Abordagem para Melhoria de Segurança Cibernética em Organizações Considerando Severas Restrições de Custo

Approach to Cybersecurity Improvement in Organizations Considering Severe Cost Constraints

Autor: Mateus Guerra

Co-Autor: Fernando Aires, Robson Medeiros

Resumo

A sociedade vem aumentado o interesse na Segurança da Informação e na Segurança Cibernética; este aumento pode ser explicado em parte pelo aumento da quantidade e complexidade de ataques cibernéticos a organizações. Dada a complexidade e o custo associados à implementação de soluções de segurança, pequenas e médias empresas frequentemente se encontram vulneráveis a ataques cibernéticos. Este artigo propõe uma abordagem para a melhoria da segurança cibernética em organizações que enfrentam restrições de orçamento. Nossa proposta se baseia na utilização de ferramentas *open-source* e de baixo custo, recomendadas por meio de um processo semi-automatizado. Este processo considera tanto a estrutura organizacional quanto o ambiente tecnológico, a fim de oferecer soluções que equilibrem custo e eficácia. Utilizando como base *frameworks* como NIST e ISO 27001, a abordagem proposta ajuda organizações a priorizar medidas de segurança considerando severas restrições orçamentárias.

Palavras-chave: Segurança Cibernética, *Open-source*, Custo, NIST, ISO 27001

Abstract

Society has acquired an increased interest in Information Security and Cybersecurity; This increase can be explained partially due to the rise in variety and complexity of cyber attacks towards organizations. Due to the complexity and cost associated with implementing security solutions, small and medium-sized businesses often find themselves vulnerable to cyberattacks. This paper proposes an approach to improve cybersecurity in organizations facing budget constraints. Our proposal relies on the use of open-source and low-cost tools, recommended through an automated process. This process considers both the organizational

structure and the technological environment to offer solutions that balance cost and effectiveness. Based on frameworks like NIST and ISO 27001, the proposed approach helps organizations prioritize security measures without compromising their budget.

Keywords: Cybersecurity, Open-source, Cost, NIST, ISO 27001

---

1. Introdução

A segurança cibernética tem emergido como uma das principais preocupações para organizações de todos os setores, devido à crescente dependência de sistemas digitais e à sofisticação dos ataques cibernéticos[1]. A vulnerabilidade de uma rede, o comprometimento de dados ou a interrupção dos serviços podem gerar consequências graves para as empresas, que variam desde prejuízos financeiros severos até a perda de credibilidade e reputação junto aos clientes e parceiros. Grandes corporações têm condições de investir em soluções de ponta e profissionais qualificados para mitigar esses riscos. Entretanto, organizações de pequeno e médio porte frequentemente enfrentam dificuldades para garantir níveis satisfatórios de proteção cibernética.

Essas dificuldades aumentam devido a restrições orçamentárias, especialmente em cenários onde a segurança digital compete por recursos com outras áreas críticas da organização. Cerca de 60% das pequenas empresas que sofrem um ataque cibernético vão à falência em até seis meses [2]. Essa vulnerabilidade se deve não apenas à falta de soluções robustas instaladas, mas também à carência de profissionais capacitados. A pandemia do COVID-19 ampliou essa vulnerabilidade ao impulsionar a transição de muitas atividades para o ambiente remoto, expondo ainda mais as falhas de segurança de pequenas e médias empresas. Com a migração de infraestruturas para o ambiente digital, o número de ataques cibernéticos aumentou significativamente [3][4]. Nesse contexto, é pertinente que soluções eficientes, de baixo custo e acessíveis, sejam desenvolvidas para proteger esses negócios.

Este artigo propõe uma abordagem para a melhoria da segurança cibernética considerando severas restrições de custo. A proposta é fundamentada no uso de ferramentas

de código aberto e metodologias que minimizem o investimento financeiro, sem comprometer significativamente a proteção da infraestrutura digital das empresas. Utilizando como base os *frameworks* NIST (*National Institute of Standards and Technology*) e ISO 27001, bem como ferramentas automatizadas, a abordagem visa oferecer recomendações específicas para organizações com recursos limitados. Além disso, foi elaborado um protótipo demonstrando as telas de uma aplicação *Web*, em formato de questionário, que aplica a abordagem aqui desenvolvida direcionada ao usuário final.

Dessa forma, o presente artigo se estrutura da maneira que se segue. A Seção 2 apresenta conceitos básicos sobre segurança cibernética e as ferramentas *open-source* que podem ser utilizadas para recomendações de segurança. A Seção 3 discute os trabalhos relacionados e o estado da arte em termos de segurança digital considerando cenários com restrições de custo. Na Seção 4, é proposto um processo específico para a implementação de segurança cibernética em organizações com orçamentos financeiros limitados. A Seção 5 descreve o protótipo automatizado desenvolvido para facilitar a implementação dessa abordagem e os resultados obtidos até o momento. Finalmente, na Seção 6, são apresentadas as conclusões do trabalho e sugestões para estudos futuros.

2. Conceitos Básicos

A segurança cibernética envolve um conjunto de práticas, tecnologias e processos projetados para proteger redes, dispositivos, programas e dados contra alterações ou acessos não autorizados. Em um cenário onde o ciberespaço se torna cada vez mais relevante para as operações comerciais, é fundamental que organizações implementem medidas robustas para garantir a integridade de seus ativos digitais. No entanto, devido à falta de recursos de muitas organizações, o desafio está em alcançar um nível satisfatório de proteção com orçamentos limitados.

O *framework* do *National Institute of Standards and Technology* (NIST) se destaca como um dos modelos mais adotados para estruturar uma política de segurança [5]. O NIST define cinco funções principais que orientam a implementação de segurança cibernética em qualquer ambiente: Identificar, Proteger, Detectar, Responder e Recuperar [6]. Cada uma dessas funções cumpre um papel específico no ciclo de segurança de uma organização:

- **Identificar**: esta função se refere à compreensão dos ativos de uma organização, seus dados sensíveis e as possíveis ameaças que possam surgir. O objetivo é identificar os pontos que necessitam de proteção e os recursos disponíveis para implementar esta proteção.
- **Proteger**: uma vez que os ativos são identificados, a próxima etapa envolve a aplicação de medidas de proteção para mitigar as ameaças. Alguns exemplos de soluções podem incluir o uso de criptografia, políticas de controle de acesso, autenticação de usuários e a implementação de *firewalls* para prevenir o acesso não autorizado.
- **Detectar**: as soluções de detecção visam monitorar continuamente a rede e os sistemas da organização para identificar eventuais ataques ou tentativas de violação. Ferramentas como sistemas de detecção de intrusão (IDS) e monitoramento de *logs* são essenciais para detectar anomalias no comportamento da rede.
- **Responder**: quando um ataque é detectado, a organização precisa de um plano de resposta eficiente. Esse plano deve incluir ações para conter o ataque, minimizar os danos e notificar as partes interessadas.
- **Recuperar**: após conter o ataque, a organização precisa restaurar os sistemas comprometidos e implementar melhorias na segurança para evitar que o incidente se repita. A recuperação inclui a restauração de dados perdidos e a retomada das operações normais.

Essas cinco funções são interdependentes e visam garantir uma abordagem abrangente para a segurança cibernética, particularmente em cenários onde os recursos são limitados. O *framework* NIST permite que as organizações implementem medidas de segurança de forma gradual, priorizando áreas críticas e ajustando as estratégias conforme os recursos disponíveis.

Outro aspecto importante da segurança cibernética é o uso de ferramentas e soluções *open-source*. Ferramentas de código aberto têm se mostrado eficazes não apenas em cenários de restrições orçamentárias, estando presentes em boa parte da indústria devido ao seu baixo custo financeiro associado e escalabilidade [7]. Além disso, o uso dessas ferramentas facilita a customização e adaptação das soluções para atender às necessidades específicas de cada organização.

