Proposta de arquitetura empresarial para monitoramento e mitigação de riscos relacionados à ameaças cibernéticas

Iago Oliveira, Giullia Nannini, Douglas Motta, Pedro Higa, Prof. Dr. Bruno da Silva Rodrigues

Faculdade de computação e informática – Universidade Presbiteriana Mackenzie
São Paulo - SP -Brasil

iagooliveiraviana@gmail.com, mbs.douglas@gmail.com, giullianb@hotmail.com, pedrokeenzo@gmail.com, bruno.rodrigues@mackenzie.br

Abstract. *In this work, we studied and conducted research on major cyber incidents and how they affect companies today, aiming to understand their challenges and how to mitigate them. We identified the main cyber incidents that occurred within national territory and thus proposed a new and enhanced organizational system for monitoring and defending corporate networks that can be adopted by companies to ensure a safer and up-to-date environment.*

Keywords: *Information security; cyber threats; Pandemic; COVID-19.*

Resumo. *Neste trabalho estudamos e realizamos pesquisas dos principais incidentes cibernéticos e como as empresas na atualidade são afetadas por eles, com o objetivo de entender suas dificuldades e como mitigá-las. Foram levantados os principais incidentes cibernéticos ocorridos em território nacional, e assim propusemos um novo sistema de organização aprimorado para o monitoramento e defesa das redes empresariais que podem ser adotados pelas empresas para garantir um ambiente mais seguro e atualizado.*

Palavras-chave: *Segurança da informação; Ameaças cibernéticas; Pandemia; COVID-19.*

1. INTRODUÇÃO

Nos dias atuais, onde a dependência da Internet e de equipamentos conectados a ela é maior do que nunca, precisamos entender a importância da segurança no meio digital. Surge então uma necessidade alarmante de proteger aqueles que estão envolvidos nesse universo, ou seja, cerca de 5 bilhões de pessoas ao redor do globo [1]. Em ambientes virtuais, os crimes ocorrem de forma diferente da que estamos acostumados, onde os criminosos por trás dos crimes buscam roubar dados preciosos de indivíduos ou empresas, vazar informações sigilosas, comprometer sistemas e, por muitas vezes, chantageando indivíduos e empresas, exigindo valores exorbitantes para reverter o dano causado [2].

Existem registros de incidentes relacionados à segurança na Internet datados do ano de 1989 [3], ou seja, a questão sempre foi uma realidade desde o início da expansão da Internet e existem diversos motivos pelos quais esses ataques ocorrem, mas tudo converge a uma palavra chave: vulnerabilidade. Seja pelo uso inadequado dos equipamentos ou por falhas

técnicas presentes neles, os ataques sempre ocorrem devido à alguma brecha encontrada pelos criminosos.

Neste sentido, podemos citar o caso do *WannaCry*, em 2017: um *ransomware* - *software* malicioso que sequestra (criptografa os dados em disco, impossibilitando o seu uso) os arquivos ou o sistema de um dispositivo, exigindo um resgate para restaurar o acesso aos dados - capaz de se espalhar rapidamente devido à uma falha no sistema operacional Windows, afetou mais de 200 mil computadores em 150 países, criptografando todos os sistemas infectados [4] e gerando prejuízos na ordem de 4 bilhões de dólares [5]. Após esse primeiro ataque, poucos meses depois, viu-se o pesadelo novamente, quando diversas empresas foram afetadas pelo ransomware *NotPetya*, que tinha o funcionamento semelhante ao do *WannaCry*. Esse segundo ataque gerou um prejuízo na ordem de 10 bilhões de dólares, sem contar os prejuízos incalculáveis de bens e serviços [6].

Essas vulnerabilidades cresceram exponencialmente com a chegada da pandemia do COVID-19, uma vez que o mundo inteiro foi forçado ao isolamento, tendo que recorrer quase que 100% a serviços que usavam meios digitais [7]. Junto à necessidade de realizar isolamento social, as empresas, por sua vez, foram as que sentiram o maior impacto quando foram obrigadas a migrar seu ambiente de trabalho físico para o remoto, afetando a estrutura tecnológica da empresa como um todo e ficando muito mais exposta à riscos cibernéticos. Aquelas empresas que possuem ativos sensíveis tornaram-se os principais alvos dos ataques e não devem medir esforços para proteger esses ativos.

Tendo em vista a complexidade do tema e o crescente número de ameaças cibernéticas, o objetivo deste trabalho é realizar um mapeamento dos principais fatores de origem dos ciberataques, quais são as técnicas utilizadas e consequências geradas, bem como as formas mais comuns e eficientes de mitigá-los, para então propor uma arquitetura de sistema que contemple técnicas e tecnologias capazes de mitigar os principais ataques e reduzindo o risco de invasões.

Para apresentar o resultado deste trabalho, este projeto de Trabalho de Conclusão de Curso (TCC) está organizado conforme os capítulos descritos a seguir. No capítulo 2, encontra-se a fundamentação teórica das principais formas de ataques cibernéticos utilizados em redes de computadores. No capítulo 3, é apresentado a metodologia que será utilizada nesta pesquisa e seus respectivos aspectos. No capítulo 4, são evidenciados os resultados e discussões onde o sistema é apresentado. Por fim, no capítulo 5, são trazidas as conclusões do trabalho. Nesta

seção é apresentada a contextualização e relevância do tema, os objetivos de pesquisa, as hipóteses, os objetivos do estudo, a justificativa e como será feita a organização do estudo.

2. REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO E A SEGURANÇA CIBERNÉTICA

A segurança da informação é um conjunto de medidas tomadas para proteger as informações e dados de uma organização, que deve considerar a informação tanto no ambiente físico tradicional em que as informações são geradas, armazenadas, processadas e compartilhadas dentro de uma organização, quanto no ambiente de tecnologia (recursos e infraestrutura tecnológica, como sistemas de computadores, redes, servidores, entre outros). Segundo McCumber [8], a segurança da informação tem como objetivo gerenciar a proteção de redes, domínios e da Internet levando em consideração os diferentes fatores que impactam as organizações e seus ativos (e.g. informações e equipamentos), para isso McCumber desenvolveu um arcabouço representado pelo chamado cubo de McCumber apresentado na figura 1.

