INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES
CAMPUS MACAPÁ

CAUÊ DA SILVA BANDEIRA
DIEGO NASCIMENTO NOBRE

SEGURANÇA EM REDES DE COMPUTADORES: medidas para detecção e prevenção de ataques cibernéticos em redes corporativas

MACAPÁ – AP
2023

CAUÊ DA SILVA BANDEIRA
DIEGO NASCIMENTO NOBRE

SEGURANÇA EM REDES DE COMPUTADORES: medidas para detecção e prevenção de ataques cibernéticos em redes corporativas

Trabalho de Conclusão de Curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Prof.° Orientador: Me Jairo de Kassio Siqueira Barreto.

MACAPÁ - AP
2023

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

B214s Bandeira, Cauê da Silva
Segurança em redes de computadores: medidas para detecção e prevenção de ataques cibernéticos em rede corporativas / Cauê da Silva Bandeira, Diego Nascimento Nobre. - Macapá, 2023.
70 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2023.

Orientador: Jairo de Kassio Siqueira.

1. Gerenciamento de redes. 2. Segurança cibernética. 3. Ataques ciberneticos. I. Nobre, Diego Nascimento. I. Siqueira, Jairo de Kassio, orient. II. Titulo.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

CAUÊ DA SILVA BANDEIRA

DIEGO NASCIMENTO NOBRE

SEGURANÇA EM REDES DE COMPUTADORES: Medidas para detecção e prevenção de ataques cibernéticos em redes corporativas.

Trabalho de Conclusão de Curso apresentado ao curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Prof.° Orientador: Jairo de Kassio Siqueira Barreto.

BANCA EXAMINADORA

PROF. ESP. JAIRO DE KASSIO SIQUEIRA BARRETO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ

PROF. ME. OLAVO NYLANDER BRITO NETO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ

PROF. ME. CÉLIO DO NASCIMENTO RODRIGUES

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ

Aprovado em:__26____/__06___/__2023_____

Nota:_____**8,5**_____

A minha família que me apoiou incondicionalmente durante todo esse percurso, especialmente aos meus pais Josilene Bandeira e Giovanni Bandeira, à minha irmã Stella Bandeira e minha namorada Thássia Machado.

(BANDEIRA, 2023)

A minha família que me apoiou incondicionalmente durante todo esse percurso, especialmente à minha querida mãe Angela Nascimento Nobre, ao meu nobre pai Delso Santana nobre, minha querida esposa Lady Kerollene chagas de Almeida, ao meu querido irmão Delso Santana nobre Júnior, ao meu nobre sogro Adinaldo Ferreira de Almeida e a Tarliso doria gerente de TI.

(NOBRE, 2023)

AGRADECIMENTOS

A Deus, pelas nossas vidas, e por nos permitir ultrapassar todos os obstáculos encontrados ao longo da realização desta monografia.

Aos familiares por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho. Especialmente aos meus pais Josilene Bandeira e Giovanni Bandeira, à minha irmã Stella Bandeira e minha namorada Thássia Machado, (BANDEIRA, 2023). Especialmente à minha querida mãe Angela Nascimento Nobre, à minha querida esposa Lady Kerollene Chadas de Almeida e a minha saudosa filha Lady Mikaela de Almeida Nobre, (NOBRE, 2023).

Aos professores, pelas correções e ensinamentos que nos permitiram apresentar um melhor desempenho no nosso processo de formação profissional ao longo do curso. Especialmente ao nosso professor orientador Jairo de Kassio Siqueira Barreto.

A todos aqueles que contribuíram de alguma forma para a realização deste trabalho. A todos que participaram, direta ou indiretamente em seu desenvolvimento, enriquecendo o nosso processo de aprendizado na área tecnológica. Às pessoas com quem convivemos ao longo desses anos de curso, que nos incentivaram e que certamente tiveram impacto em nossa formação acadêmica.

“Se tornou aparentemente óbvio que nossa tecnologia excedeu nossa humanidade”

(ALBERT EINSTEIN)

RESUMO

O objetivo geral da pesquisa foi apresentar medidas prevenção de ataques cibernéticos para segurança em redes corporativas tendo como sistema operacional o firewall Pfsense. A motivação do trabalho visa explanar sobre boas práticas de gerenciamento para proteção desse ativo precioso que é a informação. Sabe-se que não se pode negligenciar em nenhum aspecto as informações que uma empresa possui, zelando pela sua confiabilidade, integridade, disponibilidade, autenticidade, legalidade que são os pilares básicos da segurança da informação. O enfoque dos objetivos da pesquisa tem caráter explicativo para identificar os fatores que devem ser adotados para a segurança a partir dos eventos de ocorrência de invasões e ataques externos a redes corporativas. Os procedimentos técnicos e práticos foram desenvolvidos no laboratório de redes do IFAP que por sua vez está localizado no campus de Macapá. Criou-se um ambiente de TI com máquina virtual e implementou uma regra de segurança no PfSense com utilização do ping de rede, e integrou-se um ferramenta complementar a prevenção de ataques cibernéticos, o Graylog. Finalmente, com a aplicação das alterações no Firewall, foi possível realizar o ping com sucesso no Servidor Web, estabelecendo a comunicação entre as redes e demonstrando a eficácia da configuração e das regras de segurança implementadas com o pfSense. Assim, a implementação do Graylog como um sistema de gerenciamento de logs e eventos em conjunto com o firewall pfSense proporcionou benefícios significativos para a segurança e detecção de ataques externos e internos em uma rede corporativa.

Palavras-chave: gerenciamento de redes; segurança cibernética; ataques cibernéticos.

ABSTRACT

The general objective of the research is to present measures to prevent cyber attacks for security in corporate networks using the Pfsense firewall as an operating system. The motivation of the work is to explain good management practices to protect this precious asset that is information. It is known that one cannot neglect in any aspect the information that a company has, ensuring its reliability, integrity, availability, authenticity, legality that are the basic pillars of information security. The focus of the research objectives has an explanatory character to identify the factors that must be adopted for security based on the occurrence of invasions and external attacks on corporate networks. The technical and practical procedures were developed in the laboratory of networks of the IFAP that in turn is located in the campus of Macapá. An IT environment with a virtual machine was created and a security rule was implemented in PfSense using network ping, and a complementary tool for preventing cyber attacks, Graylog, was integrated. Finally, with the application of the changes in the Firewall, it was possible to successfully ping the Web Server, establishing communication between the networks and demonstrating the effectiveness of the configuration and security rules implemented with pfSense. Thus, the implementation of Graylog as a log and event management system in conjunction with the pfSense firewall provided significant benefits for security and detection of external and internal attacks on a corporate network.

Keywords: network management; cybersecurity; cyber-attacks.

SUMÁRIO

1 INTRODUÇÃO

A motivação para realização deste trabalho que discorre sobre a segurança em redes de computadores corporativas surgiu no transcorrer do processo de formação tecnológica do curso em redes de computadores do Institui Federal do Amapá - IFAP. Dentre os conteúdos das disciplinas distribuídas em 5 (cinco) períodos, a segurança em redes de computadores foi um eixo instigante para nós, enquanto acadêmicos de tecnologia. A informação é um ativo importantíssimo para as corporações, fazendo parte do mais alto nível estratégico de uma organização que preza pelo seu crescimento no mercado, o qual está a cada dia mais competitivo. A informação assume valores altíssimos para o crescimento financeiro de uma empresa fazendo seu patrimônio prosperar. Nesse sentido, a necessidade de proteção desse ativo nas corporações deve ser uma prioridade, sendo que este ativo se liga diretamente a sua permanência no mercado atual. Uma corporação precisa prezar pela segurança da informação, sendo uma opção inteligente, a adoção de um sistema operacional de gerenciamento de redes como o firewall Pfsense, posteriormente, podendo adotar outros serviços para integração de medidas para prevenção e detecção de ataques cibernéticos. Os administradores de redes devem ser profissionais competentes. Eles são componentes de uma equipe de TI no contexto organizacional na maioria das vezes.

Consonante a este entendimento, nós enquanto futuros profissionais e administradores de redes concentramos esforços para explanar sobre boas práticas de gerenciamento para priorização desse ativo precioso que é a informação. Sabe-se que não se pode negligenciar em nenhum aspecto as informações que uma empresa possui, zelando pela sua confiabilidade, integridade, disponibilidade, autenticidade, legalidade que são os pilares básicos da segurança da informação. A ênfase que se é dada sobre a segurança em redes de computadores está ligado ao valor que as informações possuem em redes empresariais, devido ao fato do crescimento tecnológico. Com isso, problemas relacionados a ataques cibernéticos em redes corporativas são exponenciais e constantes, sendo necessário que administradores competentes saibam pensar em medidas para detectar e prevenir problemáticas dessa magnitude. Portanto, a motivação desta pesquisa segue nessa lógica e concordância conjunta em seu desenvolvimento. A oportunidade de agregar valor técnico por meio de uma monografia para as corporações da era da informação nos permitiu estruturar e definir a temática deste trabalho. Assim, almejamos que os conhecimentos técnicos selecionados contribuam para agregar valor nos processos de tratamento das informações empresariais aumentando o seu nível de segurança em redes computacionais corporativas.

O objetivo geral da pesquisa é apresentar medidas detectivas e preventivas à ataques cibernéticos para segurança em redes corporativas com o firewall Pfsense. Com isso, se estipulou os seguintes objetivos específicos: (1) Definir configurações personalizadas no firewall Pfsense alinhadas com medidas segurança levando em conta ataques realizados contemporaneamente em redes de computadores; (2) Montar um cenário em laboratório para simulação de ataques externos em redes corporativas; (3) Apontar outros serviços que podem ser integrados ao Pfsense para proteção de redes corporativas. As redes corporativas são alvos frequentes de ataques cibernéticos, tanto de origem externa quanto interna. A segurança da rede é uma preocupação crítica para as empresas, pois um ataque bem-sucedido pode resultar em perda de dados, interrupção das operações comerciais e danos à reputação da empresa. Por isso, é fundamental implementar medidas de segurança para prevenir e detectar ataques cibernéticos. Com isso, o problema da pesquisa se concentra em: Quais são as medidas para detecção e prevenção de ataques cibernéticos em redes corporativas com o firewall Pfsense?, a problemática está relacionada a necessidade que as corporações têm na adoção de medidas para proteger suas informações de ataques e invasões de redes de computadores externas e internas. Ademais, a justificativa deste trabalho é sustentada pelo valor que os conhecimentos sistematizados têm para agregar valor as corporações que buscam proteger suas redes de computadores. As configurações do firewall Pfsense contribuem para que os administradores possam definir regras para conceder e bloquear acessos externos e internos, minimizando a possibilidade de acessos indevidos. Ainda, outros serviços podem ser integrados ao firewall para reforçar a proteção e segurança de redes corporativas levando ao desenvolvimento de medidas detectivas e preventivas de ataques e invasões cibernéticas. Então, a pesquisa apresenta justificativa técnica e tecnológica com conhecimentos que entreguem valor utilitário e prático para resoluções de problemas que corporações possuem na sua infraestrutura de TI.

Abordando o leque de benefícios que as empresas podem ter a partir dos conhecimentos práticos que este trabalho buscou desenvolver em laboratório, pode ser citado que as corporações têm a possibilidade de melhorar significativamente suas tomadas de decisões e mudanças organizacionais fazendo suas estratégias de negócios se tornarem mais ágeis, enxutas e efetivas. Portanto, todas as partes que buscam ser atendidas pelos processos e atividades desenvolvidas por uma empresa se beneficiam também, tecnicamente, essas partes são chamadas de stakeholders.

Stakeholders são pessoas, grupos ou organizações que podem ser afetados ou afetar as atividades, objetivos e resultados de uma empresa ou organização. Eles são indivíduos ou grupos que têm um interesse ou uma "parte interessada" (em inglês, stakeholder) em uma

organização e podem ser influenciados pelos resultados de suas atividades ou ter a capacidade de influenciar as decisões da organização. Os stakeholders podem incluir clientes, funcionários, acionistas, fornecedores, concorrentes, governo, comunidades locais e outros grupos que possam ser afetados ou interessados nas atividades de uma organização. Eles têm diferentes níveis de poder e influência sobre a organização, dependendo do tipo de relacionamento que mantêm e dos recursos que possuem.

A gestão de stakeholders envolve a identificação, análise e gerenciamento dos interesses, necessidades e expectativas dos stakeholders. Isso pode incluir o envolvimento dos stakeholders em decisões e planejamento estratégico, a criação de programas de responsabilidade social e ambiental, a comunicação transparente e a construção de relacionamentos mutuamente benéficos. O gerenciamento eficaz de stakeholders é importante para o sucesso de uma organização e pode ajudar a melhorar a sua reputação, reduzir os riscos de conflito e criar valor para todas as partes interessadas envolvidas.

Pensando no todo organizacional, os ganhos em melhorias se estendem à: (a) redução de custos, essa é uma preocupação constante das corporações em qualquer setor de atuação, sendo que ao melhorar e satisfazer suas necessidades e de seus clientes, consequentemente as receitas de uma empresa aumentará, podendo-se evitar processos em que ocorrem muitas despesas; (b) aumento da produtividade, os envolvidos nos processos organizacionais, podem obter maior produtividade, eliminando preocupações de ordem intrusiva de fatores externos, tornando-se possível entregar mais com a mesma base de recursos ou até mesmo com menos; (c) otimização de processos, medidas de segurança a nível estratégico além de tornar o trabalho mais rápido e eficiente, libera os funcionários para desempenho de tarefas mais estratégicas e que exigem raciocínio, permitindo o melhor aproveitamento do capital humano; (d) aumento do controle de qualidade, as máquinas estando menos sujeitas a erros para atividade de produção em grande escala faz com que o uso da tecnologia seja essencial para manter a qualidade e controle de itens, com o uso de um bom software a organização e gerenciamento de informações permite enxergar um quadro completo das necessidades, melhorando a entrega de resultados consistentes.

Nesse sentido, investir em medidas de segurança contribui para o crescimento e desenvolvimento constante dos processos organizacionais, impactando e elevando o nível de suas estratégias ou mesmo dando condições para o desenvolvimento mais efetivo delas. As organizações trabalham com informações todos os dias, então a segurança e proteção delas não podem ser negligenciados. Pensar em segurança é explorar condições ou estados para proteção das informações; ter a capacidade para manutenção da segurança de informações

organizacionais; adotar mecanismos para proteção contra a fuga ou escape de informações ligadas as estratégias potenciais das empresas; ainda, é ter confiança nos seus próprios processos internos com redução de incertezas e imprevistos de ordem externa. Assim, a pesquisa é embutida de justificativa genuinamente estratégica por seus administradores de redes/empresariais e o aumento substancial dos recursos monetários nas corporações.

Adiante, é detalhada a metodologia adotada pela pesquisa. Quanto a natureza da pesquisa ela é do tipo aplicada. Vários autores abordam sobre esse tipo de metodologia: (FLEURY; WERLANG, 2016); (PARANHOS; PARANHOS, 2014), esses últimos com enfoque principalmente na área tecnológica. Consonante a abordagem do problema é do tipo qualitativa, uma vez que houve a interpretação dos resultados extraídos dos procedimentos técnicos em laboratório para atribuição de significados e valores para responder ao problema levantado, sendo um processo prático e dinâmico para adaptação de soluções nos ambientes de corporações, sendo esses ambientes diversos e complexos também. O enfoque dos objetivos da pesquisa tem caráter explicativo, pois visa identificar os fatores que devem ser adotados para a segurança a partir dos fenômenos de ocorrência de invasões e ataques externos a redes corporativas.

No escopo da literatura em redes de computadores são trabalhados conceituações essenciais sobre o entendimento técnico do tema para desenvolvimento dos experimentos, relacionando os assuntos necessários para compreensão de terminologias próprias da área que envolvem a segurança e proteção de informações, o gerenciamento eficiente de redes de computadores com o firewall Pfsense, a contextualização está relacionada a vulnerabilidade das redes corporativas e as formas de ataques e invasões externas.

Os autores que trazem embasamento teórico são: Williamson e Persaud (2012), explicando pré-requisito para trabalhar de forma eficiente com o pfSense; Alves (2021), apresentando conceituações básicas sobre a ping, a forma de realização de testes, como estabilizar e interpretar os resultados dos testes que são feitos pelo termina de computadores com sistema Linux. Meyer (2016), apresentando um introdução de como os surgiu os primeiros vírus de computadores; Simmonds, Sandilands e Van Ekert (2004), retratam os principais métodos de prevenção contra ataques cibernéticos que podem ser implementados nas estruturas de redes de computadores corporativas pelos administradores.

Ao final são trazidas as considerações finais sobre a segurança, e as medidas para detecção e prevenção de ataques cibernéticos externos em redes corporativas, ainda uma síntese dos principais resultados dos testes em laboratório.

2 LITERATURA TECNOLÓGICA EM REDES DE COMPUTADORES

Essa seção inicia com considerações básicas e que são pré-requisito para trabalhar de forma eficiente com o pfSense. As informações presentes foram baseadas na obra do 'Livro do PfSense 2.0' dos autores Williamson e Persaud (2012). Com recursos abrangentes e uma interface web intuitiva, o pfSense permite implementar uma estratégia eficiente de controle e segurança do tráfego de rede, garantindo que apenas o tráfego autorizado e seguro seja permitido, protegendo a rede contra ameaças cibernéticas. Sua flexibilidade e recursos avançados fazem do pfSense uma escolha popular para a proteção e gerenciamento de redes.

2.1 **Firewall pfSense**

O pfSense é uma solução de Firewall largamente adotada e uma das mais robustas entre as opções OpenSource. Ele é um software com a licença BSD, ou seja não é preciso pagar licenças de uso. Além de ser um software gratuito, seus pacotes adicionais permite que ele seja considerado um UTM (Unified Threat Management, "Central Unificada de Gerenciamento de Ameaças"), já que se pode realizar com o pfSense muitas das atividades que esperamos de sistemas com esta funcionalidade. Ele também possui relatórios em Gráficos RRD, Modelagem de tráfego e filtragem e usa informações em tempo real. Todos os recursos disponíveis são gerenciados exclusivamente por uma interface Web de fácil interpretação, (4LINUX, 2023).

2.1.1 Principais recursos do pfSense

2.1.1.1 DashBoard

O Dashboard do pfSense é uma interface de controle e monitoramento que oferece uma visão geral detalhada da solução de firewall. Ele permite personalizar quais informações serão exibidas, proporcionando flexibilidade ao usuário. Nela é possível configurar diferentes widgets que são componentes de interface que exibem informações específicas e relevantes na Dashboard. Eles são configuráveis e fornecem uma visualização resumida e em tempo real de diversos aspectos do sistema. Cada widget exibe um conjunto específico de dados ou funcionalidades que podem ser personalizadas de acordo com as necessidades do usuário, para exibir dados relevantes, como estatísticas de tráfego, status da conexão, informações de

segurança, utilização de recursos, entre outros. Esses widgets podem ser organizados e dimensionados de acordo com as preferências do usuário.

Por meio do Dashboard, é possível ter acesso rápido a informações críticas, como o status dos serviços do firewall, o tráfego de rede em tempo real, a utilização dos recursos do sistema e a atividade de conexão. Esses dados são apresentados de forma clara e concisa, permitindo ao administrador identificar problemas, analisar tendências e tomar medidas necessárias para manter a segurança e o desempenho da rede. Além disso, também pode exibir alertas e notificações relacionados a eventos de segurança, como tentativas de invasão, violações de política de firewall ou atividades suspeitas. Isso permite uma resposta rápida e efetiva a incidentes de segurança, contribuindo para a proteção da rede contra ameaças cibernéticas.

A flexibilidade do Dashboard do pfSense permite que os administradores personalizem a exibição das informações conforme suas necessidades específicas. Eles podem escolher os widgets mais relevantes para o monitoramento diário, ajustar o layout da Dashboard de acordo com a preferência visual e até mesmo criar visualizações personalizadas para atender a requisitos específicos da organização.

2.1.1.2 Widget de status do sistema

Exibe detalhes sobre a saúde geral do sistema, como uso da CPU, memória, temperatura, tempo de atividade e disponibilidade de atualizações.

2.1.1.3 Widget de status dos serviços

Mostra o estado dos serviços essenciais, como DNS, DHCP, VPN, Captive Portal, entre outros. Permite identificar se os serviços estão em execução corretamente ou se houve alguma falha.

2.1.1.4 Widget das estatísticas de tráfego

Apresenta dados sobre a utilização da largura de banda, número de pacotes transmitidos e recebidos, gráficos de tráfego em tempo real, análise de protocolos utilizados, entre outras informações relacionadas ao tráfego de rede.

2.1.1.5 Widget de logs de firewall

Exibe registros de eventos de firewall, como conexões bloqueadas, tentativas de acesso não autorizadas, regras acionadas e informações de auditoria.

2.1.1.6 Widget de monitoramento de VPN

Mostra informações sobre conexões VPN ativas, status dos túneis, taxa de transferência e uso de recursos relacionados a VPN.

2.1.1.7 Widget de atividades de sistemas IDS/IPS

Fornece informações sobre eventos de detecção de intrusões, como tentativas de ataques, comportamentos suspeitos e alertas gerados por sistemas IDS/IPS integrados.

2.1.1.9 Widget das estatísticas de RRD

Exibe gráficos de tendência e histórico de métricas de desempenho do sistema, como utilização de CPU, memória, tráfego de rede, entre outros parâmetros monitorados.

É possível personalizar a seleção e o arranjo dos widgets na Dashboard para atender às necessidades específicas de monitoramento e controle do usuário. Através dos widgets, é possível obter informações essenciais de forma rápida e visualmente acessível, facilitando a administração e a tomada de decisões relacionadas à segurança e ao desempenho da rede.

2.1.1.10 Regras de firewall

Uma regra de firewall no pfSense é uma configuração que define como o tráfego de rede deve ser tratado e controlado pelo firewall. Ela especifica critérios e ações a serem aplicados às conexões de rede, determinando quais pacotes serão permitidos ou bloqueados.

Uma regra de firewall é composta por elementos-chave, incluindo:

1. Origem, especifica a origem do tráfego com base em endereços IP, sub-redes, grupos de endereços ou interfaces de rede.

2. Destino, define o destino do tráfego, que pode ser um endereço IP, uma sub-rede, um grupo de endereços ou uma interface de rede.

3. Protocolo, indica o protocolo usado pelo tráfego, como TCP, UDP, ICMP ou qualquer outro protocolo específico.

4. Portas, especifica as portas ou intervalos de portas associados ao tráfego, como a porta 80 para tráfego HTTP ou a porta 443 para tráfego HTTPS.

5. Ação, determina a ação a ser tomada em relação ao tráfego correspondente à regra. Isso pode ser permitir (pass), bloquear (block), redirecionar (redirect), entre outras ações possíveis.

6. Estado da conexão, define como o firewall deve tratar conexões estabelecidas, como permitir pacotes relacionados a conexões já estabelecidas (stateful) ou tratar todas as conexões de maneira independente (stateless).

Além desses elementos principais, as regras de firewall no pfSense também podem incluir opções adicionais, como definição de limites de taxa (rate limiting), filtragem de conteúdo, configurações de registro de logs e opções avançadas de manipulação de pacotes.

Ao criar regras de firewall no pfSense, é importante considerar cuidadosamente as políticas de segurança da rede e as necessidades específicas da organização. As regras devem ser configuradas de forma adequada para proteger a rede contra ameaças, permitir o fluxo adequado do tráfego legítimo e evitar falsos positivos ou bloqueios indesejados.

Através das regras de firewall, o pfSense permite implementar uma estratégia eficiente de controle e segurança do tráfego de rede, garantindo que apenas o tráfego autorizado e seguro seja permitido e protegendo a rede contra ameaças cibernéticas.

2.1.2 Configurações de segurança para detecção e prevenção de ataques cibernéticos

2.1.2.1 Filtragem de pacotes

A configuração de filtragem de pacotes desempenha um papel crucial na segurança de redes corporativas, pois ajuda a controlar e monitorar o tráfego de rede com base em critérios específicos. Essa técnica é implementada por meio de regras de firewall que permitem ou bloqueiam o tráfego de acordo com as configurações definidas.

Ao configurar a filtragem de pacotes no pfSense, é possível estabelecer uma série de regras que definem como o tráfego deve ser tratado. Essas regras podem ser baseadas em endereços IP, portas, protocolos, interfaces de rede e outras características do tráfego.

A configuração inicia-se acessando a interface de administração web do pfSense. Navega-se até a seção "Firewall" e escolhe-se "Regras" ou "Filtragem de Pacotes". A partir daí,

podem ser criadas as regras de firewall para permitir ou bloquear o tráfego com base nos critérios desejados.

Por exemplo, é possível criar uma regra para bloquear o tráfego proveniente de um determinado endereço IP ou intervalo de IPs conhecidos por serem maliciosos. Também é possível criar regras para permitir apenas o tráfego destinado a portas específicas, como permitir o acesso ao servidor web na porta 80, mas bloquear o acesso a outras portas sensíveis.

A ordem de prioridade das regras também é fundamental. Ela determina a sequência em que as regras são avaliadas pelo firewall. É importante estabelecer a ordem correta para garantir que as regras sejam aplicadas de maneira adequada, evitando conflitos e assegurando que as políticas de segurança sejam implementadas conforme planejado.

A configuração da filtragem de pacotes proporciona diversos benefícios à segurança das redes corporativas. Ela permite bloquear tráfego indesejado ou potencialmente perigoso, como tentativas de invasão, ataques de negação de serviço (DoS), comunicações com servidores maliciosos, entre outros. Além disso, a filtragem de pacotes ajuda a controlar o fluxo de tráfego, melhorando a eficiência e a disponibilidade da rede.