Por fim, é importante destacar que a implementação de segurança não é apenas uma questão técnica. Ela envolve também a conscientização dos usuários e colaboradores da organização. Ataques de engenharia social, como *phishing*, muitas vezes exploram as vulnerabilidades humanas em vez de falhas técnicas. Essas abordagens se mantêm como um dos principais veículos pelos quais agentes maliciosos conseguem invadir sistemas [8], devido à falta de cuidado que indivíduos têm com os dados que lhe são confiados por não entenderem como esses ataques os manipulam. Portanto, a educação dos colaboradores em práticas seguras é parte integrante de uma estratégia de segurança cibernética eficaz.

3. Trabalhos Relacionados

A literatura em segurança cibernética é vasta e abrange diferentes abordagens para melhorar a proteção digital de organizações. No entanto, quando o foco está em soluções voltadas para organizações com restrições orçamentárias, a quantidade de trabalhos se reduz consideravelmente, especialmente aqueles que propõem soluções práticas e acessíveis para pequenos negócios ou empresas com baixo poder de investimento disponível.

Alguns dos trabalhos mais relevantes no contexto de segurança cibernética com restrições de custo são de projetos *open-source*. Organizações como a MITRE Corporation, que mantém o banco de dados de vulnerabilidades comuns (CVE) e fraquezas comuns (CWE), desempenham um papel crucial no fornecimento de informações sobre vulnerabilidades conhecidas, permitindo que pequenas empresas possam identificar e mitigar riscos em seus sistemas antecipadamente[9]. Esse tipo de recurso público e acessível tem sido amplamente explorado para proporcionar soluções de segurança eficazes sem custos atrelados.

Outro trabalho significativo é o *framework* de segurança digital proposto pelo NIST. O *framework* NIST para Melhoria da Segurança em Infraestruturas Críticas oferece um guia estruturado que auxilia organizações na implementação de políticas de segurança digital, mesmo em ambientes onde os recursos são limitados[6]. O diferencial desse *framework* é que ele não exige grandes investimentos iniciais, já que permite a adoção progressiva de medidas de segurança. Cada organização pode implementar as etapas conforme suas necessidades e disponibilidade de recursos, começando pelas áreas mais críticas. Esse modelo de segurança cibernética permite um alto grau de flexibilidade, sendo uma escolha adequada para organizações menores.

Também há o trabalho relevante da ISO 27001, que estabelece diretrizes para a implementação de sistemas de gestão de segurança da informação[10]. Essa norma é amplamente reconhecida e, embora seja muitas vezes aplicada em grandes corporações, também pode ser adaptada para empresas de menor porte. A implementação da ISO 27001 em um ambiente com restrições orçamentárias exige foco na personalização das políticas de segurança e na priorização de investimentos em áreas que representem maior risco para a organização. Muitas das medidas descritas na norma podem ser adotadas sem a necessidade de grandes investimentos, dependendo do nível de complexidade que a organização estiver disposta a implementar. Também é válido mencionar a existência do *Self-Assessment Questionnaire* da ISO 27001, uma ferramenta que permite às empresas avaliarem a conformidade de seus sistemas com as normas de segurança estabelecidas pela ISO através do preenchimento de um *checklist* de segurança. Essa abordagem proporciona uma visão geral da maturidade do sistema de segurança da empresa, permitindo identificar áreas críticas que precisam ser aprimoradas sem a necessidade de uma auditoria formal

Além dos *frameworks* estabelecidos, iniciativas de conscientização de segurança, como a KnowBe4, também contribuem de forma significativa [11]. KnowBe4 é uma plataforma que oferece uma série de ferramentas voltadas à capacitação dos colaboradores para reconhecer e evitar ataques cibernéticos de engenharia social, como *phishing*. Em vez de focar em soluções tecnológicas, a plataforma prioriza o treinamento humano com testes e simulações de ataques, como *spear phishing*, que podem ser realizados dentro da plataforma, gerando relatórios sobre a eficácia da segurança baseada no comportamento humano. Isto é particularmente relevante em pequenas organizações, onde a infraestrutura tecnológica é limitada e a vulnerabilidade humana é um ponto crítico de exposição.

Além disso, o desenvolvimento de ferramentas de automação voltadas para a segurança também tem sido um campo de estudo crescente. Em muitos casos, ferramentas que executam varreduras automáticas, como o Nmap, permitem que pequenas organizações analisem suas redes sem a necessidade de especialistas ou consultorias externas. O Nmap, por exemplo, é uma ferramenta gratuita e *open-source* que pode ser utilizada para mapear a infraestrutura da rede de uma organização, detectando portas abertas, serviços em execução e sistemas operacionais vulneráveis. Essa análise fornece um ponto de partida valioso para organizações que precisam identificar suas fraquezas e buscar contramedidas, sem os custos associados a soluções de segurança proprietárias.

Dentre algumas obras relacionadas, vale a pena citar o trabalho de Lerums *et al*, intitulado *Simulation Modeling Cyber Threats, Risks and Prevention Costs* (2018) [12]. Neste artigo, Lerums *et al* descrevem diferentes cenários em que um agente malicioso pode invadir uma rede ou um host vulnerável, ou realizar engenharias sociais, considerando todos os nós intermediários desta rede (por exemplo modems, IDS/IPS, programas de antivírus), assim como suas respectivas contramedidas. Dessa forma, o artigo auxilia organizações a conscientizar sobre o que esperar de um ataque hacker e como remediar essas possíveis invasões. Em relação à parte financeira, este artigo apresenta estatísticas referentes aos prejuízos causados por ataques maliciosos no ano de 2016 nos Estados Unidos. Embora seja um trabalho mais informativo, Lerums *et al* foca em ações de segurança ao invés do gasto com segurança propriamente dito, não considerando o possível alto investimento que algumas dessas ações podem requisitar.

Por sua vez, A. Master, G. Hamilton e J. Dietz propõe contribuições adicionais em cima do trabalho de Lerums *et al*, trazendo dados matemáticos como estatísticas de ataques que podem ser bem sucedidos ou não a depender de certa topologia de rede [13]. Os autores propõem um software para simulação de ataques mais elaborado, que pode auxiliar organizações de várias escalas a discutir seus investimentos a serem aplicados à segurança durante sua engenharia de requisitos. Semelhante a esta proposta, existe também a ferramenta *Web* desenvolvida por J. Gallardo, R. Torres e O. Tessini [14], que propuseram usar tal ferramenta usando outros modelos de maturidade influentes no mercado de base, como o já citado NIST e principalmente o *Critical Security Controls Version 8* (CIS V8) [15]. Foi desenvolvido uma aplicação *Web* que, através de questionários, auxilia organizações a identificarem o seu nível de maturidade para com segurança da informação, de acordo com sua conformidade com os modelos de maturidade apresentados. A ferramenta oferece também dados gráficos sobre a situação atual da organização e as principais salvaguardas a serem priorizadas de acordo com o CIS V8. O trabalho de Gallardo *et al* aborda o problema discutido neste trabalho de maneira diferente. A sua ferramenta *Web*, disponível no domínio cibermadurez.cl, auxilia leigos em cibersegurança a remediar suas falhas e vulnerabilidades, porém esta ferramenta simplesmente aponta para as salvaguardas relevantes dos modelos de maturidade que estudou, servindo como um recurso intermediário com uma interface gráfica mais acessível. Neste trabalho, buscamos usar as salvaguardas descritas no NIST e associar elas a possíveis práticas, custos, ferramentas e competências profissionais.

