise meticulosa conduzida por meio do questionário de cibersegurança aponta para uma falha significativa na forma como a Pequena e Média Empresa (PME) em estudo tem vindo a abordar esta área crucial. Este facto torna-se ainda mais alarmante quando situado no contexto contemporâneo, onde a cibersegurança não é apenas uma questão de conveniência, mas sim um elemento fundamental para garantir a sustentabilidade e integridade das operações empresariais. O motivo para esta preocupação acentuada reside, em parte, na observação de que o cenário de ameaças cibernéticas atuais tem mostrado um aumento expressivo em ataques que têm como alvo as PME's, frequentemente vistas como presas mais fáceis em comparação com grandes organizações que, regra geral, dispõem de recursos mais robustos e de sistemas de defesa mais sofisticados.

A próxima fase deste estudo focar-se-á, portanto, na implementação e avaliação de uma série de estratégias de mitigação de riscos. Isto incluirá a formulação de 'Group Policies' para estruturar e padronizar as práticas de segurança dentro da organização. Além disso, serão exploradas técnicas avançadas de cibersegurança como por exemplo a utilização e configuração da ferramenta Nessus para analisar as vulnerabilidades das máquinas (Fig.20).

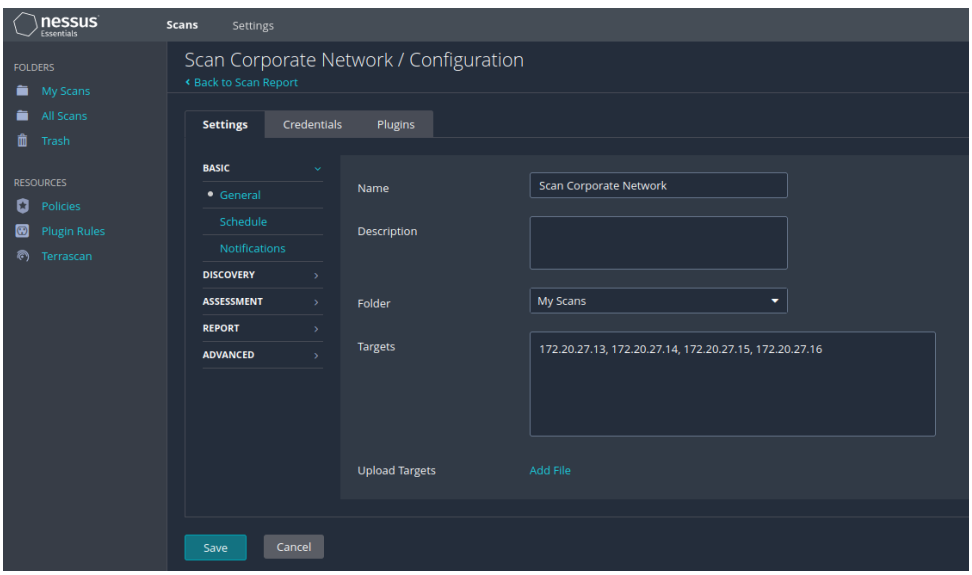


Figura 20 - Configuração do Nessus

Adicionalmente, está planeada a implementação de software altamente especializado destinado à monitorização contínua e em tempo real do ambiente de rede da organização.

Este conjunto de ferramentas informáticas não será útil apenas para a identificação e deteção imediata de anomalias que possam indicar vulnerabilidades no sistema ou ataques cibernéticos em curso. Ele vai além, permitindo uma atuação proativa na prevenção de eventuais brechas de segurança ou intrusões maliciosas que possam comprometer a integridade dos dados e das operações da empresa.

O alvo principal deste ambicioso plano de ação é consolidar uma estratégia de cibersegurança que seja ao mesmo tempo abrangente e profundamente integrada às práticas operacionais da PME em estudo. Através deste enfoque holístico, pretende-se robustecer a resiliência da organização face a um leque variado de ameaças informáticas. Este fortalecimento terá implicações diretas na proteção de ativos críticos para o negócio e, em última análise, contribuirá para a garantia de um ambiente empresarial que seja não apenas mais seguro, mas também mais eficaz e confiável nas suas operações.

4.2 Fase Proteger

No contexto das políticas de grupo, conforme descritas na metodologia adotada, é imperativo que as empresas compreendam a importância da sua implementação.

Considerando especificamente as políticas relativas a palavras-passe, a segurança varia significativamente dependendo dos requisitos estabelecidos. Por exemplo, na figura 21 pode-se observar uma palavra-passe convencional pode ser descoberta em aproximadamente um segundo.

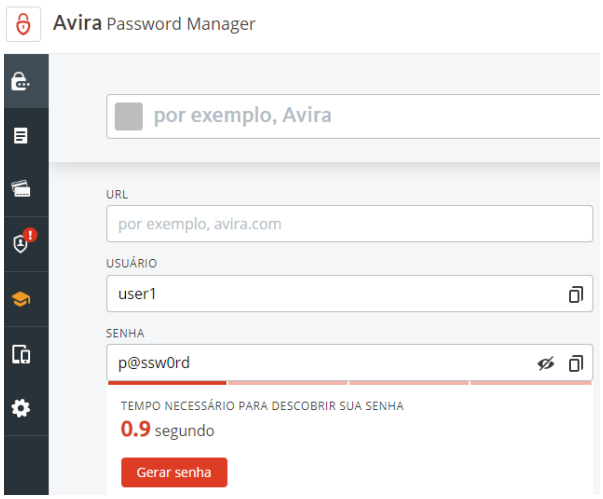


Figura 21 - Password Fraca

Conforme se apresenta na figura 22, uma palavra-passe que atenda aos critérios estabelecidos pelas políticas da empresa, tais como um número mínimo de caracteres e a inclusão de caracteres especiais, poderá resistir a tentativas de descoberta durante aproximadamente 3 mil anos. Este contraste é crucial de estabelecer e cumprir rigorosamente as políticas de segurança no ambiente empresarial.

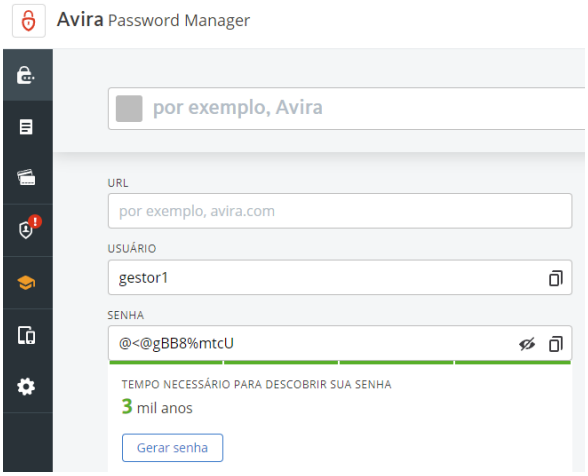


Figura 22 - Password Forte

Uma política de grupo frequentemente implementada também é o bloqueio automático de contas de utilizadores após um determinado número de tentativas de login falhadas como demonstrado na figura 23. Esta medida visa proteger os sistemas contra ataques de força bruta e tentativas não autorizadas de acesso, elevando o nível de segurança dos dados e recursos da empresa. Ao limitar o número de tentativas inválidas, a política reduz significativamente o risco de invasão, assegurando a integridade e confidencialidade das informações corporativas.

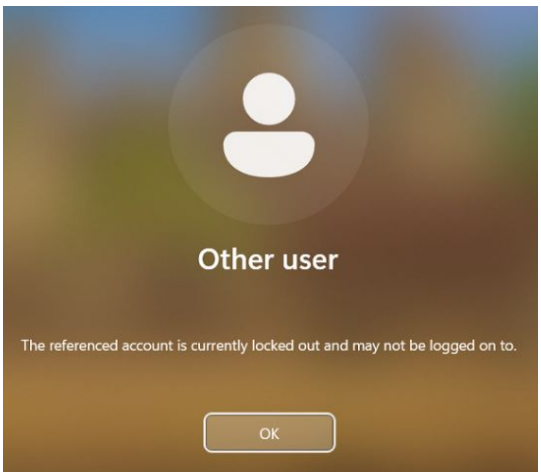
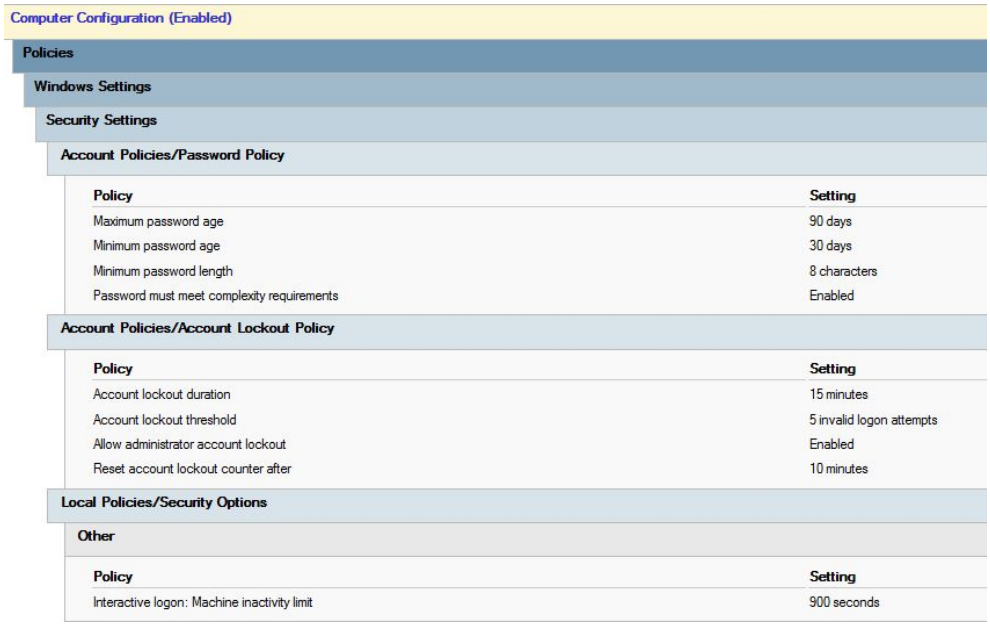


Figura 23 - Utilizador Bloqueado

Como resumo destas últimas configurações, o objetivo é que seja apresentado um gráfico como o apresentado na figura 24, estabelecendo um resumo das Group Policies que acabamos de fazer e se for necessário realizar alguma alteração nas mesmas.



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Maximum password age	90 days
Minimum password age	30 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Allow administrator account lockout	Enabled
Reset account lockout counter after	10 minutes

Local Policies/Security Options

Other

Policy	Setting
Interactive logon: Machine inactivity limit	900 seconds

Figura 24 - Resumos das Políticas de password e de conta

Na esfera da cibersegurança empresarial, as políticas de grupo relacionadas com software antivírus e configurações de firewall desempenham um papel crucial e inegável.

À medida que o cenário de ameaças informáticas continua a evoluir, tornando-se cada vez mais sofisticado e intrincado, as empresas estão a adotar uma abordagem proativa na implementação destas políticas de segurança. O objetivo principal é garantir que todos os dispositivos que estabelecem uma ligação à rede empresarial estejam equipados com soluções antivírus sempre atualizadas e firewalls meticulosamente configuradas, conforme exemplificado nas figuras 25 e 26.

Estas medidas preventivas não são apenas fundamentais para combater as ameaças emergentes como malware, ransomware e ataques de phishing, mas também desempenham um papel vital no controlo e monitorização do tráfego de rede. Ao fazê-lo, as empresas conseguem assegurar que apenas as comunicações legítimas e autorizadas são permitidas, minimizando assim o risco de exposição a vulnerabilidades.

Desta forma, através da implementação rigorosa destas políticas de grupo, as organizações não só reforçam a sua postura global de segurança como também tomam

medidas significativas para proteger os seus ativos digitais valiosos contra comprometimentos.