Ao criar regras de filtragem de pacotes de maneira cuidadosa e estratégica, as organizações podem fortalecer suas defesas contra ameaças cibernéticas, reduzir o risco de exposição a ataques e proteger seus ativos e informações confidenciais de forma mais eficaz.

2.1.2.2 Inspeção de estado

A configuração da Inspeção de Estado em um firewall, como o pfSense, desempenha um papel crucial na segurança de redes corporativas. A Inspeção de Estado é um recurso que monitora o estado das conexões de rede e aplica políticas de segurança com base nesse estado.

A Inspeção de Estado permite ao firewall rastrear o estado das conexões estabelecidas, incluindo informações como endereços IP de origem e destino, portas utilizadas e o status da conexão. Com base nesses dados, o firewall pode tomar decisões de segurança mais informadas e aplicar políticas adequadas para garantir a integridade e a segurança da rede.

O processo de configuração da Inspeção de Estado no pfSense é relativamente simples. Ele envolve os seguintes passos:

1. Acesse o painel de controle do pfSense através de um navegador da web.

2. Navegue até a seção "Firewall" e selecione "Opções Avançadas".

3. Verifique se a opção "Inspeção de Estado" está ativada. Essa opção deve estar habilitada para que a funcionalidade de Inspeção de Estado seja aplicada.

4. Ajuste as configurações de acordo com as necessidades da rede. Isso pode incluir definição do tempo limite das conexões, configuração do número máximo de conexões simultâneas permitidas, ajuste de parâmetros relacionados à fragmentação de pacotes, entre outras opções avançadas disponíveis.

Ao configurar adequadamente a Inspeção de Estado, o pfSense proporciona diversos benefícios à segurança de redes corporativas:

A Inspeção de Estado permite ao firewall controlar as conexões estabelecidas, garantindo que apenas conexões legítimas e autorizadas sejam permitidas. Conexões indesejadas ou maliciosas podem ser bloqueadas com base nas políticas de segurança configuradas.

O monitoramento em tempo real das conexões possibilitado pela Inspeção de Estado ajuda a identificar e bloquear tentativas de ataques, como intrusões ou escaneamento de portas. O firewall pode detectar padrões suspeitos e tomar medidas para mitigar ameaças potenciais.

As configurações de Inspeção de Estado permitem ajustar o tempo limite das conexões e o número máximo de conexões simultâneas permitidas. Isso ajuda a evitar sobrecarga da rede e a otimizar o uso dos recursos disponíveis.

A Inspeção de Estado contribui para a integridade da rede, garantindo que apenas pacotes associados a conexões estabelecidas sejam permitidos. Isso ajuda a evitar o recebimento de pacotes não solicitados ou indesejados, melhorando a segurança da rede corporativa.

Assim, a configuração da Inspeção de Estado no pfSense é um componente crucial para a segurança de redes corporativas. Ela permite ao firewall monitorar o estado das conexões, tomar decisões de segurança com base nesses estados e aplicar políticas apropriadas para proteger a rede contra ameaças cibernéticas.

2.1.2.3 Bloqueio de sites maliciosos

A configuração de bloqueio de sites maliciosos em uma rede corporativa desempenha um papel crucial na segurança cibernética, pois impede o acesso a sites conhecidos por hospedar conteúdo malicioso ou serem fontes de ameaças. Esse processo é realizado por meio do firewall, como o pfSense, e envolve a criação de listas de bloqueio e a configuração de regras para bloquear ou redirecionar o tráfego para esses sites.

Para configurar o bloqueio de sites maliciosos no pfSense, o seguinte processo pode ser seguido:

1. Navegue até a seção "Firewall" e escolha "Alias" ou "DNSBL". Essas opções estão relacionadas ao bloqueio de sites maliciosos no pfSense.

2. Crie uma lista de bloqueio que contenha os endereços dos sites maliciosos conhecidos. Essa lista pode ser construída manualmente, adicionando individualmente os endereços dos sites, ou pode ser obtida a partir de fontes confiáveis de listas de bloqueio, como feeds de ameaças atualizados regularmente.

3. Configure regras de firewall para bloquear o tráfego para esses endereços ou redirecioná-lo para uma página de aviso. As regras de firewall podem ser configuradas para aplicar o bloqueio ou o redirecionamento com base nos endereços presentes na lista de bloqueio criada anteriormente. Por exemplo, uma regra pode ser criada para bloquear todo o tráfego proveniente ou destinado aos endereços listados.

O bloqueio de sites maliciosos impede que os usuários acessem sites identificados como fontes de malware, phishing, ransomware e outros ataques cibernéticos. Isso reduz o risco de infecção por malware e comprometimento da segurança dos sistemas.

Ao bloquear o acesso a sites maliciosos, o firewall diminui a superfície de ataque da rede corporativa. Isso significa que menos oportunidades são fornecidas para que os usuários sejam expostos a conteúdo prejudicial e potencialmente perigoso.

O bloqueio de sites maliciosos permite que as políticas de segurança da organização sejam aplicadas de forma mais efetiva. É possível estabelecer restrições no acesso a determinadas categorias de sites ou tipos de conteúdo que possam representar riscos de segurança ou violar políticas internas.

Quando o tráfego é bloqueado ou redirecionado para uma página de aviso, os usuários são informados sobre o risco associado aos sites maliciosos. Isso aumenta a conscientização dos usuários sobre as ameaças cibernéticas e os incentiva a adotar comportamentos mais seguros durante a navegação na internet.

Portanto, a configuração de bloqueio de sites maliciosos no pfSense é uma medida importante para fortalecer a segurança de redes corporativas. Ela impede o acesso a sites conhecidos por hospedar conteúdo malicioso e contribui para a proteção contra ameaças cibernéticas. A configuração envolve a criação de listas de bloqueio e a configuração de regras de firewall para bloquear ou redirecionar o tráfego para esses sites, protegendo assim a rede corporativa de possíveis comprometimentos de segurança.

2.1.2.4 Detecção de padrões suspeitos

A configuração de detecção de padrões suspeitos no pfSense é uma medida fundamental para fortalecer a segurança de redes corporativas. Essa configuração permite identificar e alertar sobre atividades de intrusão, comportamentos anômalos e possíveis ameaças na rede, fornecendo uma camada adicional de proteção contra ataques cibernéticos.

O processo de configuração pode ser realizado da seguinte maneira:

1. O pfSense oferece integração com soluções de detecção de intrusão, como o Snort ou Suricata. Acesse a seção "Serviços" ou "IDS/IPS" no pfSense para configurar as regras de detecção de intrusão de acordo com as necessidades da organização. Essas regras são responsáveis por identificar padrões de comportamento suspeito na rede.

2. Durante a configuração, é necessário definir os padrões de comportamento suspeito a serem monitorados. Esses padrões podem incluir assinaturas de ataques conhecidos, anomalias de tráfego, tentativas de intrusão ou qualquer comportamento que indique uma possível violação de segurança. Essas definições são baseadas em bancos de dados de ameaças atualizados regularmente, que contêm informações sobre técnicas e comportamentos maliciosos.

3. Além de definir os padrões suspeitos, é necessário configurar as ações a serem tomadas em caso de detecção. Isso envolve decidir se o tráfego identificado como suspeito deve ser bloqueado, registrado para análise posterior, notificado aos administradores da rede ou a outras medidas adequadas de acordo com a política de segurança da organização.

A detecção de padrões suspeitos permite identificar atividades maliciosas ou comportamentos anômalos na rede em estágios iniciais. Isso possibilita uma resposta rápida e efetiva às ameaças, minimizando o tempo de exposição a possíveis ataques.

Ao configurar regras de detecção de intrusão baseadas em padrões conhecidos de ataques, é possível bloquear o tráfego associado a esses ataques, impedindo sua execução e protegendo a rede corporativa contra ameaças bem documentadas.

A detecção de comportamentos suspeitos também pode ajudar a identificar atividades anormais que não correspondem a padrões conhecidos. Isso permite investigações mais aprofundadas para determinar se uma nova ameaça está em andamento e implementar contramedidas adequadas.

A detecção de padrões suspeitos complementa outros controles de segurança, como firewall e antivírus. Ela proporciona uma camada adicional de defesa, identificando atividades que podem escapar da detecção por meio desses outros mecanismos.

Então, a configuração da detecção de padrões suspeitos no pfSense contribui significativamente para a segurança de redes corporativas. Essa configuração permite a

identificação precoce de ameaças, a prevenção de ataques conhecidos, a mitigação de ameaças desconhecidas e a melhoria geral da eficácia dos controles de segurança. É um componente essencial para uma estratégia de segurança cibernética abrangente e efetiva.

2.1.2.5 Controle de tráfego

A configuração de controle de tráfego no pfSense desempenha um papel crucial na segurança de redes corporativas, permitindo gerenciar a taxa de transferência e o número máximo de conexões para diferentes tipos de tráfego. Essa configuração é essencial para evitar a sobrecarga da rede, mitigar ataques de negação de serviço (DoS) e garantir o desempenho adequado dos serviços disponibilizados.

O processo de configuração do controle de tráfego pode ser realizado da seguinte maneira:

1. No painel do pfSense, vá para a seção "Firewall" e selecione "Limitadores" ou "Balanceamento de Carga". Essas opções permitem configurar o controle de tráfego no pfSense.

2. Crie limitadores de tráfego para controlar a taxa de transferência ou o número máximo de conexões para determinados tipos de tráfego. Os limitadores podem ser configurados para aplicar restrições em diferentes níveis, como por endereço IP, por porta ou por protocolo. Por exemplo, é possível criar limitadores para controlar a largura de banda de um determinado serviço ou para limitar o número de conexões simultâneas permitidas para um serviço específico.

3. Configure regras de firewall para aplicar esses limitadores aos pacotes correspondentes. As regras de firewall são responsáveis por identificar o tráfego que deve ser submetido aos limitadores criados. Por exemplo, é possível criar regras que correspondam a determinados tipos de tráfego, como tráfego HTTP ou tráfego de download, e aplicar os limitadores correspondentes a essas regras.

Ao controlar a taxa de transferência e o número de conexões, é possível evitar a sobrecarga da rede, garantindo que os recursos estejam adequadamente alocados para atender às demandas dos serviços. Isso ajuda a evitar a degradação do desempenho e a garantir a disponibilidade dos serviços para usuários legítimos.

O controle de tráfego é uma medida efetiva para mitigar ataques de negação de serviço (DoS). Ao limitar a taxa de transferência e o número de conexões, é possível reduzir o impacto de ataques que buscam sobrecarregar a rede com tráfego malicioso ou excessivo.

A configuração do controle de tráfego permite um gerenciamento eficiente dos recursos de rede. É possível priorizar determinados tipos de tráfego ou serviços críticos, garantindo a disponibilidade e a qualidade do serviço para usuários prioritários.

O controle de tráfego ajuda a prevenir abusos e utilizações indevidas da rede. Ao limitar a taxa de transferência ou o número de conexões para determinados tipos de tráfego, é possível evitar o uso excessivo de recursos por parte de usuários ou serviços, garantindo uma distribuição equitativa dos recursos disponíveis.

Portanto, a configuração do controle de tráfego no pfSense desempenha um papel importante na segurança de redes corporativas. Ela permite evitar a sobrecarga da rede, mitigar ataques de negação de serviço, gerenciar eficientemente os recursos e proteger contra abusos e utilização indevida. Ao aplicar limites e restrições adequados ao tráfego, é possível garantir a disponibilidade, a performance e a confiabilidade da rede corporativa.

2.1.3 O pfSense utilizado para prevenção de métodos de ataques cibernéticos

2.1.3.1 pfSense na prevenção vírus

O pfSense emprega recursos de detecção e prevenção de vírus, como análise em tempo real do tráfego e filtragem de conteúdo. É possível configurá-lo para bloquear downloads de arquivos suspeitos e examinar o tráfego de entrada e saída em busca de indícios de atividades maliciosas.

2.1.3.2 pfSense na prevenção DoS

O pfSense inclui recursos de mitigação de ataques DoS, tais como controle de taxa, limitação de conexões e balanceamento de carga. Essas funcionalidades garantem a disponibilidade dos serviços ao restringir o número de solicitações provenientes de um único IP e distribuir o tráfego de maneira equilibrada entre os servidores.

2.1.3.3 pfSense na prevenção de phishing

O pfSense pode ser configurado para bloquear sites maliciosos conhecidos por hospedar páginas de phishing. Ele utiliza listas atualizadas regularmente, que contêm os endereços dos

sites de phishing, a fim de evitar o acesso a esses locais e proteger os usuários contra ataques dessa natureza.

2.1.3.4 pfSense na prevenção de exploração de vulnerabilidades

O pfSense oferece recursos de filtragem de pacotes e inspeção de estado para identificar e bloquear tentativas de explorar vulnerabilidades conhecidas. Ele examina o tráfego em busca de padrões suspeitos e impede a conexão de acordo com comportamentos característicos de exploração.

2.1.3.5 pfSense na prevenção de exploits

É possível configurar o pfSense para bloquear o tráfego associado a ransomware, como comunicações com servidores de comando e controle conhecidos. Além disso, recursos como backups automatizados e restrições de acesso a compartilhamentos de rede auxiliam na prevenção e mitigação dos efeitos de ataques de ransomware.

2.1.3.6 pfSense na prevenção de injeção SQL

O pfSense pode ser configurado para filtrar e bloquear consultas SQL maliciosas, prevenindo ataques de injeção SQL. Ele examina o tráfego em busca de padrões típicos de ataques desse tipo e impede as tentativas de exploração.

Assim, o pfSense combate efetivamente esses métodos de ataques cibernéticos por meio de recursos como filtragem de pacotes, inspeção de estado, bloqueio de sites maliciosos, detecção de padrões suspeitos e controle de tráfego. Sua flexibilidade e possibilidade de configuração personalizada permitem adaptar as medidas de segurança de acordo com as necessidades e o ambiente específico de cada organização.

2.2 Descrição do Ping

A latência de rede, comumente referida como ping ou taxa de latência, é a medida do tempo necessário para um pacote de dados percorrer o caminho entre um dispositivo e um servidor na Internet e retornar ao dispositivo. Essa medida é expressa em milissegundos (ms). É fundamental salientar que um valor de ping mais elevado indica uma conectividade mais lenta

do dispositivo. Consequentemente, um alto valor de ping dificulta a sincronização de informações em tempo real, (ALVES, 2021).

Um exemplo comum é observado em videogames, nos quais um ping alto resulta em atrasos nos dados recebidos, fazendo com que as informações disponíveis para o usuário durante uma partida estejam desatualizadas em relação ao estado atual do jogo. Além disso, em transmissões online e no acesso a conteúdo em streaming, é igualmente importante possuir um ping adequado, a fim de garantir uma comunicação fluida, sem atrasos ou interrupções na recepção dos dados.

2.2.1 Teste de Ping em computadores com sistema linux

No sistema Linux, o teste do ping pode ser realizado usando o utilitário de linha de comando "ping". Os seguintes passos devem ser seguidos:

- Abrir o terminal no sistema Linux.
- Digitar o comando "ping" seguido do endereço IP ou nome de domínio do servidor que se deseja testar. Por exemplo, "ping www.google.com".
- Pressionar Enter para iniciar o teste de ping.
- Serão exibidos uma série de resultados mostrando o tempo de ida e volta (latência) dos pacotes de dados enviados para o servidor.

2.2.2 Parâmetros adequados de boa qualidade e má qualidade de teste de ping

Os parâmetros considerados adequados para a qualidade do ping podem variar dependendo da aplicação e das necessidades específicas do usuário. Alguns exemplos de referência são os seguintes:

É de boa qualidade, em geral, um ping abaixo de 100 ms, sendo considerado bom. Por exemplo, um resultado como "64 bytes from www.google.com (172.217.168.196): icmp_seq=1 ttl=117 time=13.2 ms" indica um ping de 13.2 ms, o que é considerado de boa qualidade.

É de má qualidade, um ping acima de 200 ms, geralmente indicando qualidade ruim. Por exemplo, um resultado como "64 bytes from www.google.com (172.217.168.196): icmp_seq=1 ttl=117 time=247.8 ms" indica um ping de 247.8 ms, o que é considerado de má qualidade.

É importante ressaltar que esses valores são apenas exemplos e podem variar dependendo do contexto e dos requisitos específicos da aplicação.

2.2.3 Interpretação do teste de ping

Ao interpretar os resultados do teste de ping, algumas informações relevantes podem ser consideradas:

A latência média, é a média dos tempos de ida e volta dos pacotes de dados. Quanto menor esse valor, melhor é a qualidade da conexão.

A variação (jitter), refere-se à variação nos tempos de resposta dos pacotes. Valores baixos indicam uma conexão mais estável.

A perda de pacotes, mostra a porcentagem de pacotes de dados que não retornaram. Idealmente, deve ser 0%, pois a perda de pacotes pode afetar negativamente a qualidade da conexão.

2.2.4 Estabilização do ping

Para estabilizar o ping e obter uma conexão mais consistente, algumas medidas podem ser consideradas:

Verificar a conexão física, certificar-se de que todos os cabos de rede estejam bem conectados e em bom estado. Uma conexão física instável pode causar flutuações no ping.

Fechar aplicativos em segundo plano, alguns aplicativos em execução podem consumir largura de banda e causar instabilidade na conexão. Fechar programas desnecessários garante que a largura de banda esteja disponível para a aplicação em uso.

Evitar interferências na rede, outros dispositivos eletrônicos próximos, como telefones sem fio ou micro-ondas, podem interferir no sinal Wi-Fi. Posicionar o roteador em um local adequado e evitar obstáculos físicos entre o dispositivo e o roteador ajuda a reduzir interferências.

Considerar a atualização do hardware, em alguns casos, a instabilidade do ping pode ser causada por limitações de hardware, como um roteador antigo ou uma placa de rede desatualizada. Atualizar o hardware pode melhorar a estabilidade da conexão.

Entrar em contato com o provedor de serviços de Internet (ISP), caso ocorram problemas persistentes de estabilidade do ping, é recomendado entrar em contato com o ISP

para relatar o problema. Eles podem realizar verificações e ajustes na conexão para melhorar a qualidade do ping.

É importante lembrar que a estabilização do ping pode depender de vários fatores, incluindo a configuração da rede doméstica, a qualidade do serviço de Internet e outros fatores externos.

2.3 Métodos de ataques cibernéticos utilizados ao longo do tempo

Existem vários métodos de ataques cibernéticos que podem ser utilizados em redes de computadores corporativas, e esses ataques têm evoluído ao longo do tempo, à medida que novas vulnerabilidades são descobertas e novas técnicas são desenvolvidas. Alguns exemplos de métodos de ataques cibernéticos incluem:

2.3.1 Vírus de computador (1980)

A década de 1980 testemunhou o surgimento dos primeiros vírus de computador, que eram programas maliciosos capazes de se replicar e se espalhar para outros sistemas.

Elk Cloner (1982), foi um vírus de computador notável nos primórdios da computação e é considerado a primeira praga de contaminação em massa. Criado em 1982 por Rich Skrenta, então com 15 anos de idade e estudante do ensino médio, o Elk Cloner foi desenvolvido para infectar os computadores Apple II, que eram populares naquela época, (MEYER, 2016)

O termo "vírus" só começou a ser usado mesmo em 1984, quando, nos laboratórios da Bell Computers, quatro programadores, H. Douglas Mellory, Robert Morris, Victor Vysottsky e Ken Thompson, desenvolveram um jogo nomeado de Core Wars, baseado na ideia do primeiro vírus (Elk Cloner). Brain (1986), considerado o primeiro vírus de computador para PC, o Brain foi criado por dois irmãos paquistaneses, Basit e Amjad Farooq Alvi. Ele se espalhava através de disquetes infectados e exibia uma mensagem inofensiva, indicando que o sistema estava infectado, (MEYER, 2016)

Jerusalem (1987), o vírus Jerusalem foi detectado pela primeira vez na cidade de Jerusalém, daí o seu nome. Ele infectava sistemas MS-DOS e se espalhava através de disquetes. O Jerusalem ativava em uma data específica (o dia 13 de cada mês), danificando arquivos executáveis e causando problemas no sistema, (MACIEL, 2021). Morris Worm (1988), criado por Robert Tappan Morris, o Morris Worm foi um dos primeiros worms de computador conhecidos. Ele se espalhava pela Internet explorando uma vulnerabilidade no protocolo

TCP/IP. O worm infectou muitos sistemas, causando lentidão significativa na rede, (HOMEPAGES, 2023).

2.3.2 Principais ameaças cibernéticas (1990)

Na segunda metade da década de 90 surgiu a técnica Smurf, que trouxe mais inteligência aos ataques, apesar de ainda serem realizados de forma centralizada. Ao mesmo tempo que o hacker direcionava poucas ofensivas a uma única vítima, ele poderia multiplicá-las por centenas ou até milhares de vezes, com potencial para atingir mais usuários, dependendo dos recursos de rede disponíveis, (SECURITY REPORT, 2023).

Na década de 90 se populariza o sniffing de rede, que envolve o uso de ferramentas de sniffer para interceptar e analisar dados em trânsito em uma rede. Os invasores realizavam essa atividade para obter acesso a informações confidenciais, como senhas, dados de login e outras informações sensíveis que estavam sendo transmitidas pela rede. Eles usavam essas informações para fins maliciosos, como roubo de identidade, acesso não autorizado a sistemas ou espionagem corporativa. Ferramentas populares na época, como o Wireshark (anteriormente conhecido como Ethereal), foram usadas para realizar esses ataques, (SECURITY REPORT, 2023).

Os ataques de força bruta eram comuns durante a década de 1990 e envolviam a tentativa de descobrir senhas ou chaves de criptografia por meio de uma abordagem de tentativa e erro. Os invasores usavam programas automatizados para testar uma ampla variedade de combinações de senhas em alta velocidade até encontrarem a combinação correta. Esses ataques eram frequentemente direcionados a sistemas protegidos por senhas fracas ou senhas comuns. Os invasores se aproveitavam da falta de proteção adequada e da baixa complexidade das senhas para obter acesso não autorizado a sistemas ou contas, (SECURITY REPORT, 2023).

Exploits de software aparecem durante a década de 1990, houve a descoberta e exploração de várias vulnerabilidades em software. Os invasores identificavam falhas de segurança em aplicativos ou sistemas operacionais e criavam códigos maliciosos conhecidos como exploits para explorar essas vulnerabilidades. Os exploits eram desenvolvidos para aproveitar falhas específicas e obter acesso não autorizado aos sistemas. Uma vulnerabilidade famosa descoberta na década de 1990 foi o exploit Buffer Overflow, que permitia que os invasores executem código malicioso injetado em uma área de memória além do espaço alocado para um aplicativo, (SECURITY REPORT, 2023).

2.3.3 Principais ameaças cibernéticas (2000 em diante)

2.3.3.1 Ataques de negação de serviço (DoS)

Os ataques de negação de serviço são usados para tornar-se um serviço indisponível, sobrecarregando-o com um grande volume de tráfego. Isso pode ser feito usando bots, que são computadores infectados controlados remotamente, ou por meio de ataques distribuídos de negação de serviço (DDoS), em que muitos computadores são usados para sobrecarregar o serviço alvo, (ARAÚJO; ROSSI, 2020). Na década de 2000 Ataques de Negação de Serviço (DoS) aparecem, um dos exemplos mais conhecidos de ataque de negação de serviço ocorreu em fevereiro de 2000, quando o site Yahoo! foi alvo de um ataque massivo. O ataque sobrecarregou os servidores da empresa com uma quantidade esmagadora de tráfego falso, tornando o site indisponível para os usuários por várias horas.

2.3.3.2 Ataques de phishing

Surge Ataques de phishing, um método de engenharia social usado para enganar as pessoas e levá-las a divulgar informações confidenciais, como senhas ou números de cartão de crédito. Os ataques de phishing geralmente são feitos por e-mail, mas também podem ser feitos por mensagens instantâneas, SMS ou chamadas telefônicas, (PEREIRA, 2012), (LAUDON; LAUDON, 2007), (JUNIOR; LIMA, 2010). Um marco importante no aumento dos ataques de phishing foi registrado em 2003, quando ocorreu um grande ataque de phishing contra clientes do banco online da Best Western. Os criminosos enviaram e-mails falsos solicitando aos clientes que atualizassem suas informações de conta, levando muitos deles a fornecer suas credenciais a sites fraudulentos.

2.3.3.3 Exploração de vulnerabilidade e exploits

A exploração de vulnerabilidades e exploits são termos usados na área de segurança da informação para descrever a atividade de identificar e explorar fraquezas em sistemas de computadores, softwares ou redes. Uma vulnerabilidade é uma fraqueza em um sistema ou software que pode ser explorada por um invasor para obter acesso não autorizado ou comprometer o sistema. Já um exploit é um código ou técnica que aproveita uma vulnerabilidade para executar um ataque ou assumir o controle do sistema afetado. Ademais,

um exemplo histórico significativo de exploração de vulnerabilidade ocorreu em 2008 com a descoberta da vulnerabilidade no protocolo DNS (Domain Name System). Essa vulnerabilidade permitia que os invasores redirecionassem usuários para sites falsos, redirecionando o tráfego da Internet. Esse ataque, conhecido como Kaminsky Attack, destacou a importância da segurança do DNS e levou a atualizações e melhorias em muitos sistemas DNS em todo o mundo.