Os pesquisadores I. Mlakar, P. Jeran *et al* desenvolveram uma ferramenta de *Security as a Service* (SecaaS) voltada para pequenos e microempreendimentos denominada

PALANTIR [16]. O PALANTIR consiste na ideia de se oferecer uma única ferramenta de segurança de baixo custo, sem fragmentá-la em diferentes áreas, como por exemplo grupos que são especializados em oferecer apenas ferramentas de antivírus, ou apenas *firewalls* ou apenas Sistemas de Detecção e Prevenção de Intrusão (IDPS), etc. O PALANTIR e o trabalho que o apresenta são uma das soluções que pode ser relacionada com o objetivo deste trabalho, pois apesar de existir para resolver o mesmo problema aqui discutido, se difere em como o aborda, desenvolvendo uma solução única e holística voltada para infraestruturas de virtualização de funções de redes (NFVI).

O PALANTIR e alguns outros projetos oferecem soluções de cibersegurança na forma de ferramentas e software como um produto voltado a pequenas organizações. Estes produtos muitas vezes seguem um *framework* ou um algoritmo de *Machine Learning* (ML) para tratar da logística e segurança dos dados de seus clientes, e não necessariamente levantam uma conscientização para a importância da segurança, ou transmitem um conhecimento de como implementá-la, que é um dos objetivos deste trabalho. Para citar alguns destes projetos descritos além do PALANTIR, existe o SENTINEL [17], desenvolvido com foco na conformidade com o Regulamento Geral sobre a Proteção de Dados (GDPR) e proteção de dados pessoais para pequenos empreendimentos. Por sua vez, o projeto PUZZLE [18] oferece um *marketplace* de soluções em cibersegurança utilizando tecnologias de ML e *Blockchain.* Finalmente, o projeto IRIS [19] usa inteligência artificial para monitoramento de redes e resposta a incidentes e emergências orientado a *Threat Intelligence* de vulnerabilidades em dispositivos IoT.

Portanto, os trabalhos relacionados foram selecionados por proporcionarem alternativas semelhantes à proposta deste artigo. Estas alternativas incrementam a segurança digital, nem sempre conciliando com a realidade orçamentária das pequenas e médias empresas. A combinação de *frameworks* estabelecidos, como NIST e ISO 27001, com ferramentas *open-source* e soluções de conscientização, forma a base para uma abordagem prática e viável para organizações que buscam melhorar sua postura de segurança cibernética.

4. Processo Proposto

O processo proposto neste trabalho visa oferecer uma abordagem estruturada para a melhoria da segurança cibernética, utilizando ferramentas acessíveis e de baixo custo. A

proposta tem como base a automação de tarefas e a simplificação do processo de implementação de medidas de segurança, a fim de reduzir a total dependência de especialistas em segurança e minimizar os custos associados à aquisição de soluções proprietárias. O processo segue um fluxo de atividades, culminando em *outputs* listando ferramentas de código aberto que melhor se adequam ao perfil do usuário realizando estas atividades. O usuário final é guiado por estas atividades por uma aplicação em formato de questionário, que divide estas atividades em seções diferentes.

4.1 O Processo

O processo proposto foi desenhado seguindo BPMN (*Business Process Model and Notation*), que é um padrão para modelagem de processos amplamente divulgado e utilizado atualmente. Este processo é dividido em 6 subprocessos que integram a filosofia do *framework* NIST e suas funções, como discutido a seguir:

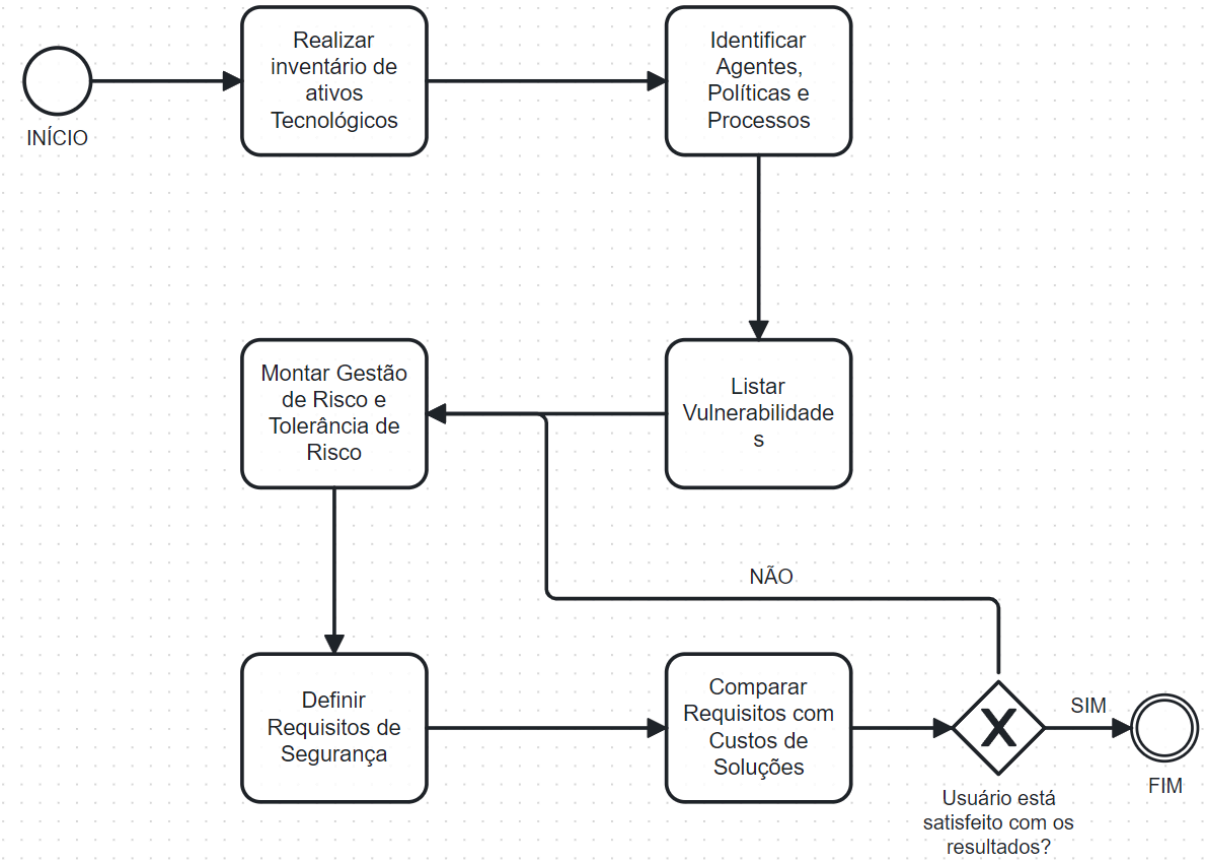

Figura 1. Estratégia para implementação de segurança descrita no BPMN.

1. **Realizar Inventário de Ativos Tecnológicos**. Essa atividade visa juntar dados que vão criar um escopo dos possíveis ataques cibernéticos que podem acontecer na organização. Nesta atividade, os usuários fornecem informações básicas sobre a sua infraestrutura e seus ativos, incluindo detalhes sobre sistemas operacionais, serviços de rede, dispositivos conectados e os tipos de dados sensíveis que são manipulados. Por ativos se entende como, por exemplo, servidores, computadores de mesa, *laptops*, impressoras, *switches* de rede, roteadores, *firewalls, access points*, dispositivos de armazenamento, UPS (fonte de alimentação ininterrupta), monitores, teclados e mouses, projetores, telefones VoIP, sistemas de conferência de áudio/vídeo, sistemas operacionais, dispositivos de *backup*, cabos de rede, licenças de *software*, máquinas virtuais, dispositivos móveis, dispositivos conectados à rede, periféricos, equipamentos de *data center*, câmeras de segurança e equipamentos de vigilância, assinaturas de serviços em nuvem, aplicativos de *software*, chaves de licença e códigos de ativação, bem como número das versões, *firmware* e *drivers* dos itens listados acima. Para auxiliar nessa tarefa, o processo pode ser implementado utilizando ferramentas como o Nmap, que realiza uma varredura automatizada da rede da empresa e gera um relatório detalhado sobre os dispositivos e serviços presentes.