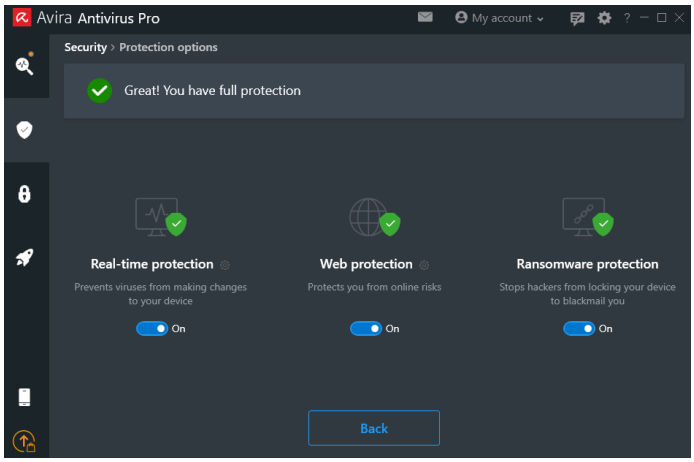


Figura 25 - Avira Antivirus Pro

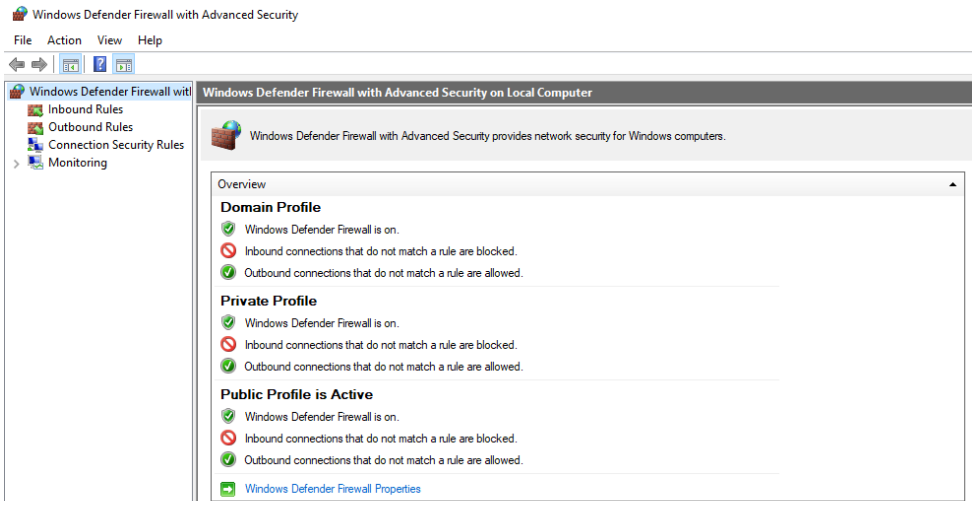


Figura 26 - Firewall

Adicionalmente, a correta gestão e atualização contínua destas ferramentas, aliada a uma formação adequada dos colaboradores, permite não só identificar, mas também prevenir possíveis vulnerabilidades, reforçando a resiliência da empresa face a potenciais ataques informáticos.

No caso da política de grupo referente ao UAC (Controle de Conta de Utilizador), esta política tem como principal objetivo elevar o nível de segurança, solicitando a confirmação ou credenciais do utilizador sempre que uma ação que requeira permissões elevadas for detetada, como a instalação de software ou alterações em configurações do sistema. Ao restringir automaticamente o acesso a funções e dados sensíveis, o UAC assegura que atividades potencialmente perigosas sejam realizadas conscientemente e por indivíduos

autorizados. Esta abordagem contribui para a mitigação de riscos de comprometimento, tanto por ações inadvertidas internas quanto por ameaças externas. Por exemplo na figura 27 podemos ver um utilizador a tentar realizar uma ação que não está habilitado numa pasta da empresa.

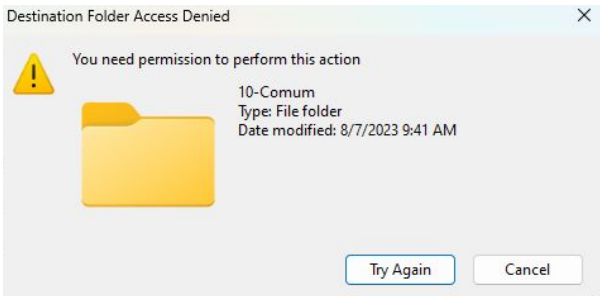


Figura 27 - Utilizador sem acesso

A política de grupo relativa ao acesso a pastas partilhadas (Fig.28) é a política que visa regular e controlar o acesso a diretórios de rede, garantindo que apenas colaboradores autorizados possam aceder, ler ou modificar os dados contidos nesses diretórios. Ao estabelecer restrições e níveis de permissão diferenciados, a empresa protege-se contra fugas de informação, acessos indevidos e potenciais comprometimentos de dados. Este tipo de política é fundamental para manter a integridade, confidencialidade e disponibilidade das informações em ambientes empresariais.

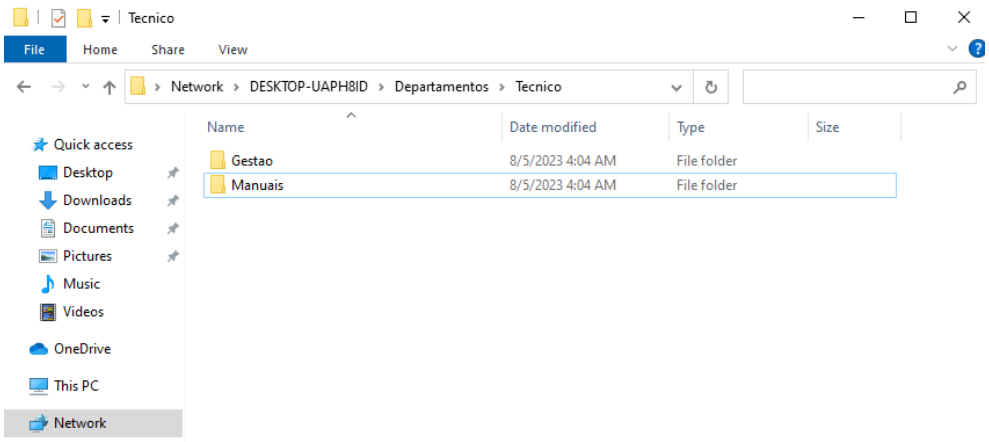


Figura 28 - Pastas na rede da empresa

No presente estudo, foram analisadas duas pastas localizadas na infraestrutura de rede da empresa, como ilustrado nas Figuras 29 e 30. Estas pastas, denominadas "gestão" e "manuais", possuem diferentes níveis de acesso atribuídos ao perfil do gestor, do técnico e dos administradores. É conferido ao gestor um acesso especializado, enquanto o técnico

detém permissões para ler, escrever e executar e os administradores tem o controlo total na pasta. Este exemplo demonstra a granularidade e especificidade com que os direitos de acesso podem ser configurados, de modo a atender às necessidades e hierarquias organizacionais.

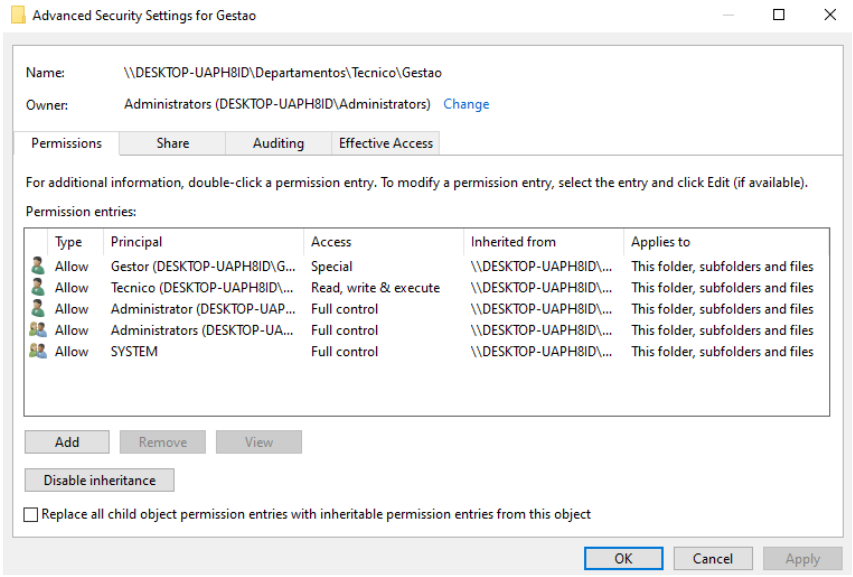


Figura 29 - Pasta Gestão

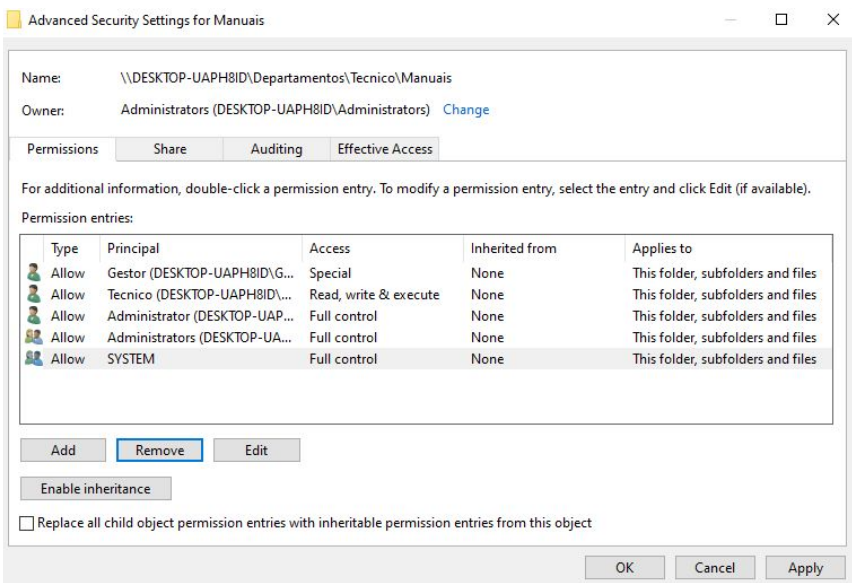


Figura 30 - Pasta Manuais

A política de grupo relativa a Logs de Auditoria assume uma importância extrema. Esta política determina que todas as atividades significativas realizadas nos sistemas da empresa sejam registadas e armazenadas de forma segura para uma análise posterior.

O objetivo primordial é monitorizar, em tempo real ou mais tarde, quaisquer ações que possam comprometer a integridade, confidencialidade ou disponibilidade das informações e recursos da empresa. Como ilustrado numa figura 31, sempre que um acesso é falhado, é gerado um evento que indica a tentativa de logon mal sucedida, sendo esta informação registada no computador onde a tentativa de acesso ocorreu.

Ao adotar uma estratégia que envolve a manutenção de um registo pormenorizado de todas as atividades relacionadas com acessos, modificações e demais operações dentro da infraestrutura de TI, a empresa não apenas aumenta a sua capacidade de detetar ameaças potenciais em estágios iniciais. Este sistema de registo serve também como uma ferramenta de investigação inestimável, sendo fundamental para o processo de atribuição de responsabilidades em casos de incidentes de segurança, sejam eles ataques, brechas ou outras formas de comprometimento dos sistemas.

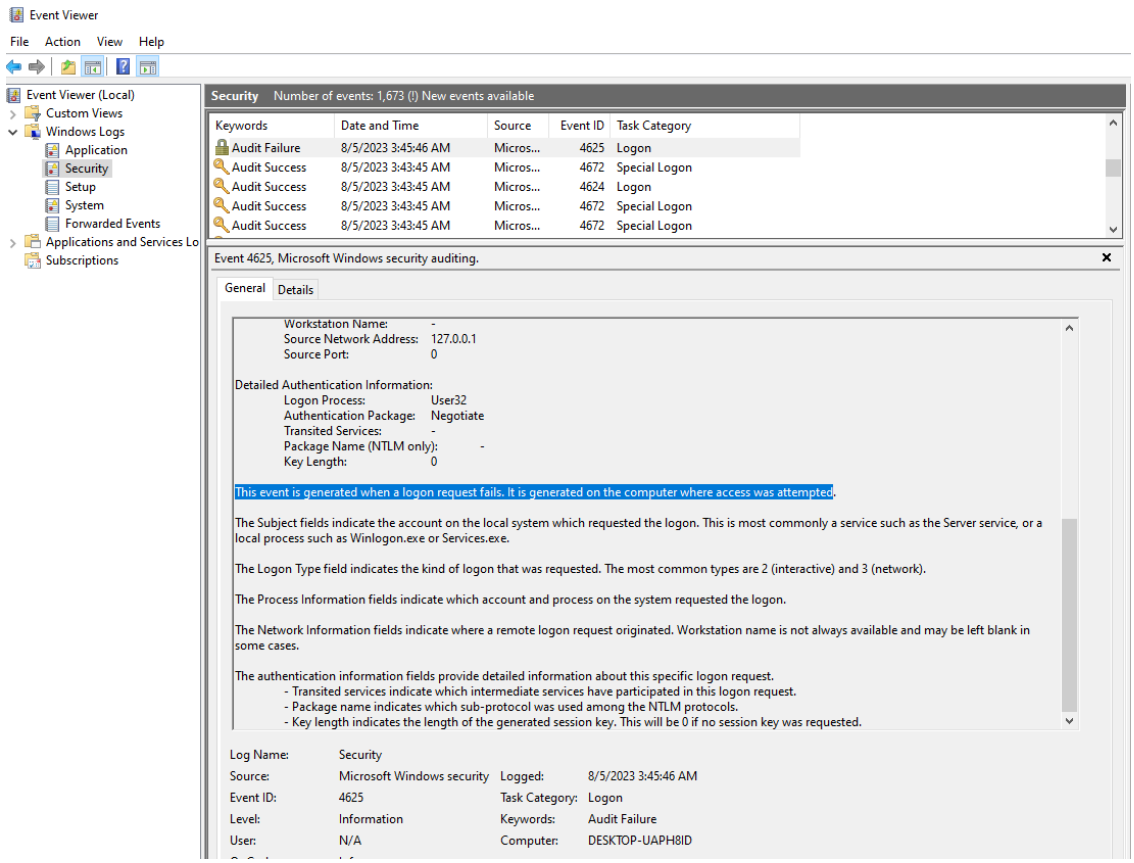


Figura 31 - Tentativa de Logon falhada

4.3

4.4 Fase Detetar

Nesta fase, foi estabelecido um ambiente virtual utilizando a plataforma VMware para emular um cenário de rede realista e controlado. Este ambiente é composto por cinco máquinas virtuais (VMs) distintas que refletem diferentes sistemas operativos e configurações, tornando-se assim um modelo representativo das variações comuns encontradas em ambientes corporativos.