2.3.3.4 Engenharia social

A Engenharia Social é uma técnica de manipulação psicológica utilizada por indivíduos mal-intencionados para enganar, persuadir ou explorar outras pessoas, a fim de obter informações confidenciais, acesso não autorizado a sistemas ou realizar ações prejudiciais. Em vez de explorar vulnerabilidades técnicas, a engenharia social explora as vulnerabilidades humanas, como a confiança, a ingenuidade, a curiosidade ou a falta de conhecimento. Um exemplo notável de um ataque de engenharia social ocorreu em 2015, quando o departamento de recursos humanos da empresa francesa TV5Monde foi alvo de um ataque cibernético. Os invasores usaram técnicas de engenharia social para obter acesso aos sistemas da emissora e causar interrupção em suas operações, incluindo a interrupção de transmissões ao vivo.

2.3.3.5 Ransomware

Ransomware é um tipo de malware (software malicioso) que criptografa os dados de um sistema ou dispositivo, tornando-os inacessíveis ao usuário legítimo. O objetivo principal do ransomware é extorquir dinheiro das vítimas, exigindo um pagamento (geralmente em criptomoedas) em troca da chave de descriptografia dos arquivos. Embora o ransomware tenha se tornado uma ameaça cada vez mais presente nos últimos anos, um evento notável foi o ataque do ransomware WannaCry em maio de 2017. Esse ataque afetou milhares de computadores em todo o mundo, explorando uma vulnerabilidade no protocolo SMB (Server Message Block) para se espalhar e criptografar os dados das vítimas, exigindo um resgate em Bitcoin para a recuperação dos arquivos.

2.3.3.6 Ataques de injeção de SQL

Os ataques de injeção de SQL têm sido uma ameaça persistente há algum tempo. Eles exploram falhas de segurança em aplicativos da web que não validam corretamente os dados inseridos pelo usuário. Esses ataques permitem que os invasores executem comandos SQL maliciosos, podendo manipular bancos de dados ou obter acesso não autorizado aos sistemas. Um dos casos mais famosos de injeção de SQL ocorreu em 2015, quando o site de encontros extraconjugais Ashley Madison foi invadido. Os invasores exploraram uma vulnerabilidade de injeção de SQL para obter acesso aos dados de milhões de usuários, expondo informações pessoais sensíveis e causando um grande impacto na reputação da empresa.

2.3.3.7 Ameaças persistentes avançadas (APTs)

As APTs são ataques altamente sofisticados e direcionados que surgiram e evoluíram ao longo do tempo. Sem um evento específico a destacar, as APTs têm sido utilizadas por grupos cibercriminosos e governos para realizar ataques prolongados e furtivos contra organizações específicas, com o objetivo de roubar informações sensíveis, obter acesso não autorizado. Um exemplo, é o Fancy Bear ou Pawn Storm, o APT28 é um grupo de hackers com supostos laços com a Rússia. Eles têm como alvo governos, organizações militares e empresas em todo o mundo. O APT28 é conhecido por usar técnicas de spear-phishing, exploits de software e malware personalizado para obter acesso não autorizado aos sistemas e roubar informações confidenciais.

2.3.4 Evolução dos métodos de ataques cibernéticos

A evolução histórica desses métodos de ataque tem sido marcada pela crescente sofisticação e complexidade dos ataques, à medida que os hackers desenvolvem novas técnicas para explorar vulnerabilidades e enganar os usuários. Alguns exemplos de evolução histórica dos ataques cibernéticos incluem que nos anos 90, os ataques eram mais simples e geralmente envolviam exploração de vulnerabilidades e ataques de negação de serviço.

Na década de 2000, os ataques começaram a se tornar mais sofisticados, com o uso de técnicas de engenharia social, phishing e malware. A partir de 2010, os ataques cibernéticos se tornaram cada vez mais avançados e complexos, com o uso de exploits zero-day, ataques DDoS de grande escala e técnicas de engenharia reversa. Atualmente, os ataques cibernéticos são ainda mais sofisticados, com o uso de inteligência artificial e aprendizado de máquina para automatizar o processo de hacking e aprimorar as técnicas de engenharia social e phishing.

2.4 Métodos de prevenção contra ataques cibernéticos

Esta seção explana sobre são algumas medidas que podem ser implementadas para garantir a segurança das redes corporativas, o início dessa discussão são as 'Políticas de segurança', conforme Simmonds, Sandilands e Van Ekert (2004) em redes de computadores na área de segurança de rede, elas consistem na provisão e políticas adotadas pelo administrador de rede para prevenir e monitorar o acesso não autorizado, uso incorreto, modificação ou negação da rede de computadores e dos seus recursos associados.

A prevenção de acesso não autorizado é uma das principais preocupações na segurança de redes de computadores, pois indivíduos mal-intencionados podem tentar obter acesso a informações confidenciais ou causar danos aos recursos da rede. O uso incorreto dos recursos da rede também pode ser problemático, pois pode levar à sobrecarga dos sistemas ou à exposição de informações confidenciais. A modificação ou negação da rede de computadores e seus recursos associados pode ser causada por malware ou outros tipos de ataques cibernéticos.

A segurança da rede corporativa é uma preocupação crítica para as empresas e é importante implementar medidas de segurança adequadas para prevenir e detectar ataques cibernéticos externos e internos. As empresas devem estabelecer políticas claras de segurança, implementar ferramentas de proteção, monitorar a rede regularmente e fornecer treinamento aos funcionários para minimizar os riscos de segurança.

Política de segurança, em geral, é um conjunto de regras que definem os mecanismos de segurança a serem implementados em uma organização, e como eles devem ser configurados e gerenciados. Toda política de segurança deve estar de acordo com as adaptações da organização e serem seguidas por todos os usuários dos meios tecnológicos que a política se refere. Uma política de segurança como qualquer outro tipo de política, deve seguir conceitos éticos e legais que não interfiram nas relações entre colaborador e companhia. É importante estabelecer políticas claras de segurança para definir regras e responsabilidades para a proteção da rede. Essas políticas devem ser revisadas e atualizadas regularmente.

As políticas de segurança da rede podem ser definidas através de um Firewall. Um firewall é uma ferramenta que ajuda a proteger a rede de ataques externos, bloqueando o tráfego de entrada não autorizado. É importante que o firewall seja configurado corretamente e atualizado regularmente para garantir a sua eficácia. Sampaio (2011) esclarece sobre três tipos básicos de firewall:

> Existem basicamente três classes de Firewall. O Firewall Filtro de Pacotes é o tipo de Firewall que filtra todo o tráfego direcionado a ele mesmo ou a rede local a qual ele isola, da mesma forma, é responsável por filtrar os pacotes que ele, ou a rede, emitem. O Firewall NAT tem a finalidade de manipular a rota do tráfego, aplicando a tradução de endereçamento sobre os pacotes. Isso possibilita a manipulação dos endereços de origem e destino entre outras coisas. Já o Firewall Híbrido, é a opção de Firewall que seria uma união entre as outras duas classes citadas anteriormente, ou seja, "agrega a si tanto funções de filtragem de pacotes quanto de NAT.", (SAMPAIO, 2011, p. 4)

Segundo Freire (2004), devemos bloquear pacotes originários de endereços inválidos previstos em RFC.

> Executar o bloqueio de endereços forjados ("spoofed" addresses). Pacotes originários do mundo exterior com origem de redes privadas (endereços internos previstos na RFC 1918 e rede 127) devem ser bloqueados e desconsiderados como tráfego de rede válido quando trafegando pelo meio público Internet. A importância do bloqueio de pacotes recebidos da Internet e que possuem endereço de origem de redes privadas ou endereços de loopback, reside em auxiliar na proteção contra o envio de pacotes forjados (spoofing), (FREIRE, 2004, p. 6).

Freire (2004) aconselha bloquear serviços de Login como Telnet (porta 23 do TCP), SSH (porta 22 do TCP), FTP (porta 21 do TCP), NetBIOS (porta 139 do TCP) e Rlogin (da porta 512 do TCP até a porta 514 do TCP). Como Telnet é utilizado para acesso remoto via terminal, onde informações como usuário, senha e dados, são exibidas abertamente e desprotegidas na rede por não possuir padrões de criptografia, estas informações automaticamente ficam expostas e passíveis de interceptação através da utilização de sniffers. A criptografia é uma técnica que ajuda a proteger os dados em trânsito na rede, impedindo que sejam interceptados ou modificados por um invasor. É importante implementar criptografia nos dados confidenciais, como senhas e informações de clientes.

Telnet também é vulnerável ao que chamamos de "captura de sessão" (session hijacking), permitindo a usuários remotos total controle sob sessões onde através da captura de uma sessão, é possível o comprometimento de um sistema diretamente através do Shell do sistema operacional. (FREIRE, 2004).

A captura de sessão é uma técnica de ataque na qual um invasor monitora e captura as informações trocadas entre o cliente e o servidor durante uma sessão. No caso do Telnet, as informações são transmitidas em texto simples, o que significa que um invasor pode facilmente capturar e ler o tráfego de rede, incluindo senhas, comandos e outras informações sensíveis.

Além disso, o Telnet não possui criptografia embutida, o que torna as informações ainda mais vulneráveis a interceptação e captura de sessão. Isso significa que um invasor pode usar

ferramentas como sniffer para interceptar o tráfego de rede e capturar informações de sessão do Telnet.

Portanto, o uso do Telnet não é recomendado em ambientes de produção, especialmente para acessar sistemas remotos que contêm informações sensíveis. Em vez disso, é recomendado o uso de protocolos de acesso remoto mais seguros, como SSH (Secure Shell), que usa criptografia para proteger o tráfego de rede e impedir a captura de sessão. Adiante, está um resumo das recomendações de Freire (2004) para bloqueio de serviços e portas:

> [...] também recomenda o bloqueio dos serviços Portmap/RPCBind (porta 111 do TCP e do UDP), NFS (porta 2049 do TCP e do UDP), Lockd (porta 4045 do TCP e do UDP). [...] também as portas 135 (TCP e UDP), 138 (UDP), 139 (TCP) além da porta 445 (TCP e UDP), que são utilizadas pela interface de desenvolvimento de aplicação NetBios. [...] todas as portas do intervalo entre 6000 e 6255 do TCP, as quais são empregadas por sistemas X-Windows. [...] o bloqueio do serviço de resolução de nomes (DNS, porta 53 do UDP) para todas as máquinas que não são servidores de DNS, e a Transferência de Zona (porta 53 do TCP) para todos os computadores que não são servidores de DNS secundários. [...] a o bloqueio de SMTP (porta 25 do TCP) para todas as máquinas que não são relays externos, POP (portas 109 e 110 do TCP) e IMAP (porta 143 do TCP). [...] recomenda a restrição de acesso à serviços HTTP somente aos servidores que necessitam prover serviços web, limitando seus acessos somente às portas 80 e 443. [...] o bloqueio do tráfego direcionado a portas abaixo das portas 20 do TCP e do UDP, assim como serviço Time (porta 37 do TCP e do UDP). [...] o bloqueio do tráfego direcionado à TFTP (porta 69 do UDP). [...] serviço Network News Transport Protocol (NNTP), o qual utiliza a porta 119 do TCP, seja bloqueado. [...] todo tráfego direcionado a porta 79 do TCP deve ser bloqueado, pois o serviço Finger permite a obtenção de informações preciosas para invasores em um estudo inicial de um servidor ou ambiente de rede. [...] a interceptação do tráfego direcionado à porta 123 do TCP, a qual é responsável pelo serviço Network Time Protocol (NTP), e que por sua vez deve ser bloqueado pelos mesmos motivos do serviço Time [...] O bloqueio do tráfego direcionado à porta 515 do TCP, que é utilizada pelo protocolo de impressão de sistemas Unix (LPD), é recomendado por Freire (2004), que indica o LPD como vulnerável a ataques de buffer overflow. [...] o bloqueio do tráfego referente ao protocolo Simple Network Management Protocol (SNMP), que atua nas portas 161 e 162, ambas do TCP e do UDP, pois é um serviço comumente identificado e explorado por invasores. [...] o bloqueio do tráfego direcionado ao Border Gateway Protocol (BGP), que atua na porta 179 do TCP [...] o bloqueio do protocolo SOCKS, que opera na porta 1080 do TCP, (FREIRE, 2004, p. 8-17).

Esclarecendo sobre alguns conceitos e definições dos serviços e bloqueios recomendados por Freire (2004), depreender-se que o Portmap (também conhecido como RPCBind) é um serviço de rede que mapeia as solicitações de programas de rede para os números de porta TCP e UDP correspondentes nos sistemas UNIX e Linux. Ele é usado para permitir que os programas cliente encontrem os serviços que precisam acessar em um servidor remoto.

O Portmap atua como um serviço de registro para programas que usam o Remote Procedure Call (RPC), que é um mecanismo de comunicação entre processos que permite a

execução de código em um computador remoto. Quando um programa cliente faz uma solicitação RPC, o Portmap é usado para determinar o número de porta correspondente no servidor, permitindo que a solicitação seja encaminhada ao serviço correto.

O Portmap é executado como um serviço em segundo plano em sistemas UNIX e Linux e usa o número de porta 111. Ele é essencial para o funcionamento de muitos serviços de rede em sistemas UNIX e Linux, incluindo NFS (Network File System) e NIS (Network Information Service). o Portmap pode ser vulnerável a ataques de negação de serviço (DoS) e a exploração de vulnerabilidades de segurança. Para mitigar essas ameaças, é recomendado que as organizações limitem o acesso ao serviço Portmap e implementem medidas de segurança, como firewalls e atualizações de segurança regulares.

O NetBIOS é um conjunto de protocolos de rede usados em sistemas operacionais Windows para permitir que os computadores se comuniquem entre si em uma rede local. O NetBIOS é responsável pela descoberta de nomes de computadores, compartilhamento de recursos, gerenciamento de sessões e resolução de nomes de computador em endereços IP.

Adiante, são apresentadas as definições das portas supracitadas por Freire (2004), assimilar para quais acessos elas se direcionam é relevante no entendimento de mantê-las bloqueadas.

A Porta 2049, é usada pelo protocolo NFS (Network File System) para compartilhar arquivos e diretórios em uma rede. O NFS é um protocolo cliente-servidor que permite que os usuários acessem arquivos remotos como se estivessem localmente no computador. A Porta 4045, é usada pelo protocolo Games for Windows - LIVE, que é uma plataforma de jogos online da Microsoft para jogos em PCs com Windows. Ele permite que os jogadores se conectem, joguem e interajam com outros jogadores online.

A Porta 135, é usada pelo protocolo Microsoft Remote Procedure Call (RPC), que permite que os programas em um computador se comuniquem com programas em outros computadores em uma rede. Ele é usado para compartilhar recursos, como arquivos, impressoras e serviços, entre computadores em uma rede Windows. A Porta 138, é usada pelo protocolo NetBIOS Datagram Service, que é um protocolo de comunicação usado em redes Windows para permitir que os computadores compartilhem recursos e se comuniquem entre si.

A Porta 139, é usada pelo protocolo NetBIOS Session Service, que é um protocolo de rede usado em redes Windows para estabelecer e manter sessões de comunicação entre computadores. A Porta 445, é usada pelo protocolo SMB (Server Message Block), que é um protocolo de compartilhamento de arquivos e impressoras usado em redes Windows. O SMB

permite que os usuários acessem e compartilhem arquivos e pastas em uma rede, além de fornecer recursos de impressão compartilhada.

O Intervalo entre 6000 e 6255 são geralmente usadas por aplicativos de terceiros que não possuem uma atribuição de porta padrão. Eles podem ser usados por aplicativos personalizados ou para serviços específicos que foram projetados para operar nesse intervalo. A Porta 53 do UDP é usada pelo protocolo DNS (Domain Name System), que é usado para converter nomes de domínio em endereços IP e vice-versa. O DNS é fundamental para a operação da Internet, permitindo que os usuários acessem sites e serviços por meio de nomes de domínio fáceis de lembrar em vez de endereços IP.

A Porta 53 do TCP é usada pelo protocolo DNS para transferir zonas DNS de um servidor para outro. A Porta 25 do TCP é usada pelo protocolo SMTP (Simple Mail Transfer Protocol), que é usado para enviar e receber e-mails. É a porta padrão usada para enviar e-mails de um cliente de e-mail para um servidor de e-mail. A Porta 109 do TCP é usada pelo protocolo POP2 (Post Office Protocol version 2), que é um protocolo de email usado para baixar e-mails de um servidor de e-mail para um cliente de e-mail.

A Porta 110 do TCP é usada pelo protocolo POP3 (Post Office Protocol version 3), que é um protocolo de email usado para baixar e-mails de um servidor de e-mail para um cliente de e-mail. A Porta 143 do TCP é usada pelo protocolo IMAP (Internet Message Access Protocol), que é um protocolo de email usado para acessar e-mails em um servidor de e-mail. A Porta 80 é a porta padrão usada pelo protocolo HTTP (Hypertext Transfer Protocol), que é usado para acessar sites e recursos da web. O HTTP é o protocolo usado para a maioria das transações na web.

A Porta 443 é a porta padrão usada pelo protocolo HTTPS (Hypertext Transfer Protocol Secure), que é uma versão segura do HTTP. O HTTPS é usado para acessar sites e recursos da web de forma segura e criptografada. A Porta 20 do TCP é usada pelo protocolo FTP (File Transfer Protocol), que é usado para transferir arquivos entre computadores em uma rede. A Porta 37 do TCP é usada pelo protocolo TIME (Time Protocol), que é usado para obter a hora atual de um servidor.

A Porta 37 do UDP é usada pelo protocolo TIME (Time Protocol) para obter a hora atual de um servidor. A Porta 69 é usada pelo protocolo TFTP (Trivial File Transfer Protocol), que é usado para transferir arquivos de forma simples e rápida entre computadores em uma rede. A 119 do TCP é a porta padrão usada pelo Protocolo de Correio Eletrônico (NNTP) de Rede de Notícias, que permite aos usuários acessar e postar mensagens em grupos de discussão baseados em notícias.

A 79 do TCP é a porta usada pelo serviço de gerenciamento remoto do Terminal Virtual. Esta porta é usada para permitir que um computador se conecte a outro computador usando o protocolo rlogin.

A 123 do TCP é a porta padrão usada pelo protocolo NTP (Network Time Protocol), que é usado para sincronizar os relógios de um conjunto de computadores em uma rede. A 515 do TCP é a porta usada pelo serviço de impressão remota do UNIX (LPD - Line Printer Daemon). Quando um usuário imprime um arquivo em uma impressora remota, o arquivo é enviado para a porta 515 da impressora.

A 161 do TCP é a porta usada pelo protocolo SNMP (Simple Network Management Protocol), que é usado para gerenciamento de rede. A 162 do TCP é a porta usada para receber mensagens de armadilha SNMP (SNMP Traps), que são alertas enviados por dispositivos de rede para um sistema de gerenciamento de rede quando ocorrem eventos importantes. A 161 do UDP é a porta usada pelo protocolo SNMP (Simple Network Management Protocol), que é usado para gerenciamento de rede.

A 162 do UDP é a porta usada para receber mensagens de armadilha SNMP (SNMP Traps), que são alertas enviados por dispositivos de rede para um sistema de gerenciamento de rede quando ocorrem eventos importantes.

A 179 do TCP é a porta usada pelo protocolo BGP (Border Gateway Protocol), que é usado para trocar informações de roteamento entre sistemas autônomos. A 1080 do TCP é a porta usada pelo protocolo SOCKS (SOCKet Secure), que é usado para encapsular conexões de rede em um proxy SOCKS para permitir que aplicativos de cliente se comuniquem com servidores através de um firewall.

É importante destacar que uma boa política de segurança aplicada em um firewall não se refere apenas a bloqueio de portas e serviços, e sim a um conjunto de regras e métodos que devem garantir tanto a segurança quanto a disponibilidade das informações, ou seja, usuários, senhas, permissões, serviços, entre outros recursos, devem ser cuidadosamente elaborados e configurados para que não haja dificuldades em garantir, de forma adequada, as políticas estabelecidas para a segurança da rede.

Ainda, implementar controles de acesso para garantir que apenas usuários autorizados tenham acesso à rede. Isso inclui o uso de senhas fortes, autenticação multifatorial e a limitação do acesso aos recursos apenas aos usuários necessários. Portanto, é necessário monitorar a rede regularmente em busca de atividades suspeitas e implementar ferramentas de detecção de intrusão para alertar os administradores da rede sobre possíveis ataques.

2.5 Engenharia social: boas práticas a segurança pelos usuários

As boas práticas de segurança pelos usuários para mitigar a engenharia social em redes de computadores são fundamentais para prevenir ataques que exploram a confiança e a persuasão para enganar usuários e obter acesso a sistemas e dados sensíveis. Para compreender a dimensão da engenharia social, além de expor algumas das boas práticas para mitigar as ações de um engenheiro social, autores como: Silva, Rosa, chaim, et al. (2012); Alencar, Lima, Firmo, et al. Batista (2015); Maulais (2016) apresentam conceituações a respeito desse tipo de engenharia com enfoque de segurança mais eficientes para desarticular, identificar, mitigar e conscientizar sobre a engenharia social nos ambientes corporativos.

O Trabalho de Silva, Rosa, chaim, et al. (2012), propõem a avaliação de nível de segurança da organização com a integração de três métodos criando a parametrização denominada PSU. Este trabalho relaciona um conjunto de boas práticas que podem auxiliar no combate de Engenharia Social.

O trabalho de Silva, (2012) tem como objetivo conceituar a engenharia social, onde aplica-se no cotidiano, de que maneira se usa a técnica e como é possível ser despercebida por pessoas e empresas, o estudo tem como propósito a conscientização contra os ataques. O trabalho proposto tem o objetivo apresentar as boas práticas para prevenir ataques e verificar a percepção das pessoas quanto ao tema Engenharia Social. Diferente do trabalho de Alencar, Lima, Firmo, et al. (2013) que visa verificar a eficiência obtida através do processo contínuo de conscientização e treinamento de funcionários de empresas privadas de áreas externas à TI, sobre segurança da informação e prevenção de incidentes de segurança de dados, este trabalho tem como propósito verificar se as pessoas possuem conhecimento sobre Engenharia Social. O trabalho de Batista (2015) busca responder a problemática: Por que, mesmo com a melhor tecnologia de SI, os profissionais ainda estão vulneráveis a ataques de Engenharia Social?, com base em conceitos abordados na literatura. Este estudo apresenta uma visão geral e descreve as boas práticas de Engenharia Social citadas na literatura e a percepção das pessoas sobre Engenharia Social.

O trabalho de Maulais (2016) tem foco na análise das técnicas ataques e defesa de engenharia social em empresas de pequeno, médio e grande porte, este estudo apresenta uma lista de boas práticas para auxiliar na prevenção de ataque de Engenharia Social. Ramos et al (2019) elaboraram uma modalidade de pesquisa científica denominada de RB. O objetivo desta RB foi descrever as boas práticas relacionadas à Engenharia Social que são utilizadas para prevenir ataques, de forma a auxiliar na segurança e prevenção de obtenção das informações.

Os resultados obtidos na RB de boas práticas de Ramos et al (2019) são extremamente relevantes no contexto deste trabalho também. Adiante no (Quadro) são apresentadas boas práticas mapeadas na literatura pelos autores, essas por sua vez tem caracterização mais generalizadas e a frequência com que apareceram nos trabalhos analisadas foi substancial.

Quadro 1 - Boas práticas de Engenharia Social

ID	BOAS PRÁTICAS	PUBLICAÇÕES	TOTAL DE CITAÇÕES
BP1	Conscientização	[P1], [P2], [P3], [P5], [P7], [P8],[10], [11], [P14], [P15], [P16], [P17], [P18], [P19], [P20], [P21], [P23], [P24], [P26], [P27], [P29],[P31], [P33]	23
BP2	Treinamento	[P3], [P5], [P7], [P9], [P10], [P11], [P15], [P16], [P17], [P21], [P22], [P25], [P27], [P29]	14
BP2	Políticas de Segurança	[P2], [P3], [P4], [P5], [P6], [P7], [P8], [P10], [P11], [P12], [P13], [P15], [P16], [P17], [P18], [P19],[P20], [P21], [P22] [P23], [P24], [P25], [P26], [P27], [P28], [P30], [P31], [P33]	28

Fonte: Ramos et al (2019) (Adaptado)

A identificação das boas práticas permitiu perceber que dentro das Políticas de Segurança existem políticas específicas que foram abordadas e que podem auxiliar no combate de Engenharia Social. O (Quadro 2) a seguir apresenta todas as boas práticas de políticas de segurança identificadas nas publicações e o quantitativo de vezes em que elas foram mencionadas

Quadro 2 - Boas práticas de políticas de segurança

ID	BOAS PRÁTICAS	PUBLICAÇÕES	TOTAL DE CITAÇÕES
PS1	Ferramentas Tecnológicas	[P3], [P4], [P6], [P7], [10], [11], [P15], [P17], [P23], [P24], [P26] e [P31]	12
PS2	Prevenção para o Acesso as Máquinas/ Informações	[P3], [P4], [P5], [P6], [P17], [P19], [P24], [P26], [P31] e [P33]	10
PS3	Prevenção para Ataque por e-mail (e similares)	[P3], [P4], [12], [P22], [P30], [P31], [P32] e [P33]	8
PS4	Prevenção para Segurança Física	[P4], [P5], [10], [P17], [P20], [P31], [P33]	7

PS5	Prevenção para o lixo	[P4], [10], [P24], [P26], [P31], [P32] e [P33]	7
PS6	Políticas de Senha	[P10], [P17], [P19], [P24], [P31] e [P33]	6
PS7	Prevenção para Controle/ Fiscalização de Comportamentos	[P10], [P17], [P18] e [P26]	4
PS8	Prevenção para Ataques por telefone (ou qualquer meio VoIP)	[P4], [10], [P32] e [P33],	4
PS9	Prevenção para Redes Sociais	[P2], [P4], [P28] e [P32]	4
;PS10	Prevenção para Navegação na Internet	[P30], [P31] e [P33]	3
PS11	Políticas de backup	[P17] e [P24]	2
PS12	Plano de Resposta a Incidentes	[P27] e[P33]	2
PS13	Medidas para Usuários não Técnico	[P6]	1
PS14	Políticas de privacidade	[P17]	1
PS15	Políticas de Confidencialidade	[P17]	1
PS16	Política de uso aceitável (UPA)	[P17]	1
PS17	Prevenção para Ataques meio de Contatos Interpessoais	[P17]	1
PS18	Prevenção para Identificar Possíveis Alvos	[P20]	1
PS19	Postura Questionadora	[P32]	1
PS20	Métodos de Segurança	[P27]	1

Fonte: Ramos et al (2019) (Adaptado)

Os resultados das boas práticas identificadas na RB apresentaram várias medidas que estão relacionados na prevenção de ataques de Engenharia Social. De forma resumida cada prática e política de segurança serão abordadas de acordo com o apresentado nas publicações contidas no Anexo A deste trabalho.