   A automação dessa etapa é importante, pois permite que pequenas organizações obtenham uma visão clara de seus pontos de vulnerabilidade com acurácia. As informações coletadas nesta etapa são numerosas e sensíveis a muitas variações, tornando uma coleta manual pouco eficaz e suscetível a erros. Com o uso do Nmap, por exemplo, é possível detectar portas abertas, identificar sistemas operacionais e serviços vulneráveis dentro de uma rede alvo.
2. **Identificar Agentes, Políticas e Processos**. Neste segundo subprocesso é onde será consolidado todo o escopo do ambiente de trabalho da organização que deseja implementar a cibersegurança. Além de ter em mente toda a abrangência de tecnologias disponíveis, é igualmente importante determinar qual o nível de maturidade das pessoas deste ambiente. Por maturidade entende-se como as políticas aplicadas neste ambiente, a conformidade dos agentes com essas políticas, como esses agentes tratam dados sensíveis da organização, e a consciência de sua responsabilidade para com esses dados. Isto porque a cibersegurança herda os três pilares mencionados no *framework* PPT (comumente usado em gerenciamento de negócios): Pessoas, Processos e Tecnologia. A etapa anterior a esta aborda a segurança das tecnologias do ambiente, enquanto este passo enfatiza a definição de

um escopo de quais processos são utilizados, e como as pessoas se comportam neste ambiente. O inventário de agentes e de políticas exige que a organização submeta sua força de trabalho a alguns tipos de testes para medir sua maturidade, e para tal é importante distribuir questionários que abordam temas de segurança. Alguns autores de *frameworks* de segurança populares já desenvolveram guias que detalham sobre como manter uma boa cultura de segurança em sua organização. Por exemplo, a ISO e KnowBe4 são entidades populares que desenvolveram questionários que avaliam seu nível de maturidade em segurança.

3. **Listar Vulnerabilidades**. Os dois subprocessos anteriores montam o escopo dos meios pelos quais um agente malicioso pode atacar um sistema através de suas respectivas vulnerabilidades. Portanto, esta atividade conclui a montagem da superfície de ataque deste agente, compilando estas vulnerabilidades que podem ser exploradas. Por superfície de ataque entende-se como o escopo de opções que um agente malicioso pode interagir com sua infraestrutura, e explorar suas falhas. Um *endpoint* operando com um sistema operacional antigo, com poucas atualizações de segurança, faz tanto parte de uma superfície de ataque quanto um funcionário suscetível a práticas de engenharia social. Com os itens listados nas etapas anteriores, é possível percorrer bases de dados em busca de vulnerabilidades que dizem respeito ao inventário realizado. Com isto, é possível anotar extensivamente quais são essas vulnerabilidades. É importante não desconsiderar nenhuma vulnerabilidade, independente de sua criticidade, pois a decisão de quais vão ser consideradas ou ignoradas não diz respeito ao subprocesso atual, cabendo, sim, ao gerenciamento de risco. Algumas bases de dados importantes para consultar vulnerabilidades são o *Common Weakness Enumeration* e *Common Vulnerabilities and Exposures*. Importante destacar a diferença entre a CWE e CVE, esta sendo que a primeira é uma base de dados focada em vulnerabilidades genéricas, separadas em categorias, enquanto a CVE documenta vulnerabilidades específicas de acordo com a data e a plataforma em que foi descoberta. Por exemplo, uma vulnerabilidade de *buffer overflow* recém descoberta em uma aplicação nova seria documentada na base CWE dentro da mesma categoria CWE-120 que aborda todos os *buffer overflows* conhecidos, enquanto que na CVE estaria documentada com um identificador único como CVE-2023-12345. O OWASP *Top 10* também é uma base de dados importante, mas é voltada para segurança de aplicações *Web* [20].

4. **Montar Gestão de Risco e Tolerância de Risco**. Tendo a superfície de ataque completamente mapeada, neste momento é possível avaliar quais são as vulnerabilidades mais importantes a serem corrigidas dentro da organização, de acordo com seus objetivos. Quais dados devem ser criptografados? Quais terminais devem ser protegidos? Que treinamento deve ser submetido à força de trabalho? A gestão da organização deve ter seus objetivos de negócio em mente para discernir o que se adequa a sua gestão de risco e apetite de risco. É válido mencionar também a diferença entre apetite e tolerância de risco. O apetite de risco se refere a uma qualificação de alto nível de quanto risco uma organização está disposta a se submeter em suas atividades diárias. A tolerância de risco existe dentro desta ideia de apetite, representando quantas perdas ou declínios em seu desempenho a organização está disposta a sofrer antes de mudar seu comportamento, possivelmente reestruturando seu apetite de risco.
5. **Definir Requisitos de Segurança**. Neste momento, a organização possui ciência de quais riscos ela está submetida, e quais destes riscos ela busca mitigar. Com esses dados, este subprocesso foca em quais são os requisitos técnicos de segurança que se deseja perseguir. Se a atividade anterior identificou que deve se priorizar a segurança em *endpoints*, é interessante priorizar ferramentas de IDPS *host-based*. Caso tenha se identificado que é necessário priorizar a segurança de toda a rede, é interessante priorizar ferramentas IDPS *network-based*. Para filtragem de tráfego, priorizar *firewalls*, para evitar ataques de *malware*, antivírus, etc. Nesta etapa passamos a associar o gerenciamento de risco da organização com soluções em tecnologia, sem nomear especificamente quais ferramentas serão usadas ainda.
6. **Comparar Requisitos com Custos de Soluções:** Por fim, a organização deve considerar o seu contexto financeiro a fim de decidir quais soluções específicas ela deseja adotar. Neste momento, a mesma deve saber quais tecnologias ela precisa em seu ambiente de trabalho, e também tem acesso às soluções que melhor se adequam a dito ambiente. Caso não esteja satisfeito com os resultados, o usuário deve elaborar novamente sua gestão e apetite de risco. Isto porque sua infraestrutura não vai mudar, e ele deve alcançar um resultado satisfatório revendo sua estratégia de negócios para receber recomendações de segurança que o satisfaçam. Com este subprocesso feito, a estratégia de implementação de segurança está finalizada.

4.2 Ferramentas Analisadas

A fim de conseguir demonstrar resultados para as etapas finais do processo proposto, foram estudadas algumas soluções de código aberto. Seguindo o *framework* NIST, as funções que englobam maior empregabilidade de soluções de tecnologia são as funções de Proteção, Detecção e Resposta, dado que as funções Identificar e Recuperar descrevem salvaguardas mais relacionadas a gerenciamento e conformidade. Estas funções são melhor reforçadas através de programas de educação e conscientização de ameaças.

A metodologia usada para a amostragem das ferramentas foi feita usando um comparativo direto entre as salvaguardas do *framework* NIST e soluções de segurança já existentes. Por exemplo, o item DE.AE-1 da função de Detecção, categoria de Anomalias e Eventos, fala sobre estabelecer e gerenciar um padrão de operações e fluxo de dados esperado para os usuários e seus sistemas. Utilizando consultas em motores de busca como *Google* e *Brave Search*, essas características são encontradas em tecnologias de sistemas de detecção de intrusão (IDS). Uma das tecnologias estudadas que se encaixa nas descrições de Proteção são o uso de programas de antivírus. E as tecnologias que melhor se encaixam nas descrições das funções Detectar e Responder são os sistemas de detecção e prevenção a intrusões (IDS/IPS).