As máquinas virtuais configuradas incluem:

- Windows XP: Este sistema operativo, embora obsoleto, ainda é encontrado em certos ambientes devido a necessidades específicas de software ou hardware. É importante avaliar a seu segurança dado o seu potencial para ser um ponto vulnerável numa rede.
- Windows 10 Home: Representa uma versão comum do Windows para utilizadores domésticos e pode ser encontrada em ambientes de trabalho flexíveis ou em empresas que não necessitam das funcionalidades empresariais adicionais do Windows 10 Pro.
- Windows 10 Pro: Uma versão mais robusta do Windows, com funcionalidades avançadas de segurança e gestão, frequentemente usada em ambientes corporativos.
- Kali Linux: Este é um sistema operativo baseado em Linux, amplamente reconhecido pela sua vasta coleção de ferramentas de testes de penetração e auditoria de segurança. No nosso cenário, ele funciona como a máquina principal para monitorização e avaliação da rede.
- Ubuntu Linux: Uma das distribuições Linux mais populares, utilizada tanto por particulares como por empresas, serve como um representante comum dos ambientes Linux.

O Kali Linux, particularmente, desempenha um papel crucial neste ambiente. Ele está equipado com as ferramentas Nessus e o Nmap. O Nessus é um scanner de vulnerabilidades amplamente utilizado que permite identificar potenciais pontos fracos nas VMs. Já o Nmap, é uma ferramenta para exploração de rede e auditoria de segurança, que permite avaliar a topologia da rede virtual e identificar portas abertas e serviços a correr nas máquinas alvo.

Ao usar estas ferramentas no Kali Linux, conduz a uma série de scans e testes nas outras máquinas virtuais para compreender o seu estado de segurança e identificar possíveis vulnerabilidades.

No processo inicial de mapeamento da rede empresarial, é optado por utilizar a função *netdiscovery* (Fig.32), uma técnica crucial quando se pretende identificar e catalogar todos os dispositivos conectados numa determinada rede. O objetivo deste procedimento é obter uma representação clara dos endereços IP ativos e, assim, estabelecer uma base para análises de segurança subsequentes.

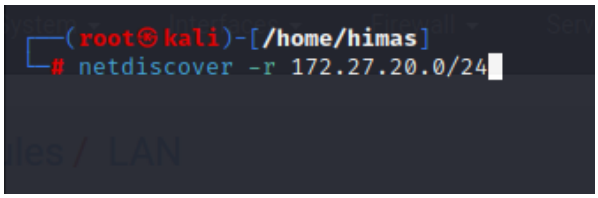


Figura 32 - Netdiscovery

Após a execução da função *netdiscovery*, obteve-se uma lista detalhada dos endereços IP em uso na rede da empresa. Estes resultados fornecem uma visão inicial da estrutura e composição da rede, e serão essenciais para etapas subsequentes da análise. Os detalhes específicos desta descoberta, incluindo os endereços IP identificados e outras informações associadas, estão apresentados na Figura 33.

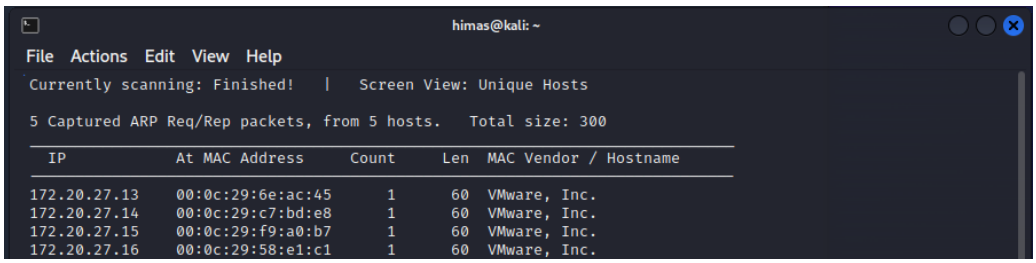


Figura 33 - Resultados Netdiscovery

No âmbito da análise de segurança das máquinas virtuais estabelecidas, foi utilizado o Nmap, uma ferramenta conhecida na área de segurança da informação, para realizar um mapeamento detalhado dos ambientes virtuais. O objetivo principal deste scan foi identificar as portas ativas e obter informações adicionais sobre os serviços em execução e os possíveis pontos vulneráveis de cada sistema.

Ao conduzir o scan, foi procurado não apenas portas abertas, mas também configurações inseguras ou desatualizadas, bem como serviços desnecessários que poderiam ser explorados por atacantes (Fig.34 a 37). O Nmap oferece uma visão clara dessas configurações através das suas opções de scan e scripts especializados.

Com base nos resultados do scan realizado com o Nmap da figura 34 à Figura 27, pode-se observar numa primeira visão que host estão a usar SO's legacy e as portas abertas para saber que serviços podem estar abertos para exploração de vulnerabilidades.

Consegue-se observar que na Figura 34 a máquina Linux Ubuntu está mais segura demonstrado um scan sem erros e sem portas abertas.

```
┌──(root㉿kali)-[/home/himas]
└─# nmap -sV -A -Pn 172.20.27.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 09:32 WEST
Nmap scan report for 172.20.27.15
Host is up (0.00021s latency).
All 1000 scanned ports on 172.20.27.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:F9:A0:B7 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.21 ms 172.20.27.15

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.77 seconds
```

Figura 34 – Nmap Ubuntu

Relativamente ao Windows 10 Pro (Fig.35), a máquina tem uma porta aberta com dois serviços, mas sem informação de qualquer perigo.

```
┌──(root㉿kali)-[/home/himas]
└─# nmap -sV -A -Pn 172.20.27.16
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 11:27 WEST
Nmap scan report for 172.20.27.16
Host is up (0.00028s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 00:0C:29:58:E1:C1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms 172.20.27.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.12 seconds
```

Figura 35 – Nmap Windows 10 Pro

No caso do Windows 10 Home (Fig.36), a máquina tem três portas abertas e neste caso já aparece alguma informação adicional de algumas vulnerabilidades.

```
┌──(root㉿kali)-[/home/himas]
└─# nmap -sV -A -Pn 172.20.27.13
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 09:31 WEST
Nmap scan report for 172.20.27.13
Host is up (0.00024s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 00:0C:29:6E:AC:45 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-61QORBR, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:6e:ac:45 (VMware)
| smb2-time:
|   date: 2023-08-05T08:32:12
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms 172.20.27.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.97 seconds
```

Figura 36 – Nmap Windows 10 Home

Por último, o Windows XP (fig.37), é o que apresenta mais vulnerabilidades, muito provavelmente devido à falta de atualizações de segurança do SO.

```
┌──(root㉿kali)-[/home/himas]
└─# nmap -sV -A -Pn 172.20.27.14
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-05 09:31 WEST
Nmap scan report for 172.20.27.14
Host is up (0.00015s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp open  microsof@  Windows XP microsoft-ds
MAC Address: 00:0C:29:C7:BD:E8 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: himas-8e17932ab
|   NetBIOS computer name: HIMAS-8E17932AB\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-08-05T09:32:16+01:00
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -30m00s, deviation: 42m24s, median: -1h00m00s
|_nbstat: NetBIOS name: HIMAS-8E17932AB, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c7:bd:e8 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.15 ms 172.20.27.14

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.48 seconds
```

Figura 37 – Nmap Windows XP

Após a identificação inicial dos dispositivos conectados na rede, foi imperativo aprofundar o entendimento sobre possíveis pontos frágeis nos hosts identificados. Para alcançar este objetivo e obter uma análise minuciosa das vulnerabilidades presentes, foi utilizado o software Nessus (Fig.38), uma das melhores ferramentas na área de avaliação de vulnerabilidades.

Consequentemente ao mapeamento inicial de IPs ativos na rede, houve um avanço para uma fase mais analítica e detalhada do nosso estudo. Foram inserimos os endereços IP previamente identificados no software Nessus. O objetivo deste passo é submeter esses hosts a um scan para identificar possíveis vulnerabilidades.

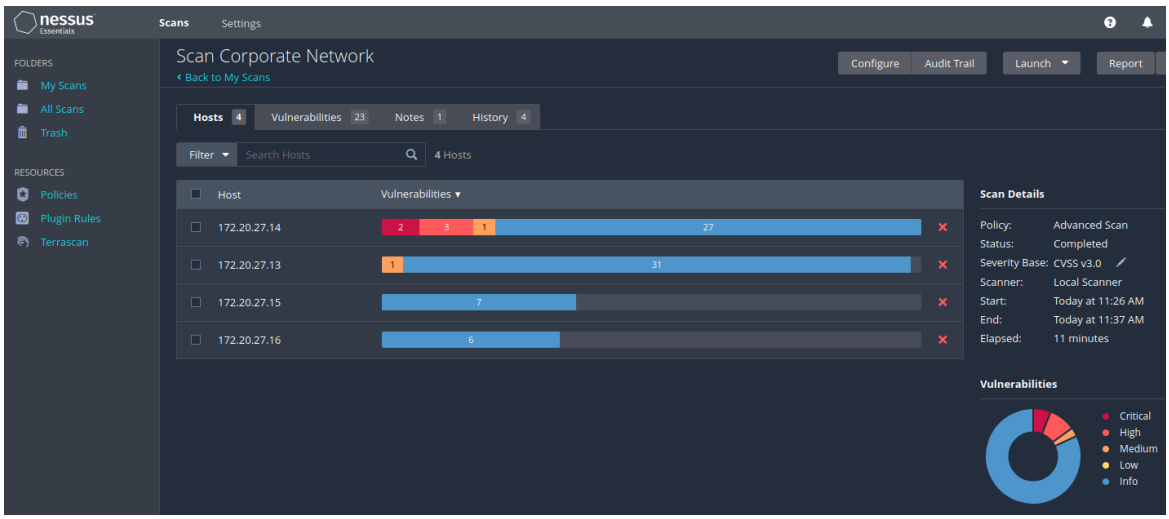


Figura 38 - Scan no Nessus

Através da utilização do Nessus, pretende-se não apenas identificar vulnerabilidades, mas também compreender o grau de exposição de cada host, a gravidade das falhas encontradas e as possíveis implicações dessas falhas no panorama global da segurança das informações da empresa. Ao detalhar essas informações, torna-se possível estabelecer um plano de mitigação eficaz e priorizado, onde as ameaças mais críticas são priorizadas.

A partir dos resultados obtidos pelo software Nessus, foi possível identificar um panorama preocupante relativo ao Windows XP na rede. Este host, de forma destacada, apresentou diversas vulnerabilidades, que, se não devidamente tratadas, poderiam oferecer múltiplos pontos de entrada para agentes mal-intencionados (Fig.39). No contexto de cibersegurança, a presença de múltiplas vulnerabilidades num único host é particularmente

alarmante, pois aumenta a superfície de ataque e, consequentemente, as chances de um ataque bem-sucedido.

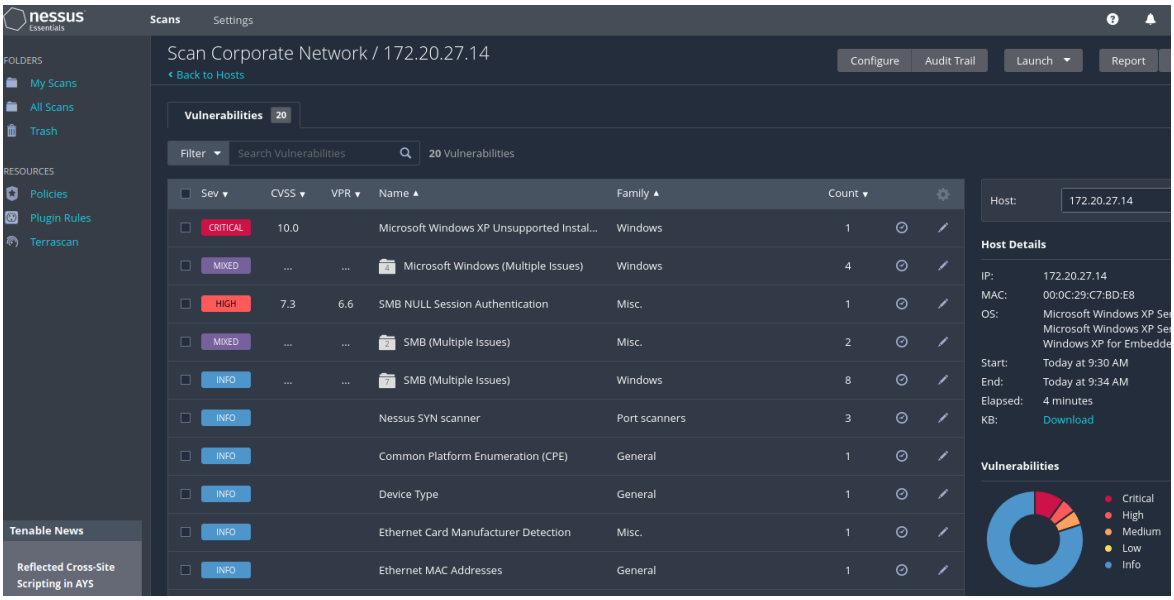


Figura 39 - Lista de vulnerabilidades Windows XP

Uma das abordagens mais eficazes para corrigir vulnerabilidades associadas a sistemas desatualizados (Fig.40) é proceder à atualização para uma versão mais recente do sistema operativo. As versões mais modernas frequentemente incorporam correções para vulnerabilidades conhecidas e oferecem aprimoramentos em termos de segurança, que são essenciais para combater as ameaças informáticas contemporâneas.