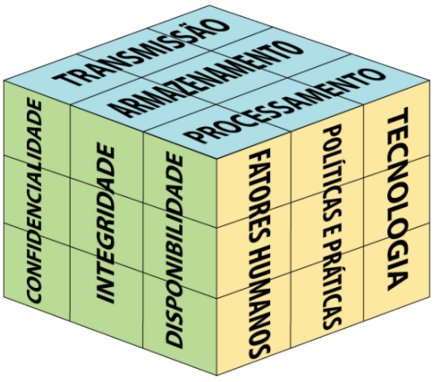

Figura 1. Cubo de McCumber arcabouço desenvolvido para direcionar profissionais na implementação de sistemas de segurança da informação [9].

O arcabouço apresentado na figura 1 apresenta 3 dimensões: a primeira face do cubo trata os três pilares da segurança da informação (descritos na face verde), na segunda face são os três estados da informação (descritos face azul) e na terceira face estão as contramedidas de proteção (descritas na face amarela). A descrição da importância de cada face do cubo, assim como ela pode contribuir para a implementação de sistemas de segurança da informação serão descritas nos tópicos subsequentes.

2.1.1 OS TRÊS PILARES DA SEGURANÇA DA INFORMAÇÃO

Conforme descrito pela norma ISO/IEC 27000 [10], uma das principais referências internacionais em segurança da informação, os três principais pilares que norteiam as práticas da segurança da informação, são conhecidos pelo acrônimo CID, cujas siglas representam: Confidencialidade, a Integridade e a Disponibilidade das informações. Este mesmo acrônimo também é enfatizado na face do cubo relativa aos princípios da segurança da informação. Além disso, outras propriedades, como autenticidade, responsabilidade, não repúdio, e confiabilidade também podem estar envolvidas. De acordo com Amoroso, a segurança de um sistema de computação pode ser expressa através de algumas propriedades fundamentais relativas à segurança da informação [11]. Assim, a ISO/IEC 27000 [10] define:

- A confidencialidade como a propriedade de que a informação não esteja disponível ou revelada a entidades não autorizadas;
- A integridade como propriedade de que a informação seja precisa, completa e confiável ao longo de seu ciclo de vida;
- A disponibilidade como propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada;
- A autenticidade como propriedade de que uma entidade é o que ela diz ser;
- A responsabilidade como propriedade na qual o responsável pela informação deve prestar contas da mesma;
- O não repúdio como capacidade de comprovar a ocorrência de uma reivindicação de um evento ou ação e suas entidades originárias e a confiabilidade como propriedade de que o comportamento e o resultado são consistentes com a intenção.

2.1.2 OS TRÊS ESTADOS DA INFORMAÇÃO

Segundo a ISO/IEC 27000 [10], a informação é um ativo essencial para o funcionamento de uma organização e, consequentemente, precisa ser devidamente protegida. A segunda face do cubo de McCumber descreve os três possíveis estados da informação. Cada estado representa uma fase diferente do ciclo de vida da informação e descreve o seu contexto e características específicas, sendo elas: o armazenamento, o processamento e a transmissão.

O estado de armazenamento descreve como é feita a preservação da informação em algum tipo de dispositivo ou mídia. Ele pode ser feito de diversas formas, incluindo: formato digital

(por exemplo, em disco rígido, servidores em nuvem, bancos de dados, entre outros), formato material (por exemplo, em papel) e também na forma de conhecimento dos funcionários.

O estado de transmissão se refere a como garantir a segurança na transferência de uma informação de um local para o outro. Geralmente, a propagação desses dados é feita, em maioria, através de redes cabeadas e redes sem fio.

Já o estado de processamento retrata as atividades realizadas sobre a informação para transformá-la, analisá-la ou extrair conhecimento. Isso envolve operações como cálculos, análise de dados, execução de algoritmos, processamento de texto, entre outros. Independentemente da forma que a informação assume ou do meio pelo qual é transmitida, ela sempre requer proteção adequada, portanto, esses são atributos fundamentais para identificar os estágios em que a informação pode estar suscetível a riscos e ameaças.

2.1.3. CONTRAMEDIDAS DE SEGURANÇA

Por fim, a face do cubo relativa às contramedidas descreve algumas medidas de segurança externas à informação para prevenir, detectar e responder às ameaças cibernéticas e, novamente, garantir a confidencialidade, integridade e disponibilidade dos dados, assegurando todos os princípios da segurança da informação e proporcionando um ambiente seguro e mitigando os danos causados por ataques cibernéticos.

Essas medidas externas à informação consistem também em três principais fatores: as tecnologias que englobam *softwares*, os serviços com a finalidade de proteger e garantir a integridade do sistema e os dados presentes nele. Exemplos notáveis dessas tecnologias incluem os serviços em nuvem, *VPN*, *firewall* nativo do sistema, entre outras soluções.

Seguindo, temos as Políticas e Práticas, que são, em resumo, regras e normas determinadas visando a segurança dos dados e de quem os manipula, a integridade da rede e do sistema. Como exemplos, encontramos a documentação de procedimentos, políticas de troca de senha, manuais de boas práticas e recomendações.

Por último, mas não menos importante, as contramedidas incluem os Fatores Humanos. Esse item descreve o comportamento humano como fator de risco frente às tecnologias. As medidas, nesse caso, giram em torno de conscientização e capacitação através de palestras, workshops e treinamentos sobre os temas inerentes à proteção e segurança no ambiente

digital, tema melhor desenvolvido no tópico 2.4.5. Esses e demais tópicos de mitigação de riscos e conceitos de segurança da informação serão abordados ao longo do tópico 2.2.

2.2 PRINCIPAIS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes de segurança da informação são eventos que podem, de alguma forma, comprometer a confidencialidade, integridade e disponibilidade das informações, em qualquer estado da informação, conforme explicado no tópico 2.1. *Phishing, scans, DDoS, Backdoor* e fraudes são exemplos de eventos que se enquadram como incidentes de segurança da informação, podendo comprometer dados sensíveis, pessoais ou empresariais.