No contexto da segurança cibernética, as ferramentas de *Intrusion Detection Systems* e *Intrusion Prevention Systems* desempenham um papel fundamental ao monitorar o tráfego de rede e identificar potenciais ameaças. Durante o desenvolvimento deste trabalho, foram avaliadas várias soluções *open-source* de IDS e IPS, com o objetivo de selecionar aquelas que oferecessem a melhor relação entre custo e funcionalidade em organizações com recursos limitados.

4.2.1 Snort

Uma das principais ferramentas estudadas foi o *Snort*, um IDS amplamente utilizado na comunidade de segurança cibernética. O *Snort* é uma ferramenta de código aberto que se destaca por sua capacidade de detectar uma ampla gama de ataques, incluindo tentativas de exploração de vulnerabilidades, varreduras de portas, ataques de negação de serviço (DoS), entre outros. A ferramenta funciona monitorando o tráfego de rede em tempo real e comparando esse tráfego com uma base de dados de assinaturas de ataques conhecidos. O grande diferencial do *Snort* é sua flexibilidade. Ele pode ser configurado tanto como um IDS (apenas detectando ataques) quanto como um IPS, bloqueando ativamente o tráfego

malicioso antes que ele afete a rede. Além disso, o *Snort* permite que os usuários criem suas próprias regras de detecção, adaptando a ferramenta às necessidades específicas da organização. Essa característica torna o *Snort* uma escolha interessante para empresas que precisam de soluções personalizáveis, mas que não têm os recursos para investir em IDS/IPS proprietários.

4.2.2 Suricata

Outra ferramenta de IDS/IPS estudada foi o *Suricata*. Assim como o *Snort*, o *Suricata* é uma ferramenta de código aberto projetada para monitorar o tráfego de rede em busca de padrões de ataque. No entanto, o *Suricata* se diferencia por seu desempenho superior em redes de alta velocidade, uma vez que é capaz de utilizar várias *threads* de processamento simultaneamente, o que permite a análise de grandes volumes de tráfego de forma eficiente. O *Suricata* também suporta a detecção de intrusões baseadas em regras e assinaturas, além de ser compatível com regras de *Snort*, o que facilita a transição entre as ferramentas ou a adoção conjunta. Outro ponto positivo do *Suricata* é sua capacidade nativa de realizar a análise profunda de pacotes (DPI), o que permite identificar ataques que estão ocultos em camadas superiores do protocolo, como em aplicações *Web* ou em comunicações criptografadas. Isso amplia a cobertura de detecção, tornando-o adequado para empresas que precisam monitorar tráfego variado e não têm recursos para investir em soluções comerciais mais avançadas.

4.2.3 Zeek (antigo Bro)

O *Zeek* (anteriormente conhecido como *Bro*) é uma ferramenta de análise de tráfego de rede que, embora possa ser utilizada como IDS, adota uma abordagem diferente das soluções tradicionais baseadas em assinaturas. O *Zeek* realiza a análise dos eventos gerados pelo tráfego de rede e armazena essas informações em *logs*, permitindo uma inspeção detalhada posterior. Isso torna o *Zeek* mais adequado para cenários em que a organização deseja ter uma visão mais profunda das atividades da rede, ao invés de apenas detectar e bloquear ataques em tempo real. Uma das grandes vantagens do *Zeek* é sua flexibilidade e a capacidade de ser adaptado a diversos cenários de uso, graças à sua linguagem de *script* que permite criar políticas específicas de monitoramento. No entanto, essa mesma flexibilidade pode ser um desafio para pequenas organizações, que podem não ter o conhecimento técnico necessário para explorar completamente as capacidades da ferramenta.

4.2.4 OSSEC

O *OSSEC* é outra ferramenta de código aberto estudada neste trabalho, especialmente no contexto de monitoramento de *host* e detecção de intrusões. Diferente do *Snort* e do *Suricata*, que são voltados principalmente para o monitoramento de rede, o *OSSEC* atua como um *Host-based Intrusion Detection System* (HIDS), monitorando atividades e mudanças dentro dos sistemas operacionais dos dispositivos. Essa ferramenta é especialmente útil em ambientes onde o monitoramento de cada *host* individual é necessário, sendo capaz de identificar comportamentos anômalos diretamente nos servidores ou computadores monitorados.

O *OSSEC* trabalha verificando *logs* do sistema, registros de eventos, arquivos de configuração, e outras atividades críticas, e é capaz de identificar tentativas de invasão, alterações não autorizadas e outros comportamentos suspeitos. Uma das vantagens da ferramenta é que ela não apenas detecta atividades maliciosas, mas também pode ser configurada para responder automaticamente a determinados eventos, aplicando políticas de segurança que bloqueiam ou isolam o sistema comprometido. Essa capacidade de resposta automática é um diferencial importante, permitindo que organizações de pequeno porte, com recursos limitados, possam reagir de forma rápida e eficiente a incidentes de segurança. Além disso, o *OSSEC* pode ser configurado para gerar relatórios periódicos que detalham as atividades monitoradas e as respostas aplicadas, permitindo que as organizações tenham um registro detalhado de incidentes e ações tomadas, o que é essencial para auditorias e análises posteriores.

4.2.5 Comparativos entre IDS/IPS

No contexto do processo proposto, as ferramentas de IDS/IPS desempenham um papel central na detecção e resposta a incidentes. A implementação dessas ferramentas permite que as organizações monitorem seu tráfego de rede de forma contínua, identificando padrões anômalos que podem indicar tentativas de intrusão. Para organizações com restrições de custo, a escolha entre *Snort*, *Suricata* e *Zeek* depende da complexidade de suas redes e de suas necessidades específicas de segurança.

Para clarificar o porquê de alguns tópicos específicos serem selecionados como comparativos entre IDPS, segue aqui uma breve explicação: um sistema de detecção e/ou prevenção de intrusão é um *software* configurado para monitorar o tráfego que passa por algum nó de uma rede, a fim de evitar ataques cibernéticos. Um IDPS pode tanto estabelecer um *baseline* de operações que seja esperado numa rede, bloqueando toda atividade fora de conformidade (*log based*), ou usa conjuntos de regras (*rulesets*) para detectar ameaças comuns e padrões no tráfego de pacotes que sejam indício de algum ataque conhecido em sua base de dados (*rule based*). IDS são focados em detectar essas anormalidades de rede e alertar as partes responsáveis para repelir o ataque, enquanto IPS são focadas em prevenir ataques detectados, como, por exemplo, bloqueando endereços de IP. Apesar desta distinção, alguns desses sistemas são capazes de realizar os dois, e portanto são classificados como IDPS.

Outros tópicos relevantes para comparação são o suporte a *multi-threading* ou escalabilidade, ser baseado em *hosts* ou em redes, e tecnologia de *Packet Capture Acceleration*. Escalabilidade e tecnologia de *multi-threading* são relacionadas, pois um IDPS que seja capaz de executar diferentes *threads* em um processador ao mesmo tempo, é capaz de processar quantidades maiores de pacotes, oferecendo um tempo de execução menor para filtrar o tráfego de uma rede. Isto permite que seus usuários possam expandir sua infraestrutura numa organização, sem se preocupar tanto com a quantia de pacotes adicionais gerados, enquanto que IDPS de *thread* única podem provocar gargalos devido a sua menor eficácia. Naturalmente, tecnologia de *multi-threading* reflete um gasto maior no consumo dos recursos computacionais das máquinas em que está instalado, enquanto que IDPS de *thread* única geralmente apresentam custos mínimos. IDPS baseados em rede ou em *host* diferem-se na localização onde são configurados numa topologia de rede. Se este for baseado em redes, tipicamente este fica configurado em um roteador, *switch*, ou outros nós de borda. Se for baseado em *hosts*, fica tipicamente instalado nas máquinas dos usuários com acesso à *internet*. Esta diferenciação é importante, pois a gama de ataques que podem ser detectados também é diferente. Por exemplo, existe uma diferença entre uma infraestrutura de rede ser atacada por algum agente malicioso diretamente da *Internet* (como um ataque externo) e entre ser infectada internamente por algum usuário que conectou um aparelho infectado na rede (intencionalmente ou não). Por fim, *Packet Capture Acceleration* é uma tecnologia que tira proveito de algumas placas de rede que possuem capacidade de processar pacotes. Um IDPS que possui suporte a PCA consegue filtrar os pacotes que passam pelo seu nó da rede

sem precisar consumir recursos do processador de uma máquina, por exemplo, aumentando assim sua eficácia.