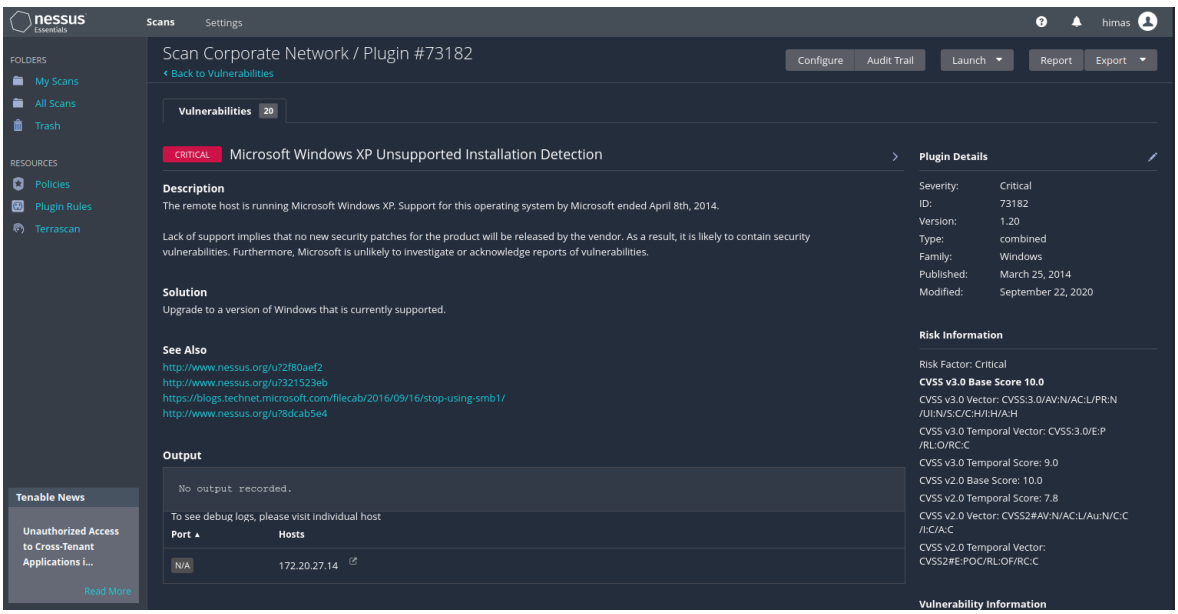


Figura 40 - Vulnerabilidade Critica Windows XP

No entanto, no contexto industrial, tal atualização nem sempre é viável. Uma das razões principais para esta limitação está relacionada à compatibilidade dos sistemas. Muitas indústrias operam com Controladores Lógico Programáveis (PLCs) e outros sistemas automatizados que, devido às suas especificações ou à antiguidade do software em execução, podem não ser compatíveis com versões mais recentes dos sistemas operativos. Nesses cenários, uma atualização imprudente pode resultar em incompatibilidades, levando a falhas operacionais ou mesmo interrupções na produção.

Face a tais restrições, uma estratégia alternativa, e muitas vezes recomendada, é a segmentação da rede. O host vulnerável pode ser isolado numa sub-rede ou segmento específico, limitando assim a capacidade de comunicação com outros dispositivos. Ao restringir o acesso a este host, minimiza-se o risco de um ataque bem-sucedido de propagar-se para outras partes da rede. A implementação de firewalls ou outras soluções de segurança pode ainda fortalecer esta segmentação, assegurando que o tráfego entre o host isolado e o resto da rede seja estritamente controlado e monitorizado.

Em análise ao ambiente da rede, especificamente ao avaliar o sistema operativo Windows 10 Home, também identificamos uma vulnerabilidade categorizada com um nível de risco médio como está demonstrado na figura 41.

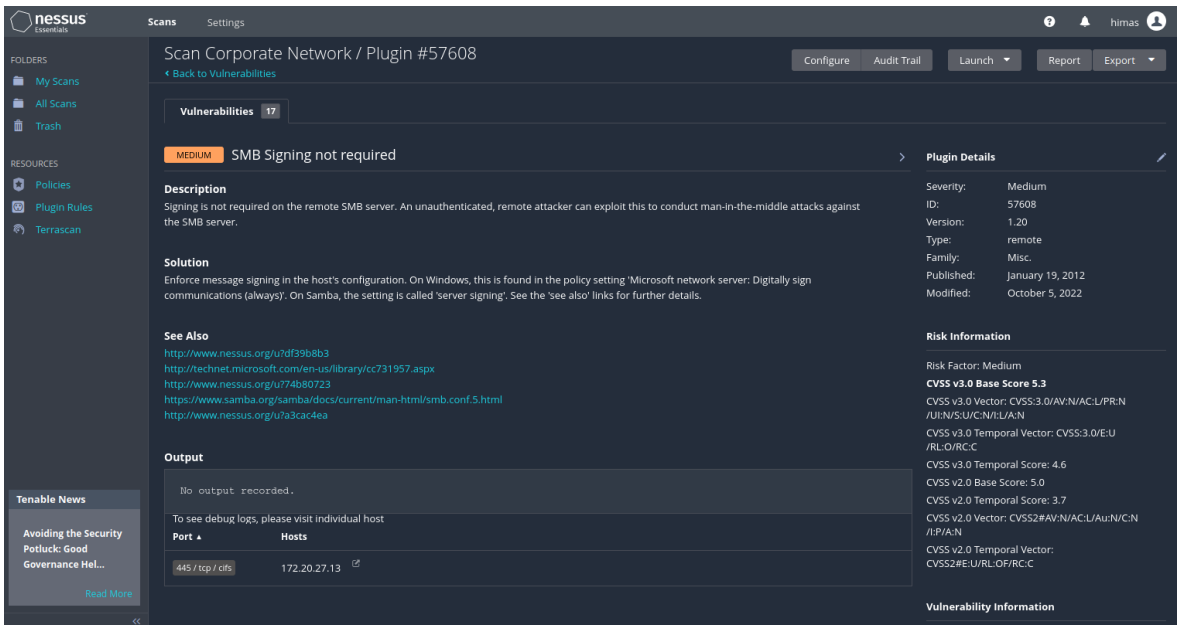


Figura 41 - Vulnerabilidade média Windows 10 Home

Foi identificado que o host em questão está a operar com um sistema que, originalmente, não foi projetado para ser utilizado em redes de maior complexidade. Tal característica é evidenciada pela ausência de um ecrã de logon no acesso, uma falha de segurança significativa em ambientes corporativos ou de maior escala. Esta ausência facilita a entrada não autorizada, visto que elimina uma camada crucial de autenticação.

É pertinente realçar que, enquanto algumas configurações podem ser aceitáveis ou até mesmo intencionais em ambientes isolados ou de teste, são altamente arriscadas em redes mais amplas, onde a integridade e confidencialidade dos dados são primordiais.

A boa notícia é que estes tipos de vulnerabilidades podem ser corrigidos através da implementação das políticas de segurança estabelecidas na fase anterior da pesquisa. Ao aplicar diretrizes rigorosas e configurar adequadamente os mecanismos de autenticação, podemos mitigar os riscos associados à ausência de um ecrã de logon e garantir que o acesso ao host seja restrito apenas a utilizadores autorizados.

Em conclusão, esta análise sublinha a importância de uma avaliação contínua e abrangente da segurança da rede em ambientes empresariais. A diversidade e evolução constante das ameaças informáticas requerem uma abordagem proativa e informada, onde ferramentas avançadas, práticas recomendadas e educação contínua desempenham papéis cruciais na proteção de ativos digitais e na manutenção da integridade e confidencialidade dos dados.

4.5 Fase Responder

4.5.1 Cenário

A organização do cliente descobriu que alguns dos seus dados sensíveis foram detetados numa aplicação de partilha de texto online. Devido às obrigações legais e para fins de continuidade de negócios, a equipa de CSIRT (Cibersecurity Incident Response Team) foi encarregue de conduzir uma resposta e investigação de incidentes para mitigar as ameaças.

A violação contém dados sensíveis e inclui um aviso de ameaça de que mais dados serão divulgados em breve. Uma vez que a violação conduz ao computador de um funcionário específico, a equipa de CSIRT, encarregada de investigar o incidente, segue as pistas.

4.5.2 Implementação

Após identificarmos a necessidade de uma análise forense no computador suspeito de infeção, procedeu-se à aquisição da imagem do disco rígido do referido equipamento. Esta máquina foi especificamente selecionada a partir dos Casos de Estudo fornecidos pela ENISA, uma autoridade reconhecida em segurança informática na Europa.

Com a imagem do disco, denominada de "disk.raw", em mãos, iniciámos o processo de avaliação forense ao utilizar a ferramenta Autopsy. Ao importar "disk.raw" para o Autopsy, o primeiro passo foi recuperar informações fundamentais sobre o sistema operativo.

Ao selecionar a opção "Operation System Information" no software (Fig.42), foi conseguido extrair dados essenciais sobre o computador em questão. De forma precisa, foi identificado o sistema operativo instalado, o nome atribuído ao computador e as informações do proprietário. Estes dados são cruciais não apenas para a contextualização da análise, mas também para correlacionar a máquina infetada com possíveis incidentes ou atividades suspeitas na rede.

A identificação desses elementos básicos do sistema constitui o alicerce para as próximas etapas da análise forense. Ao entender o contexto operativo da máquina, a Equipa CSIRT pode desenvolver uma estratégia de investigação mais informada e focada, visando identificar, com precisão, a natureza, bem como as potenciais implicações associadas.

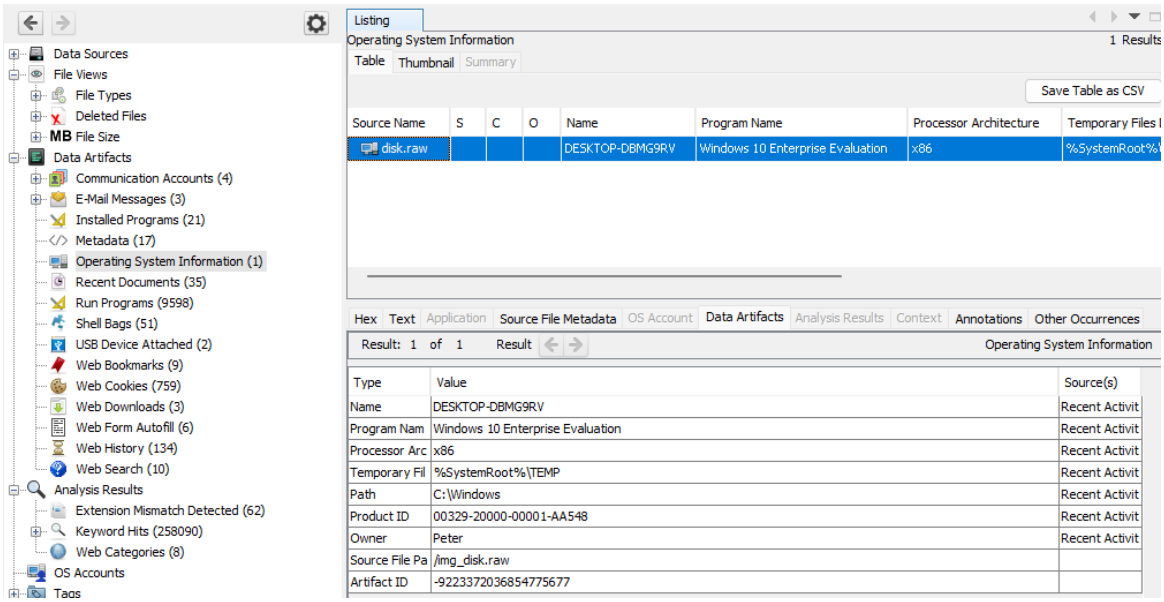


Figura 42 - Operation System Information

No decorrer desta investigação forense, houve a necessidade de examinar o sistema para procurar potenciais ameaças de malware. Para esta tarefa, foi optado pelo uso do ClamAV (Fig.43), um antivírus de código aberto usado neste tipo de ambientes devido à sua flexibilidade e base de dados de assinaturas de malware.