Foi possível observar por meio da leitura das 33 publicações que muitas medidas não necessitam de altos investimentos para serem utilizadas. Existe uma diversidade de meios preventivos que podem ser adotados de acordo com o ramo e necessidade das corporações e indivíduos para manter os dados seguros e íntegros, e assim evitar que possíveis ataques por engenheiros sociais possam ocorrer e prejudicá-los. Portanto, o treinamento e a conscientização dos usuários são uma parte importante da segurança cibernética. Isso pode incluir treinamentos regulares para ajudar os usuários a identificar e prevenir ataques de engenharia social, bem como fornecer informações sobre as últimas ameaças e práticas recomendadas de segurança.

3 METODOLOGIA

3.1 Definição da metodologia

A natureza da pesquisa ela é do tipo aplicada. Vários autores abordam sobre esse tipo de metodologia: (FLEURY; WERLANG, 2016); (PARANHOS; PARANHOS, 2014), esses últimos com enfoque principalmente na área tecnológica.

Consonante a abordagem do problema é do tipo qualitativa, uma vez que houve a interpretação dos resultados extraídos dos procedimentos técnicos em laboratório para atribuição de significados e valores para responder ao problema levantado, sendo um processo prático e dinâmico para adaptação de soluções nos ambientes de corporações, sendo esses ambientes diversos e complexos também.

O enfoque dos objetivos da pesquisa tem caráter explicativo, pois visa identificar os fatores que devem ser adotados para a segurança a partir dos eventos de ocorrência de invasões e ataques externos a redes corporativas.

3.3.1 Pesquisa de laboratório

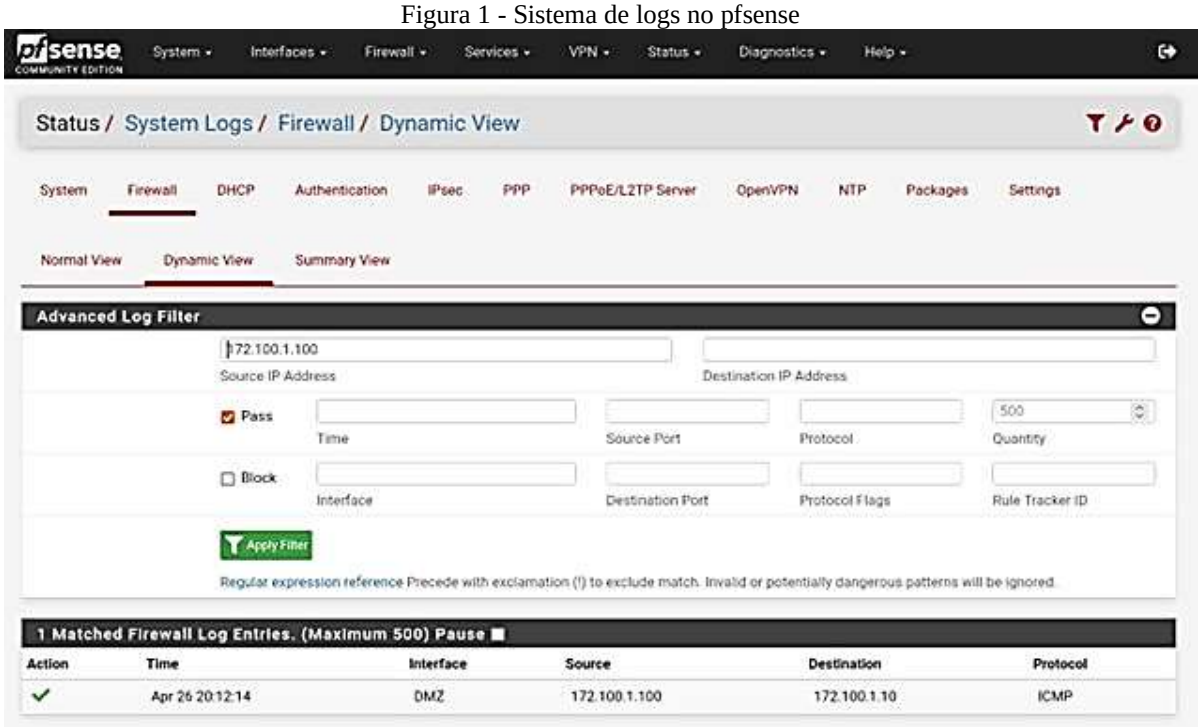
Os procedimentos técnicos práticos envolveu a pesquisa de laboratório de redes do IFAP. O laboratório fica localizado no campus de Macapá com endereço na Rodovia BR-210, S/N, km. 3, Brasil Novo, AP, CEP: 68909-398.

3.3.2 Cenário 1 – Prática de administração em redes de computadores com pfSense

O objetivo é dar uma compreensão clara de como visualizar e analisar a atividade da rede, identificando comportamentos suspeitos e possíveis vulnerabilidades. Para tanto, aborada-se conceitos como logs, sua importância na segurança da rede e visualização de logs com o firewall pfSense. Além disso, a captura de tráfego pfSense, que fornece informações mais detalhadas sobre conexões de rede e pacotes que serão exploradas.

O monitoramento de conexões de rede é fundamental para garantir a segurança e o bom funcionamento de seus sistemas. Ao visualizar e analisar a atividade da rede, pode-se identificar ameaças, comportamentos suspeitos e possíveis vulnerabilidades. Duas abordagens comuns para esse monitoramento são o uso de logs e a captura de tráfego. Exploraremos como essas técnicas podem ser aplicadas utilizando o firewall pfSense.

Figura 1 - Sistema de logs no pfsense



Fonte: Bandeira e Nobre (2023)

Os logs, também conhecidos como histórico ou registros, são registros detalhados de eventos que ocorrem em um sistema. No contexto de redes de computadores, os logs registram tudo o que está acontecendo no sistema, permitindo o monitoramento de atividades e comportamentos suspeitos. A OWASP (Open Web Application Security Project), uma fundação de segurança sem fins lucrativos, destaca a importância dos logs na detecção de vulnerabilidades e falhas de monitoramento.

No pfSense, um firewall bastante utilizado, podemos acessar os logs e informações do sistema da seguinte forma:

1. Acesse a página "Status" no topo da interface do pfSense e selecione "System Logs" no menu. Isso nos levará a uma página com dois menus superiores, "System" e "General".

2. Como queremos visualizar informações da rede e não apenas do sistema, clique em "Firewall" na parte superior da página. Aqui, encontraremos uma lista de informações.

3. Na visualização padrão, chamada de "Normal View", é exibida uma tabela com o horário do registro, interface, regra aplicada, origem, destino e protocolo.

4. Também é possível utilizar a visualização dinâmica, chamada de "Dynamic View", que fornece quase as mesmas informações, porém de forma dinâmica.

5. Na coluna "Action" (Ação), o "X" indica um bloqueio, e ao passar o mouse sobre ele, veremos a indicação "Block". O campo "Time" representa o horário em que o registro ocorreu, e "Interface" indica a interface de rede relacionada.

6. Nas colunas "Source" (Origem) e "Destination" (Destino), são exibidos os endereços IP seguidos por dois pontos e a porta, por exemplo, "172.100.2.100:55245". O protocolo também é indicado.

7. Para filtrar os logs e verificar uma determinada ação, como um ping autorizado, podemos utilizar o ícone de filtro vermelho no canto superior direito da página.

8. Ao expandir a opção "Advanced Log Filter" (Filtro de Registro Avançado), insira o IP da origem no campo "Source IP Address" (Endereço IP de Origem).

9. Clique no botão verde "Apply Filter" (Aplicar Filtro) na parte inferior esquerda.

10. Serão listados os logs correspondentes ao filtro. Por exemplo, um ping bloqueado será exibido com ação "Block", enquanto um ping autorizado terá ação "Pass".

11. Os logs fornecem informações básicas, mas caso desejemos visualizar mais detalhes, como os endereços MAC na segunda camada do modelo OSI, podemos capturar o tráfego através do pfSense:

12. Acesse a página "Diagnostics" (Diagnósticos) e selecione "Packet Capture" (Captura de Pacotes).

13. Configure os detalhes da captura, como selecionar a interface e o protocolo (por exemplo, ICMP para ping). Certifique-se de habilitar o modo promíscuo.

14. Deixe o campo "Address Family" como "Any" (Qualquer) e "Host Address" em branco. A porta também pode ser deixada como qualquer uma.

15. Se desejar, ajuste o nível de detalhe para "Full" (Completo) para obter informações mais abrangentes.

16. Clique no botão verde "Start" (Iniciar) para iniciar a captura.

17. Execute o comando de ping no servidor e, em seguida, clique no botão amarelo "Stop" (Parar) na página.

Assim, a visualização e análise da atividade da rede, juntamente com o uso de logs e a captura de tráfego, são componentes essenciais para garantir a segurança e a detecção de ataques externos e internos em uma rede de computadores. Ao utilizar o firewall pfSense, é possível acessar os logs do sistema e do firewall para monitorar eventos e comportamentos suspeitos.

Os logs fornecem um registro detalhado das atividades da rede, permitindo a identificação de possíveis vulnerabilidades e a detecção de ameaças. Através da visualização dos logs no pfSense, é possível analisar informações como horário dos registros, interfaces de rede envolvidas, regras aplicadas, endereços IP de origem e destino, protocolos utilizados e

ações executadas. Além disso, é possível filtrar os logs para verificar a ocorrência de ações específicas, como autorizações ou bloqueios de determinados tipos de tráfego.

No entanto, para obter informações mais detalhadas sobre as conexões de rede, como endereços MAC na camada 2 do modelo OSI, é recomendado realizar a captura de tráfego por meio do pfSense. A captura de pacotes permite analisar em maior profundidade o tráfego de rede, identificando padrões e comportamentos anômalos. Através da página de captura de pacotes do pfSense, é possível configurar os detalhes da captura, selecionar a interface e o protocolo desejado, iniciar a captura e analisar os resultados obtidos.

Adiante, descreve-se um ambiente preparado na máquina virtual:

À esquerda do Virtualbox, na seção "Ferramentas", encontram-se três Máquinas Virtuais (VMs) necessárias: WAF, Server e Firewall. No entanto, antes de iniciar essas máquinas, é necessário que alguns campos sejam configurados.

Na seção "Ferramentas", pode ser encontrado, à esquerda do Virtualbox, um conjunto de três Máquinas Virtuais (VMs) necessárias: WAF, Server e Firewall. Antes do início dessas máquinas, é necessário realizar a configuração de alguns campos.

Ao clicar em "Arquivo", localizado no canto superior esquerdo, um menu será exibido, no qual uma das opções disponíveis é o "Gerenciador de Rede do Hospedeiro", acessível por meio do atalho "Ctrl + H".

Uma vez selecionada essa opção de configuração, uma aba intitulada "Gerenciador de Redes do Hospedeiro" será aberta. Na coluna "Servidor DHCP", o adaptador "VirtualBox Host-Only Ethernet Adapter" será desabilitado, embora possa ser exibido como "Vboxnet0".

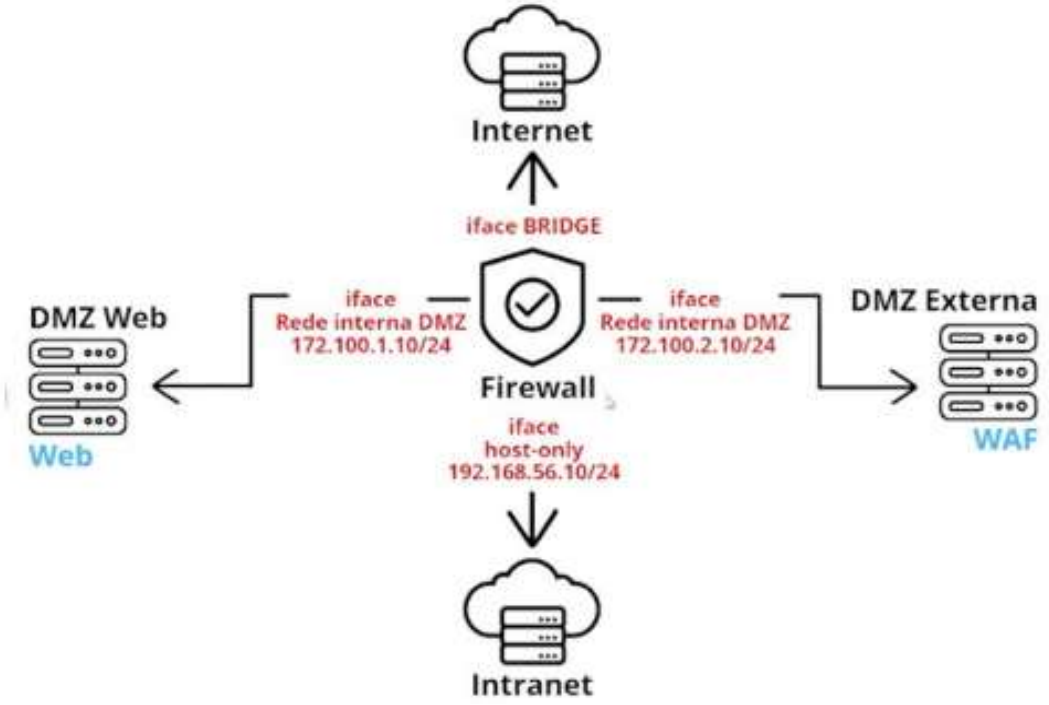
Após a desabilitação dessa opção, o botão "Aplicar", localizado no canto inferior direito, será clicado. A configuração do Servidor Web será realizada na Virtualbox, por meio de uma iface (interface de rede) configurada como uma rede interna DMZ, com o endereço IP 172.100.1.10/24.

No Diagrama 1, observa-se que a Intranet será configurada na interface de rede "host-only", com o IP 192.168.56.10/24. A designação de "host-only" indica que essa interface está configurada para acessar apenas a nossa rede.

Adicionalmente, a máquina WAF estará localizada na DMZ interna, com o IP 172.100.2.10/24. Dentro do contexto do Virtualbox, essa máquina é denominada "interna", em virtude de se tratar de uma rede privada, ou seja, a DMZ. O Firewall será configurado em uma interface de rede Bridge, constituindo-se como uma ponte com a conexão à Internet, estabelecendo uma ligação com o roteador ao qual estamos conectados.

Resumindo, esse o Diagrama 1 representa a configuração do sistema configurado:

Diagrama 1 – Sistema configurado com pfSense



Fonte: Dias (2023)

Na sequência, o teste de Ping é realizado na interface DMZ do Servidor Web, localizado à esquerda. A rede 172.100.1.10 está conectada ao Firewall.

O Firewall desempenha um papel fundamental como um Gateway, que atua como um portão entre duas redes, facilitando a troca de dados entre elas. É análogo ao funcionamento de um roteador em uma casa ou empresa, permitindo a conexão dos dispositivos à Internet. Sem essa funcionalidade, a comunicação seria impossível. No contexto do projeto em questão, o objetivo é estabelecer a conexão entre a rede DMZ Interna ou Web do Servidor e a Intranet, utilizando o Firewall como o Gateway responsável por mediar essa comunicação entre as duas redes.

No Virtualbox, damos dois cliques em "Server" para iniciar a máquina. Em seguida, fazemos o login como usuário root e utilizamos a mesma senha do Firewall ("qwerty"). Para testar a comunicação entre o Server e o Firewall, utilizamos a ferramenta "ping" para enviar pacotes para o Gateway.

Retornamos ao terminal do Server e executamos o comando "ping 172.100.1.10" para enviar pacotes para o endereço IP fornecido. No entanto, até o momento, os pacotes não foram enviados com sucesso. Por isso, interrompemos o comando pressionando as teclas "Ctrl + C".

Isso indica que o Server não está conseguindo se conectar ao Gateway. Para solucionar esse problema, é necessário configurar o Firewall criando uma regra que permita o comando "ping".

Retornamos ao Pfsense e acessamos as "RULES" do Firewall. Na página de "RULES", selecionamos a interface DMZ para autorizar o "ping". Adicionamos a regra necessária acima da regra de bloqueio geral, pois o Firewall analisa as regras de cima para baixo.

Configuramos a ação da regra como "PASS" e selecionamos a interface DMZ como origem e destino. No campo "PROTOCOL", alteramos para ICMP, pois o "ping" é uma ferramenta do protocolo ICMP. Definimos a estrutura de mensagem do "ping" como permitida, selecionando as opções "ECHO REPLY" e "ECHO REQUEST".

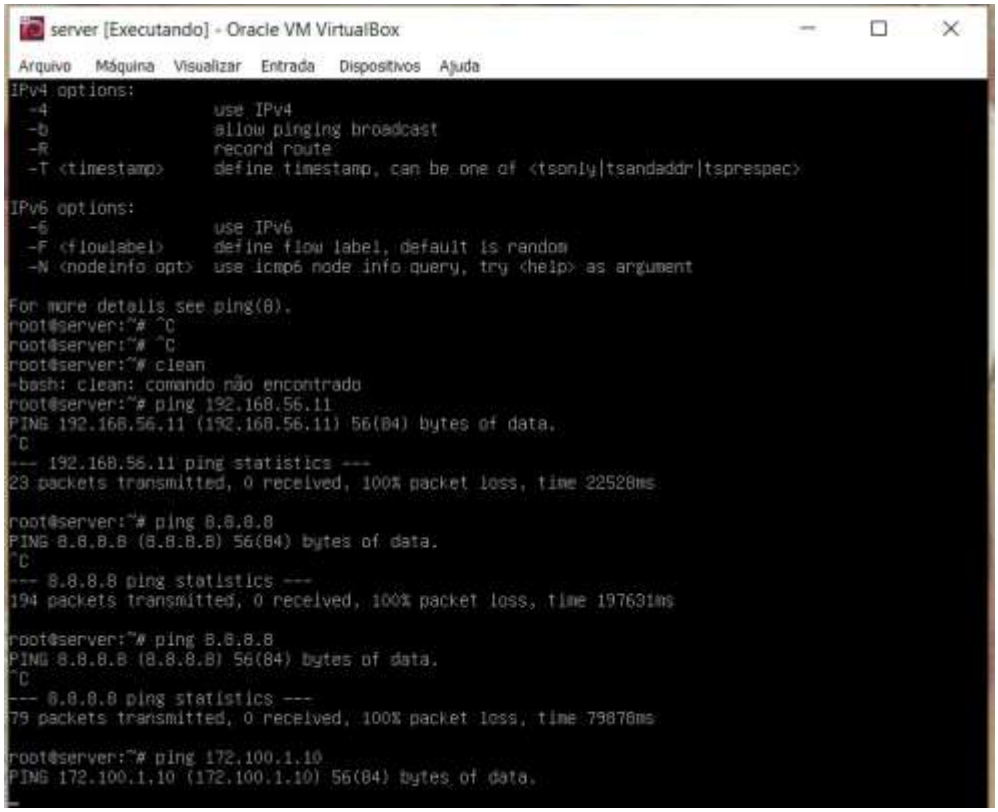
Configuramos a origem como "DMZ NET" e o destino também como "DMZ NET". Optamos por registrar todas as atividades ativando a opção "LOG" em "EXTRA OPTIONS". Adicionamos a descrição "Ping na DMZ". Salvamos a regra.

Figura 2 – Regra para permitir o ping

Fonte: Dias (2023)

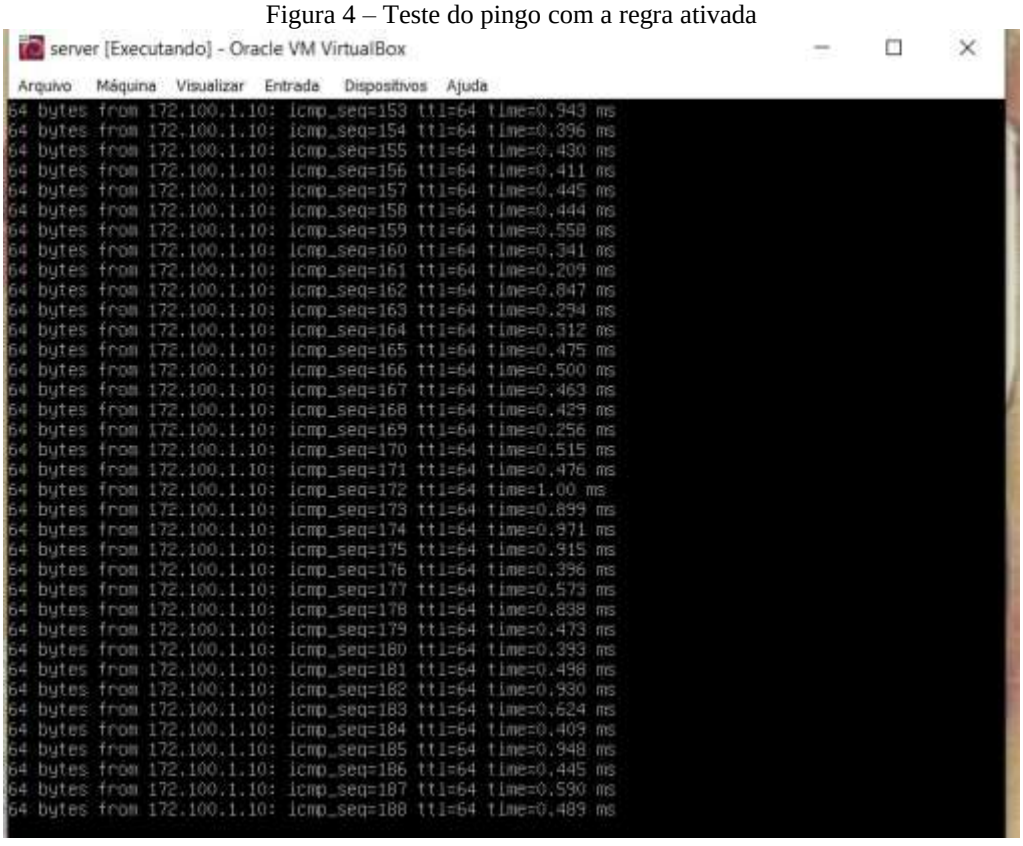
Aplicamos as alterações no Firewall para que entrem em vigor. Retornamos ao Servidor Web para verificar se conseguimos enviar o "ping". No terminal do Servidor Web, digitamos "ping 172.100.1.10".

Figura 3 – Teste do ping com a regra desativada



Fonte: Bandeira e Nobre (2023)

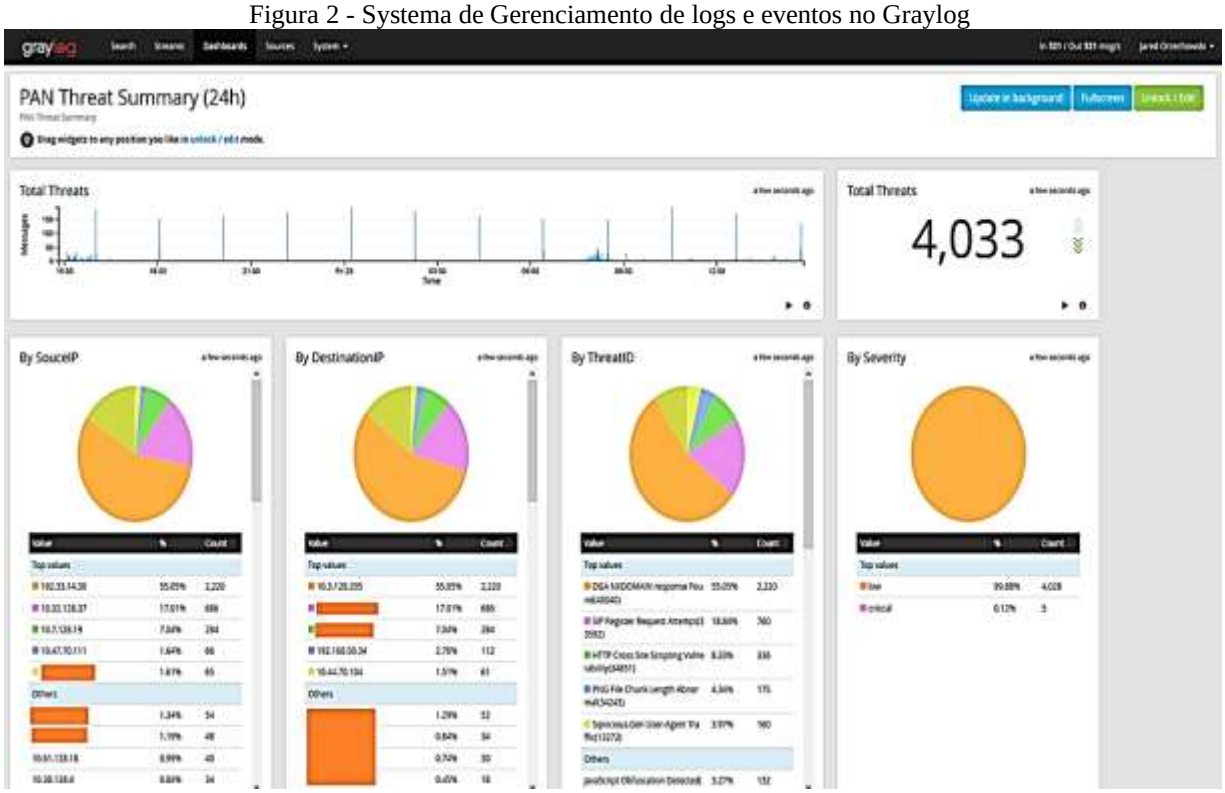
Figura 4 – Teste do pingo com a regra ativada



Fonte: Bandeira e Nobre (2023)

Nesta última parte, abordaremos as etapas de configuração e implantação do Graylog em nosso ambiente de rede, bem como os desafios encontrados e as soluções adotadas para tornar o sistema acessível e funcional.