Em relação a esses eventos, ainda segundo a norma ISO/IEC 27000 são definidos como "um único, ou uma série de eventos indesejados ou inesperados de segurança da informação, que têm uma probabilidade significativa de comprometer as operações do negócio e de ameaçar a segurança da informação". [10]

Buscando propor análises e resultados, o CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, principal grupo de resposta a incidentes de segurança na Internet brasileira - tem como objetivo identificar, analisar e reagir a incidentes de segurança ocorridos no território digital nacional [13]. A classificação e distribuição das informações coletadas pela instituição, nos permite entender quais são as principais ocorrências de incidentes cibernéticos no país. A Figura 2 apresenta um gráfico quantificando esses incidentes recebidos pelo CERT.br no período de 2018 a 2022.

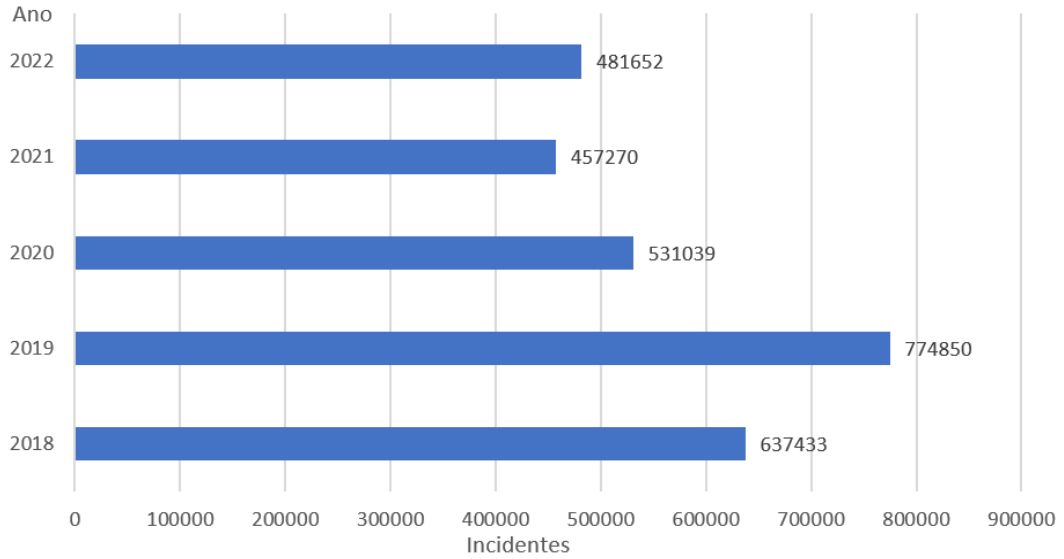

Figura 2. Total de Incidentes Notificados ao CERT.br no período de 2018 a 2022 [14].

Na figura 2 podemos observar que a somatória de todos os incidentes de 2018 a 2022 resulta em um total de quase 3 milhões de incidentes reportados no país. Vale ressaltar que esses números são referentes a incidentes voluntariamente reportados ao instituto, portanto pode-se constatar, assim como declarado no estudo “Panorama de Ameaças 2021”, levantamento anual de dados feito pela empresa da Kaspersky [16] constata que o número de tentativas de cibercrimes é expressivamente maior, totalizando cerca de 481 milhões. Esse número reflete diretamente a situação trazida pela pandemia da COVID-19: a adoção do home-office exige cuidados, principalmente voltados à segurança da informação, que as empresas não estavam preparadas para lidar e, portanto, não tinham medidas de proteção eficientes para garantir um ambiente digital seguro, tanto para o funcionário quanto para a empresa [17]. Essas adaptações ao estilo de trabalho remoto trouxeram inúmeras outras mudanças na estrutura tecnológica da empresa, como equipamentos, redes, arquitetura, softwares e serviços.

A Figura 3 oferece uma exploração mais detalhada e abrangente das informações previamente expostas na Figura 2, permitindo uma análise mais aprofundada e enriquecida, apresentando detalhadamente quais foram os incidentes mais recorrentes e seus respectivos números de casos durante o período de 2018 a 2022.

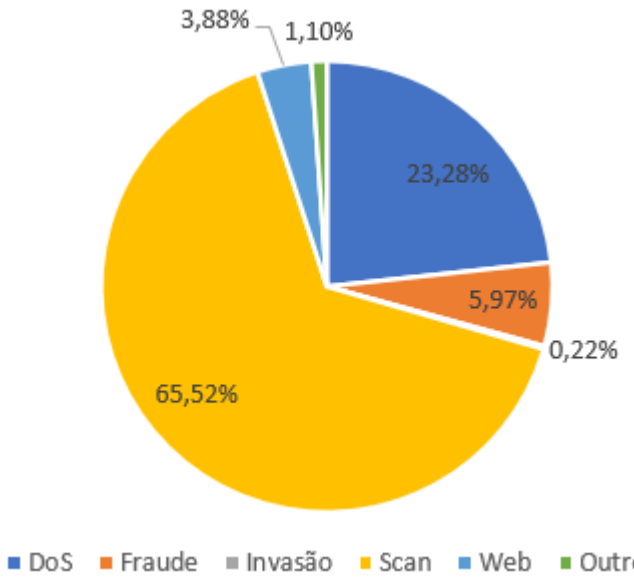

Figura 3. Detalhamento das notificações recebidas – 2018 a 2022 [14].

Na Figura 3 é possível constatar que os ataques do tipo "*scan*" representaram a maior parcela de incidentes cibernéticos notificados, correspondendo a 65,52%, ou seja, 1.888.679 em números absolutos do total de dos casos registrados. Em seguida, o segundo ataque mais provável apresentado na Figura 3 é o ataque de negação de serviço (*DoS*) representando

23,28% dos incidentes e 671.162 em números absolutos. Já as fraudes, sendo o terceiro ataque mais provável, representaram 5,97% dos casos, totalizando 172.293 casos. Seguindo o quarto ataque mais provável são os ataques *web*, que totalizaram 3,88% das ocorrências ou 111.843 em números absolutos. Na sequência, como quinto ataque mais provável, temos os outros tipos de ataques que respondem a 1,10% dos casos ou 31.884 em casos totais, e por fim, os ataques de invasão com o menor número de casos de 6.393 representa apenas 0,22% dos casos registrados.