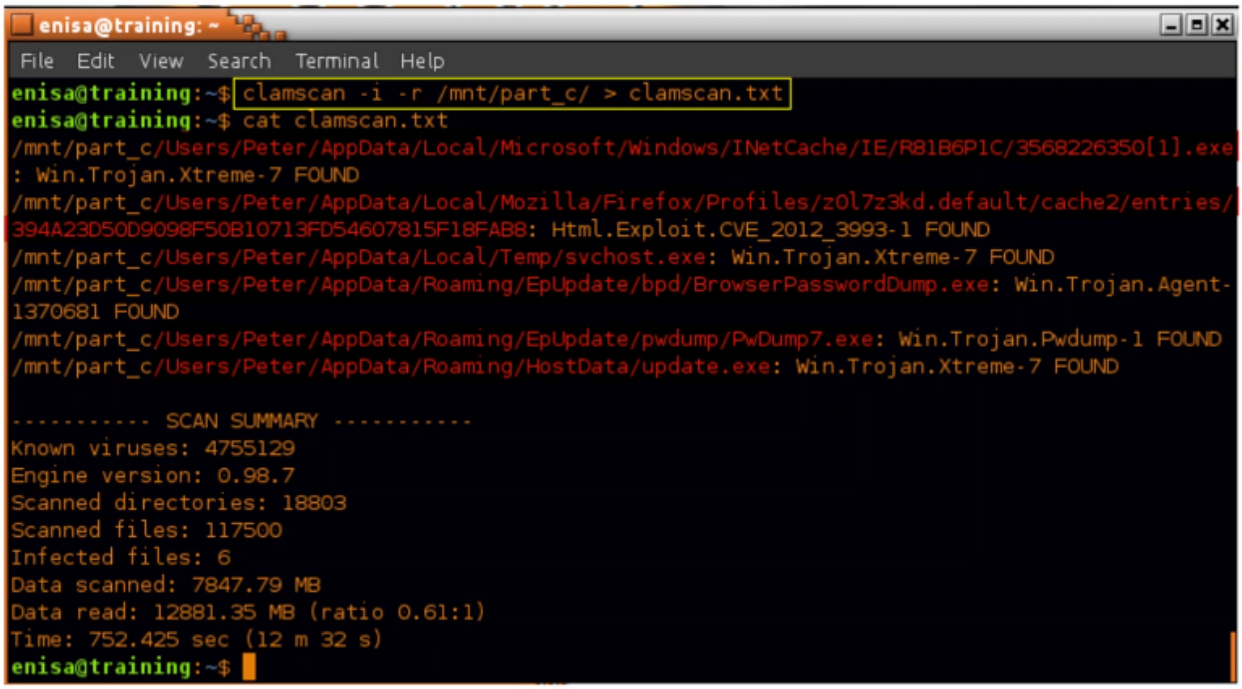


Figura 43 - ClamAV

Ao concluir a execução do clamscan, foram apresentados uma série de resultados que detalham as potenciais ameaças encontradas, foram detetados 5 ficheiros com Malware e um ficheiro com um Hmtl.Exploit (CVE_2012_3993). Estes resultados são fundamentais para compreender a extensão do comprometimento do sistema e para guiar as próximas etapas desta investigação.

As próximas capturas de ecrã apresentam os detalhes e resultados obtidos da análise dos ficheiros em questão.

4.5.3 3568226350[1].exe

No seguimento da análise forense e após a identificação de potenciais ficheiros suspeitos, foi procedido com a documentação visual. As próximas capturas de ecrã apresentam os detalhes e resultados obtidos da análise dos ficheiros em questão.

A identificação destes ficheiros pelo Antivírus AVIRA (Fig.44) reforça a importância de usar múltiplas ferramentas em análises forenses, uma vez que diferentes programas podem ter diferentes bases de assinaturas e, consequentemente, variar na deteção de determinados tipos de malware. Esta abordagem ao usar várias ferramentas, não só enriquece a robustez da investigação, como também minimiza a probabilidade de se passar ao lado de ameaças ocultas.

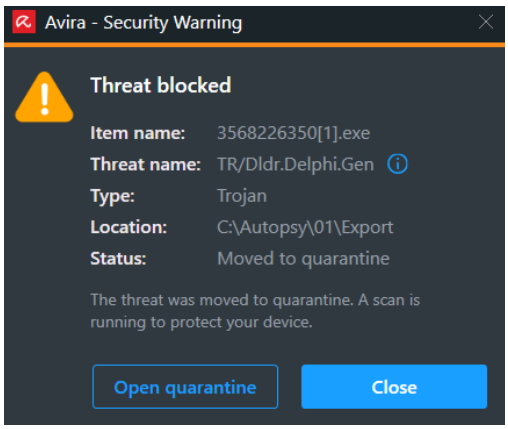


Figura 44 - 3568226350[1].exe (Avira)

4.5.4 HTML.Exploit (CVE_2012_3993)

Na figura 45 ao utilizar o Autopsy foi realizada uma descoberta significativa relacionada à segurança do sistema. Foi identificada a presença de uma vulnerabilidade conhecida pelo identificador CVE-2012-3993. As entradas CVE (Common Vulnerabilities and Exposures) servem como um repositório padronizado de informações sobre falhas de segurança e são largamente reconhecidas na indústria da segurança informática.

A vulnerabilidade CVE-2012-3993, de acordo com os registos, tem o potencial de ser explorada por atacantes mal-intencionados. Uma exploração bem-sucedida desta vulnerabilidade poderia permitir a um atacante executar código arbitrário[2], potencialmente comprometendo o sistema alvo ou ganhando privilégios elevados. É crucial, portanto, compreender o contexto e a gravidade dessa vulnerabilidade dentro do sistema em análise.

[2] Em cibersegurança, "execução arbitrária de código" é a capacidade de um invasor executar qualquer comando atacante numa máquina ou processo de destino

O facto de esta vulnerabilidade ter sido identificada demonstra a importância de manter sistemas atualizados e monitorizados. Também destaca o valor de ferramentas forenses como o Autopsy em processos investigativos, já que elas podem desenterrar detalhes críticos que podiam ser facilmente ignorados em inspeções menos rigorosas.

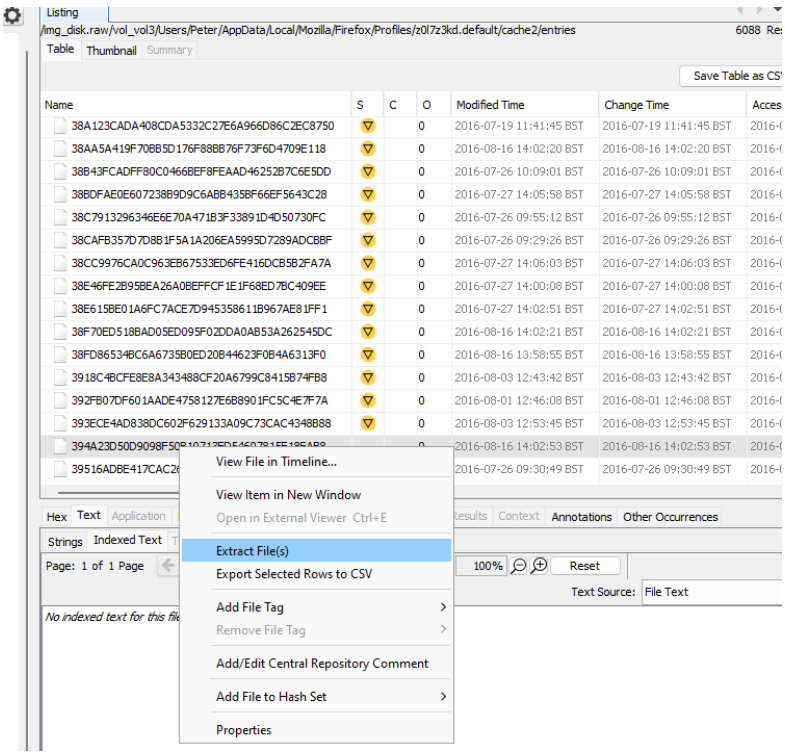


Figura 45 - HTML.Exploit (Autopsy)

Perante a identificação desta vulnerabilidade e a necessidade de aprofundar o entendimento sobre o contexto e as implicações da mesma, optei por consultar dois recursos na área da cibersegurança.

Primeiramente, dirigi-me ao repositório CVE (Common Vulnerability and Exposure), que é uma base de dados amplamente reconhecida que cataloga e descreve vulnerabilidades de software de maneira detalhada (Figura 46). Este repositório, administrado pela MITRE Corporation, oferece aos profissionais da área um recurso inestimável, fornecendo informações sobre o funcionamento, os impactos e as formas de mitigação das vulnerabilidades registadas. Ao analisar a entrada específica para a vulnerabilidade em questão no site oficial (CVE - CVE (mitre.org)), procurei uma compreensão abrangente de como essa vulnerabilidade poderia ser explorada por potenciais atacantes e quais seriam as consequências para os sistemas comprometidos.

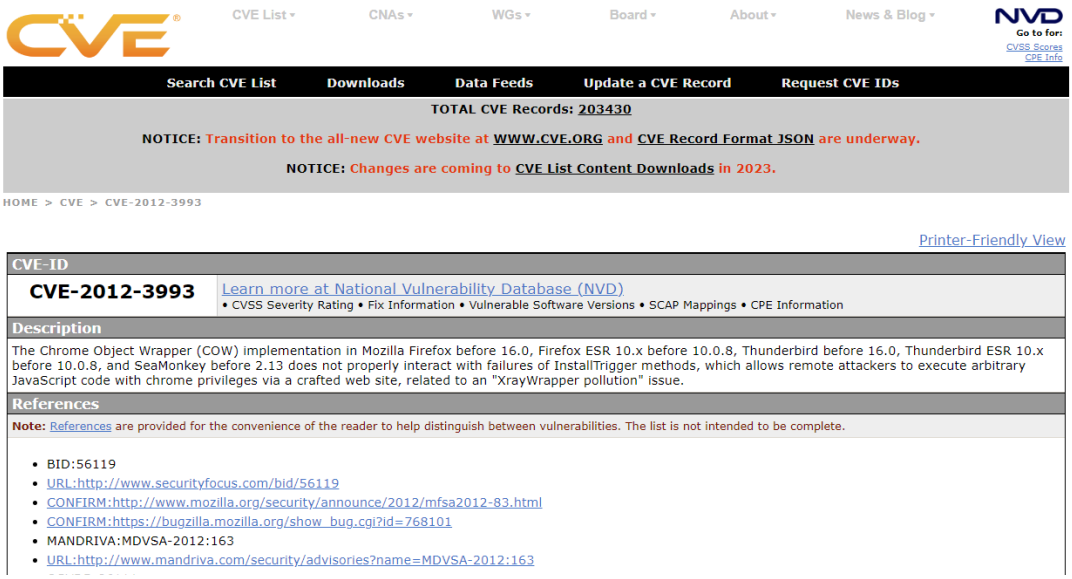


Figura 46 - CVE (Common Vulnerability and Exposure)

.

Em paralelo, como exemplificado na figura 47, para obter informações adicionais e contextualizadas sobre o arquivo suspeito identificado durante a análise, recorri ao programa VirusTotal. Esta plataforma agrega informações de vários antivírus e soluções de segurança, fornecendo uma análise holística dos arquivos. Ao inserir o arquivo em questão no VirusTotal, a intenção era avaliar a natureza exata do malware, entender o comportamento que podia ter, identificar qualquer assinatura associada e, se possível, obter recomendações de mitigação ou remoção.

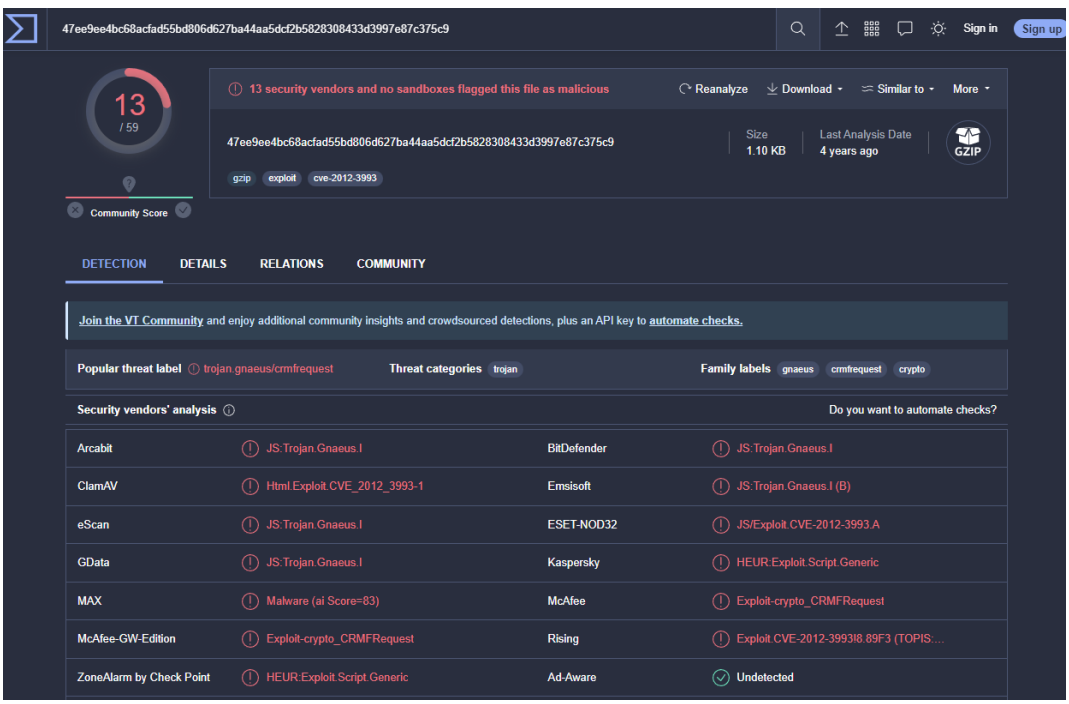


Figura 47 - HTML.Exploit (VirusTotal)

4.5.5 PwDump7.exe

Dentro do ecossistema de ferramentas voltadas para a segurança informática e análise de sistemas, o Pwdump destaca-se como uma ferramenta especializada, cujo principal objetivo é a extração de hashes de palavras-passes diretamente do arquivo SAM (Security Account Manager) do sistema operativo Windows. O arquivo SAM é um componente crítico do Windows, responsável pelo armazenamento de perfis de utilizadores, juntamente com os respetivos hashes das palavras-passes (Fig.48).