Figura 2 - Systema de Gerenciamento de logs e eventos no Graylog



Fonte: Bandeira e Nobre (2023)

O objetivo deste trabalho é aprimorar a visualização de logs e informações de segurança em nosso sistema de rede, por meio da implementação de um SIEM utilizando o Graylog. O Graylog foi escolhido por sua interface web intuitiva e pela disponibilidade de ferramentas gratuitas e pagas que atendem às nossas necessidades.

A primeira etapa consistiu na importação da máquina virtual do Graylog para o VirtualBox, que servirá como base para o nosso sistema de gerenciamento de logs. Nesta etapa, verificamos as configurações de rede da VM do Graylog no VirtualBox. O adaptador 1 foi configurado para a nossa rede interna DMZ, pois o Graylog estará na mesma rede do nosso firewall, recebendo as informações de segurança.

A VM do Graylog foi iniciada no VirtualBox para que pudéssemos acessar o sistema, utilizando as credenciais de login (root, senha: qwerty), acessamos o sistema do Graylog por meio de sua interface web. Acessamos o pfsense, nosso firewall, para entender como ocorre a tradução de IP necessária para que nossa intranet reconheça o IP do Graylog.

Selecionamos a opção de redirecionamento de porta (port forward) e adicionamos uma regra para traduzir o IP do Graylog para um IP reconhecido pela intranet. Essa tradução é realizada pelo gateway, que é nosso firewall. Continuando no pfsense, acessamos a opção de IP virtual para criar um IP virtual vinculado ao Graylog.

Criamos um IP virtual usando o tipo "IP Alias" e definimos o endereço como 192.168.56.11 com máscara de rede 24. Essa configuração permite que o IP seja reconhecido pela intranet. Ainda no pfsense, acessamos as regras de firewall para permitir o acesso ao Graylog.

Criamos as regras de firewall necessárias para permitir o tráfego de entrada e saída para o Graylog. Definimos as portas específicas que o Graylog utiliza para receber logs e eventos de segurança, garantindo que o tráfego seja direcionado corretamente. Identificamos as fontes de logs em nosso ambiente, como servidores, dispositivos de rede e aplicativos, que enviarão suas informações de log para o Graylog.

No sistema do Graylog, configuramos as fontes de logs, definindo os protocolos de envio, como syslog ou GELF (Graylog Extended Log Format), e as informações de conexão necessárias para que os dispositivos enviem os logs.

Estabelecemos regras de alerta no Graylog com base em padrões de log específicos, como eventos de segurança críticos ou comportamentos anormais. Essas regras são configuradas para acionar notificações quando determinadas condições forem atendidas. Definimos os métodos de notificação, como e-mail ou mensagens instantâneas, que serão utilizados para alertar a equipe de segurança sobre eventos importantes ou suspeitos.

Utilizamos a interface do Graylog para monitorar os logs em tempo real, visualizando as informações conforme são recebidas e processadas pelo sistema. Também exploramos as funcionalidades de busca e filtro do Graylog para analisar logs históricos, permitindo identificar padrões, investigar incidentes de segurança passados e tomar medidas corretivas.

A implementação do Graylog como um sistema de gerenciamento de logs e eventos em conjunto com o firewall pfSense oferece benefícios significativos para a segurança e detecção de ataques externos e internos em uma rede de computadores corporativa. Ao alcançar os objetivos específicos desta pesquisa, foram estabelecidas medidas preventivas e detectivas para fortalecer a segurança em redes corporativas.

As configurações personalizadas no pfSense buscou levar as medidas de segurança necessárias para enfrentar os ataques contemporâneos em redes de computadores. Essas configurações personalizadas incluem regras de firewall, redirecionamento de porta e criação de IP virtual para garantir que o Graylog seja acessível e funcional.

A montagem de um cenário em laboratório permitiu simular ataques externos em redes corporativas, proporcionando um ambiente controlado para testar a eficácia das medidas de segurança implementadas. Essa abordagem possibilitou identificar vulnerabilidades e ajustar as configurações do pfSense e do Graylog para melhorar a proteção da rede.

A pesquisa também identificou outros serviços que podem ser integrados ao ambiente de rede corporativa para fortalecer a segurança. O uso do Graylog como SIEM (Security Information and Event Management) permite consolidar e analisar os logs de várias fontes, identificando eventos de segurança críticos ou comportamentos anormais. Essa integração amplia a capacidade de detecção e resposta a ameaças.

Ao implementar medidas detectivas e preventivas com o pfSense e o Graylog, é possível fortalecer a segurança em redes corporativas. A análise detalhada dos logs, a configuração de regras de alerta e a monitoração em tempo real fornecem uma visão abrangente da atividade da rede, facilitando a detecção de ameaças e a resposta rápida a incidentes de segurança. Combinadas, essas ferramentas e abordagens ajudam a proteger os ativos corporativos e a garantir a integridade, confidencialidade e disponibilidade dos sistemas e dados.

O pfSense registra os eventos de rede em tempo real, permitindo a detecção imediata de atividades suspeitas ou maliciosas. Esses eventos são encaminhados ao Graylog para análise e visualização em tempo real, fornecendo uma visão atualizada da atividade da rede. O Graylog possui recursos avançados de análise e correlação de logs, permitindo identificar padrões e comportamentos anômalos.

Assim, a implementação do Graylog como um sistema de gerenciamento de logs e eventos em conjunto com o firewall pfSense oferece benefícios significativos para a segurança e detecção de ataques em uma rede corporativa. Através da configuração personalizada do pfSense, foram estabelecidas medidas preventivas e detectivas para fortalecer a segurança da rede. O uso do Graylog como SIEM permite consolidar e analisar os logs de várias fontes, identificando eventos de segurança críticos ou comportamentos anormais. A capacidade de monitorar em tempo real, analisar logs históricos e configurar alertas ajuda a identificar ameaças e responder rapidamente a incidentes de segurança. Combinadas, essas ferramentas e abordagens contribuem para proteger os ativos corporativos, garantindo a integridade, confidencialidade e disponibilidade dos sistemas e dados. A implementação do pfSense e do Graylog fornece uma visão abrangente da atividade da rede, facilitando a detecção de atividades suspeitas ou maliciosas, permitindo uma resposta proativa e mitigação de ameaças.

4 RESULTADOS

A experiência de visualização e análise da atividade da rede, utilizando logs e captura de tráfego com o firewall pfSense, proporciona resultados relevantes para a detecção e prevenção de ataques cibernéticos em redes de computadores corporativas.

Começando pela identificação de comportamentos suspeitos, pois ao analisar os logs do pfSense, é possível identificar atividades anormais ou suspeitas na rede. Isso inclui tentativas de acesso não autorizado, tráfego malicioso, varreduras de portas, entre outros comportamentos que podem indicar a presença de um ataque em andamento. A detecção de possíveis vulnerabilidades, uma vez que através da análise dos logs, é possível identificar eventos que indiquem a existência de vulnerabilidades na rede. Por exemplo, se um determinado serviço estiver gerando muitos registros de falha de autenticação, pode ser um sinal de que essa área específica precisa de medidas de segurança adicionais.

A análise de tráfego em detalhes, pois a captura de tráfego com o pfSense permite obter informações mais detalhadas sobre as conexões de rede. Isso inclui endereços MAC na camada 2 do modelo OSI, que podem ser úteis para identificar dispositivos específicos envolvidos em uma comunicação. Esses detalhes são especialmente relevantes para investigações mais aprofundadas em casos de incidentes de segurança. A filtragem e busca eficiente de eventos, uma vez que o uso de filtros nos logs do pfSense permite a busca eficiente de eventos específicos. Por exemplo, é possível filtrar os registros para exibir apenas as ações bloqueadas ou permitidas de um determinado endereço IP de origem. Essa capacidade de filtragem facilita a análise de eventos relevantes e ajuda a identificar padrões ou tendências preocupantes.

A melhoria das medidas de segurança, pois com base nos resultados obtidos, é possível tomar ações corretivas e implementar medidas de segurança adicionais para fortalecer a proteção da rede. Por exemplo, se forem identificadas várias tentativas de acesso não autorizado de um endereço IP específico, é possível bloquear esse endereço ou tomar outras medidas para mitigar a ameaça.

Assim, a visualização e análise da atividade da rede utilizando logs e captura de tráfego com o pfSense oferecem insights valiosos para a detecção e prevenção de ataques cibernéticos em redes corporativas. Ao utilizar essas técnicas, os administradores de rede podem identificar comportamentos suspeitos, detectar possíveis vulnerabilidades, analisar o tráfego em detalhes e tomar medidas proativas para melhorar a segurança da rede.

Os principais resultados dessa experiência de redes com o ping estão relacionados à configuração e segurança do sistema, utilizando o pfSense como Firewall. Ao realizar o teste

de ping na interface DMZ do Servidor Web, foram identificadas dificuldades na comunicação com o Gateway, indicando a necessidade de configurar o Firewall para permitir o comando "ping". Por meio do pfSense, foram realizadas as seguintes ações: desabilitação do adaptador "VirtualBox Host-Only Ethernet Adapter", configuração da rede interna DMZ para o Servidor Web com o IP 172.100.1.10/24, definição da Intranet na interface "host-only" com o IP 192.168.56.10/24, e localização da máquina WAF na DMZ interna com o IP 172.100.2.10/24. Além disso, o Firewall foi configurado na interface de rede Bridge, estabelecendo a conexão com a Internet.

Através do teste de ping, verificou-se que o Server não estava conseguindo se conectar ao Gateway. Para solucionar esse problema, foi necessário adicionar uma regra no Firewall para permitir o ping. Essa regra foi configurada para a interface DMZ, utilizando o protocolo ICMP e permitindo apenas as estruturas de mensagem "ECHO REPLY" e "ECHO REQUEST". Adicionalmente, ativou-se o registro de atividades para monitoramento.

Com a aplicação das alterações no Firewall, foi possível realizar o ping com sucesso no Servidor Web, estabelecendo a comunicação entre as redes e demonstrando a eficácia da configuração e das regras de segurança implementadas com o pfSense.

Os principais resultados da experiência de configuração e implantação do Graylog em um ambiente de rede incluem a implementação de um SIEM eficaz, com o objetivo principal foi aprimorar a visualização de logs e informações de segurança por meio da implementação de um SIEM utilizando o Graylog. O Graylog foi escolhido por sua interface web intuitiva e disponibilidade de ferramentas adequadas às necessidades da rede. A configuração do ambiente do Graylog, sendo que a primeira etapa envolveu a importação da máquina virtual do Graylog para o VirtualBox e a configuração das redes. O adaptador foi configurado para a rede interna DMZ, permitindo que o Graylog recebesse informações de segurança do firewall.

A tradução de IP e acesso à intranet, pois foram realizadas configurações no firewall (pfsense) para permitir a tradução de IP e acesso à intranet. Isso envolveu a criação de um IP virtual vinculado ao Graylog e a definição das regras de firewall apropriadas para permitir o tráfego de entrada e saída. A configuração das fontes de logs, um vez que no sistema do Graylog, foram configuradas as fontes de logs, definindo os protocolos de envio (syslog ou GELF) e as informações de conexão necessárias para que os dispositivos enviassem os logs.

Assim, a implementação do Graylog como um sistema de gerenciamento de logs e eventos em conjunto com o firewall pfSense proporcionou benefícios significativos para a segurança e detecção de ataques externos e internos em uma rede corporativa.

5 CONSIDERAÇÕES FINAIS

Podemos destacar que as configurações personalizadas no pfSense buscaram levar as medidas de segurança necessárias para enfrentar os ataques contemporâneos em redes de computadores. Essas configurações personalizadas incluíram regras de firewall, redirecionamento de porta e criação de IP virtual para garantir que o Graylog fosse acessível e funcional. A montagem de um cenário em laboratório permitiu simular ataques externos em redes corporativas, proporcionando um ambiente controlado para testar a eficácia das medidas de segurança implementadas. Essa abordagem possibilitou identificar vulnerabilidades e ajustar as configurações do pfSense e do Graylog para melhorar a proteção da rede.

A pesquisa também identificou outros serviços que podem ser integrados ao ambiente de rede corporativa para fortalecer a segurança. O uso do Graylog como SIEM (Security Information and Event Management) permite consolidar e analisar os logs de várias fontes, identificando eventos de segurança críticos ou comportamentos anormais. Essa integração amplia a capacidade de detecção e resposta a ameaças.

Ao implementar medidas detectivas e preventivas com o pfSense e o Graylog, é possível fortalecer a segurança em redes corporativas. A análise detalhada dos logs, a configuração de regras de alerta e a monitoração em tempo real fornecem uma visão abrangente da atividade da rede, facilitando a detecção de ameaças e a resposta rápida a incidentes de segurança. Combinadas, essas ferramentas e abordagens ajudam a proteger os ativos corporativos e a garantir a integridade, confidencialidade e disponibilidade dos sistemas e dados.

O pfSense registra os eventos de rede em tempo real, permitindo a detecção imediata de atividades suspeitas ou maliciosas. Esses eventos são encaminhados ao Graylog para análise e visualização em tempo real, fornecendo uma visão atualizada da atividade da rede. O Graylog possui recursos avançados de análise e correlação de logs, permitindo identificar padrões e comportamentos anômalos. Através de suas funcionalidades de busca e filtro, é possível investigar incidentes de segurança passados, analisar logs históricos e tomar medidas corretivas adequadas.

Através do teste de ping, verificou-se que o Server não estava conseguindo se conectar ao Gateway. Para solucionar esse problema, foi necessário adicionar uma regra no Firewall para permitir o ping. Essa regra foi configurada para a interface DMZ, utilizando o protocolo ICMP e permitindo apenas as estruturas de mensagem "ECHO REPLY" e "ECHO REQUEST". Adicionalmente, ativou-se o registro de atividades para monitoramento. Com a aplicação das alterações no Firewall, foi possível realizar o ping com sucesso no Servidor Web, estabelecendo

a comunicação entre as redes e demonstrando a eficácia da configuração e das regras de segurança implementadas com o pfSense.

O Graylog permite definir regras de alerta com base em padrões de log específicos. Isso possibilita a configuração de alertas para eventos de segurança críticos ou comportamentos anormais. As notificações podem ser enviadas por e-mail ou outros meios, permitindo uma resposta rápida a incidentes de segurança.

A experiência de visualização e análise da atividade da rede, utilizando logs e captura de tráfego com o firewall pfSense, proporcionou resultados relevantes para a detecção e prevenção de ataques cibernéticos em redes de computadores corporativas. Durante a pesquisa, foram identificados comportamentos suspeitos, possíveis vulnerabilidades e foram estabelecidas medidas preventivas e detectivas para fortalecer a segurança em redes corporativas.

Foi possível observar por meio da leitura das 33 publicações que muitas medidas não necessitam de altos investimentos para serem utilizadas no combate a engenharia social. Existe uma diversidade de meios preventivos que podem ser adotados de acordo com o ramo e necessidade das corporações e indivíduos para manter os dados seguros e íntegros, e assim evitar que possíveis ataques por engenheiros sociais possam ocorrer e prejudicá-los.

O Dashboard do pfSense oferece um controle completo e monitoramento detalhado da solução de firewall. Com sua flexibilidade e personalização, fornece aos administradores as informações necessárias para manter a segurança da rede, identificar problemas e tomar ações preventivas ou corretivas adequadas.

o pfSense é uma solução de Firewall amplamente adotada e altamente robusta, sendo uma das melhores opções de código aberto disponíveis. Sendo licenciado sob a BSD, não é necessário pagar por licenças de uso, o que o torna uma opção acessível e econômica para empresas e organizações. Além de ser um software gratuito, o pfSense oferece uma variedade de pacotes adicionais que ampliam suas funcionalidades, permitindo que ele seja considerado um UTM (Unified Threat Management - Central Unificada de Gerenciamento de Ameaças). Com o pfSense, é possível realizar diversas atividades esperadas de sistemas com essa funcionalidade, fornecendo uma camada de segurança eficaz e abrangente para as redes. Através do pfSense, é possível configurar regras de Firewall, realizar monitoramento de tráfego, criar VPNs, controlar acesso à Internet, entre outras funcionalidades, tornando-o uma solução completa e confiável para garantir a segurança das redes. Sua popularidade e a confiabilidade demonstrada na experiência com o ping reforçam sua posição como uma escolha sólida para a proteção e gestão de ameaças em redes de todos os tamanhos.

REFERÊNCIAS

4LINUX. **O que é pfSense?** 2023. Disponível em: https://4linux.com.br/o-que-e-pfsense/. Acesso em: 8 jul. 2023.

ALENCAR, G.; LIMA, M.; FIRMO, A. O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phisching. **IX Simpósio Brasileiro de Sistemas de Informação (SBSI),** João Pessoa, p. 254-259, 2013.

ALVES, P. **Teste de Ping:** o que é e como fazer para testar velocidade da Internet. 2021. Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/2021/06/teste-de-ping-o-que-e-e-como-fazer-para-testar-velocidade-da-internet.ghtml. Acesso em: 9 jul. 2023.

ARAÚJO, F. C.; ROSSI, J. M. **A evolução dos ataques cibernéticos.** 2020. Disponível em: http://ric-cps.eastus2.cloudapp.azure.com/bitstream/123456789/5272/1/1S2020_Franciele%20Cassimiro%20de%20Ara%c3%bajo_OD0878.pdf. Acesso em: 19 fev. 2023.

BATISTA, F. **Métodos e Práticas Utilizadas em Engenharia Social com o Intuito de Obstar o Roubo de Informações Sensíveis**, 2015. 28 f. Monografia (Curso de Pós-Graduação Lato Sensu na área de Redes de Computadores com Ênfase em Segurança) - o Centro Universitário de Brasília (UniCEUB/ICPD), 2015.

FLEURY, M. T. L.; WERLANG, S. R.. Pesquisa aplicada: conceitos e abordagens. **Anuário de Pesquisa GVPesquisa,** 2016.

FREIRE, A. **Sistemas de Firewall e Defesa de Perímetros.** Portal Módulo Security, 2004.

HOMEPAGES. **Internet "Worm",** 2023. Disponível em: https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/worm/index.html. Acesso em: 13 maio 2023.

JUNIOR, M. G.; LIMA, S. M. Segurança e confiabilidade em sistemas de informação: dois lados da mesma moeda. In **Revista Eletrônica da faculdade adventista de administração do Nordeste – FAAD,** 2010.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais.** Thelma Guimarães (trad.). Ed 7. São Paulo: Pearson Prentice Hall, 2007.

MACIEL, R. **Você sabia que Sexta-Feira 13 também foi um vírus que infectou PCs mundo afora?** 2021. Disponível em: https://canaltech.com.br/seguranca/voce-sabia-que-sexta-feira-13-tambem-foi-um-virus-que-infectou-pcs-mundo-afora-149667/. Acesso em: 13 maio 2023.

MAULAIS, C. **Engenharia Social:** Técnicas de Ataque e Defesa em Empresas De Micro, Médio e Grande Porte. 2016. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) - Universidade FUMEC, 2016.

MEYER, M. **Os primeiros vírus de computador da história.** 2016. Disponível em: https://www.oficinadanet.com.br/post/13962-os-primeiros-virus-de-computador-da-historia. Acesso em: 13 maio 2023.

PARANHOS, L. R. L; PARANHOS, P. J. R. **Metodologia da pesquisa aplicada à tecnologia.** São Paulo: SENAI-SP Editora, 2014.

PEREIRA, C. G. **Phishing:** Conceitos e ações preventivas aplicadas à empresa. 2012. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/8136/1/50910909.pdf. Acesso em: 19 fev. 2023.

RAMOS, R. F. et al**. Um estudo sobre as boas práticas de engenharia social e a percepção das pessoas sobre o seu conceito.** 2019. Disponível em: https://riu.ufam.edu.br/handle/prefix/5719. Acesso em: 11 abri. 2022.

SAMPAIO, A. B. **Implantação de políticas de segurança em redes de computadores com PIX Firewall.** 2011. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/17250. Acesso em: 10 abr. 2023.

SECURITY REPORT. **A evolução dos ataques cibernéticos: Até onde os hackers podem ir?** 2023. Disponível em: https://www.securityreport.com.br/overview/a-evolucao-dos-ataques-ciberneticos-ate-onde-os-hackers-podem-ir/#.ZF9ROxHMK00. Acesso em: 13 maio 2023.

SILVA, C.; ROSA, A; CHAIM, D.; CARVALHO, R.; CHIMENDES, V. Engenharia Social: O Elo mais Frágil da Segurança nas Empresas. **Revista Eletrônica Do Alto Vale Do Itajaí.** Fatec Guaratinguetá. n. 02, 2012.

SILVA, D. **Análise de Métodos de Defesa Contra Engenharia Social em Ambientes Corporativos.** FBUNI, 2012. Disponível em: http://fbuni.edu.br/sites/default/files/tcc_-_2012_2_-_davi_miranda_siqueira_silva.pdf. Acesso em: 11 abr. 2023.

SIMMONDS, A; SANDILANDS, P; VAN EKERT, L. An Ontology for Network Security Attack. **Lecture Notes in Computer Science.** p. 3285: 317–323, 2004.

WILLIAMSON, M.; PERSAUD, C. **Livro do PfSense 2.0.** 2012. Disponível em: https://docplayer.com.br/21628716-Livro-do-pfsense-2-0-um-guia-pratico-com-exemplos-ilustrados-de-configuracoes-para-usuarios-iniciantes-e-avancados-sobre-o-pfsense-2.html. Acesso em: 9 jul. 2023.

ANEXO A - RESULTADOS DAS BOAS PRÁTICAS IDENTIFICADAS NA RB

[BP1] Conscientização

Na [P1] como formação da conscientização das pessoas se fala da criação de rotinas de palestras sobre o tema com regularidade, para que membros da empresa possam identificar um ataque desta natureza.

A [P2] aborda a conscientização como forma de instruir a população quanto aos comportamentos que podem oferecer riscos no ambiente digital, no caso de redes sociais online.

Na [P3] é mencionada a consciência que os colaboradores precisam ter com as informações, sejam elas pessoais ou corporativas.

Menciona-se na [P5] a importância de as pessoas conhecerem o valor da informação que elas manipulam.

Na [P7] a conscientização é tratada como forma de fornecer conhecimentos, tomadas de ações diante de situações de risco, para minimizar fraquezas humanas a serem exploradas pelos engenheiros sociais.

Na [P8] se fala que é fundamental as organizações conscientizem todos seus colaboradores a respeito das consequências que a divulgação indevida de dados pode acarretar.

Para criar e disseminar a consciência a [P10] diz que as organizações devem educar e treinar os funcionários, para serem capazes de identificar as situações de riscos, sendo que, para propagar essa consciência as empresas devem criar e divulgar suas políticas, normas e procedimentos de segurança da informação, através de programas de conscientização e treinamento contínuo para que as pessoas sempre conheçam quais são as novas técnicas utilizadas e como lidar com cada uma delas. Também se fala da divulgação ampla por toda empresa através de circulares internas, boletins periódicos on-line ou pela própria Intranet, os casos frustrados de quebra de segurança onde um funcionário atuou de maneira correta evitando que algo pior ocorresse.

A [P11] menciona que as pessoas precisam ser conscientizadas que elas podem estar sendo observadas e que poderão se tornar um alvo em potencial de um Engenheiro Social. Algumas orientações que podem estar contidas nessa Política de Educação continuada são: Nunca revele por telefone ou e-mail dados sensíveis como senhas, informações pessoais, dados de cartão de crédito, entre outras. Nunca clique em links de site que cheguem através de e-mails ou por redes sociais e que não haja certeza da origem. Desconfie de qualquer mensagem de e-mail que ofereça facilidades e promoções fora do comum. Não fale mais do que o necessário com estranhos e tenha em conta que a Engenharia Social é uma técnica utilizada há centenas de anos. Muito antes da criação da internet, já se utilizava técnicas com objetivos maldosos.