A Tabela 1 apresenta uma visão comparativa das principais IDPS pesquisadas. Snort, Suricata, OSSEC e Zeek, classificadas por suporte a GUI, ser baseado em *rulesets* ou em *logs*, baseado em redes ou em *hosts*, escalabilidade/suporte a *multi-threading*, suporte a *Packet Capture Acceleration*, abundância de *plugins* desenvolvidos, e quão eficazes esses softwares são (em questão da quantidade de recursos computacionais consumidos durante a execução)

\	GUI	*Rule-based*	*Log-based*	Network-based	*Host-based*	Multi-thread	PCA	*Plugins*
Snort	X	X		X				X
Suricata		X		X		X	X	X
OSSEC		X	X		X	X		
Zeek	X	X*	X*	X		X	X	

Tabela 1. Comparação entre os IDPS Snort, Suricata, OSSEC e Zeek

Os tópicos de configuração baseado em *rulesets* ou *logs* estão destacados no caso do Zeek, pois este usa um método diferente para buscar anomalias no tráfego de sua rede, o já mencionado *ZeekScript* uma linguagem semelhante a C.

Certos IDPS apresentam algumas das funcionalidades descritas anteriormente, mesmo que isto não seja refletido na tabela. Por exemplo, o OSSEC possui suporte a monitoramento a nível de redes (não apenas de *hosts*), assim como também existem *softwares* e *plugins* terceiros que oferecem uma interface gráfica para o usuário, mas nenhum destes é o foco do produto. O motivo de alguns destes itens estarem desmarcados na Tabela 1 é porque a maioria destes *softwares* são flexíveis o suficiente para funcionarem com funções não imediatamente disponíveis a eles. Portanto, muitos deles cumpririam vários, senão todos os critérios listados na tabela. A fim de traçar uma comparação mais concreta, foram marcados os itens que mais condizem com a proposta inicial de cada uma destas ferramentas e os pontos que mais se destacam em suas versões mais básicas.

Com isto em mente, a Tabela 1 mostra uma seleção de ferramentas financeiramente acessíveis que são flexíveis o suficiente para suprirem a maioria dos requisitos de segurança de uma organização para Detecção e Resposta de ameaças, mas destaca os seus pontos fortes para melhor alinhar os objetivos de ditas organizações com uma seleção ideal do *software*

Por último, os antivírus são soluções que também foram consideradas como parte da função de Proteger do *framework* NIST, e são soluções igualmente importantes para a segurança, quando comparadas com outras já citadas aqui. Entretanto, não existem antivírus que sejam mais ou menos adequados para um nível corporativo, se comparados com o uso pessoal. Existem diferenças de performance e funcionalidades entre eles, mas como são ferramentas para uso exclusivo de detecção de *malwares* em *endpoints*, há pouca diferença entre os critérios que uma pessoa jurídica e uma pessoa física buscam em uma solução de antivírus. Dito isso, como são ferramentas de segurança populares, existe uma abundância de materiais comparativos entre os principais antivírus no mercado. Neste trabalho, são recomendadas as análises disponíveis no domínio *antivirusguide.com*, que mostra tabelas atualizadas dos antivírus mais eficientes no momento, comparando-os com seus concorrentes e listando suas funcionalidades [21].

5. Protótipo Automatizado e Avaliação

O protótipo desenvolvido neste trabalho tem como objetivo instanciar de forma prática a estratégia aqui descrita, a fim de recomendar medidas de segurança com baixo (ou nenhum) investimento financeiro. O protótipo foi conceitualizado como um aplicativo *Web* em formato de questionário, onde os usuários podem fornecer detalhes sobre sua infraestrutura de TI, o nível de maturidade de suas políticas de segurança e os recursos disponíveis. A partir dessas informações, o sistema gera recomendações com base nos *frameworks* estudados. O protótipo foi concebido com uma interface simples, e as telas desenvolvidas foram criadas utilizando a plataforma de mapas mentais, Miro [22]. A Figura 2 apresenta um exemplo de perguntas, retirada de um screenshot da própria ferramenta.

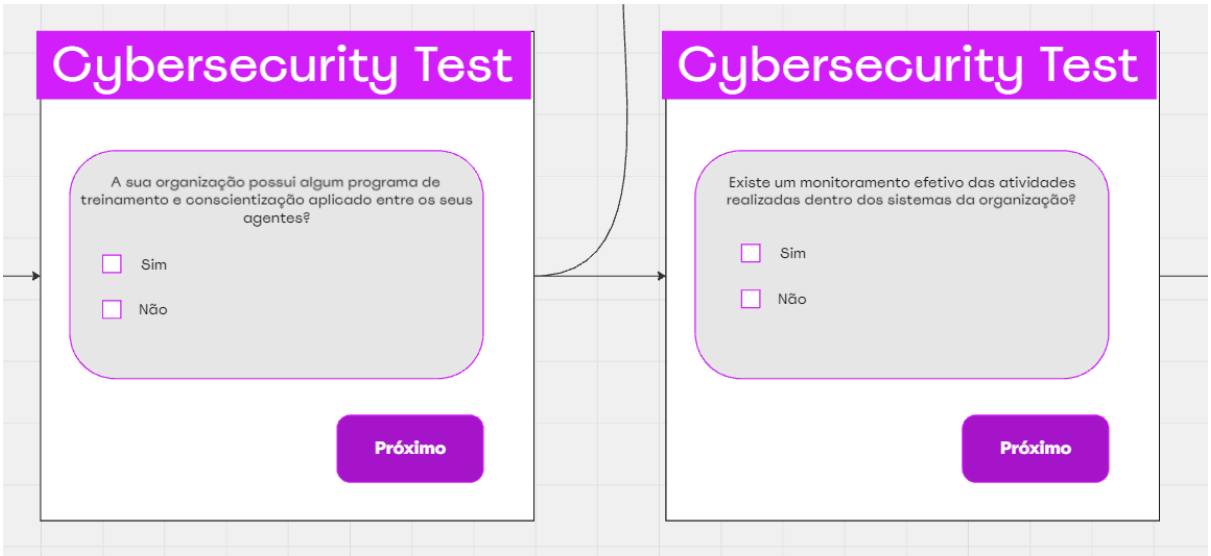

Figura 2. Exemplos de perguntas relevantes em um *screenshot* do protótipo da ferramenta

5.1 Funcionamento do Protótipo

O sistema se baseia em um conjunto de etapas automatizadas, onde o usuário preenche informações sobre seu ambiente de trabalho. Essas informações incluem os sistemas operacionais em uso, as ferramentas de segurança já implementadas e o apetite de risco da organização. O sistema então processa essas entradas e sugere ações e ferramentas adequadas para mitigar vulnerabilidades relevantes.