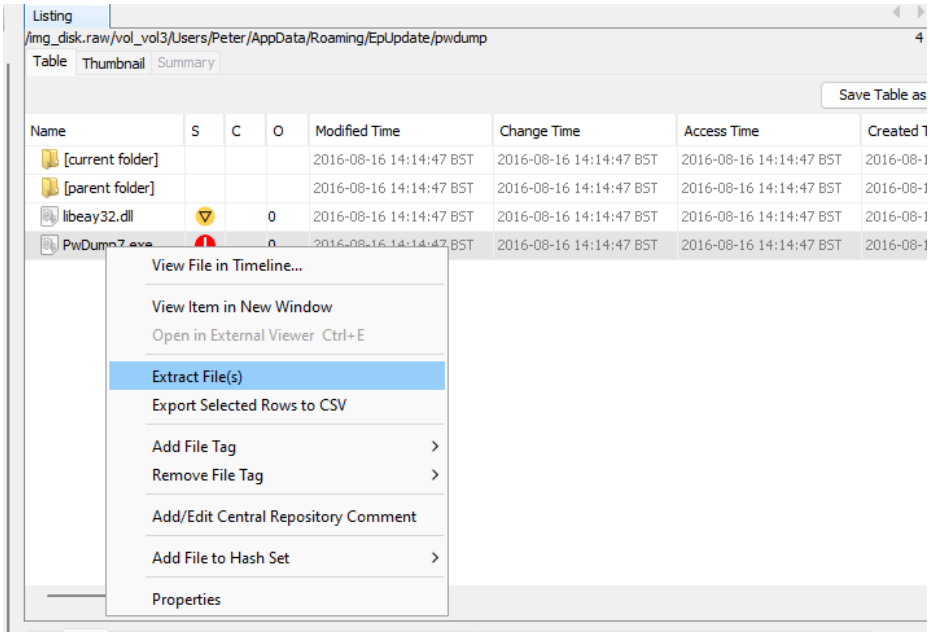


Figura 48 - Pwdump (Autopsy)

O mecanismo subjacente de armazenamento de senhas do Windows envolve a conversão de palavras-passes inseridas em hashes criptográficos, que são armazenados no SAM. Em circunstâncias normais, estas representações criptográficas servem como uma medida de segurança, pois não revelam diretamente a senha em texto claro.

No entanto, quando ferramentas como o Pwdump são usadas para extrair esses hashes, surge uma vulnerabilidade potencial (Fig.49). Uma vez que o oponente está na posse desses hashes, ele pode utilizá-los em estratégias de ataque como "brute force". Nestes ataques, o adversário tenta adivinhar a palavra-passe por meio da comparação do hash da senha criada por tentativa e erro com o hash extraído. Utilizando ferramentas e técnicas adequadas, e dependendo da complexidade da palavra-passe, essa tarefa pode ser mais rápida e eficiente do que se imagina.

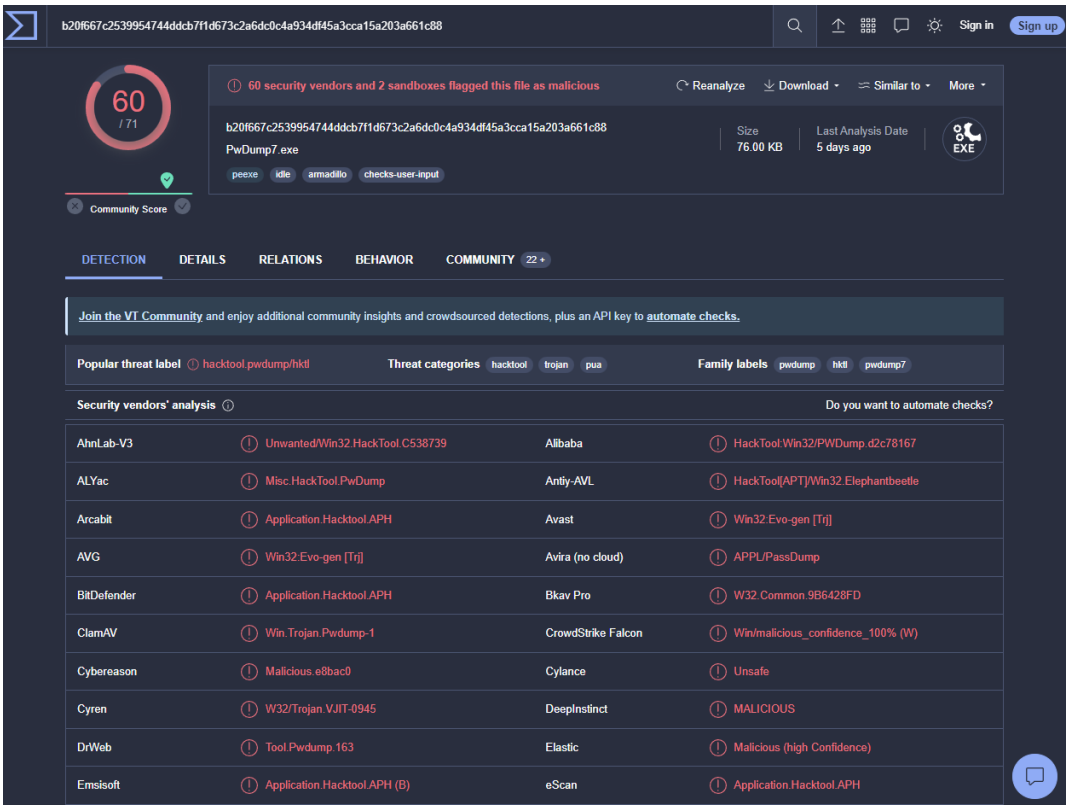


Figura 49 - Pwdump (VirtusTotal)

4.5.6 XtremeRAT

Para além dos ficheiros anteriormente descrevidos também foi identificado o malware XtremeRAT, que é um tipo de programa de acesso remoto que permite que um oponente assuma o controlo total do computador infetado. Pode ser instalado num computador por meio de várias técnicas, incluindo o Drive-by-Compromise.

Um dos sinais de que um computador foi infetado por um ataque Drive-by-Compromise é a existência de processos desconhecidos em execução, o que neste caso acontece conforme identificado na análise ao dump de memória efetuado no relatório anterior.

A vulnerabilidade explorada para instalação deste malware provavelmente terá sido o CVE_2012_3993 pois a exploração bem-sucedida desta vulnerabilidade poderia permitir a execução de código JavaScript malicioso com privilégios do Chrome, o que poderia ser usado para instalar o malware XtremeRAT no sistema.

Além destes ficheiros identificados anteriormente na pasta EpUpdate, foram identificados os seguintes ficheiros:

- **Passwords.txt:** Este ficheiro contém uma lista de passwords. O objetivo provável deste ficheiro é armazenar senhas roubadas ou recolhidas de várias fontes, o que permitiria ao oponente aceder a contas do utilizador.
- **Mimikatz:** É uma ferramenta usada para extrair credenciais de segurança do Windows, como senhas em texto claro e hashes. O objetivo desse ficheiro é roubar e extrair informações de autenticação de sistemas e utilizadores que acedam a este computador.
- **Nircmd.exe:** É um utilitário de linha de comando que permite ao oponente executar comandos e manipular configurações do sistema. Esse ficheiro pode ser usado para realizar várias ações maliciosas, como alterar configurações, obter informações confidenciais ou executar comandos remotos no computador comprometido.
- **BrowserPasswordDump.exe:** Este ficheiro é uma ferramenta projetada para extrair senhas armazenadas em navegadores da web, como Chrome, Firefox, Internet Explorer, entre outros. O objetivo é obter senhas salvas nos navegadores dos utilizadores para acesso a contas online, como e-mails ou redes sociais.

Com o objetivo de determinar especificamente qual site foi responsável pela criação do ficheiro associado à vulnerabilidade em questão, procedeu-se à seleção do Common Vulnerabilities and Exposures (CVE) no software de análise forense Autopsy. Este CVE foi identificado como contendo a vulnerabilidade que poderia ser potencialmente explorada. Posteriormente, efetuou-se um acesso minucioso à *timeline* do software para rastrear o histórico de atividades. Através desta abordagem meticulosa, conseguiu-se identificar que o site responsável era http://blog.mycompany.ex, como é evidenciado nas Figuras 50 e 51 deste documento de pesquisa.

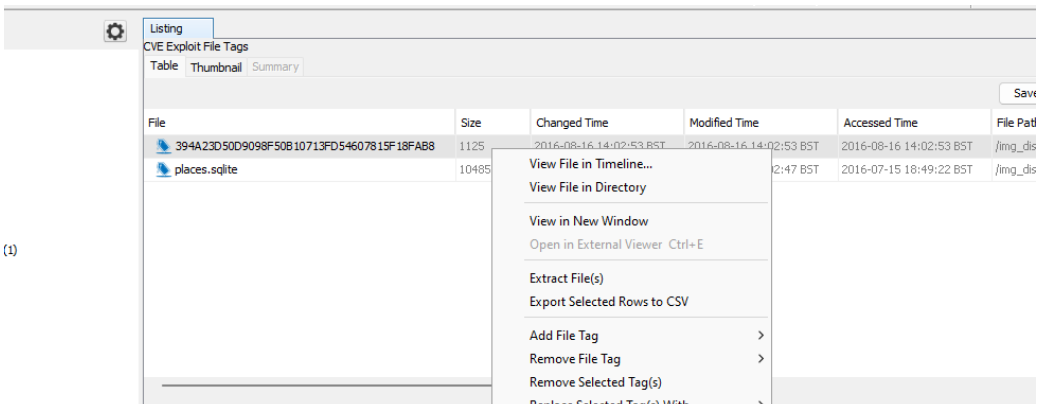


Figura 50 - CVE_2012_3993 (Autopsy)

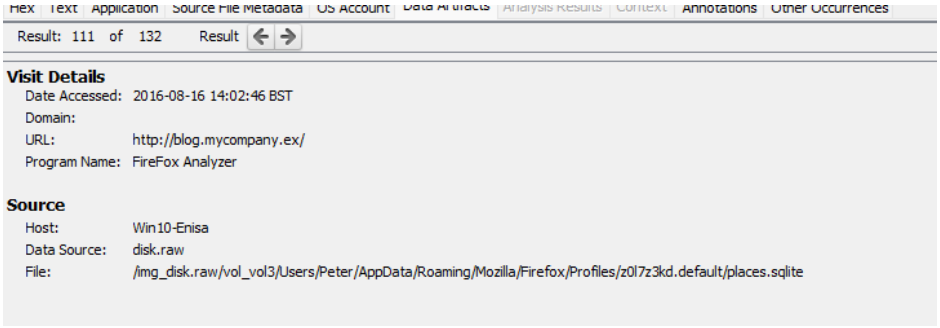


Figura 51 - site http://blog.mycompany.ex/

De seguida procurou-se pelo Perfetch File (que permite identificar que um executável foi acedido em ambiente Windows) para verificar que executável foi aberto pelo link identificado acima (Fig.52).

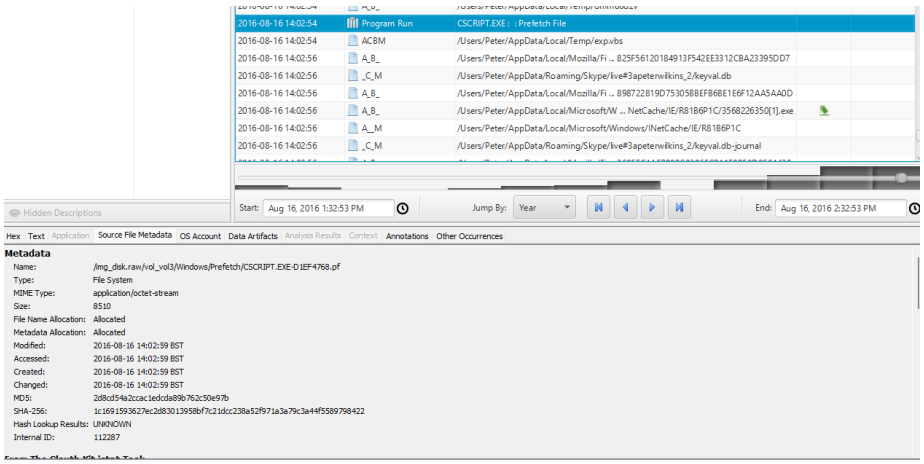


Figura 52 - Perfetch File (Autopsy)

Ao examinar a entrada subsequente no arquivo Perfetch, conforme ilustrado na Figura 53, identifiquei um script escrito em Visual Basic. Uma análise mais detalhada deste script revelou que é responsável por acionar o download do arquivo anteriormente identificado por nós, nomeadamente "3568226350.exe", que foi categorizado como malware.