A abordagem de conscientização na [P14] sugere que as Instituições Bancárias poderiam dispor em seus sites as informações assuntos sobre as políticas de segurança da informação, de forma mais interativa, não dependendo da ação única e exclusiva dos usuários, através de alertas de segurança antes de realizarem uma transação financeira, além de concordância com tais políticas no primeiro acesso realizado pelo usuário. Também se fala que a sensibilidade das pessoas ao reconhecerem a importância de protegerem as suas informações sigilosas da atuação dos engenheiros sociais, tendo ciência do subterfúgio utilizado, dependem da sua conscientização. A educação voltada para a gestão da segurança da informação nas organizações e de seus usuários, como correntistas de Instituições Bancárias, é um importante aliado ao enfrentamento dessa ameaça social, a engenharia social. O conhecimento pelos usuários da Internet das ferramentas utilizadas pelos engenheiros sociais nas suas práticas criminosas é essencial para os auxiliarem na proteção contra as ameaças presentes na rede.

A [P15] cita que os colaboradores precisam estar conscientes de que as informações, sejam elas pessoais ou corporativas, são ativos de muito valor e que seu papel na proteção desse ativo é muito importante. A conscientização em profundidade reduz o risco de ataques e torna a organização menos vulnerável para isso deve-se disponibilizar para os funcionários: - Políticas de segurança sobre o manuseio correto das informações da empresa ou de pessoal; Auditorias para garantir que os funcionários da organização estejam seguindo as políticas e procedimentos; Cópias impressas de dados organizacionais, registros ou informações pessoais devem ser destruídas antes de serem descartadas. A utilização de incineradores e trituradores são formas eficazes para destruir as informações. Os funcionários ou indivíduos precisam ser treinados para questionar as credenciais da pessoa que está se promovendo para estar em posição de autoridade na organização; As organizações devem ter cuidado com o que estão postando no site da empresa. Detalhes da empresa como nomes de pessoas com autoridade e números de contato devem ser evitados.

A [P16] diz que é necessário fazer as pessoas que um simples clique, pode gerar um prejuízo incalculável a corporação. É importante que haja uma maturidade visível com relação ao que lhe atrai e para isso é necessária uma estratégia que envolva a todos que de alguma maneira desempenha alguma função dentro da corporação.

A [P17] sugere a educação como aliada contra os ataques de phishing, os usuários devem ser informados sobre e como reconhecer um e-mail phishing, ciberataques, telefonema de ataque, e o que fazer quando se deparam com os mesmos.

É mencionado na [P18] diz que é preciso tomar certos cuidados a quem se confia a informação. Além de realizar trabalhos de prevenção para confiar adequadamente, também é preciso ter controle dinâmico sobre as relações de confiança estabelecidas para poder revogar determinadas autorizações, arriscadas demais, por exemplo, passíveis de engenharia social.

A [P19] fala que conscientização é importante tornar os funcionários cientes do termo de responsabilidade apresentando suas responsabilidades e/ou confidencialidade sobre as informações das empresas em que trabalham. Orientar os funcionários para ter consciência da importância da informação.

De acordo com a [P20] o conhecimento é muito importante, saber o que é a engenharia social, entender como funciona, saber das fraquezas que os seres humanos possuem isso, no caso informar as pessoas do que se trata a prática pode diminuir significativamente um ataque. É importante alertar para sempre conferir se os dados que uma pessoa apresentou conferem com o real. Pedir a carteira de identificação, conferir o crachá da pessoa para ter certeza de que ela pode ter acesso aquele lugar. Conferir com alguém superior se o pedido daquela pessoa é verdadeiro. A educação e avisos dentro de uma empresa podem evitar ataques, assim como proporcionar cursos, workshops, newsletters, posters, etc.

A [P21] cita medidas motivadoras, como por exemplo, dramatização, vídeos educativos, para prender a atenção e aumentar a receptividade acerca da implementação do plano durante a formação dos funcionários. Existem alguns tópicos que são fundamentais para a elaboração de um bom plano de conscientização sobre SI, entre eles estão: As principais táticas, técnicas e fatores psicológicos utilizadas pelos engenheiros sociais para manipular suas vítimas; Como proceder frente a uma solicitação suspeita; Quem informar sobre uma tentativa de ataque independentemente do seu sucesso; Os procedimentos para proteger as informações confidenciais; Métodos para confirmar a identidade das pessoas que solicitam algum tipo de informação, independentemente do cargo que ocupam. • Como fazer a divulgação de informação restrita; Boas práticas para a utilização do correio eletrônico, de modo a evitar malware e phishing; Descrição de cada política de segurança e a sua importância na proteção da informação; Explicar a obrigação e a responsabilidade do cumprimento das regras, bem como, as consequências do seu não cumprimento; Incentivar os funcionários a cumprir as políticas de segurança.

Na [P23] diz que usuário deve ser preparado para identificar e lidar com situações de vulnerabilidade, reforçando dessa forma o elo mais frágil e reduzindo o espaço de atuação dos sabotadores e em consequência aprimorando os mecanismos de segurança da informação, para isso é preciso disponibilizar treinamento adequado por meio de cursos de capacitação profissional, campanha de conscientização e mecanismo de estímulo, visando com isso.

A [P24] menciona que é necessário ter consciência do valor da informação e de que as ações podem influenciar direta ou indiretamente a segurança da informação. A implementação das medidas de segurança poderá ser realizada através do desenvolvimento de programas de sensibilização. Estes programas poderão ser usados para garantir que as políticas de segurança e as melhores práticas sejam implementadas e cumpridas. As políticas de segurança são um elemento fundamental e estratégico para implementar a segurança.

A [P26] diz que promover a conscientização peculiar e continuada dos funcionários em relação às chantagens e intimidações por parte do engenheiro social; realizar a classificação e armazenamento da informação conforme o seu nível; programar políticas de segurança nas organizações e sua ampla divulgação podem ajudar nos combate a taques.

Segundo a [P27] a melhor forma que as organizações têm para proteger a sua privacidade contra os ataques dos "engenheiros sociais" é formar as suas equipes sobre o uso adequado das políticas de segurança: Criar uma "Firewall Humana" – As 47 quebras de segurança por parte dos colaboradores está a se tornar o maior risco de segurança do século XXI. Defender o lado humano da Segurança – Necessidade de se estabelecer uma cultura de segurança na organização.

Na [P29] a educação é tratada como algo necessário para pessoas, indo muito além de simplesmente treiná-las para que se tornem menos vulneráveis e representem mais uma camada de segurança para proteger os dados empresariais.

A [P31] fala que os funcionários com conhecimento avançado de SI podem utilizar uma técnica chamada de engenharia social inversa, que é a defesa em que o alvo reconhece o ataque e usa princípios psicológicos de influência para tirar o máximo possível de informações do atacante, preservando, assim, os ativos visados da empresa. Educar e treinar é importante para conscientizar as pessoas sobre o valor da informação que elas dispõem e manipulam, seja ela de uso pessoal ou institucional, também se deve informar para os usuários sobre como age um engenheiro social.

A [P33] cita que conscientização pode ser realiza por meio de demonstração das técnicas de engenharia social através da dramatização, reportagens ou através de vídeos educativos sobre o assunto, que exibam casos reais de maneira que seja ao mesmo tempo algo educativo e divertido. Algo muito interessante que também pode ser colocado em prática é a recompensa para os funcionários que seguem as boas práticas de segurança da empresa de maneira correta. Pois sabemos que o incentivo é sempre algo muito motivador. Também é interessante divulgar amplamente por toda empresa através de circulares internas, boletins periódicos on-line ou pela própria Intranet, os casos frustrados de quebra de segurança onde um funcionário atuou de maneira correta evitando algum sinistro. Recursos como Intranet ou correio eletrônico podem ser tão úteis para a divulgação, por exemplo, de lembretes de segurança como mudança de senhas, pois o grande risco é quando os funcionários relaxam na questão da segurança. Para os riscos inerentes aos fatores humanos, podem-se destacar como exemplo os seguintes controles: Seminários de sensibilização; Cursos de capacitação; Campanhas de divulgação da política de segurança; Crachás de identificação; Procedimentos específicos para demissão e admissão de funcionários; Termo de responsabilidade; Termo de confidencialidade; Softwares de auditoria de acessos; Softwares de monitoramento e filtragem de conteúdo; fala do processo de conscientização sobre SI que não pode deixar de lado os seguintes tópicos: O processo de conscientização sobre SI não pode deixar de lado os seguintes tópicos: - Descrever a forma com que engenheiros sociais utilizam suas aptidões para manipular e ludibriar. Táticas empregadas pelos engenheiros sociais para cumprirem suas metas. Como identificar a ação de um engenheiro social. Como agir ao desconfiar de alguma solicitação suspeita. quem reportar as tentativas de ataque fracassadas ou que tiveram êxito. - Questionar solicitações, independentemente do cargo ou importância que o solicitante julga ter. Não confiar em pessoas que fazem solicitações de informações, sem antes examinar perfeitamente sua real identidade. Como proceder para proteger informações sigilosas. Como encontrar as políticas e procedimentos de segurança da informação e sua importância na proteção das informações. Sintetizar e explicar o sentido de cada política de segurança como, por exemplo, a questão da criação de senhas difíceis de serem descobertas. - A obrigação do cumprimento das políticas de segurança e as consequências para o empregado e para a organização caso haja algum descumprimento. Como divulgar material ou informação restrita. Melhores práticas de uso do correio eletrônico de maneira a não se tornar vítima da engenharia social, vírus e armadilhas em geral. Questões físicas da segurança como, por exemplo, a utilização de crachás e o questionamento para com aqueles que estão nas dependências da organização sem utilizá-lo. - Eliminação de documentos que contenham informações confidenciais independentemente se sua natureza é física ou eletrônica. Deixar bem claro que testes serão feitos periodicamente dentro da organização para verificar quais funcionários estão procedendo corretamente e quais não estão. Fornece material informativo como, por exemplo, lembretes através do meio de comunicação que julgar conveniente. Parabenizar publicamente o(s) funcionário(s) destaque(s) na segurança da informação. - Testes de intrusão e vulnerabilidades usando a engenharia social podem ser feitos periodicamente com o objetivo de encontrar falhas ou descobrir o descumprimento das políticas de segurança e até mesmo pontos fracos no próprio treinamento dos funcionários. - E ficar atento com relação a qualquer tipo de abordagem, independente do meio utilizado, como por exemplo, e-mails, telefone e etc. Não fornecer informações confidenciais como, por exemplo, senhas.

[BP2] Treinamento

Na [P3] menciona-se que alguns pontos devem ser considerados ao se elaborar um programa de treinamento para conscientização contra ataques de engenharia social e, assim tornar a organização menos vulnerável: a) Definir escopo, metas e objetivos: o escopo deve contemplar todos os profissionais que interagem com os sistemas e com as

informações sensíveis para a organização; b) Identificar os instrutores: é importante que os profissionais dominem as técnicas e os princípios de segurança; c) Identificar o público-alvo: Identificar e separar os grupos de profissionais que receberão o treinamento. Somente os conceitos necessários devem ser apresentados para obter o melhor resultado; d) Motivação dos funcionários e da alta administração: O apoio dos funcionários e da alta administração é fundamental para que o programa tenha efetividade e é responsabilidade da alta administração assegurar que todos os usuários dos sistemas de informação saibam como proteger seus ativos; e) Continuidade: dar atenção às 49 mudanças tecnológicas e de segurança de informação. um programa desenvolvido hoje pode tornar-se obsoleto e ineficaz quando houver mudança no ambiente tecnológico; f) Avaliação: a avaliação dos funcionários após a realização do treinamento é uma boa opção para verificar o aprendizado dos conceitos e avaliar o nível de conscientização e no direcionamento do reforço necessário.

A [P5] diz que conceitos, ferramentas e métodos utilizados por essa prática devem ser apresentados às pessoas, assim também aborda a [P7] falando dos treinamentos contínuos de conscientização e disponibilização de guias que tratem do assunto.

Na [P9] é abordada a atenção da qualidade da política de segurança da informação aplicado nas unidades de informação, devido a proteção dos livros raros nas bibliotecas ser notavelmente frágil assim a equipe responsável pelos materiais informacionais raros deve ser instruída a respeito de como um engenheiro social age para evitar a ocorrência de extravios nas bibliotecas. Propor rotinas que incluem a capacitação dos profissionais da informação é uma forma de combate a respeito das ameaças e vulnerabilidades para que estes tenham a percepção das situações que são capazes de comprometer seus ativos.

É citado na [P10] que os colaboradores devem ser treinados e educados sobre quais são as informações que devem ser protegidas e como devem protegê-las, pois assim estarão aptos a identificar situações de riscos, como um ataque de um engenheiro social.

Na [P11] aborda que oferecer o treinamento de segurança da informação e medidas preventivas que tratam de assuntos sigilosos pode ajudar o indivíduo a ter habilidade em detectar, de maneira mais apurada, o tipo de ataque, além de saber como agir nesses casos.

Na [P15] são apresentadas orientações que devem conter para treinamento: -Estar ciente dos ataques de engenharia social: Muitas pessoas sequer têm consciência de que essa ameaça existe; Usar a simulação de papéis para treinar funcionários: dois métodos que são usados para demonstrar a efetividade da engenharia social: (1)Analisar casos de engenharia social para ilustrar o quanto as pessoas estão suscetíveis a esses ataques e (2) fazer com que os funcionários relatem suas experiências durante um seminário de segurança da informação. O treinamento vai servir para examinar o funcionamento dos ataques, analisar por que funcionou e discutir como podem ser reconhecidos e evitados; Esclarecer aos trainees que eles se sentirão tolos se forem manipulados em um ataque de engenharia social depois do treinamento: As pessoas são motivadas a não se sentirem ”tolas“ ou ”estúpidas“. A responsabilidade de cada funcionário em ajudar a proteger os ativos da organização deve ser enfatizada; Desenvolver procedimentos para ações dos funcionários quando houver suspeita de um ataque de engenharia social ou quando ele for detectado: Políticas devem ser consideradas como referência, depois que os procedimentos da 50 empresa forem desenvolvidos e colocados em prática, a informação deve ser divulgada na Intranet da empresa, que pode ser rapidamente acessada; Desenvolver orientações simples para funcionários, definindo que informações a empresa considera confidenciais: É importante transmitir aos funcionários que até as informações que não são consideradas tão confidenciais podem ser úteis a um atacante, que pode coletar qualquer informação aparentemente inútil e juntá-las para criar a ilusão de credibilidade e confiabilidade Um programa de conscientização e treinamento ser eficaz deve-se realizar o planejamento, implementação manutenção e avaliação periódicos do programa. Alguns pontos devem ser considerados ao se elaborar um programa de treinamento e conscientização contra-ataques de engenharia social: a) Definir escopo, metas e objetivos: o escopo deve contemplar todos os profissionais que interagem com os sistemas e com a informações sensíveis para a organização; b) Identificar os instrutores: é importante que os profissionais dominem as técnicas e os princípios de segurança; c) Identificar o público-alvo: Identificar e separar os grupos de profissionais que receberão o treinamento. Somente os conceitos necessários devem ser apresentados para obter o melhor resultado; d) Motivação dos funcionários e da alta administração: O apoio dos funcionários e da alta administração é fundamental para que o programa tenha efetividade e é responsabilidade da alta administração assegurar que todos os usuários dos sistemas de informação saibam como proteger seus ativos; e) Continuidade: dar atenção às mudanças tecnológicas e de segurança de informação. um programa desenvolvido hoje pode tornar-se obsoleto e ineficaz quando houver mudança no ambiente tecnológico; f) Avaliação: a avaliação dos funcionários após a realização do treinamento é uma boa opção para verificar o aprendizado dos conceitos e avaliar o nível de conscientização e no direcionamento do reforço necessário.

Na [P16] diz que se deve implantar um programa de treinamento e conscientização com objetivos claros: a) Promover a conscientização sobre a ameaça do ataque de engenharia social (interno e/ou externo) b) Treinar os usuários para cumprir e apoiar as medidas defensivas de segurança sistêmica que protegem as informações e sistemas de ataque. c) Entender o perfil e como pensa e age um Engenheiro Social. É necessário um treinamento contínuo para que as pessoas sempre saibam quais são as novas técnicas utilizadas e como lidar com cada uma delas. Utilizar como ferramenta o ciclo PDCA (P- Plan (planejar); D - Do (executar); C - Check (verificar) e A - Act (agir)) para o melhoramento contínuo da segurança da informação, pois através dele pode se identificar as falhas e tratratá-las PDCA é um ciclo de desenvolvimento que tem foco na melhoria contínua. Seu princípio é tornar mais claros e ágeis os processos envolvidos na execução da gestão.

Na [P17] se fala em treinar funcionários, realizar avaliações regulares dos controles de segurança implementados para garantir um padrão aceitável para todos da organização. Também pode ser realizado é um ataque simulado, permitindo, assim, a manutenção segura e preventiva em prol da segurança da informação. As técnicas preventivas sugeridas para treinamento aplicado a ataques de hackers nas Grandes Empresas são: Treinamento das políticas e procedimentos, como também utilização de treinamentos e seminários de orientação para o usuário informando-o que os acessos a ele concedidos são intransferíveis. Investimentos em recursos tecnológicos. Além disso, os funcionários devem ser treinados para não tratarem de assuntos confidenciais, seja em suas redes sociais ou em conversas com outras pessoas. Para as Média Empresas: a responsabilidade pela proteção de ataques aos sistemas de tecnologia de informação deve ser coordenada por um analista. A centralização das atividades de segurança de informação e TI na empresa pode se restringir a coordenação dos dispositivos utilizados para monitorar os ataques. Para Pequenas Empresas: Ter atenção às mensagens recebidas, em nome de instituições conhecidas, que tentam induzir o usuário a fornecer informações, instalar/executar programas ou clicar em links. É necessário questionar a veracidade do envio, já que é esperado que ele não aconteça vindo de instituições com as quais não se tem contato. Treinamento para o funcionário no momento da contratação é primordial para a prevenção contra-ataques de hackers.

A [P21] aborda que os planos de treino devem ser realizados com alguma regularidade para que as pessoas estejam preparadas para identificar as novas ameaças e técnicas de engenharia social que estão em constante evolução. Para um resultado mais eficaz, o plano de treinamento pode ser adaptado de acordo com os requisitos de cada grupo dentro da organização, por exemplo: recepcionista, administrativo, gestor, administrador de sistemas. Outro ponto importante é não excluir nenhum funcionário mesmo que ele não tenha acesso aos sistemas. Por exemplo, o segurança ou o funcionário da limpeza, pois os engenheiros sociais costumam utilizá-los para conseguirem obter acesso a locais restritos, o que posteriormente poderá proporcionar um ataque. O treino é importante para: Criar um "Firewall Humano": preparar as pessoas para que estejam mais aptas a identificar um ataque de engenharia social; Fortalecer o lado humano da segurança: tornar as pessoas mais conscientes da importância da segurança das informações, estabelecendo uma cultura de segurança na organização; É fundamental que as organizações treinem seus funcionários assim que são admitidos, salientando a importância dos tópicos acima referidos. 52 Realizar uma auditoria para identificar as vulnerabilidades de ataques de engenharia social na organização; Criar um plano de resposta a ataques para perceber como ocorreu e determinar qual o impacto desta falha de segurança na organização a fim de prever e prevenir novos ataques.

Na [P22] são citados os meios de controle que não devem faltar no plano de treinamento dos colaboradores: Seminários de sensibilização; Cursos de capacitação; Campanhas de divulgação da política de segurança; Crachás de identificação; Procedimentos específicos para demissão e admissão de funcionários; Termo de responsabilidade; Termo de confiabilidade; Software de auditoria de acessos e Software de monitoramento e filtragem de conteúdo. Criar políticas de segurança centralizadas e bem divulgadas, para que seus colaboradores possam ter conhecimento sobre segurança da informação, o que é uma informação confidencial e o que não é confidencial, o que fazer em situações de risco e a quem reportar. As intranets podem ser um bom recurso para essa divulgação, assim como boletins periódicos on-line, lembretes no correio eletrônico e requisitos de mudança de senha. Para que os funcionários não se tornarem complacentes e relaxarem na segurança, a insistência é importante.

A [P25] aborda que o treinamento deve ser tanto de forma técnica com o uso de antivírus e firewall, mas principalmente um treinamento considerando o fator humano.

Na [P27] o treino e educação dos colaboradores são práticas para ajudar a identificar ataques e a reportar interações estranhas que podem revelar-se uma defesa eficaz, também é preciso proporcionar para as pessoas formação adequada no que respeita ao tratamento de informação empresarial (e mesmo pessoal), de forma a criar políticas de segurança internas para a gestão dos ativos empresariais (e mesmo pessoais).

A [P29] cita que os treinamentos sobre ESoc e phishing podem ser feito focando em casos práticos para exemplificar e melhor transmitir a teoria sobre os referidos assuntos e teste prático com algum tipo de phishing para a conta de e-mail.

O treinamento especializado e planejado é tratado na [P32] como essencial para minimizar ações de uma pessoa ou empresa rival que possam comprometer informações da empresa.

E na [P33] o plano de treinamento visa influenciar os funcionários a mudarem seus hábitos e motivá-los a participarem do treinamento, para assim conscientizá-los que eles são parte da SI na empresa e que ela poderá sofrer um ataque a qualquer momento, os funcionários precisam ser treinamos e educados de maneira que possam ter consciência das informações que precisam ser protegidas e como protegê-las para que assim possam identificar facilmente um ataque de engenharia social. Técnicas de engenharia social podem ser demonstradas através de dramatização, reportagens ou vídeos educativos, que exibam casos reais de maneira que seja ao mesmo tempo algo educativo e divertido é algo favorável no combate da prática, algo que também pode ser colocado em prática é a recompensa para os funcionários que 53 seguem as boas práticas de segurança da empresa de maneira correta, pois o incentivo é sempre algo muito motivador. Também é interessante divulgar amplamente por toda empresa através de circulares internas, boletins periódicos on-line ou pela própria Intranet, os casos frustrados de quebra de segurança onde um funcionário atuou de maneira correta. Recursos como Intranet ou correio eletrônico podem ser tão úteis para a divulgação, por exemplo, de lembretes de segurança como mudança de senhas, pois o grande risco é quando os funcionários relaxam na questão da segurança.

[BP3] Políticas de Segurança

São descritas a seguir o que foi mencionado nas publicações quanto ao uso das Políticas de Segurança.

Na [P4] diz que devem ser adotados um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação.

Na [P8] o papel da política de segurança é fornecer orientações acerca da conduta do funcionário e constitui-se em um elemento relevante para o desenvolvimento de controles apropriados para combater às diversas ameaças que possam vir a trazer riscos para a organização.

A [13] diz que a política agrega benefícios de como evitar relapsos que acabem tornando em vazamentos, fraudes, espionagem proveniente de concorrentes, uso indevido, sabotagens são esperados, tangendo ainda na precaução em diversos outros problemas que venham a prejudicar a empresa de alguma forma. Quando uma organização realiza teste de penetração de segurança e mantém sua equipe consciente dos perigos e precauções desejáveis a fim de evitar problemas possuem um índice muito melhor de defesa e segurança de seus dados.

É falado na [P16] sobre a Política de Segurança da Informação e Comunicação - POSIC que tem a finalidade de orientar o usuário a comportar-se de maneira adequada dentro de sua entidade, resguardando sua própria identidade e evitando o comprometimento muitas vezes da rede de seu ambiente corporativo.

São abordadas na [P17] as Políticas Institucionais de SI para Grandes Empresas, que devem instruir o funcionário quanto ao risco de compartilhar usuário e senha com outras pessoas não autorizadas. Nas Médias Empresas se deve conscientizar os funcionários com relação aos problemas que este tipo de informação pode causar em mãos erradas. E as Pequena Empresas podem adotar normas internas de conduta para prevenir invasões de engenharia social; Proibição do uso de e-mails pessoais no ambiente de trabalho. Para contornar esses transtornos é adotado o e-mail institucional em que se torna possível controlar a origem e o conteúdo das mensagens recebidas. Além dessas 54 orientações específicas para o corpo funcional, prevalece o impedimento para funcionários utilizarem equipamentos computacionais próprios. O controle realizado por meio de dispositivos de hardware – portas de entrada e firewalls – e restrições de uso dos modens no ambiente organizacional.

Na [P19] se fala da adotar política de segurança para conscientizar os funcionários sobre as suas responsabilidades conforme o grau de importância da informação para a empresa. • A abordagem na [P2] menciona que a política deve deixar esclarecido como tudo dentro da empresa funciona. O que pode e que não pode. E sempre deixar procedimentos bem explicados, detalhados do que fazer caso algum tipo de ataque venha a acontecer.

A [P21] diz que as políticas de segurança devem ser alteradas e adaptadas às novas técnicas utilizadas pelos engenheiros sociais de acordo com o seu surgimento, e para que esta atualização seja feita regularmente, devem-se estabelecer procedimentos regulares com o objetivo de identificar novas ameaças. Uma das formas para se tentar travar as oportunidades dos ataques de engenharia social é a criação de políticas de segurança internas. Estas políticas consistem na definição clara, de um conjunto de instruções que forneçam orientação para preservar as informações, combatendo e prevenindo possíveis ameaças ou ataques que possam comprometer a sua segurança.

Na [P25] o desenvolvimento de uma boa política de segurança, combinada à educação e treinamento adequados, aumenta bastante a consciência do empregado sobre o tratamento correto das informações comerciais corporativas.

É citado na [P27] que é preciso definir com clareza uma política de segurança na empresa, com um conjunto de regras e regulamentos definidos pela organização em consonância com a lei geral, regulação setorial e decisões dos administradores da empresa.

A [P28] menciona que nos ambientes corporativos, para sanar ou minimizar os diferentes tipos de falha humana é necessária a criação de diretrizes organizacionais que estabeleçam normas de conduta – as Políticas de Informação, por meio delas as empresas planejam sua defesa diante de um possível ataque de um engenheiro social, entre outras ameaças.