Segundo a classificação feita pelo CERT.br [14] os principais tipos de ataques são:

- Ataques *DoS* (*denial of service*): Ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, dispositivo ou rede. Além disso, é importante mencionar o *DDoS* (*Distributed Denial of Service Attacks*) que possui o mesmo propósito, porém a diferença entre o *DoS* está de ataque está na quantidade de máquinas necessárias para desempenhar o ataque, visto que em ataques *DoS* somente um atacante participa do ataque e em ataques *DDoS* múltiplas máquinas são tipicamente utilizadas [15]. ;
- Fraude: Incidentes em que ocorre uma tentativa de obter vantagem, que pode ou não ser financeira;
- Invasão: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede;
- *Scan*: engloba além de notificações de varreduras em redes de computadores (*scans*), notificações envolvendo força bruta de senhas, tentativas mal sucedidas de explorar vulnerabilidades e outros ataques sem sucesso contra serviços de rede disponibilizados publicamente na Internet;
- *Web*: um caso particular de ataque visando especificamente o comprometimento de servidores web ou desfigurações de páginas na Internet. Com base nas estatísticas nacionais de incidentes cibernéticos é importante que empresas projetam sistemas que visam mitigar as ameaças citadas acima, já que como dito anteriormente causam grandes perdas econômicas para civis e companhias, além de o vazamento de dados que podem colocar pessoas e sócios em risco por seus dados ficam na mão de criminosos.
- Outros: notificações de incidentes que não se enquadram nas demais categorias;

2.3 PRINCIPAIS VULNERABILIDADES

Neste tópico serão abordadas as principais vulnerabilidades que viabilizam os incidentes do tópico 2.2. As vulnerabilidades podem se dar tanto por natureza técnica, explicadas no tópico 2.3.1, quanto por natureza humana, explicadas no tópico 2.3.2.

2.3.1 VULNERABILIDADES DE NATUREZA TÉCNICA

Vulnerabilidades técnicas são aquelas que se dão por falhas e/ou brechas em equipamentos e sistemas. Dentre elas, as mais comuns se dão por conta de versões obsoletas de sistemas operacionais e *softwares* que, por consequência, possuem métodos de segurança desatualizados [18].

Um exemplo prático dessas vulnerabilidades é a falta de instalação de atualizações de segurança. As recorrentes atualizações de segurança de sistemas operacionais como o *Windows* ou sistemas operacionais de *smartphones*, como o *Android* ou o *iOS* trazem consigo alterações no código e funcionalidades do sistema operacional que os tornam mais robustos e dispõem de menos brechas para que ocorram os incidentes citados. Essas atualizações são disponibilizadas com frequência e devem ser instaladas sempre que possível, visando a mitigação das vulnerabilidades causadas tanto por *software* quanto por *hardware,* uma vez que ambos andam de mãos dadas. Esses sistemas também precisam utilizar recursos como criptografia de ponta e outros recursos para mitigação de incidentes (citados no tópico 2.4) para proteger os dados e sanar ao máximo essas vulnerabilidades técnicas.

2.3.2 VULNERABILIDADES DE NATUREZA HUMANA

Por outro lado, o comportamento humano compõe grande parte das vulnerabilidades encontradas como causas dos incidentes de segurança. Por muitas vezes o usuário é o responsável por gerar brechas para que ocorram esses incidentes, persuadido pelo criminoso por trás do ato ou simplesmente pela falta de conhecimento de processos e práticas adequadas no ambiente de trabalho [19].

Tomemos como exemplo a seguinte situação: um funcionário comum de uma empresa que recebe um email alegando que precisa atualizar suas informações pessoais e clica no link para o suposto site que teria como função atualizar essas informações. Na realidade, o link se trata de um site malicioso e, ao entrar nele, o criminoso por trás consegue acesso ao computador do funcionário e rouba informações confidenciais presentes naquela máquina, comprometendo os dados, o próprio equipamento em si e gerando a possibilidade do criminoso invadir a rede e outros equipamentos conectados nela. Ou seja, o criminoso não se aproveitou de nenhuma

brecha técnica, mas persuadiu o funcionário através de técnicas de engenharia social (técnicas de persuasão, trabalhando a partir da manipulação psicológica para obter informações confidenciais e dados sigilosos) para que o próprio funcionário gerasse a oportunidade de praticar o crime.

2.4 PRINCIPAIS RECURSOS E TÉCNICAS PARA MITIGAR INCIDENTES DE SEGURANÇA

Em meio às brechas e vulnerabilidades citadas no tópico anterior, é fundamental que existam profissionais capacitados dedicados ao monitoramento e à segurança dos sistemas dentro da empresa. Dessa forma, uma equipe de segurança tem como principal responsabilidade monitorar as estruturas e recursos tecnológicos da empresa, bem como seus procedimentos, hábitos e especificações técnicas, a fim de identificar as vulnerabilidades (citadas no tópico 2.3) e mitigar os riscos de incidentes de segurança (citados no tópico 2.2), propondo soluções rápidas e eficientes para esses problemas [20]. Esta equipe deve utilizar ferramentas e técnicas avançadas de detecção de ameaças para identificar comportamentos suspeitos, anomalias, vulnerabilidades e outros indicadores de comprometimento que possam indicar uma possível ameaça à segurança do ambiente. Como exemplo, podemos citar a utilização de antivírus e *firewalls*, a adoção de práticas como controles de acessos, realização consistente de *backups*, criptografia e protocolos de segurança e a realização de treinamentos de segurança para todos aqueles que estão envolvidos nesse cenário, a fim de disseminar conhecimento e conscientizar sobre a importância dos conceitos de segurança [21].