Também foi observado que havia operações para guardar outros arquivos. Como o "svchost.exe". Embora o mesmo tenha um nome distinto, uma comparação cuidadosa das hashes confirmou que se tratava efetivamente do mesmo arquivo malicioso que o "3568226350.exe". Esta é uma prática comum entre atacantes, que renomeiam ficheiros de malware com designações comuns do sistema para mascarar a presença e confundir os administradores ou ferramentas de segurança.

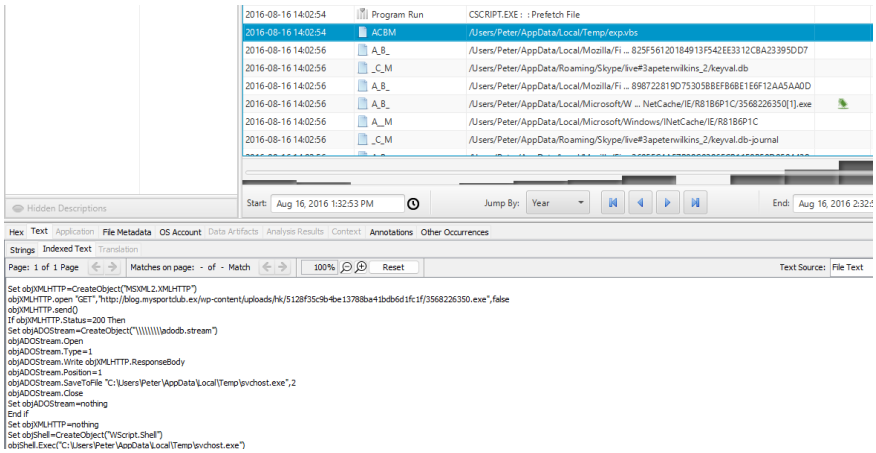


Figura 53 - svchost.exe (Autopsy)

Em última instância, para confirmar a execução da aplicação específica destinada à pesquisa de passwords, nomeadamente o programa 'BrowserPasswordDump.exe', efetuei uma análise pormenorizada à *timeline* associada à pasta 'EpUpdate'. Esta análise é ilustrada e documentada na Figura 54. Através deste exame meticuloso, foi possível verificar e confirmar que a referida aplicação de pesquisa de passwords efetivamente foi executada no sistema em análise.

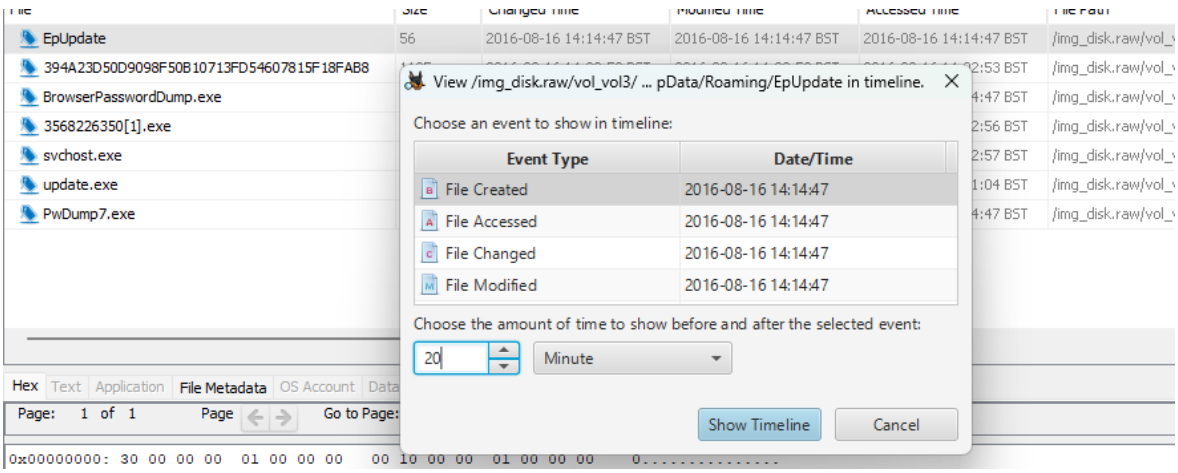


Figura 54 - EpUpdate (Autopsy)

Com esta informação além de identificadas as vulnerabilidades usadas pelo atacante foi identificado o seu método de ataque. O atacante ao enviar um email aparentemente legitimo com um link adulterado, fez com que o utilizador tenha feito o download de malware sem se ter apercebido. Este malware deu então acesso a algumas passwords de sistema que lhe deu acesso a informação sensível a qual ele usou para ganhos financeiros.

4.6 Fase Recuperar

Na fase recuperar analisou-se um cenário hipotético em que uma companhia seguradora no sector automóvel foi alvo de um ataque informático. No âmbito desta análise, procedeu-se à elaboração meticulosa dos procedimentos a serem adotados, com o intuito de alinhar a gestão do incidente com as estratégias estipuladas no plano de recuperação.

4.6.1 Cenário

Título: Recuperação de um Ataque Informático: A salvaguarda de Dados Sensíveis

Cenário: A XXL-Seguros, uma empresa de seguros de automóveis, sofreu um ataque informático, resultando na perda de dados sensíveis dos clientes na Internet.

4.6.2 Identificação e Avaliação do Impacto

Assim que a XXL-Seguros foi informada do ataque informático, o sistema de gestão de incidentes entrou em ação. Uma equipa de resposta a incidentes de segurança das informações (SCIRT) foi formada, composta por especialistas em IT, profissionais de segurança informática, advogados e relações-públicas. A equipa determinou a comprimento da perda e avaliou o potencial impacto sobre os clientes e a empresa. As análises iniciais revelaram que os atacantes conseguiram obter dados sensíveis, como nomes, endereços de email e detalhes do cartão de crédito.

4.6.3 Contenção e Erradicação

A equipa procedeu à contenção do incidente, para prevenir danos adicionais. Isolaram os sistemas afetados e executaram uma análise forense, para compreender a natureza do ataque e identificar possíveis vulnerabilidades exploradas pelos atacantes. Foi então criada uma estratégia de erradicação para eliminar a ameaça do sistema.

4.6.4 Comunicação

Com a confirmação da perda de dados, a empresa iniciou a sua estratégia de comunicação. Esta incluía a notificação das autoridades competentes, como a Comissão Nacional de Proteção de Dados, bem como dos clientes afetados, explicando-lhes a situação, os possíveis riscos e as medidas a serem tomadas para protegerem a sua informação.

4.6.5 Recuperação

A equipa de IT, em conjunto com os especialistas em cibersegurança, iniciou a recuperação dos sistemas. Backups previamente armazenados foram utilizados para restaurar os dados, garantindo que a operação da empresa poderia continuar sem perdas significativas. A equipa também trabalhou na correção das vulnerabilidades descobertas durante a análise forense.

4.6.6 Análise Pós-Incidente e Melhoria

A equipa conduziu a uma análise pós-incidente para identificar falhas na segurança da informação e áreas para melhoria. Implementaram um plano para fortalecer as defesas da empresa, incluindo a formação dos colaboradores em segurança informática, o aperfeiçoamento dos procedimentos de resposta a incidentes e a atualização regular dos sistemas e software de segurança.

O ataque cibernético à XXL-Seguros demonstrou que, apesar das melhores práticas e políticas de segurança em vigor, nenhum sistema é completamente à prova de falhas. No entanto, a rápida identificação do problema, a eficiente resposta ao incidente e a transparência na comunicação foram cruciais para a recuperação. A análise pós-incidente e as melhorias contínuas garantirão que a empresa estará mais preparada para eventuais ataques futuros.

5 DISCUSSÃO

5.1 Resposta à Questão de Investigação

Analisando os resultados do questionário e da implementação feita em cada fase, obteve-se as seguintes conclusões em resposta à questão de investigação. **Contribuir para a melhoria da resposta das PME's aos desafios da cibersegurança.**

Fase Identificar:

- Embora PME's demonstrem um grau mínimo de consciencialização sobre cibersegurança, os resultados do questionário indicam que tal nível de sensibilização é insuficiente. Contrariamente à perceção predominante nas PME's, estas encontram-se inadequadamente preparadas para enfrentar ameaças de cibersegurança.

Fase Proteger:

- A implementação de *Group Policies* constitui um elemento crítico para o funcionamento eficaz e a gestão de segurança das estações de trabalho dentro de uma Pequena e Média Empresa (PME), especialmente no contexto do uso quotidiano das máquinas.
- A implementação *Group Policies* específicas para a gestão de palavras-passe é de extrema relevância, particularmente quando consideramos que uma palavra-passe que esteja alinhada com as diretrizes de segurança dessas políticas pode aumentar o tempo requerido para a sua descoberta de um segundo para aproximadamente 3 mil anos.

Fase Detetar:

- Compreendeu-se que estações de trabalho que operam com versões desatualizadas de software dentro de uma organização estão intrinsecamente mais expostas a vulnerabilidades, tornando-se, assim, alvos potencialmente mais fáceis para ataques informáticos.
- Com o uso de apenas duas ferramentas de diagnóstico, como o Nmap e o Nessus, é possível obter uma visão abrangente do estado de segurança das estações de trabalho dentro de uma organização. Estas ferramentas fornecem *insights* valiosos

sobre o grau de vulnerabilidade das máquinas e podem indicar até que ponto estas podem estar comprometidas

Fase Responder:

- Tornou-se evidente como uma empresa com deficiências em cibersegurança pode ser facilmente suscetível a ataques. Nesse contexto, um atacante pode explorar as vulnerabilidades existentes para infiltrar-se na rede empresarial e conseguir dados sensíveis através de um dos computadores pertencentes à própria organização.
- Com a presença de uma equipa especializada em Tecnologias da Informação (IT), é possível desenvolver estratégias eficazes de resposta a ataques informáticos. Utilizando um conjunto de ferramentas específicas, tais como Autopsy, ClamAV e VirusTotal, foi-se capaz de identificar a natureza da ameaça informática e discernir o método de ataque empregado pelo atacante, permitindo assim uma resposta mais precisa e direcionada.

Fase Recuperar:

- No evento de uma Pequena e Média Empresa (PME) necessitar de acionar um plano de recuperação de desastres, é imperativo que este esteja atualizado e bem documentado para que a equipa IT possa implementá-lo de forma eficaz e minimizar os impactos negativos sobre as operações da organização.

Os resultados alcançados neste estudo reforçam a importância crítica de uma implementação rigorosa e abrangente de medidas de segurança informática nas Pequenas e Médias Empresas (PME's).

Estes dados confirmam a noção de que a falta de cibersegurança adequada torna as PME's alvos particularmente atrativos para atacantes informáticos, em contraposição às grandes empresas que geralmente têm recursos mais substanciais para investir em medidas de segurança robustas. Portanto, serve como um alerta e um guia prático para as PME's, sublinhando a necessidade de elevarem a sua postura de cibersegurança como forma de mitigar os riscos e vulnerabilidades a que estão expostas no ambiente digital atual.

5.2 Discussão dos resultados

Ao confrontar os resultados obtidos neste estudo com aqueles apresentados na revisão da literatura existente, é possível extrair diversas conclusões significativas. Por exemplo, o

estudo de Gonçalves (2019) também realçou a ideia de que as estratégias de cibersegurança não devem ser generalizadas para todas as organizações, pois cada uma apresenta necessidades e vulnerabilidades específicas. No entanto, uma constatação geral é que as grandes empresas parecem estar mais sensibilizadas e mais bem preparadas no que diz respeito à cibersegurança. Estas organizações frequentemente dispõem de recursos consideráveis e know-how especializado para implementar estratégias de segurança robustas.

Em contrapartida, as Pequenas e Médias Empresas (PME's) tendem a possuir um nível de conhecimento técnico inferior nesta área e, muitas vezes, não atribuem a devida importância à cibersegurança. Isto coloca-as em uma posição particularmente vulnerável a riscos informáticos. É importante notar que, embora exista um crescente reconhecimento da importância de uma sólida postura de cibersegurança entre algumas PME's, essa perceção do risco raramente se traduz em ações práticas e medidas concretas para mitigar ameaças (Gonçalves, 2019).

Ao contrário do presente estudo, Amrin (2014) foca-se não só, mas também, na apresentação dos resultados dos principais softwares de tecnologia usados pelas PME's.

Os softwares que mais prevalecem são soluções de Antivírus, Malware, Spam e Phishing. Estas opções de segurança de TI gozam de um elevado grau de reconhecimento e, consequentemente, a sua adoção generalizada era previsível (Amrin, 2014). É importante salientar que o uso dos softwares usados no meu estudo vai de encontro ao estudo de Nabila Amrin.