Na [P33] as políticas são abordadas como uma das mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social. A Política de segurança da informação pode ser definida como uma série de instruções bem claras a fim de fornecer orientação para preservar as informações.

Para cada tipo de Política de Segurança identificada será apresentado de forma resumida o que foi mencionado nas publicações correspondentes a cada item a seguir:

[PS1] Ferramentas Tecnológicas

Na [P3] os seguintes mecanismos de proteção são mencionados: antivírus, firewalls, intranet, sistemas de autenticação, token, dentre outros, tecnologias que têm função importante para manter os dados em segurança.

Na [P4] as boas práticas são proibir a utilização de dispositivos móveis de armazenamento (pendrives, HD externos ou cartões de memória), particularmente em ambientes onde operam máquinas com dados sensíveis. Quando absolutamente necessário, liberar o acesso de tais dispositivos, sob supervisão. Configurar o antivírus para verificar automaticamente todos os dispositivos de armazenamento removíveis (CD, DVD, pendrive, cartão de memória, HD externo etc.) conectados ao computador.

A [P6] cita que o software Firewall é capaz de: Registrar as tentativas de acesso aos serviços habilitados no computador; Bloquear o envio para terceiros de informações coletadas por invasores e códigos maliciosos; Bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador e possibilitar a identificação das origens destas tentativas; Também consegue analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado e evitar que um código malicioso já instalado seja capaz de se propagar, impedindo que vulnerabilidades em outros computadores sejam exploradas. Na publicação o Antivírus também é citado como ferramenta "método mais comum que um antivírus utiliza para detectar a presença de um vírus informático é comparar arquivos contra um banco de dados com registros de vírus. Também é possível detectar atividade maliciosa para identificar vírus desconhecidos ou imitar arquivos e registrar as atividades realizadas pelos programas".

Na [P7] sugere-se a Criação de uma Storyboard de Capacitação, ou seja, um guia de capacitação de colaboradores em forma de história em quadrinhos que auxiliem de forma simples e objetiva conceitos de Engenharia Social, Segurança da Informação, e auxilie todos os envolvidos no ambiente organizacional na implementação de mecanismos de proteção contra ataques promovidos pelos engenheiros sociais, assim como boas práticas de manipulação e proteção de toda e qualquer informação que detenham.

Na [P10] o procedimento, monitoração, firewall, filtro de conteúdo, detecção de intrusos, testes de invasão podem ser utilizados, no qual permite a manutenção segura e preventiva em prol da Segurança da Informação, software, configurações, hardware, backup, e outras técnicas são empregadas para mitigar as vulnerabilidades organizacionais.

O uso de recursos tecnológicos é abordado na [P11] para a proteção de informações, com: Firewall, Internet com VPN, transmissão de mensagens criptografadas pode ajudar na proteção, porém se usuário ingênuo ou desinformado clica em um link enviado por e-mail ou trata de assuntos sensíveis durante um cafezinho na copa da empresa onde trabalha as informações ficam vulneráveis.

Na [P15] as soluções de defesa devem incluir camadas técnicas que envolvem controles de acesso, antivírus, firewalls, etc. e camadas de gerenciamento de políticas de segurança, conscientização de usuários e respostas a incidentes.

A[P17] diz que para melhorar a segurança deve ser feito uso de ferramentas tecnológicas, isso pode incluir criptografia, protocolos de segurança, firewalls e software antivírus. Para ataques realizados por meio de softwares para extração de dados a prevenção pode ser feita por Grande Empresas por meio de uma política de segurança, que deve implementar o bloqueio de acesso por meio de entradas USB, bem como o aperfeiçoamento de recursos físicos como firewall e IPS. É recomendado o uso de alguns antivírus licenciados, cuja parametrização permite a criação de regras de segurança especifica. Uso de firewalls, antivírus, bloqueios de acessos a pendrives, mídias removíveis, nem todos podem ter acesso, monitoramento de sites, monitoramento de e-mails. Estratégias de defesa para ataques realizados por meios de estruturas físicas. Instalação de catracas, deve-se pedir a obrigatoriedade do uso de crachá para circulação nas dependências da empresa. É importante também que os funcionários da portaria e os recepcionistas sejam treinados e orientados para o fato de que não é permitida a entrada de ninguém dentro da empresa sem autorização prévia do setor a ser visitado. Instalação de câmeras de segurança monitoradas por IPs. Para as Médias Empresas os usuários devem ser orientados e alertados com relação a ataques de engenharia social e estar cientes das punições se comprovada à

participação do funcionário em um ato criminoso. Treinamento para os usuários deve contemplar os riscos das invasões por meio de e-mails com links falsos, bem como as penalidades aos funcionários que contribuírem conscientemente com esta prática. E nas Pequenas Empresas utilizar Firewalls, servidores de proxys e de redirecionamento de portas, adoção de senhas de alto padrão de segurança, conjugando letras maiúsculas, minúsculas, uma quantidade mínima de caracteres, números e caracteres especiais, essas senhas, preferencialmente, não devem conter palavras que se encontrem em listas de dicionários para evitar exatamente que softwares que vão na base da tentativa e erro consigam montar a senha. Uso de dispositivos de rede que filtram pacotes de dados recebidos, servidores que agem como intermediários de requisições que veem do ambiente cibernético externo da organização e a prática de política de segurança de senhas. Adotar softwares originais e realizar cópias diárias dos dados organizacionais, os recursos usados para barrar a entrada de softwares maliciosos no ambiente de TI da organização não se restringem apenas aos dispositivos de software e hardware, mas, também de orientações de proteção repassadas ao usuário interno dos dados, diretrizes essas nem sempre seguidas e difíceis de controlar o seu cumprimento. Ferramentas Também podem ser usadas para o diagnóstico para ataques de hackers as Grandes Empresas devem escolher um Software de segurança para monitorar e controlar os acessos ao ambiente de informações de informações residentes nos computadores de acordo com os procedimentos desenvolvidos com base na política de segurança. Implantação do IDS e IPS, como ferramentas de diagnóstico para prevenção de ataques de hackers, ajuda a mensurar o tráfego de rede e os processos considerados rotineiros e não rotineiros. Criação de redes virtuais privadas. Utilização de recursos técnicos, como firewall, antivírus e VPNs. As Média Empresas fazer uso preventivo de sistemas operacionais e antivírus licenciados, fazer a manutenção preventiva periodicamente, em todas as estações de trabalho e servidores da empresa, utilizando recursos de antivírus. Uso de Proxy Squid é um software livre seu objetivo primário é agilizar o acesso à um conteúdo Web qualquer através do armazenamento em cache local, funciona como um intermediário no contato dos computadores da rede local com outras máquinas do ambiente externo a rede, como, por exemplo, na Internet. Ele recebe as requisições de qualquer navegador de rede por conteúdo que está no servidor de rede. Uso de sistema de Firewall controla o tráfego de dados através da verificação das informações que entram e saem da rede a fim de garantir que não ocorram acessos não autorizados a infraestrutura de computadores. O Active Directory (AD), é composto por um conjunto de ferramentas para o armazenamento e controle de informações sobre toda configuração da rede, incluindo dispositivos e usuários. Enquanto as Pequenas Empresas podem adotar recursos como firewall, redirecionamento de portas externas, bem como o bloqueio de pendrives.

A [P23] diz que para prover segurança em uma rede de computadores, normalmente, a equipe de suporte utiliza diversas ferramentas e métodos, que em geral são baseadas em hardware e software como, por exemplo: antivírus, backup, firewall.

Na [P24] são sugeridas a Instalação de soluções antivírus; utilização de firewall; atualização do software; destruição dos documentos; e não utilização de pens-usb externas para empresas. E medidas de segurança aplicadas aos utilizadores: instalação do antivírus; o utilização de firewall; e o software atualizado.

Sugere-se na [P26] o uso de mecanismos de segurança como criptografia, assinatura digital, antivírus, controle de acesso (senhas, firewalls, sistemas biométricos e smartcards), políticas de segurança, dentre outros podem auxiliar no combate de ESoc, além de executar a implementação e monitoramento dos mecanismos de segurança.

São citados na [P31] que se deve usar ferramentas como recursos tecnológicos, o cuidado que a empresa deve ter é deixar sempre o antivírus e o firewall atualizados e ativos, além de sempre fazer "varredura de dados" periódicas, (sugere-se pelo menos uma vez a cada três dias). Com essas ações, é possível se defender de alguns ataques mais fracos de rootkits e vírus, que infeccionam os dados da CPU, podendo causar danos irreversíveis. Outras medidas de segurança também devem ser tomadas a fim de atenuar o sucesso do engenheiro social: Uso do antivírus e verificar os dados do sistema a fim de encontrar arquivos infectados. A melhor maneira de evitar o Cavalo de Tróia é verificar sempre a autenticidade do remetente, além de manter os antivírus, firewalls e o sistema operacional sempre atualizados. Contra o Rootkit, é necessário manter e fazer uma varredura de dados no sistema operacional, além de manter o antivírus e o firewall sempre atualizados. Caso o rootkit continue na CPU, é preciso fazer uma restauração do sistema.

[PS2] Prevenção para o Acesso as Máquinas/Informações

Na [P4] diz que não se deve deixar senhas e login de usuários expostas. Evitar deixar senhas e login salvos nos navegadores, pois as senhas podem ser facilmente obtidas com recursos básicos de informática. Executar rigoroso controle das máquinas e dos usuários que podem ter acesso à rede de computadores. Não permitir que máquinas de visitantes sejam conectadas à rede local. Não possuir senhas "universais" (iguais para todos os sistemas). Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. Os cadastros de usuários que acessam os sistemas devem ser mantidos atualizados e supervisionados pela contra inteligência da organização. Estabelecer uma política clara e supervisionada relativa ao descredenciamento de usuários que tenham sido transferidos da organização ou de função.

Na [P5] a prática de mecanismos de controle e acesso têm por objetivo evitar que usuários sem permissão possam ter acesso a informações ou a equipamentos.

Assim também sugere a [P6] o objetivo controlar o acesso à informação, esse controle deve ser estabelecido, documentado e analisado criticamente com base nos requisitos de acesso dos negócios e segurança da informação.

A prevenção na [P17] está voltada para manter um estado de precisão permanente para um ataque. É importante realizar revisões periódicas dos controles que foram instalados, garantindo, assim, que um padrão aceitável é mantido em uma base contínua da política de segurança da informação. Para ajudar no controle, pode-se simular um ataque. Para uma contínua proteção, como forma de controle, é importante: a proteção e configuração de portas remotas de diagnósticos, a segregação de redes de grupos de serviços de informação, controle de conexão de rede, controle de roteamento da rede, controle de acesso ao sistema operacional e o controle de isolamento de sistemas sensíveis.

Na [P19] para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, as empresas devem 59 considerar a adoção de uma política de "mesas limpas" para os papéis e mídias de armazenamento removível e igualmente uma política de "telas limpas", contra o perigo de ter um usuário logado e ausente.

É abordado na [P24] que a utilização dos dispositivos móveis de armazenamento de dados nas empresas está tipicamente associados aos dispositivos do tipo pens-usb, que deverão ter atenção aos perigos associados à sua utilização. O primeiro perigo está relacionado com a perda do dispositivos e, consequentemente , a perda da própria

informação da empresa. O segundo está relacionado com a utilização de pens-usb externas dentro da organização que poderão resultar em ataques de baiting, malware, spying, entre outros.

A [P26] fala que não pode manusear informações corporativas fora da empresa e nem fornecer informações pessoais ou secretas;

Enquanto na [P31] são mencionados que os mecanismos de controle de acesso têm por objetivo e implementar privilégios mínimos a usuários a fim de que estes possam realizar suas atividades. O controle de acesso pode também prevenir que usuários sem permissão possam criar/remover/alterar contas e instalar software danosos a organização. Também é preciso ter um tempo limite para tentativas de login (entrar) e logoff (sair). Perguntar sempre ao superior se as informações, mesmo as mais comuns, devem ser repassadas; Inutilizar materiais que contenham informações sigilosas da empresa (não basta descartá-los).

Na [P32] utilizar comunicação internamente com funcionários ajuda a verificar pela conversa e analisar se realmente aquele funcionário trabalha ou não na empresa, adotar também código interno para a transferência de dados, é importante para que só ocorra a transferência de qualquer tipo de informação mediante senha e contrasenha, se a pessoa do outro lado da linha ou pessoalmente conhecer o código de autorização de dados a conversa acontece.

Para manter o controle de acesso a [P33] cita que se deve manter sala dos servidores sempre trancada, e o inventário de equipamentos atualizado; Manter os documentos confidenciais fora do alcance de pessoas não autorizadas, de preferência em envelopes fechados. • Deixar expostos arquivos de backup, não guardando em lugar seguro e confiável, além de demonstrar explicitamente que é um backup. Nome de usuário e senhas expostas para qualquer um que passar ver e ter acesso. Disquetes, Pen-drives, CDs, documentos, material particular como bolsas, carteiras em cima da mesa ou expostos, com grande facilidade de alguém se apoderar ou ter acesso, principalmente se as portas ou janelas ficam sempre abetas. Programas, documentos digitais gravados em disquete ou CDs, não sendo devidamente guardados em lugares seguros onde somente aqueles que podem ter realmente acesso seriam portadores da informação; Não deixar o computador ligado exibindo informações confidenciais como senha, login de usuário, códigos fontes; Acessos a sites indevidos, não confiáveis, ou fora das políticas de trabalho da empresa; Computador ligado e, sobretudo, logado com a senha e nome de algum usuário esquecidinho, deixando o uso da máquina disponível para alguém não autorizado. Sistema de alarme desativado, desligado ou inoperante, em caso de alguma urgência ou emergência; Jogo via internet ou mesmo por disquetes, Pen-drives ou CD-ROM são passíveis de conter armadilhas, como ativação de worms, cavalos de troia, vírus e dentre outros perigos que se escondem por trás dos envolventes jogos, ou diversões oferecidas por isso não devem ser usados; Não deixar Softwares em lugar não seguro; bem como livros, apostilas etc., que contenham informações que sirvam como um facilitador em trazer palavras de cunho técnico de modo a disponibilizar id, senhas, sejam elas default ou não; Enfeites, como vasos, quadros, dentre outros, servindo como mera distração, fugindo do habitual e tradicional layout de arranjo do ambiente de trabalho, podendo ser alvo de suspeita, pois atrás desses "enfeites" podem estar guardados, escondidos ou implantados sistemas de escuta, gravadores, dentre outros pequenos sistemas que podem colher informações ditas ou vivenciadas naquele ambiente. Para prevenção em manter os computadores seguros. Abaixo, algumas dicas são listadas o acesso à Internet: Instalar um bom programa de antivírus e, pelo menos uma vez por semana, fazer uma verificação completa do computador; Usar sempre cópia original do programa de antivírus, pois as cópias "piratas" geralmente já estão infectadas e não funcionam corretamente; Configurar o antivírus para procurar por atualizações diariamente; Usar o antivírus para verificar todo arquivo baixado antes de abri-lo ou executá-lo pela primeira vez; Utilizar cópias originais do Windows são mais seguras e são atualizadas periodicamente pela Microsoft; Manter o sistema operacional do computador e programas sempre atualizados para protegê-los contra as falhas de segurança, que são descobertas todos os dias; Somente instale programas de fontes confiáveis. Evite os serviços de compartilhamento (por exemplo: Kazaa, Bittorrent, Limeware, Emule, etc.). Eles são uma das principais fontes de disseminação de programas nocivos; Não abrir e-mails e arquivos enviados por desconhecidos; Não abra programas ou fotos que dizem oferecer prêmios; Cuidado com os e-mails falsos de bancos, lojas e cartões de crédito; Jamais abra arquivos que terminem com PIF, SCR, BAT, VBS e, principalmente, os terminados com EXE e COM; Se desconfiar de um e-mail recebido, mesmo quando enviado por pessoa conhecida, ter cuidado, pois pode ser um e-mail falso; Verificar o endereço que está aparecendo no navegador se é realmente o que deseja acessar; Não confiar em tudo o que vê ou lê; 61 Não autorizar instalação de software de desconhecidos ou de sites estranhos; Antes de clicar em um link, veja na barra de status do navegador se o endereço de destino do link está de acordo com a descrição do mesmo; Sempre desconfiar de ofertas e sorteios dos quais não tenha prévio conhecimento. Ao realizar compras pela Internet procurar por sites reconhecidamente seguros; Se utilizar o cartão de crédito ou tiver dados bancários, verificar se a página acessada utiliza tecnologia de criptografia, ou seja, o endereço da página acessada deve começar com "https" e deve aparecer o ícone de um cadeado na barra de status (parte inferior) ou à direita da caixa do endereço, dependendo do navegador. Uma observação importante a ser feita, é que Crackers colocam imagens de cadeados para fazer com que os usuários pensem que o site é seguro, mas na realidade não é. Se desconfiar de um site de compra, deixar lado e comprar em outro lugar. Ao preencher qualquer cadastro seja ele virtual ou não, só fornecer informações de extrema necessidade. Não acredite em todos os e-mails sobre vírus, principalmente aqueles de origem duvidosa que trazem anexo arquivo para ser executado, prometendo solucionar o problema; Jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por e-mail. Comunicar por telefone com a instituição que supostamente enviou o e-mail e confira o assunto. Nunca realizar operações bancárias ou transações pela internet que possuam informações pessoais de lugares públicos como, por exemplo, LAN-Houses, pois computadores públicos muitas vezes contêm códigos maliciosos, instalados por pessoas mal-intencionadas, capazes, por exemplo, de registrar tudo o que você digitar no teclado, facilitando a quebra de sigilo dos seus dados confidenciais. Os mecanismos de busca são perigosos em grande parte porque usuários são descuidados.

[PS3] Prevenção para Ataques por E-mail (similares)

Na [P3] em relação a e-mails falsos enviados por bancos deve-se observar o direcionamento da página de protocolo, pois os bancos utilizam somente o protocolo de segurança "https", outro detalhe importante é suspeitar do link recebido por e-mail, visto que as instituições financeiras não se comunicam dessa forma com seus clientes. Desconfiar quando a mensagem é enviada para várias pessoas, nem todas essas pessoas possuem conta no banco, as instituições financeiras, por questão de segurança, não solicitam quaisquer que sejam informação via e-mail.

A [P4] diz que para se prevenir: deve-se desconfiar sempre de mensagens de instituições financeiras, de ofertas imperdíveis, prêmios de promoções e mensagens com conteúdo do tipo "fotos comprometedoras". Evitar fornecer informações sigilosas, mesmo para usuários de confiança. Mensagens de conhecidos nem sempre são confiáveis (o campo de remetente do email pode ter sido falsificado, ou podem ter sido enviadas de contas falsas ou invadidas). Utilizar exclusivamente o correio eletrônico corporativo para troca de mensagens relativas ao serviço. Não clicar em links ou abrir arquivos recebidos por e-mail, a menos que se tenha absoluta certeza da origem e integridade do mesmo. Ter em mente que um arquivo enviado por uma pessoa de confiança pode não ter sido realmente enviado por ela. Não

utilizar a conta de correio corporativo funcional em cadastros de sítios na Internet. Se necessário, manter uma conta em provedor público (Gmail, Yahoo, Hotmail, etc) para esta finalidade.

É preciso ter alguns cuidados de acordo coma a [P12] ao fornecer informações pessoais através da Internet, às empresas podem a adotar estratégias antiphishing a fim de reduzir a ocorrência deste tipo de incidente. Indivíduos devem assumir atitudes contra o phishing, como segue: proteção de e-mail, evitar a transmissão de informações pessoais pela rede (salvos casos utilizando sites seguros). Tomar cuidado com esquemas de phishing via telefone; cuidado com downloads, e; atenção na utilização de links. Outras ações preventivas estão relacionadas ao controle do acesso a pop-ups, manutenção dos sistemas atualizados, adoção de firewall, filtros de spam, antivírus e software anti-spyware. Ainda, deve ser sempre feita uma verificação das contas online e extratos bancários regularmente para garantir que não haja transações não autorizadas realizadas. Por fim, para não cair nas armadilhas de ataques de phishing é possível ainda utilizar ferramentas antiphishing gratuitas ou pagas e filtrar boa parte dessas ameaças.

A [P22] faz algumas recomendações para o combate: Ler a URL do site de trás para frente. Comece pelo fim. O endereço pode muito bem começar com "www.seubanco.com.br", mas quando terminar com vários caracteres sem sentido, pode desconfiar. Não cair no que está sendo chamado de "phishing de mão dupla", em que você pode responder ao e-mail com uma pergunta, "Você é realmente meu amigo Jim?". Cibercriminosos são espertos o suficiente para esperar um pouco, mostrar que a resposta não é automatizada, e então responder com: "Sim, sou eu, Jim". É claro que não é ele. Nunca abrir um arquivo em PDF de alguém que você não conhece, afinal crackers podem se aproveitar para esconder seus arquivos maliciosos e executáveis dentro desses arquivos aparentemente inofensivos; Jamais fornecer senha ou informações pessoais/confidenciais em resposta a uma consulta não-solicitada; Profissionais de segurança de TI devem considerar treinamentos que visem especificamente spear phishing.

Na [P30] cita que não se pode abrir anexo de desconhecidos ou de conhecidos com erros grotescos de digitação. Abra apenas aqueles dos quais tiver certeza da origem e do possível envio de arquivo anexado. Não atestar a veracidade da mensagem apenas pelo remetente que aparece no cabeçalho de um e-mail, pois ela pode ser facilmente forjada pelos atacantes. Dados importantes como senhas e números de cartões de crédito, em hipótese alguma devem ser encaminhadas via e-mail. São apresentadas na publicação Técnicas De Defesas para os e-mails como SPF – que combate à falsificação de endereços de retornos de e-mail. Sender ID- sistema antispam para verificação do domínio remetente do email e a integridade da mensagem. Possui função semelhante ao SPF em se tratando da averiguação de mensagens adulteradas, possibilitando rastreamento e comprovação de adulteração com mais facilidade. DKIM- possibilita que o dono do domínio publique políticas sugerindo ao servidor de destino uma espécie de direcionamento de ações, como por exemplo, o descarte de todas as mensagens sem devida autenticação. DMARC ajudar pequenas e grandes empresas na redução do abuso sofridos pelos servidores de e-mail no que diz respeito a envio forjados em nome de seus domínios Além dessas técnicas cita meios de como identificar a fraude de phishing como: ler atentamente a mensagem, suspeitando daquelas com muitos erros gramaticais e de ortografia; Os fraudadores utilizam técnicas para ofuscar o real link para o arquivo malicioso, apresentando o que parece ser um link relacionado à instituição mencionada na mensagem. Uma sugestão que costuma apresentar êxito é que o usuário deslize o cursor do mouse sobre o link, desta forma é possível visualizar o real endereço do arquivo na barra de status, ou navegador, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este link será diferente do apresentado na mensagem; Atenção particular aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões frequentemente utilizadas por fraudadores são ".com", ".rar" e ".dll". Mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa devem ser sempre tidas como suspeitas; Deve-se acessar a página da instituição remetente e procurar por informações relacionadas com a mensagem que você recebeu. Em muitos casos, pode-se observar que não é política da instituição enviar emails para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.

A prevenção contra o Phishing é abordada na [P31], o conhecimento para reconhecer fraudes virtuais e cuidado no acesso dos links enviados por e-mail são práticas previdentes. Desconfiar quando receber um e-mail desconhecido. Se for conhecido, verificar o assunto e falar pessoalmente ou por via tecnológica se o remetente realmente mandou a mensagem.

De acordo com a [P32] para se proteger de phishing nunca se deve fazer atualizações via internet solicitadas por bancos, pois, bancos nunca solicitam este tipo de serviço online, e ao fazer algum tipo de transação online, deve-se programar o serviço de envio ao seu celular onde uma mensagem de hora dia e o valor da transação é enviada 64 ao celular sempre que feita, sendo assim, ao receber algo que não foi feito comunicase imediatamente o banco responsável.

Na [P33] sugere não clicar em links antes de verificar a autenticidade da solicitação. Várias são as vítimas de e-mails falsos. Para não ser mais uma vítima dessa armadilha, entre em contato com a fonte da solicitação seja ela uma pessoa, empresa, órgão público e etc. Nos casos de mensagens que tentam induzir a clicar em links contidos no e-mail ou em alguma página da Internet, a melhor coisa a fazer é entrar em contato com o remetente do e-mail ou com a instituição se for o caso, para certificar-se a respeito do assunto.

[PS4] Prevenção para Segurança Física

Na [P4] sugere-se para as Organizações Militares: Nunca deixar documentos sigilosos sobre as mesas ou de fácil acesso, assim como senha e login expostos. Ter controle de entrada e saída de pessoas pela guarda deve ser criterioso. Pessoal externo à Organização Militar deve andar sempre acompanhado por um militar. Evitar digitar senhas na presença de outras pessoas. Exigir a apresentação do documento de identidade militar. Não fornecer informações a recém conhecidos.

É citado na [P5] que somente pessoas autorizadas devem ter acesso a determinadas dependências de uma organização e sempre que possível devem ser usados o monitoramento por câmeras das entradas da dependência. • a como forma de segurança física devem ser reinados os funcionários da segurança para não permitirem o acesso de pessoas sem o devido crachá de identificação e mesmo assim fazer uma verificação visual; Todos os visitantes devem ser acompanhados por um funcionário da empresa; Fechar e monitorar a sala de correspondência; Manter sala dos servidores sempre trancada, e o inventário de equipamentos atualizado; Manter os documentos confidenciais fora do alcance de pessoas não autorizadas, de preferência em envelopes fechados.