Dentre as principais ferramentas utilizadas na implementação de controles de segurança podemos citar:

2.4.1 *HONEYWALL GATEWAY*

Segundo Abbasi e Harris [22] *honeypot gateway* (ou *gateway* de *honeypot)* é uma solução de segurança que coloca um *honeypot* entre a rede interna protegida e a rede externa não confiável (como a Internet). O *honeypot* é um dispositivo projetado para parecer vulnerável e desprotegido, a fim de monitorar e analisar as atividades dos invasores. O objetivo do *honeypot gateway* é detectar e analisar as táticas, técnicas e procedimentos utilizados pelos invasores, permitindo que os administradores de segurança cibernética identifiquem ameaças potenciais e ajustem suas defesas de segurança para proteger melhor a rede real, minimizando e/ou evitando os danos causados por ataques cibernéticos, de acordo com SPECHT e LEE. [34] ataques como *DoS* e *DDoS* conforme descritos no tópico 2.2

2.4.2 *VPN*

VPN é a sigla em inglês para *Virtual Private Network* (Rede Privada Virtual), e pode ser descrita como "um ambiente de comunicações onde o acesso é controlado a fim de permitir conexões de mesmo nível apenas dentro de um certo grupo definido, construído a partir do particionamento de um meio de comunicações subjacente, onde tal meio fornece serviços à rede de forma não-exclusiva" [23]. A segurança desse processo é garantida através da tecnologia de tunelamento, predecessora das *VPNs*.

A definição disponível no site oficial da Cisco descreve o tunelamento como uma técnica que permite que os usuários de acesso remoto se conectem a uma variedade de recursos de rede (*gateways* domésticos corporativos ou um provedor de serviços de Internet) por meio de uma rede de dados pública [24]. Esse processo é feito encapsulando um tipo de pacote dentro de outro para facilitar algum tipo de vantagem no transporte de uma informação dentro da rede [25]. Segundo Cardoso [26], esse processo é composto pelas seguintes etapas:

- Criptografia dos dados: Criptografar o pacote a ser transportado, de forma que o torne ilegível em caso de interceptação da transmissão;
- Encapsulamento: Um dado protocolo de tunelamento encapsula os pacotes com um cabeçalho que contém informações de roteamento, com identificação do destino do pacote;
- Transmissão ao longo da rede: Os pacotes são roteados entre as extremidades do túnel na rede intermediária (rede pública), até chegarem ao seu destino;
- Desencapsulamento: No destino, o pacote é desencapsulado, deixando apenas informações do protocolo da rede local;
- Descriptografia dos dados: Realiza a descriptografia dos pacotes finais, de forma que o torne legível para a outra extremidade do túnel.

2.4.3 FIREWALL

Um *firewall* é um dispositivo de segurança da rede que monitora e filtra o tráfego da rede, controlando todos os pacotes que tentam entrar ou sair da rede, permitindo ou bloqueando o acesso aos recursos da rede de acordo com as políticas de segurança estabelecidas pela empresa [27]. Por meio deste, a instituição consegue um monitoramento e controle do tráfego de rede de forma granular e restringindo o acesso a determinados tipos de tráfego, aplicativos ou sites da web e possibilitando a detecção de possíveis ameaças à segurança em tempo real.

2.4.4 TWO-STEP AUTHENTICATION

Two-step authentication (autenticação de duas etapas ou autenticação de dois fatores, em português) é uma medida que adiciona uma camada adicional de segurança para proteger as contas dos usuários contra invasões de *hackers* e outros tipos de ataques cibernéticos [28]. É amplamente utilizada em contas de email, redes sociais, serviços bancários online e em outros aplicativos e serviços que requerem altos níveis de segurança.

A primeira etapa da autenticação é simples e contempla o tradicional, solicitando as credenciais de acesso, como login e senha. Após essa primeira verificação, caso as credenciais estejam corretas, o usuário é direcionado para a segunda etapa, a qual solicitará uma segunda autenticação, geralmente em outro dispositivo (*smartphone* pessoal, por exemplo), para garantir que o acesso seja legítimo e feito somente por pessoas autorizadas. Essa segunda autenticação pode ser feita de algumas formas (e.g. através de um código de verificação por *SMS*, onde o usuário recebe um código em seu dispositivo móvel registrado e deve inseri-lo na tela de login para continuar, ou por um aplicativo de autenticação, onde o usuário usa um autenticador instalado em seu dispositivo móvel para gerar um código temporário que deve ser inserido no processo de login).

Dessa forma, ao solicitar a verificação em duas etapas, a chance de realização de um acesso indevido é minimizada drasticamente. Mesmo que um invasor descubra ou roube as credenciais de login de outra pessoa, eles ainda precisam passar pela segunda etapa de autenticação para de fato conseguir acesso à conta ou sistema. Isso ajuda a proteger as contas contra ataques de força bruta, roubo de identidade e acessos não autorizados.

2.4.5 DEFINIÇÃO DE POLÍTICAS DE SEGURANÇA E CONSCIENTIZAÇÃO

Conforme abordado no tópico 2.3.2, o comportamento humano também é fonte de diversas vulnerabilidades. Visando mitigar essas vulnerabilidades, existem alguns recursos que podem ser adotados pela empresa com o objetivo de disseminar informações e práticas adequadas no ambiente de trabalho, como a realização de palestras e treinamentos voltados à conscientização sobre segurança da informação [21]. Esses eventos, por muitas vezes, são promovidos em parceria com empresas especializadas em segurança. Dessa forma, os funcionários são capacitados e desenvolvem um panorama mais claro dos comportamentos necessários para evitar incidentes por falha humana.

A definição de políticas internas de segurança também é um fator determinante, ao estabelecer práticas e procedimentos seguros e adequados que evitem o comprometimento de

dados e sistemas. A adoção e disseminação das práticas presentes na norma ISO/IEC 27001 [29], por exemplo, é um bom começo para a definição dessas políticas.

2.5 TRABALHOS CORRELATOS

De acordo com Tsunoda e Keeni [30] aborda o monitoramento de tráfego de rede como uma medida de segurança. Os autores propõem um método de detecção de intrusão baseado na análise do tráfego de rede, e reforçam que essa análise pode ser feita de forma passiva, sem nenhuma carga adicional na rede. A ação específica descrita no artigo envolve a instalação de ferramentas de monitoramento de tráfego de rede em diferentes pontos da infraestrutura de rede da organização. Essas ferramentas capturam e analisam o tráfego de rede, identificando padrões de comunicação, identidades desconhecidas, comportamentos anômalos ou atividades maliciosas. A partir da análise do tráfego de rede, são aplicadas ações de segurança, como bloqueio de tráfego indesejado, identificação de tentativas de invasão ou atividades suspeitas, notificação de incidentes de segurança às equipes responsáveis e implementação de medidas de proteção adicionais, como atualizações de *software* e configurações de *firewall*. Também é enfatizado que, com as ferramentas adequadas e configurações adequadas, é possível obter insights valiosos sobre a segurança da rede e melhorar a proteção contra ameaças cibernéticas. No geral as técnicas em conjunto com sua abordagem simples e eficiente possibilita que a solução para a segurança de redes seja implementada de forma mais acessível e efetiva, contribuindo para a proteção e integridade das redes.