No estudo de Berger e Jones (2016) pode-se extrair várias conclusões fundamentais a partir deste estudo, especialmente no que diz respeito à eficácia da utilização de testes de penetração para identificar falhas de segurança e vulnerabilidades na rede empresarial de Pequenas e Médias Empresas (PME's). Uma vez que essas fragilidades sejam devidamente identificadas, torna-se viável a implementação de soluções e medidas corretivas que aumentem a robustez da infraestrutura de segurança da empresa.

Adicionalmente, este estudo, ao encontro do meu, demonstrou que a aplicação de um conjunto diversificado de ferramentas gratuitas de teste de penetração pode potencializar significativamente as oportunidades de localizar e remediar vulnerabilidades que poderiam ser exploradas por atacantes mal-intencionados para obter acesso a informações sensíveis e

confidenciais. É relevante salientar que o uso de ferramentas de código aberto apresenta uma solução particularmente benéfica para PME's, que frequentemente operam com recursos financeiros e humanos mais limitados (Berger & Jones, 2016).

Benz e Chatterjee (2020) estudam a metodologia do NIST cibersecurity framework e afirmam que a mesma não serve apenas como um instrumento valioso para a identificação dos pontos fortes e vulnerabilidades na infraestrutura de cibersegurança de uma organização, mas também oferece um conjunto de recomendações e melhores práticas para abordar eficazmente essas lacunas de segurança. Tal como foi apresentado no meu estudo, ao adotar uma estratégia de avaliação (NIST) tão abrangente, os responsáveis pela Tecnologia da Informação (TI) nas organizações têm a oportunidade de (Benz & Chatterjee, 2020):

- Rapidamente destacar as vulnerabilidades mais críticas que requerem atenção imediata;
- Avaliar o grau de maturidade da sua infraestrutura de cibersegurança em comparação com organizações semelhantes, com base num conjunto de métricas e indicadores padrão;
- Priorizar os esforços de melhoria que se mostram mais valiosos e impactantes para a segurança global da organização.

Deste modo, os resultados deste estudo, em conjunto com as observações da literatura académica, sublinham a necessidade imperativa de uma maior conscientização e ação efetiva em relação à cibersegurança, especialmente no contexto das PME's, que frequentemente carecem tanto de recursos como de especialização na matéria.

5.3 Limitações do trabalho

Uma das limitações deste estudo reside na sua inserção numa área de conhecimento caracterizada por uma evolução constante e acelerada, nomeadamente a tecnologia da informação e a cibersegurança. Este dinamismo intrínseco impõe a necessidade de atualização contínua em relação às mais recentes ferramentas, técnicas e metodologias emergentes, o que pode tornar alguns dos achados deste trabalho rapidamente obsoletos ou menos relevantes com o avanço do tempo.

Outra restrição do presente trabalho foi a impossibilidade de conduzir a implementação do estudo num cenário empresarial real, com dados e resultados empiricamente validados.

Esta limitação deveu-se à complexidade associada à execução prática do projeto em questão, o que levou à decisão de recorrer a um sistema simulado como base para a análise e as respetivas conclusões. Embora esta abordagem permita uma investigação controlada e teoricamente rica, a mesma pode comprometer a generalização e a aplicabilidade prática dos resultados obtidos.

6 CONCLUSÃO

Em resposta à questão de investigação inicial que guiou este estudo, "Contribuir para a melhoria da resposta das PME's aos desafios da ciber segurança", foram extraídas diversas conclusões de relevância prática e teórica.

Os resultados do estudo sublinham que é não apenas viável, mas crucial implementar mecanismos específicos nas diferentes fases do ciclo de cibersegurança. Optou-se por basear no estudo da metodologia NIST Cybersecurity Framework que se revelou bastante eficaz, onde foi complementado com ferramentas, todas elas open source.

Através da implementação desta abordagem, torna-se acessível às PME's um conjunto de práticas e ferramentas de cibersegurança que, se seguidas com rigor, têm o potencial de melhorar significativamente a sua postura de cibersegurança, minimizando riscos e aumentando a resiliência contra diversas ameaças informáticas.

Este estudo abre também portas para futuras investigações que possam aprofundar o entendimento e a eficácia das várias ferramentas e metodologias aqui propostas, através da sua aplicação prática em contextos empresariais reais. Com uma implementação deste tipo, seria possível observar e comparar as diferenças nos níveis de cibersegurança entre diversas empresas, oferecendo assim uma base empírica robusta para futuras comparações e ajustes de estratégia.

BIBLIOGRAFIA

AccessData. (2020). *FTK Imager User Guide.*

Amrin, N. (2014). *The Impact of Cyber Security on SMEs.*

Arquilla, J.,, & Ronfeldt, D. (1993). *Cyberwar is coming! Comparative Strategy.*

Avira Operations GmbH & Co. KG. (2019). *White Paper: Avira's Advanced Heuristic Analysis and Detection.* Avira Official Documentation.

Baptista, I. (2017). *O fator humano na cibersegurança (Dissertação de Mestrado).* Instituto Superior Técnico, Lisboa.

Benz, M., & Chatterjee, D. (2020). *Calculated risk? A cybersecurity evaluation tool for SMEs.*

Berger, D., & Jones, A. (2016). *Cyber Security & Ethical Hacking For SMEs.*

Calder, A., & Khalid, N. (2018). *EU GDPR - A Pocket Guide.*

Casey, E., Ferraro, M., & Nguyen, L. (2009). *The Sleuth Kit and Autopsy: Forensic tools for Linux and other Unixes.* Syngress Publishing.

CERT. (2013). *Unintentional Insider Threats: A Foundational Study.* Obtido de https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

Checkpoint. (2023). *How to Create a Cybersecurity Disaster Recovery Plan* . Obtido de https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/how-to-create-a-cybersecurity-disaster-recovery-plan/

Chronicle. (2019). *The Evolution of VirusTotal.* Chronicle Blog.

ClamAV Team. (2020). *ClamAV User Manual.* ClamAV Documentation.

Climer, S., & Khan, M. (s.d.). *Red Team Vs Blue Team: The Two Sides Of Cybersecurity: A Cybersecurity Report*. Obtido de Mindsight: https://gomindsight.com/insights/blog/red-team-vs-blue-team/

Collins, D. (2016). *Network Security Through Data Analysis: Building Situational Awareness.* . O'Reilly Media.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining Cybersecurity. Technology Innovation Management Review.*

Desmond, B. . (2020). *Microsoft Windows Group Policy Guide. .* O'Reilly Media.

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity - Attack and Defense Strategies.*

Doherty. (2018). *The role of information security in business continuity management. In Handbook of research on information management for effective logistics and supply chains.* IGI Global.

ENISA. (2018). *Cyber Security Culture in Organisations.* Obtido de https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Fernandes, J. (2012). *Utopia, Liberdade e Soberania no Ciberespaço. IDN Nação e Defesa.*

Gaspar, F. (2018). *Ciber (in)segurança.*

Gonçalves, R. (2019). *O Fator Humano da Cibersegurança nas Organizações.*

Guarnizo, J.D., Buitrago, S.O., Gharib, M.A., Ochoa, M., & Tippenhauer, N.O. (2018). *SMT-based Game for Data Correction in Security Information and Event Management Systems.* IEEE European Symposium on Security and Privacy (EuroS&P).

Haight, K. M. (2018). *Red team vs. blue team: How to run an effective simulation. .* Journal of cybersecurity education, research and practice.

Hiller, J. S.,, & Russel, R. S. (2013). *The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law & Security Review.*

Information Commissioner's Office. (2017). *Preparing for the GDPR: A Guide for Small and Micro Businesses.*

Isik, H. (2019). *An Overview of Cybersecurity Roles: Blue, Red, and Purple Teams.* Journal of Cyber Security Technology.

ITU. (2008). Recommendation ITU-T X.1205. Series X: data networks, open system communications and security. 2.

J. Carey, M., & Jin, J. (2020). *Tribe of hackers Blue Team.* Wiley.

Kim, D. K., Chung, K. H., & Kim, J. H. (2019). *A Study on the Process of Response to Cyber Security Incidents in Companies. Journal of Security Engineering.*

Kosa, T. A. (2019). *Understanding GDPR: A Practical Guide to Global Privacy.*

Kottler, B. (2020). *Nmap: Network Exploration and Security Auditing.*

Kozierok, C. (2013). *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.* No Starch Press.

Lamping , U., Sharpe, R., & Warnicke, E. (2012). *Wireshark User's Guide for Wireshark 1.9.*

Lyon, G. . (2009). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning.*

Mahn, A., Marron, J., Quinn, S., & Topper, D. (2021). Getting Started with the NIST Cybersecurity Framework.

Marpillero, S., Laskov, P., & Düssel, P. . (2008). *Learning from our Mistakes: Predicting the Evolution of Malware with Recurrent Neural Networks.* Journal of Computer Security.

Marshall, N., & Baldwin, G. (2018). *Mastering VMware vSphere.* Packt Publishing.

Matos, P. C. (2018). *Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas (Dissertação de Mestrado).* ISCTE, Lisboa.

Microsoft. (2020). *Update Management Guide.*

Microsoft. (2021). Obtido de How to use Group Policy to enforce complex password requirements.: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

Microsoft. (2022). *Group Policy for Beginners.*

Microsoft. (2023). *O que é a resposta a incidentes?* Obtido de https://www.microsoft.com/pt-pt/security/business/security-101/what-is-incident-response

Morgan, S. (2017). *2017 Cybercrime Report.* Obtido de Cybercrime Magazine.

Moskowitz, J. D., & Barber, M. (2019). *Group Policy: Fundamentals, Security, and Troubleshooting. Wiley Publishing.*

National Institute of Standards and Technology. (2018). *Contingency Planning Guide for Federal Information Systems.* Obtido de https://www.nist.gov/privacy-framework/nist-sp-800-34

Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to Computer Forensics and Investigations. Cengage Learning.*

Nessus. (2018). *Nessus Professional Official Documentation.* Tenable Network Security.

NIST. (2017). *Digital Identity Guidelines: Passwords.* NIST Special Publication 800-63B.

NIST. (2018). *Guide to Reducing the Risk of Software Vulnerabilities.*

Peltier, T. R., Peltier, J. W., & Blackley, J. A. (2018). *Information security fundamentals.* CRC Press.

Pennington, J. (2019). *The blue team handbook: SOC, SIEM, and threat hunting.*

Pfeffer, K., Eckert, C., & Holz, T. . (2017). *Learning from the Past: Automated Rule Generation for Malware Detection.* International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

Ponemon Institute. (2012). The Human Factor in Data Protection.

Raposo, R. G. (2016). *Gestão do risco e garantia da informação: a influência do fator humano e da ética na segurança da informação e cibersegurança nas organizações (Dissertação de Mestrado).* Universidade de Lisboa, Lisboa.

Richardson, R., & Marjie, T. (2018). *Windows Forensics Analysis.*

SANS Institute. (2014). *Backup Policy.*

SANS Institute. (2021). *Blue Team Fundamentals.*

Santos, S. I. (2018). *Estudo das Perceções de Cibersegurança e Cibercrime e das Implicações na Formulação de Políticas Públicas (Dissertação de Mestrado).* Universidade de Lisboa, Lisboa.

Skoudis, E., & Liston, T. (2014). *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Prentice Hall.

Stanek, W. R. (2018). *Windows Group Policy: The Personal Trainer for Windows Server and Windows Client. Reagent Press.*

Steele, S.,, & Wargo, C. (2007). *An Introduction to Insider Threat Management. Information Systems Security,.* Obtido de https://www.sciencedirect.com/science/article/pii/S0167404805001045?via%3Dihub

Suchan, W., & Sobiesk, E. (2006). *Strengthening the weakest link in digital protection.*

Symantec. (2016). *Attackers Target Both Large and Small Businesses.*

Tanner, N. H. (2019). *Cybersecurity Blue Team Toolkit.* Wiley.

The Nmap Project. (2022). *Nmap: The Network Mapper.* Obtido de https://nmap.org/.

Toesland, F. (2016). *Why SME's are big targets for cyber crime.* London, UK.

Tulloch, M., Northrup, T., & Honeycutt, J. (2019). *Windows 10 Inside Out. Microsoft Press.*

Tzu, S. (2022). *Art of War.*

US State of Cybercrime Survey. (2013). Obtido de https://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

Virtualbox, O. V. (2022). *User Manual.* Obtido de https://www.virtualbox.org/manual/

VMware, Inc. (2019). *VMware vSphere Basics.* . VMware Documentation.

Watkins, S. (2019). *Implementing ISO 27001 in Small Businesses.*

Whitman, M. E., & Mattord, H. J. . (2018). *Management of information security.* Cengage Learning.

Wireshark. (2023). Obtido de Wikipedia: https://en.wikipedia.org/wiki/Wireshark

Zeller, J. (2019). *Blue team basics: A guide to the essentials of network security.* Packt Publishing.

Zenko, M. (2015). *Red team: how to succeed by thinking like the enemy.* New York: Routledge.