O protótipo trabalha em conjunto com o Nmap, uma ferramenta *open-source* amplamente usada para varredura de redes. Durante o processo, o usuário da aplicação é instruído a utilizar o programa executando as seguintes flags em seu *gateway* da rede: nmap -sS -sV -O [Endereço de IP e máscara de rede do *gateway*]. As *flags* servem para detectar, respectivamente, portas abertas, e seus serviços, número de versão dos ditos serviços e informações sobre o sistema operacional. Estes dados retornados são as informações que serão usadas para filtrar a base de dados de vulnerabilidades nas próximas etapas. Por exemplo, a partir de um número de versão ultrapassada de um determinado serviço que esteja sendo executado em um *endpoint* é possível encontrar uma vulnerabilidade que não tenha sido corrigida ainda. Caso os sistemas não estejam devidamente atualizados, a aplicação seria capaz de detectar este risco. O comando no Nmap gera uma varredura que pode ser registrada em um arquivo de saída, que deve ser enviado ao protótipo *Web*, que o processa automaticamente, cruzando os dados obtidos com uma base de dados pública de vulnerabilidades (CVE) mantida pela MITRE Corporation. O comando usado para o *scan* é ilustrado na Figura 3.

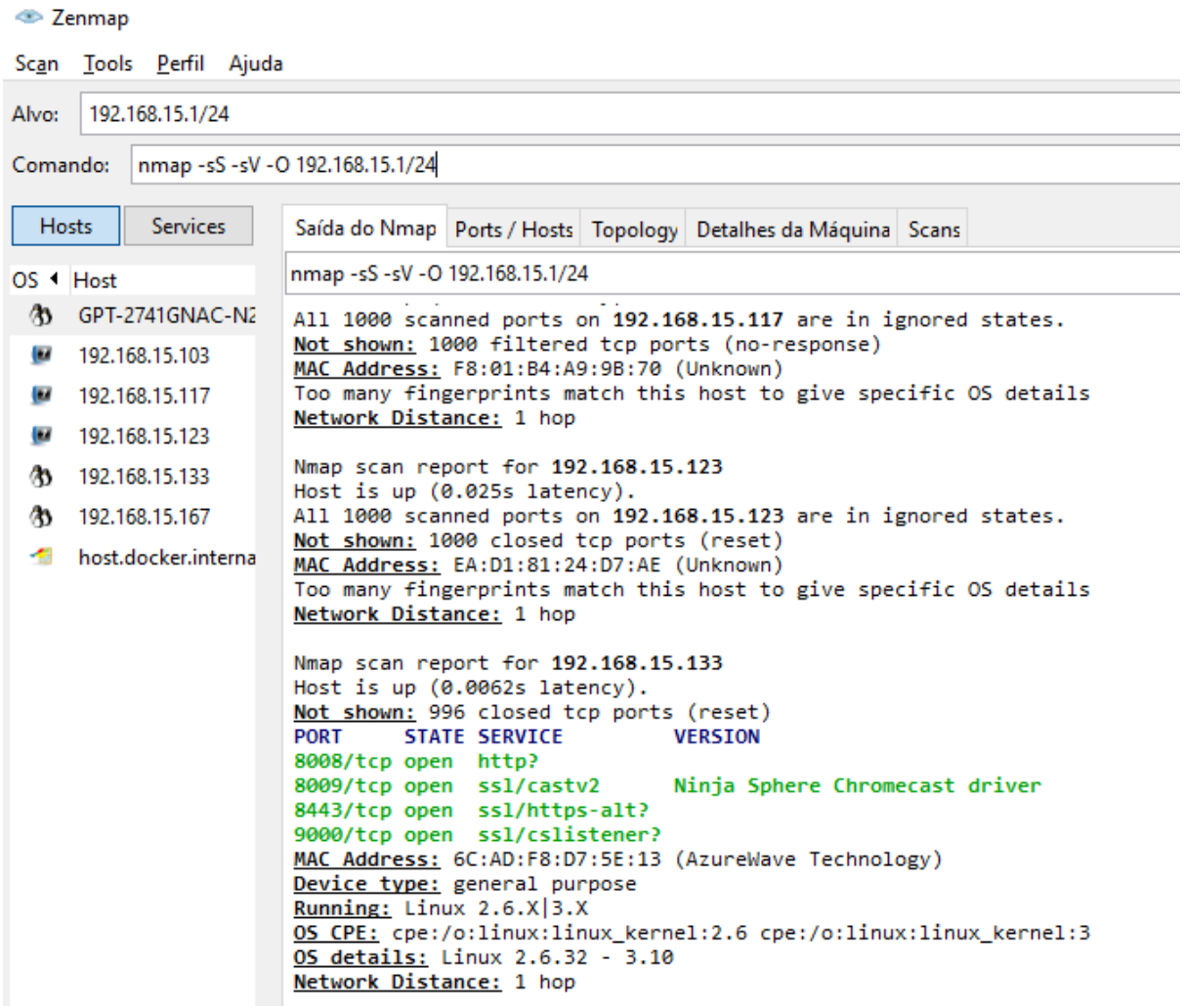

Figura 3. Resultado do *scan* usando as *flags* citadas

A análise automatizada permite identificar vulnerabilidades específicas associadas ao ambiente da organização. O sistema então prioriza essas vulnerabilidades, sugerindo medidas corretivas e ferramentas que podem ser implementadas com o menor custo possível. O uso do *Nmap* torna a coleta de dados mais precisa e menos sujeita a erros humanos, que é importante em organizações que não possuem especialistas dedicados à segurança digital.

O questionário é dividido em seções, cada uma indagando sobre um aspecto específico da segurança da informação, como controle de acesso, criptografia, políticas de *backup*, e gerenciamento de vulnerabilidades. Essas perguntas englobam aspectos mais relevantes a questões de conformidade e políticas de segurança, dizendo respeito à função de Identificação e Recuperação do *framework* NIST e sendo inspiradas em questões do *Self-assessment Questionnaire* da ISO 27001.

Ao final do questionário, o sistema gera uma lista de vulnerabilidades que podem acometer o ambiente em análise. Com o intuito de facilitar o uso deste protótipo, as próximas perguntas são customizadas para o dito ambiente, pedindo para o usuário avaliar quão grave seria a consequência de uma vulnerabilidade selecionada da lista gerada anteriormente. O grau de severidade serve para montar a tolerância de riscos da gestão do negócio, sem exigir uma profundidade de conhecimento técnico das vulnerabilidades encontradas. Os *sliders* ilustrados na Figura 4 servem para o usuário final quantificar quão graves esses cenários seriam para seu negócio, avaliando situações menos severas (à esquerda) e mais severas (à direita).