Segundo Donaldson, S.E. et al. [31] aborda de forma abrangente a arquitetura de segurança cibernética para empresas, fornecendo estratégias e orientações eficazes para proteger os ativos digitais em um ambiente corporativo em constante evolução. Os autores exploram os diferentes componentes e camadas de uma arquitetura de segurança cibernética, abrangendo redes, sistemas operacionais, aplicativos e dados, fornecendo uma visão abrangente do panorama de segurança. Através desse artigo conseguimos entender um pouco sobre arquiteturas empresariais e sua relação com a segurança cibernética e tivemos a chance ver como esses problemas seguem os planos de ação e processos estratégicos para mitigação deles. Os autores oferecem insights valiosos sobre temas como identificação e autenticação de usuários, criptografia, detecção e prevenção de intrusões, além de abordar o gerenciamento de incidentes e resposta a incidentes de segurança. Outro aspecto relevante do livro é a consideração de questões regulatórias e conformidade, que desempenham um papel fundamental na proteção dos sistemas e dados empresariais. Os autores enfatizam a

importância de aderir às melhores práticas de segurança e abordam as últimas tendências e tecnologias emergentes no campo da segurança cibernética.

Segundo as declarações de Baptista e Dian [32] é enfatizado a importância da segurança da informação, especialmente durante a pandemia do COVID-19, embora tenham sido implementadas medidas e leis ao longo dos anos para combater crimes digitais, os incidentes continuaram a ocorrer com frequência crescente, especialmente durante a pandemia. Dessa forma o artigo salienta e corrobora as informações descritas ao longo deste artigo, reforçando a importância da segurança da informação para proteger os ativos digitais e dados sensíveis das organizações, principalmente diante dos desafios impostos pela pandemia do COVID-19.

De acordo com Dowlinge, Schukat, e Barrett [33] idealizam em seu trabalho um *framework* de desenvolvimento e implantação de *honeypots* num cenário de ameaças de malware em evolução constante. Utilizando como base as classes propostas pela taxonomia de Seifert em 2006, categorizando os tipos de *honeypots* mais comuns, foi imaginado um processo cíclico para auxiliar o desenvolvimento de *honeypots* ágeis e adaptáveis, indo do desenvolvimento do *honeypot* adaptável, para a implantação em tempo limitado com captura de dados até a otimização do *honeypot*, voltando para o primeiro passo. O *framework* imaginado consiste de uma parte "adaptativa", onde é utilizado modelos de aprendizado supervisionados e não supervisionados de *machine-learning* para reconhecer e categorizar ataques de malwares em desenvolvimento constante, e uma parte "ágil", onde a natureza dos ataques coletados é analisada a fim de decidir o quão relevante é manter a implementação , permitindo-a trabalhar de forma mais eficiente, cortando operações irrelevantes. Dessa forma o *honeypot* desenvolvido se encontrará em constante otimização, capaz de reconhecer ataques de malware de forma mais efetiva e sem necessidade de constante manutenção manual, cobrindo brechas comumente encontradas na implementação dessas tecnologias e possivelmente prevenindo erros por intervenção humana.

3. MATERIAIS E MÉTODOS

3.1 METODOLOGIA DE PESQUISA

Em relação à metodologia empregada neste trabalho, para o desenvolvimento do projeto, inicialmente foi realizada uma revisão da literatura sobre os temas relacionados. Esta revisão teve como objetivo auxiliar o grupo a entender o que são, como ocorrem e quais os impactos dos incidentes cibernéticos, bem como auxiliar na tomada de decisão sobre os componentes necessários para analisar, identificar e propor soluções visando a

mitigação de riscos e impactos causados por esses incidentes, assegurando todos os princípios da segurança da informação e proporcionando um ambiente seguro.

A fundamentação teórica do trabalho foi realizada através de pesquisas nos principais motores de busca como Google Acadêmico e Biblioteca da Faculdade Presbiteriana Mackenzie onde foram selecionadas pesquisas científicas, sites, artigos, publicações, documentação descritiva e teses que dessem suporte para a pesquisa. Para atender os objetivos do trabalho, são propostas as seguintes atividades:

1. Revisão Bibliográfica;
2. Levantamento de incidentes nas empresas durante a pandemia;
3. Análises dos dados levantados;
4. Idealização da proposta inicial de combate aos incidentes;
5. Aplicação da proposta idealizada;
6. Reflexão sobre os resultados;
7. Elaboração e escrita da documentação do projeto.

4. RESULTADOS E DISCUSSÃO

4.1 ARQUITETURA PROPOSTA

Após o estudo feito sobre os incidentes (descritos no tópico 2.2), as vulnerabilidades (descritas no tópico 2.3) e as técnicas e recursos para mitigar os riscos (descritos no tópico 2.4), foi elaborada uma proposta de arquitetura de sistema, contemplando os diversos temas abordados no desenvolvimento do artigo. A ideia da proposta é construir um ambiente mais seguro e confiável, focando principalmente em empresas que não possuem o conhecimento do tema ou condição de adotar recursos complexos e custosos existentes no mercado. A arquitetura é apresentada a seguir, na figura 5.