As estratégias de defesa de ataques mencionadas na [P17] para as estruturas físicas de Médias Empresas, diminuem os riscos da terceirização de manutenção dos dispositivos computacionais, uma das estratégias encontradas foi primarizar estes serviços. Restringir a utilização interna de redes de comunicação. Enquanto para Pequenas Empresas o bloqueio do uso de wifi é eficiente quando o impedimento é geral para toda a organização. Controle ou a proibição de hardwares específicos, como pendrives, aumenta o nível de segurança, diminuindo a vulnerabilidade física da empresa.

Investimento em versões originais e seguras de antivírus traz maior segurança aos sistemas e ativos computacionais das organizações. Controle de acesso das portas de endereçamento em conexões remotas realizadas pela empresa.

Para a garantir a segurança física [P20] deve-se sempre conferir se os dados que uma pessoa apresentou conferem com o real. Pedir a carteira de identificação, conferir o 65 crachá da pessoa para ter certeza de que ela pode ter acendido aquele lugar. Conferir com alguém superior se o pedido daquela pessoa é verdadeiro.

Na [P31] é citado como boa prática a permissão ao cesso das dependências de uma organização apenas às pessoas devidamente autorizadas, bem como dispor de funcionários de segurança a fim de monitorar entrada e saída da organização. E solicitar um documento de identificação oficial (RG, carteira de motorista, carteira de trabalha, etc..) de quem solicita os dados. Requerer a assinatura da pessoa que solicitar informações importantes da empresa.

A [P33] diz que se deve verificar a identidade da pessoa para ter certeza se ela é realmente quem diz ser. Certificar se a pessoa realmente possui autorização. Ficar sempre atento ao ser abordado por alguém, principalmente se você não conhece a pessoa. Independente se a abordagem foi feita através do telefone, carta ou e-mail, não forneça informações sensíveis, pessoais ou até mesmo da organização onde trabalha. Treinar os funcionários da segurança para não permitirem o acesso de pessoas sem o devido crachá de identificação e mesmo assim fazer uma verificação visual; Permitir que visitantes tenham acesso à área interna na empresa, obtendo contato com as informações confidenciais; Permitir entrega de informações sem o devido conhecimento real de quem as está levando; Entrada de pessoas não autorizadas ou principalmente sem identificação, com portas abertas e expostas à entrada de qualquer um; Recebimento de informações digitais (disquete, CD etc.) sem o prévio conhecimento da procedência (de onde realmente vem e de quem vem e do que se trata), sem fazer primeiramente uma inspeção do material recebido em algum lugar ou equipamento que não comprometa a empresa ou organização.

[PS5] Prevenção para o Lixo

A [P4] menciona que não se deve jogar fora documentos com informações sigilosas. Separar e eliminar de forma eficiente.

Na [P10] diz que o lixo da empresa deve ser guardado em lugar seguro, triturar todo tipo de documento, e destruir todo o tipo de mídia magnética fora de uso.

Como forma de prevenção a [P24] cita que certos cuidados devem ser tomados com a destruição de documentos, o perigo está associado à não destruição da informação, de forma adequada (no sentido de “com segurança”), reside na perda da confidencialidade. O problema reside no perigo da informação cair nas mãos de alguém mal-intencionado, uma vez que poderá ser usada na realização de um ataque. O Dumpster Diving é uma técnica, de engenharia social, que consiste no recurso ao lixo como fonte de informação.

Também na [P26] é mencionado os cuidados especiais com o lixo eletrônico, assim como em qualquer outro meio, através de regras de descarte. • Para combater ataques por meio da técnica de lixo (Dumpster Diving) a [P31] cita que deve ser feita a destruição de dados que não sejam mais necessários. Entre os 66 procedimentos utilizados para isso, estão a incineração de arquivos, destruição de HDs (Hard Drive – Disco Rígido) e a adoção de equipamentos para picotar papel.

A [P32] diz que a melhor maneira de se prevenir é nunca usar folhas impressas erradas e não jogar nenhum tipo de comprovante, recibo ou extrato de conta bancária no lixo ou na rua. É mais seguro queimar ou picotar esse tipo de dado do que deixar exposto para muitas pessoas.

A[P33] fala em guardar o lixo da empresa em lugar seguro, triturar todo tipo de documento, e destruir todo o tipo de mídia magnética fora de uso. Descarte incorreto de material que se acha inútil, como por exemplo, não triturar documentos antes de jogá-los fora e de preferência em diversas lixeiras ou o descarte de disquetes, CDs e outros, sem eliminar definitivamente as informações contidas neles; Deixar gavetas abertas, de fácil acesso a documentos.

[PS6] Políticas de Senha

Na [P10] para políticas de senha uma característica importante de ser implementada é a criação de histórico de senhas. Devem ser definidas regras para que o usuário troque pelo menos 3 ou 4 caracteres da senha anterior. Não permitindo que ele utilize a mesma combinação de strings e só altere um número. Desenvolver na empresa uma política de mudança frequente de senhas e treinar os demais funcionários para nunca passarem senhas ou outras informações confidenciais por telefone; Criar senhas fortes e fazer uso consciente da mesma, alterando-a periodicamente.

Enquanto na [P17] diz que as política de senhas definem as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca.

A [P19] diz que as senhas devem ser de uso pessoal, portanto não se deve fornecer senhas para outros funcionários.

Aborda-se na [P24] que as empresas, no desenvolvimento das suas políticas de segurança, deverão definir regras na utilização de passwords. As regras deverão ter em atenção a dimensão, a composição, a validade e, de forma não menos importante, a exclusividade da password. A password é um elemento importante na identificação de um utilizador perante um sistema ou rede.

A [P31] cita que não pode não utilizar nome ou sobrenome na senha. Em vez disto, misturar letras, caracteres especiais e números.

E por fim a [P33] apresenta os seguintes critérios que podem ajudar sua senha a se tornar forte: Escolha senhas longas, pois para cada caractere adicionado, maior será a proteção. A quantidade mínima de caracteres recomendável é oito para uma senha segura. O ideal seria no mínimo quatorze caracteres. Uma frase secreta é fácil de lembrar e por ser mais longa, será mais seguro ainda. A combinação de letras, números e símbolos ajudam bastante a aumentar a força da senha. Quanto maior a variedade de caracteres, mais poderosa será a senha. Quanto menor a variedade de caracteres maior deverá ser a senha. Uma senha que possui quinze caracteres composta somente por letras e números aleatórios é cerca de 33.000 vezes mais forte do que uma senha de oito caracteres que é composta por elementos de todo o teclado. É lógico que uma senha ideal possui vários tipos de caracteres diferentes e ao mesmo tempo é longa. Use a tecla "Shift", pois sua senha será muito mais forte se você combinar os símbolos gerados através dessa tecla. Use frases ou palavras que você lembre com facilidade, mas que ao mesmo tempo seja difícil de alguém adivinhar. Alguns passos para criar

sua senha forte: 1. Escolha uma frase fácil de lembrar como por exemplo. "Meu filho Carlos tem três anos" ou então utilize a primeira letra de cada palavra que ficaria assim "mfctta". 2. Uma ótima opção se o sistema aceitar é a utilização de espaços entre as palavras ou caracteres. 3. Lembre-se de que quanto maior e mais complexas as combinações forem, mais forte será a senha, então ao invés de usar "mfctta" como no primeiro exemplo, pode-se usar "Mfc tA", "Meu FilhO CarLos tem 3 a os" ou "MeuFilhO KrlOs t&m 3 @no$.". Essa é a oportunidade de usar a imaginação. Teste sua senha em um verificador de senhas. Este é um recurso que ajuda a medir a força da sua senha. Estratégias para evitar senhas fracas: Evite escolher sequencias repetidas como, por exemplo: " 23456", "3333333", "abcdefg" ou letras próximas no teclado. Evite também substituições semelhantes como, '1' no lugar de 'i' ou '@' no lugar de 'a', como em "M1cr0$0ft" ou "Senh@", lembrando que essas substituições podem sim se tornar fortes mais somente quando combinadas com vários outros caracteres. Não use nome de login, data de aniversário, parte do nome, número de documentos, informações de familiares, pois informações pessoais e de familiares são as primeiras a serem testadas pelos invasores. Também não use palavras encontradas em dicionários, pois existem softwares sofisticadíssimos que utilizam essa técnica, e inclusive palavras de trás para frente, erros comuns de digitação, substituições e até mesmo aquelas palavras que um adulto consciente jamais falaria perto das crianças. Use uma senha diferente para cada site ou sistema. Pois se você utiliza a mesma senha para tudo e alguém descobrir, todas as outras também serão descobertas e a catástrofe será bem maior. Desenvolver na empresa uma política de mudança frequente de senhas e treinar os demais funcionários para nunca passarem senhas ou outras informações confidenciais por telefone; Não digitar senhas na presença de pessoas

[PS7] Prevenção para Controle/Fiscalização dos Comportamentos

A [P10] no que diz respeito a fiscalização e direcionamento do comportamento dos colaboradores práticas como auditorias de e-mails, relatórios gerenciais de sites acessados, avaliação comportamental e exploração de clima podem ser utilizadas.

Na [P17] se fala em utilizar escutas telefônicas, auditorias de e-mails, relatórios gerenciais de sites acessados, avaliação comportamental, exploração de clima são práticas que podem ajudar na fiscalização do comportamento dos funcionários. Assim como a adoção de controles básicos como: políticas de segurança, segurança física, educação / sensibilização, boa arquitetura de segurança, limitar o vazamento de dados, estratégia de resposta a incidentes e cultura de segurança.

Na [P18] os modelos de comportamento obrigatório devem ser ajustados constantemente para aprimorar as condutas dentro do contexto, especialmente ligadas à garantia de autenticidade nas comunicações da informação sobre meios digitais. Isso é, o fortalecimento do controle sobre a autenticidade das relações sociais deve ser consequência do desenvolvimento dessa consciência situacional sobre os riscos de exploração da confiança em comunicações digitais. Para se garantir o estado das coisas, são necessários o controle e o monitoramento. A supervisão direta da conduta das pessoas é item do controle. A supervisão da conduta em uma organização é essencial, pois sem ela não há qualidade nos processos.

Para controlar o comportamento a [P26] cita a criação de uma cultura que incentive um comportamento humano consciente no domínio das informações.

[PS8] Prevenção para Ataques por telefone (ou qualquer meio VoIP)

Como recomendação a [P4] que aborda a ESoc na Organização Militar diz que um atendente de telefone deve evitar se identificar de imediato ao atender a ligação; sempre confirmar a veracidade de informações recebidas; não fornecer/confirmar informações que não dizem respeito ao seu trabalho ou quando não se tem certeza de quem está do outro lado da linha.

A [P10] cita que atendentes devem solicitar sempre um código de acesso, para só então prestarem o suporte solicitado; Controlar chamadas para o exterior e para longas distâncias, e recusar pedidos de transferências suspeitas.

A [P32] recomenda que para combater os ataques de ligações telefônicas realizadas por detentos que informam ter sequestrado uma pessoa e pedem depósito em dinheiro em troca da liberdade da suposta vítima, aconselha-se como prevenção ter calma e procurar saber onde o parente que está "sequestrado" se encontra.

Como prevenção para ataques por telefone a [P33] diz que os atendentes devem solicitar sempre um código de acesso, para só então prestarem o suporte solicitado; Todos os visitantes devem ser acompanhados por um funcionário da empresa; Fechar e monitorar a sala de correspondência; Controlar chamadas para o exterior e para longas distâncias, e recusar pedidos de transferências suspeitas; Criar senhas fortes e fazer uso consciente da mesma, alterando-a periodicamente. Mencionar senha por telefone, pois antes de disponibilizar qualquer tipo de informação, deve-se saber com quem se fala e de onde fala, além de conferir através de aparelhos identificadores de chamada se o telefone de origem da ligação está realmente batendo com o mencionado. É importante conferir o motivo pelo qual solicitaram determinada informação.

[PS9] Prevenção para Redes Sociais

Na [P2] são citadas algumas ações que podem minimizar os ataques de engenharia social nas Redes Sociais online: - Ter consciência de que na Internet nem tudo é apenas virtual: as empresas e pessoas com as quais se interage são reais e os mesmos danos causados no dia a dia podem se repetir nesse ambiente; O melhor modo de impedir que a identidade seja furtada é protegendo bem os dados pessoais através de senhas bem elaboradas, identificação de termos de uso de um serviço assim como a política de segurança e privacidade oferecidas; Dar atenção a mensagens que contém links e formulários que devem ser preenchidos com dados pessoais; que solicitem sigilo ou que solicitem o repasse a sua lista. Manter-se informado, uma vez que novas formas de tentativas de golpes surgem a cada dia necessitando atualização constante. Recomenda-se o exame da "Cartilha de segurança para Internet" elaborada pelo Centro de Estudos, Resposta e ratamento de Incidentes de Segurança no Brasil (CERT). Também é válido o exame do site SaferNet Brasil, que é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos, que busca oferecer respostas eficientes quanto a problemas relacionados ao uso indevido da Internet para a prática de crimes e violações contra os Direitos Humanos.

Na [P4] as prevenções são: Manter suas contas com configurações de privacidade mais restritas possíveis (evitar a configuração pública). Evitar expor informações pessoais como telefone, e-mail, endereço e até mesmo as relações familiares existentes com outros usuários. Desconfiar de perfis desconhecidos que solicitam permissão para se tornar "amigo" nas redes sociais. Evitar diálogos com perfis desconhecidos que exponham informações pessoais ou

relacionadas com o trabalho em “chats” das diversas redes sociais existentes. Desconfiar de perfis de conhecidos solicitando informações (contas podem ser falsificadas facilmente).

Como boas práticas a [P28] menciona as configurações de segurança e privacidade do Facebook que são disponibilizadas os usuários: possibilidade de classificação da informação (postagens, fotos e vídeos) nas opções: público, para amigos, somente para o próprio usuário, personalizado (pessoas) ou por lista (grupo de pessoas); Outras opções disponíveis são: a ativação da navegação segura; notificação de login quando a conta for acessada de um computador ou dispositivo móvel não cadastrado; ativação de um código de segurança para acessar a conta a partir de navegadores desconhecidos; utilização de senha específica para uso de aplicativos (em vez de utilizar a mesma senha do Facebook). Dentre as outras opções de segurança e privacidade, o Facebook disponibiliza ainda ao usuário, na sua Central de Ajuda, informações sobre: Como fazer para bloquear alguém? Como controlar quem pode o localizar no Facebook com suas informações de contato? Como controlar quem pode lhe enviar mensagens? Como fazer para controlar quem pode ver publicações e fotos nas quais está marcado em sua linha do tempo? Como ativar a opção para analisar marcações que amigos adicionam às publicações antes de elas aparecerem? Como denunciar problemas (com base nos padrões da comunidade do Facebook)? Além dessas, são fornecidas informações sobre o gerenciamento de aplicativos e de conexões. Os usuários devem ser atentos às pessoas adicionadas a sua rede de amizades, é necessário atenção para o uso correto das ferramentas de gerenciamento da informação, observando o tipo de conexão estabelecida com os outros usuários, tais como amigos, melhores amigos, conhecidos, e integrantes de listas/grupos específicos.

Na [P32] diz que ao criar perfis em sites de relacionamento é preciso ter cautela com os dados fornecidos. Não é aconselhável colocar telefones, endereço, empresa na qual trabalha e qualquer tipo de informação pessoal em seu perfil.

[PS10] Prevenção para Navegação na Internet

A [P30] cita recomendações são para usuários e empresas. Para usuários: Separar os e-mails para assuntos pessoais, cadastros online, profissionais e compras online. Isso evita receber determinados assuntos indesejados no e-mail do trabalho por exemplo. Manter ativo um programa anti-spam, ou utilizar os recursos oferecido pelo provedor. Bem como ferramentas de proteção como firewall, antivírus, antispyware, reduzindo o número de mensagens indesejadas no e-mail. Para empresas: Adotar estratégias de defesa em camadas. Desativar serviços que não são necessários. Se algum código malicioso ou alguma outra ameaça explora um ou mais serviços de rede, desabilite ou bloqueie o acesso a esses serviços até que seja aplicado um patch. Isole os computadores infectados. Manter os patches atualizados (sistema operacional e aplicações). Considerar implementar soluções de acesso e conformidade com políticas de rede. Implementar políticas efetivas de senhas e controle de dispositivos. Usar softwares de criptografia para proteger as informações. Promover treinamento sobre segurança da informação para os funcionários. O site Internetsegura.org, responsável pelo movimento internet segura, elenca mais algumas ações para uma navegação mais segura: Nunca fornecer senha ou informações pessoais – sob nenhum argumento. Atentar para barra de endereços – Verifique se o endereço permanece o mesmo durante a navegação. Certificando sempre a existência do cadeado fechado, em endereço iniciados por HTTPS://. Clicando neste cadeado as informações referentes ao certificado são relacionadas ao site em questão. Cuidado com promoções tentadoras normalmente recebidas via e-mail, maioria das vezes são encaminhadas por endereços falsos, e 71 prometem descontos e prêmios instantâneos. ão navegar e sair “clicando em tudo” - controlar sempre a curiosidade e suspeitar de e-mail que oferecem benefícios de formas fáceis ou por valores muito baixos

Também são apresentadas algumas recomendações para navegação na [P31]: Ao acessar sites de vendas ou que envolvam dados, verificar se estes possuem a extensão HTTPS (Hyper Text Transfer Protocol) com mecanismo de segurança SSL (Secure Socket Layer)2 e/ou observar se a página possui a imagem de um cadeado no canto inferior direito, indicando sua autenticidade e segurança. É extremamente importante verificar a grafia do nome do site que o usuário irá acessar. Diversas pessoas são enganadas por páginas e links que pareciam conhecer, mas cujos endereços estavam grafados de forma errada, direcionando o usuário a sites maliciosos. Estes, por sua vez, podem armazenar informações pessoais da vítima, como dados do cartão de crédito. A troca ou ausência de uma letra, como no endereço eletrônico www.peixeurbao.com.br3, pode expor um usuário desatento a um ataque.

Na [P33] a melhor coisa a fazer enquanto estiver navegando na Web é ser cauteloso e manter o antivírus e detectores de pragas virtuais em geral sempre atualizados. Escolher senhas fortes e não compartilhar com outras pessoas.

[PS11] Política de backup

Na [P17] as políticas de backup definem as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução.

É citado os backups ou cópias de segurança na [P24], como uma importante medida de segurança, que deverão ser implementados não só para recuperar a informação no caso de perda acidental seja por falha física ou por falha humana, mas também da consequência de uma possível infecção por vírus ou de uma invasão.

[PS12] Plano de Resposta a Incidentes

Na [P27] quando existe quebra de segurança, é importante que a resposta da organização seja rápida e eficaz de forma a: Perceber exatamente como é que a quebra de segurança ocorreu; determinar o impacto que terá; Prever os próximos passos que o “engenheiro social” dará; romover a conscientização dos colaboradores sobre como dar resposta à quebra corrente e a futuros ataques por parte do “engenheiro social”. Detectar a intrusão por parte de “engenheiros sociais”: através da implantação de sistemas de monitorização de várias fontes de risco potencial (e-mail, telefone, mensagens instantâneas, World Wide Web, wireless e infraestruturas) que permitam o drill-down de uma visão geral até um incidente isolado.

As empresas devem estar preparadas para reconhecer, analisar e responder aos incidentes de segurança o mais rápido possível é o que diz a [P33] pois isso é fator fundamental para amenizar os estragos ou diminuir custos com reparos. Experiências anteriores com outros incidentes sejam usadas para prevenir ocorrências semelhantes no futuro ou até mesmo para aprimorar a segurança atual. Ele possui os procedimentos e medidas a serem tomadas para remediar, corrigir ou contornar os incidentes. As seguintes medidas não podem ser deixadas de lado em um Plano de Resposta a Incidentes: Identificar a autoria dos ataques, assim como sua seriedade, estragos causados e responsáveis pelo incidente. Divulgar o mais rápido possível o acontecimento ocorrido para que o mesmo incidente não ocorra em outras áreas da empresa. Tomar as medidas necessárias para restaurar aquilo que foi afetado como, por exemplo, mudar senhas, trocar funcionários, aumentar o nível de controle. Contatar os órgãos de segurança para que o fato seja registrado, assim como tentar entrar em contado com os responsáveis pelos ataques.

[PS13] Medidas para Usuários não Técnicos

A [P6] cita práticas para o usuário não técnico, com alguns cuidados que devem ser tomados: Manter o sistema operacional atualizado- novas ameaças surgem todos os dias, com isso o usuário deve manter seu sistema operacional e suas aplicações atualizados, tornando assim o sistema mais seguro. Ter cuidado com as senhas: não divulgar suas senhas para ninguém, pois são individuais, não escrever uma senha em local público ou de fácil acesso, criar senhas com mais de oito caracteres e que misture letras maiúsculas, minúsculas, números e caracteres especiais e mudá-las regularmente. Sempre usar criptografia: manter os arquivos criptografados, principalmente quando armazenados em notebooks e mídia móveis (como pendrive, por exemplo). Tomar cuidado com o e-mail: verificar por meio do antivírus os arquivos recebidos, mesmo que sejam de fontes confiáveis, verificar a origem dos emails com anexos duvidosos, desconfiar de arquivos executáveis recebidos e tomar cuidado ao visualizar imagens armazenadas externamente aos e-mails. Através desses links, o remetente do e-mail tem a possibilidade de descobrir a localização do usuário na Internet. Proteger dados pessoais: Nunca fornecer informações sensíveis em sites desconhecidos e que não possuam o cadeado na barra de endereço do navegador e um informativo de certificado digital. O mais importante para que o usuário se proteja de possíveis ameaças é o bom senso

[PS14] Política de privacidade

Na [P17] define como são tratadas as informações pessoais, sejam elas de clientes, usuários e funcionários.

[PS15] Política de confidencialidade

Na [P17] define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros.

[PS16] Política de uso aceitável (PUA) e Acceptable Use Policy (AUP)

Na [P17] também chamado de "Termo de Uso" e "Termo de Serviço", define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas.

[PS17] Prevenção para Ataques meio de Contatos Interpessoais

Na [P17] como para este tipo de ataque Grandes Empresas podem adotar de uma política de segurança da informação em uma organização aumenta o nível de segurança, ao mesmo tempo, que diminui o comprometimento das informações da organização em mãos de um funcionário recém contratado na empresa. Apresentar a política de segurança adotada pela organização, bem como o treinamento de conduta em relação a esta política e as punições mediante o não cumprimento das diretrizes descritas. E utilizar treinamentos e a conscientização de usuários, os funcionários devem ser treinados e orientados sobre os riscos de clicar em qualquer e-mail de origem duvidosa. Contar com recursos tecnológicos, colocando Firewall, antivírus. O usuário deve ter um login de acesso individual para acessar o sistema, o próprio computador, o e-mail, à própria internet e estar atento às orientações recebidas do setor de TI. As Médias Empresas podem realizar treinamentos e alertas para os funcionários, inclusive sobre as penalidades para quem infringir diretrizes de conduta no uso de tecnologias e sistemas de informação. Já as Pequenas Empresas podem implantar uma política de segurança da informação que estabelece diretrizes de conduta formalizadas e reforçadas por intermédio de treinamentos e técnicas de sensibilização do corpo funcional. Orientação dos usuários para que não abram e-mails suspeitos.

[PS18] Prevenção para Identificar Possíveis Alvos

A [P20] fala que para evitar um ataque primeiramente se deve identificar possíveis alvos, existem algumas categorias que podem ajudar identificá-los: Atitudes: pessoa com um extremo bom humor, muito carinhosa, muito educada, muito paciente, querendo ajudar demais. Pessoas desconhecidas com pedidos autoritários. Talvez com um extremo mal humor, pedindo para realizar coisas agressivamente. Ou até mesmo sendo muito emocional, chorando demais ou fincando muito chateada com alguma coisa. Tentativa de conexão: Tentar estabelecer uma conexão com suas vítimas é uma tarefa importante para os engenheiros sociais. Usar nomes de pessoas conhecidas sendo que a tal pessoa nunca te falou do atacante. Agir particularmente amigável e até usar informasse pessoais sobre a vítima. Pequenos erros: Mesmo que engenharia social seja uma técnica bastante eficiente, ser um bom engenheiro exige experiência e muita técnica. Sabendo disso engenheiros menos experientes comentem muitos pequenos erros, às vezes despercebidos aos olhos de uma pessoa comum, mas para alguém que já conhece suas técnicas pode ser suficiente para evitar o ataque.

[PS19] Postura Questionadora

Em relação a melhor postura de combate ao engenheiro social mal-intencionado o funcionário deve ser tão questionador como uma criança cita a [P32], demonstrando interesse nos mínimos detalhes, ouvindo mais, estando fortemente atento a tudo a sua volta, e principalmente fazendo o uso dos poderosos “porquês”, com certeza as empresas transformariam os frágeis cadeados em legítimos dispositivos dificultantes da segurança da informação.

[PS20] Métodos de Segurança

Realizar auditorias de vulnerabilidade a ataques de ESoc são citados na [P27]: No sentido de perceber o nível de fragilidade da companhia, através da análise: Da informação da empresa que está abertamente disponível; Das políticas e procedimentos de segurança estabelecidos; do tráfego telefônico; do tráfego de e-mail e das pesquisas na Internet; Do comportamento dos colaboradores; Do nível geral de segurança das instalações;

Fonte: Ramos et al (2019) (Adaptado)