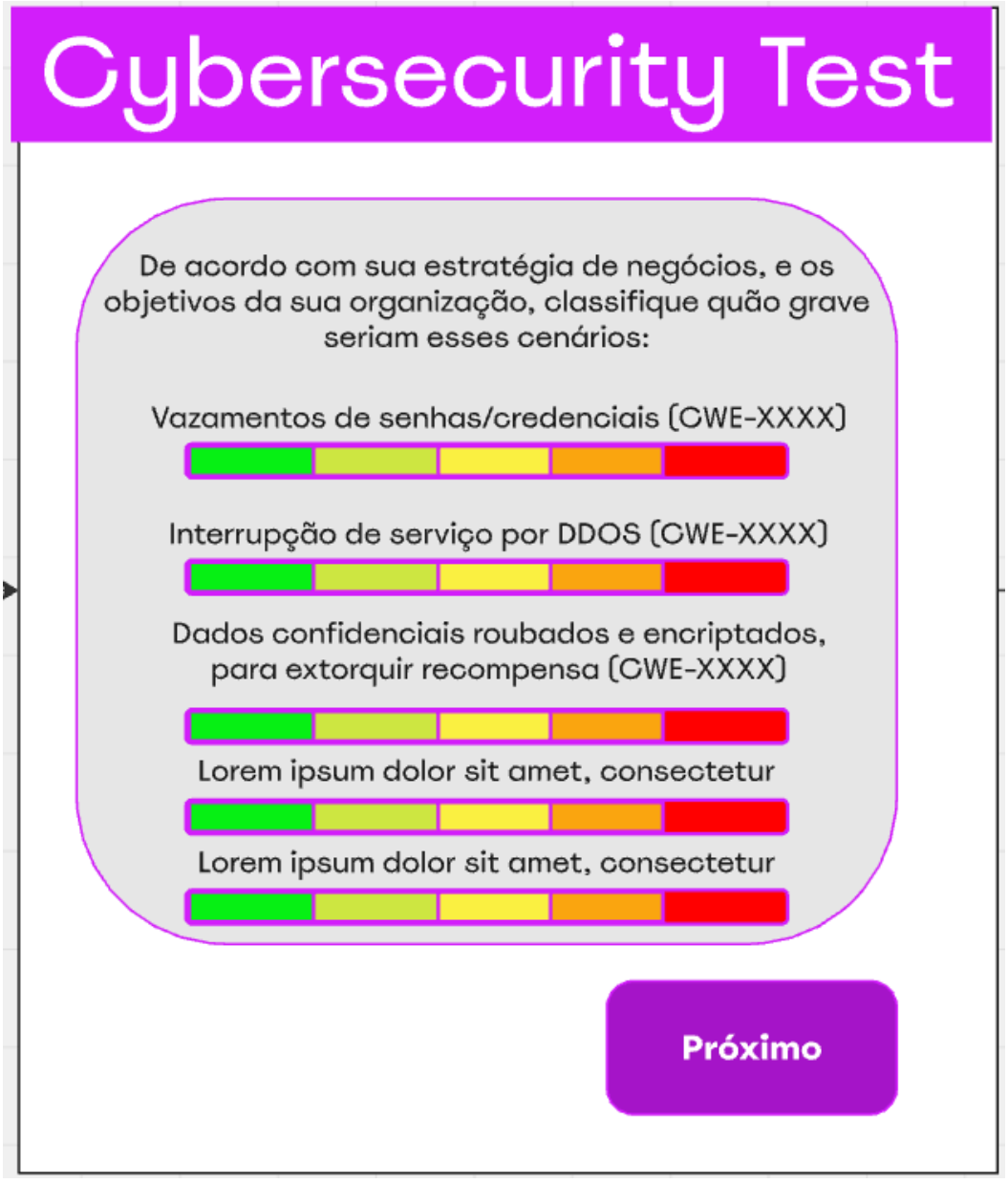

Figura 4: Alguns exemplos da gestão de risco facilitada que o protótipo oferece

Por fim, a aplicação retorna uma lista das soluções *open-source* aqui estudadas, de acordo com o que melhor se enquadra para os objetivos da organização. Uma ilustração da tela final é mostrada na Figura 5.

Figura 5: Protótipo da tela final, mostrando as ferramentas recomendadas

6. Conclusão

O uso de ferramentas *open-source* e a automação das etapas de identificação, monitoramento e resposta a ameaças representam uma alternativa prática e econômica para pequenas e médias empresas. Dado que o processo desenvolvido é inspirado em *frameworks* bem estabelecidos de segurança, o mesmo tem o potencial de incrementar a segurança digital para seu usuário final. E também dado que o protótipo se ateve a soluções de código aberto, o mesmo mostrou que é possível elevar o nível de segurança digital dessas organizações sem demandar grandes investimentos financeiros, o que atende diretamente aos objetivos do trabalho. O processo proposto facilita o mapeamento das vulnerabilidades da rede e sugere ações corretivas, tornando a implementação de práticas de segurança cibernética mais acessível, mesmo em empresas com pouca experiência técnica.

No entanto, ainda há aspectos que podem ser aprimorados em estudos futuros. A estratégia proposta ainda está para ser avaliada em um estudo de caso real. É necessário também uma implementação do servidor que hospeda o questionário montado, bem como avançar no projeto e implementação do protótipo para dar suporte a recomendações customizadas de segurança.

[1] S. Lake,“Companies Are Desperate for Cybersecurity Workers - More than 700k Positions Need To Be Filled”, 2022 https://fortune.com/education/articles/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/

[2] G. Miller, “60% of Small Companies That Suffer a Cyber Attack Are Out Of Business Within Six Months”, 2016
https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/
[3] A. Dolezal, “Cyber Threats Have Increase 81% Since Pandemic” , 2021
https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic
[4] K. Arneson, “How Companies Around The World Are Shifting The Way They Work”, 2021
https://www.bbc.com/worklife/article/20210915-how-companies-around-the-world-are-shifting-the-way-they-work
[5] A. Borgeaud “Cybersecurity standards usage for control systems in organizations worldwide in 2021”, 2021
https://www.statista.com/statistics/1273188/cybersecurity-standards-usage-control-systems/#:~:text=Cybersecurity%20standards%20usage%20for%20control%20systems%20in%20organizations%20worldwide%202021&text=According%20to%20a%20recent%20survey,map%20their%20control%20systems%20to.
[6] NIST “Framework for Improving Critical Infrastructure Cybersecurity” v1.1, 2018
[7] Synopsys Inc., “2021 Open Source Security and Risk Analysis”, 2021
[8] C. Griffiths, “The Latest 2024 Phishing Statistics”, 2024
https://aag-it.com/the-latest-phishing-statistics/#:~:text=In%202021%2C%20the%20average%20click,12%25%20delivered%20malware
[9] MITRE Corporation, “Common Weakness Enumeration & Common Vulnerabilities and Exposures”, 2024
https://www.cve.org/About/RelatedEfforts
[10] ISO 27001 Sistema de Gestão de Segurança da Informação https://www.27001.pt
[11] KnowBe4 Inc., “Data Confirms Value of Security Awareness Training and Simulated Phishing” , 2023
[12] J. Lerums et al, *“Simulation Modeling Cyber Threats, Risks and Prevention Costs”*, 2018
[13] A. Master, G. Hamilton, J. E. Dietz“*Optimizing Cybersecurity Budgets with AttackSimulation”*, 2022
[14] J. Gallardo, R. Torres, O. Tessini *“Surveillance Platform of cybersecurity maturity of micro and small enterprises”*, 2020

[15] Center for Internet Security, “CIS Critical Security Controls Version 8”, 2022 https://www.cisecurity.org/controls/v8

[16] I. Mlakar, P. Jeran, V. Safran, V. Logothetis *“A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case”*, 2021

[17] T. Tratindou, G. Bravos, P. Valoggia *“SENTINEL - Approachable, tailor-made cybersecurity and data protection for small enterprises”*, 2022

[18] *PUZZLE Project* *https://puzzle-h2020.com*

[19] *IRIS Project https://www.iris-h2020.eu*

[20] A. Stock, B. Glas, N. Smithline, T. Gigler, “*OWASP Top Ten*”, 2021 https://owasp.org/www-project-top-ten/

[21] “The Best Antivirus for Mac in 2023” https://www.antivirusguide.com/best-antivirus-mac/?lp=default&utm_source=google&utm_medium=cpc&sgv_medium=search&utm_campaign=14951368784&utm_content=133723268772&utm_term=mac%20virus%20scan&cid=553000325697&pl=&feeditemid=&targetid=aud-754909914186:kwd-39728972&mt=b&network=g&device=c&adpos=&p1=&p2=&geoid=1001625&sgv_gclid=Cj0KCQjw3JanBhCPARIsAJpXTx4_MpPba-lc6x0RjOF0bugfKFiuCobzi6GECrKzRL2LnCjp_Bltb5oaAl5AEALw_wcB&wbraid=CjgKCAjwuZGnBhBrEigADwewAym_VBO_-8gu1gcoCY99YVu1NDoJTEq9OL8_KT--pN0wtUMGGgJfqA&gclid=Cj0KCQjw3JanBhCPARIsAJpXTx4_MpPba-lc6x0RjOF0bugfKFiuCobzi6GECrKzRL2LnCjp_Bltb5oaAl5AEALw_wcB

[22] Mapa mental: Protótipo da aplicação com questionário https://miro.com/app/board/uXjVNrODOSA=/?share_link_id=185456999217