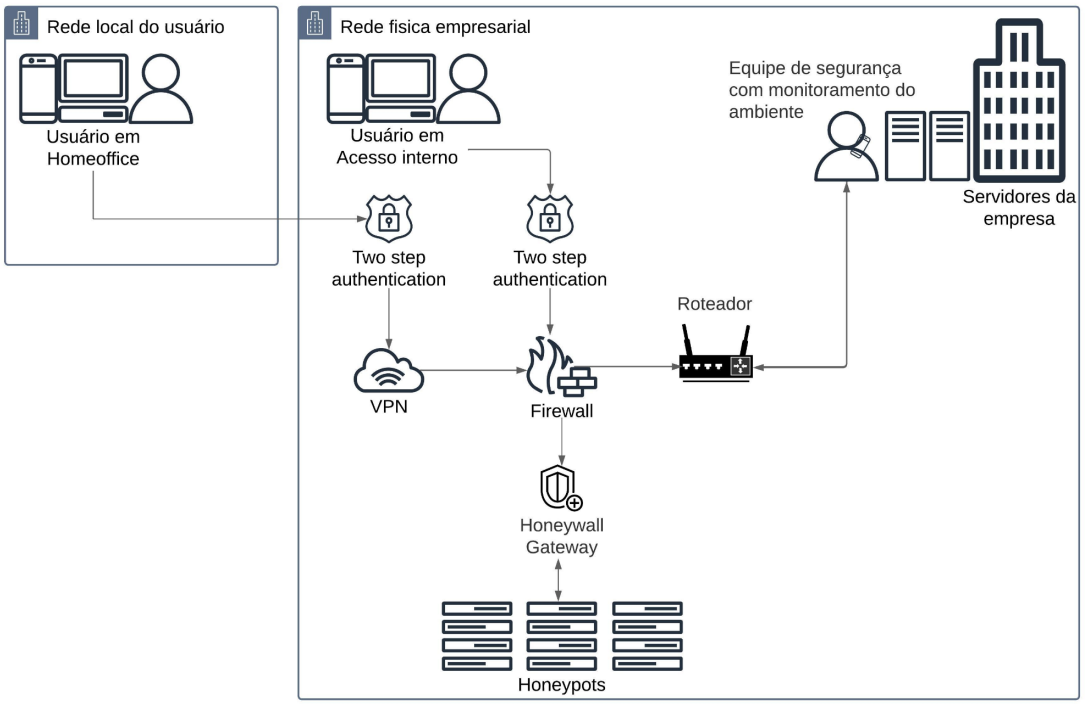

Figura 5. Arquitetura de sistema proposta.

Para mitigar as vulnerabilidades de natureza humana, já o comportamento humano é responsável por grande parte das vulnerabilidades (descrito no tópico 2.3) é crucial que os funcionários sejam treinados e orientados de acordo com as políticas internas de segurança da informação na empresa (descrito no tópico 2.4.5). Após a capacitação, os funcionários devem seguir as práticas e procedimentos necessários para manter um ambiente seguro e adequado, reduzindo o comprometimento por essa extremidade externa à arquitetura. Em sequência, iniciando os recursos e técnicas utilizados na arquitetura, o funcionário ao tentar logar na rede interna da empresa, é obrigado a passar pela autenticação de dois fatores (descrita no tópico 2.4.2). Se obtiver sucesso nas autenticações, em caso de estar na sua rede local (de *home office*) estabelece conexão à rede interna através da *VPN* (descrita no tópico 2.4.4). Ao adentrar à rede interna o usuário passa pelo *firewall* (descrito no tópico 2.4.3), garantindo que a conexão é legítima e segura para a empresa.

Caso seja identificado comportamento suspeito, o *firewall* direciona a conexão para o *Honeywall Gateway* que, por sua vez, direciona a conexão do usuário aos *Honeypots* de alta interatividade, um tipo avançado de *honeypot* projetado para simular um ambiente operacional realista e engajar os invasores em atividade*s* maliciosas, também utilizado para obter informações valiosas sobre as táticas e ferramentas utilizadas pelos invasores, além de

fornecer insights sobre as vulnerabilidades dos sistemas reais (descrito no tópico 2.4.1). Caso a conexão seja, de fato, identificada como legítima e segura, o usuário é finalmente direcionado ao ambiente real da empresa, tendo acesso aos servidores e serviços internos. Essa proposta busca a construção de um ambiente mais seguro e confiável, minimizando os riscos e danos causados por incidentes cibernéticos.

Em resumo, o monitoramento de segurança dentro de uma empresa pode evitar uma série de riscos, permitindo uma detecção precoce de atividades maliciosas, violações de segurança e comportamentos não autorizados. Isso permite uma resposta rápida e eficaz, minimizando os danos e protegendo a empresa contra ameaças cibernéticas.

5. CONCLUSÃO E TRABALHOS FUTUROS

A implementação em massa do ambiente de trabalho híbrido era inevitável no contexto tecnológico atual, mas a chegada inesperada da pandemia de COVID-19 em 2020 transformou essa mudança em um impacto repentino, no qual poucos conseguiram se adaptar adequadamente. Infelizmente, os cibercriminosos se aproveitam dessa situação, evoluindo constantemente suas táticas e representando um perigo constante para as empresas, que muitas vezes estavam despreparadas durante a quarentena devido à mudança repentina na sua forma de trabalho para o regime híbrido. Esse regime corporativo continuará sendo uma prática comum, e o perigo das ameaças digitais não diminuirá. A única forma de combatê-las é se adaptar e evoluir junto com elas.

A implementação da arquitetura proposta neste trabalho oferece uma abordagem abrangente para mitigar os riscos de segurança em ambientes corporativos. Embora tecnologias como *VPN*, *firewall* e *honeypot*, todas recomendadas de acordo com a arquitetura, possam prevenir e combater ataques direcionados aos sistemas da empresa, o fator humano sempre apresenta o risco de erros que podem passar despercebidos pelas defesas automatizadas das ferramentas. Com táticas e ferramentas como autenticação de dois fatores, *VPN*, *Firewall*, *Honeywall Gateway, Honeypot*, roteadores especializados e uma equipe de monitoramento interno, além de conscientizar constantemente os funcionários sobre os perigos do descuido, as empresas podem fortalecer sua postura de segurança, proteger seus recursos e dados sensíveis e mitigar diversas ameaças cibernéticas de várias origens. Essa abordagem é especialmente relevante no contexto atual de trabalho remoto e sofisticação crescente dos ataques cibernéticos.

No futuro, esperamos que outros profissionais da área possam utilizar e validar esta pesquisa, reconhecendo seu potencial para complementar e enriquecer o conhecimento adquirido. Ao

disponibilizar nossos resultados obtidos, buscamos incentivar colaborações e contribuições de especialistas que possam explorar novas perspectivas e aplicar abordagens complementares.

6. REFERÊNCIAS

[1] Crescimento da internet desacelera e 2,7 bilhões ficam fora da rede. ONU News, 2022. Disponível em <https://news.un.org/pt/story/2022/09/1801381>

[2] O que são crimes cibernéticos? Como se proteger dos crimes cibernéticos. Kaspersky, [s.d.] Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>

[3] Conheça a evolução dos ataques cibernéticos!. UPX, 2022. Disponível em: <https://upx.com/post/evolucao-ataques-ciberneticos/>

[4] Ransomware WannaCry: saiba o que é e como se precaver. CCUEC - Centro de Computação da Universidade Estadual de Campinas, 2017. Disponível em: <https://www.ccuec.unicamp.br/ccuec/noticias/2017/05/17/ransomware-wannacry-saiba-o-que-e-e-como-se-precaver>

[5] O que é o ransomware WannaCry?. Kaspersky, [s.d.]. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry>

[6] NotPetya - Five Facts to Know About History's Most Destructive Cyberattack. hypr, [s.d.]. Disponível em: <https://www.hypr.com/security-encyclopedia/notpetya>

[7] CARVALHO, Sara. O Cenário Da Segurança Da Informação Nas Empresas Durante A Pandemia Da COVID-19. Safeway Consultoria, 2021. Disponível em: <https://safewayconsultoria.com/o-cenario-da-seguranca-da-informacao-nas-empresas-durante-a-pandemia-da-covid-19/>

[8] MCCUMBER, John. Information systems security: A comprehensive model. In: Proceedings of the 14th National Computer Security Conference. Baltimore, Maryland, USA: National Institute of Standards and Technology, 1991. p. 328-337.

[9] Performance - Sistemas & Métodos. Disponível em: <http://performance.eti.br/publicacoes_detalhes.php?post=10>. Acesso em: 25 maio. 2023.

[10] ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary

[11] E. Amoroso. Fundamentals of Computer Security Technology. Prentice Hall PTR, 1994.

[13] CERT.br FAQ. Disponível em: <https://www.cert.br/docs/certbr-faq.html>. Acesso em: 01 maio. 2023.

[14] CERT.BR. CERT.br - Estatísticas. Disponível em: <https://stats.cert.br/incidentes/>. Acesso em: 01 maio. 2023.

[15] JANTSCH, R. Mitigação de ataques DDoS em redes baseadas em infraestruturas SDN/NFV. lume. Universidade Federal do Rio Grande do Sul, 2016.

[16] Ciberataques crescem 23% no Brasil em 2021. Kaspersky Daily, 2021. Disponível em:<https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020/>

[17] BARROS, Leonardo. Segurança da Informação: Quais os Perigos e Como Proteger o Home Office da Sua Empresa?. Tangerino Blog, 2023. Disponível em: <https://tangerino.com.br/blog/seguranca-da-informacao/>

[18] Entenda o que é vulnerabilidade de segurança e quais são as mais comuns. iTeam, 2020. Disponível em: <https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/>

[19] Quais são as formas mais comuns de fraudes por engenharia social?. Incognia, [s.d.]. Disponível em: <https://www.incognia.com/pt/dicionario-da-autenticacao-mobile/quais-as-formas-mais-comuns-de-engenharia-social>

[20] Segurança da informação: o que é, 5 pilares e como garantir nas empresas?. FIA, 2022. Disponível em: <https://fia.com.br/blog/seguranca-da-informacao/>

[21] Quais são as ferramentas de segurança da informação para empresas?. Ohub, [s.d.]. Disponível em: <https://www.ohub.com.br/ideias/ferramentas-seguranca-informacao/>

[22] F. H. Abbasi and R. J. Harris, "Experiences with a Generation III virtual Honeynet," 2009 Australasian Telecommunication Networks and Applications Conference (ATNAC), Canberra, ACT, Australia, 2009, pp. 1-6, doi: 10.1109/ATNAC.2009.5464785.

[23] Ferguson, Paul, and Geoff Huston. "What is a VPN?." (1998): 01-22. https://cpham.perso.univ-pau.fr/ENSEIGNEMENT/COMMUN/vpn_ferguson.pdf

[24] CISCO. Tunneling. Disponível em: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/tunneling/index.html>. Acesso em: 25 mai. 2023

[25] GUIMARÃES, A. G.; LINS, R. D.; OLIVEIRA. R. Segurança com redes privadas virtuais VPNs. Rio de Janeiro: Brasport, 2006.

[26] CARDOSO, Felipe Cesar. Conceitos de rede virtual privada para streaming seguro de vídeo. Universidade São Franscisco, p. 48, 2010.

[27] KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet: Uma Abordagem Top-Down. 6th ed. São Paulo: Pearson Education, 2017.

[28] A two‐step authentication framework for Mobile ad hoc networks Komninos, N., Vergados, D. D. & Douligeris, C. (2007). A two‐step authentication framework for Mobile ad hoc networks. China Communications Journal, 4(1), pp. 28-39.

[29] O que é a norma ISO 27001?. Disponível em: <https://www.27001.pt/>

[30] TSUNODA, H.; KEENI, G. M. Security by simple network traffic monitoring. Proceedings of the Fifth International Conference on Security of Information and Networks - SIN ’12, 2012.

[31] Donaldson, S.E. et al. (2015). Enterprise Cybersecurity Architecture. In: Enterprise Cybersecurity. Apress, Berkeley, CA. <https://doi.org/10.1007/978-1-4302-6083-7_3>

[32] Baptista Junior, J.H. e Dian, M. de O. A CRESCENTE IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, SOBRETUDO DURANTE A PANDEMIA. Revista Interface Tecnológica, [S. l.], v. 18, n. 1, p. 56–67, 2021. DOI: 10.31510/infa.v18i1.1109. Disponível em: <https://revista.fatectq.edu.br/interfacetecnologica/article/view/1109>. Acesso em: 25 maio. 2023.

[33] Dowling, S., Schukat, M. and Barrett, E. (2020), New framework for adaptive and agile honeypots. ETRI Journal, 42: 965-975. <https://doi.org/10.4218/etrij.2019-0155>

[34] Specht, Stephen M. and Ruby B. Lee. “Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures.” Parallel and Distributed Computing Systems (ISCA) (2004).