PAULO BORGES FILO

PARADIGMAS E ANTAGONISMOS ENFRENTADOS NO RAMO DA SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Timóteo
2022

PAULO BORGES FILO

PARADIGMAS E ANTAGONISMOS ENFRENTADOS NO RAMO DA SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado à Faculdade Pitágoras Ipatinga, como requisito parcial para a obtenção do título de graduado em Engenharia da Computação.

Orientador: Bruno Roberto

Timóteo
2022

PAULO BORGES FILO

PARADIGMAS E ANTAGONISMOS ENFRENTADOS NO RAMO DA SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado à Faculdade Pitágoras Ipatinga, como requisito parcial para a obtenção do título de graduado em Engenharia da Computação.

BANCA EXAMINADORA

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Ipatinga, 12 de dezembro de 2022

Dedico este trabalho primeiramente a Deus pois sem ele nada disto seria possível.

AGRADECIMENTOS

Agradeço a minha esposa por ter me apoiado e aos meus pais por me terem dado condições de trilhar esse caminho e ter desenvolvido esse trabalho. Sou grato por todos os professores dessa instituição que tive a honra de adquirir conhecimento e a todos que fazem e ou fizeram parte dessa jornada.

A educação é simplesmente a alma de uma sociedade a passar de uma geração para a outra. G.K Chesterton

FILO, Paulo Borges. **Paradigmas e antagonismos enfrentados no ramo da segurança da informação em redes de computadores**. 2022. 34. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Faculdade Pitágoras, Ipatinga, 2022.

RESUMO

Dando importância para os riscos e conceitos que envolvem o tema segurança da informação este trabalho trata os paradigmas dos problemas que foram surgindo ao longo das novas tecnologias e as várias técnicas empregadas do ramo. Refere-se a uma revisão da literatura dos autores que discursaram sobre o tema proposto. Os principais pontos do tema analisado foram sobre as principais características da segurança da informação e o que a levam a ser tão crucial que a partir do seu avanço tecnológico foi necessária uma ampliação de processos e boas práticas como uma forma de proteção e integridade dos dados virtuais. As técnicas envoltas ao tema foram cada vez mais envolvendo persuasão humana e desenvolvimento técnico de defesa e ataque, causando um certo tipo de antagonismo cibernético causando um dinamismo mundial de trocas de informações que nem sempre são seguras e outras que são criadas para evitar a comunicação dessas informações inseguras que tem a capacidade de causar impactos nem sempre tão fáceis de contornar. É notório cada vez mais a implementação de técnicas de segurança da informação para conter possíveis avanços criminosos nas redes.

Palavras-chave: Informação. Protocolos. Dados. Ameaças. Segurança.

FILO, Paulo Borges. **Paradigms and antagonisms faced in the business of information security in computer networks**. 2022. 34. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Faculdade Pitágoras, Ipatinga, 2022.

ABSTRACT

Giving importance to the risks and concepts that involve the topic of information security, this work deals with the paradigms of the problems that have arisen over the course of new technologies and the various techniques used in the field. It refers to a literature review of the authors who spoke on the proposed topic. The main points of the analyzed topic were about the main characteristics of information security and what make it so crucial that from its technological advance it was necessary to expand processes and good practices as a way of protecting and integrity of virtual data. The techniques involved in the theme were increasingly involving human persuasion and technical development of defense and attack, causing a certain type of cybernetic antagonism causing a worldwide dynamism of information exchanges that are not always secure and others that are created to avoid the communication of these insecure information that could cause impacts that are not always so easy to circumvent. It is increasingly notorious the implementation of information security techniques to contain possible criminal advances in networks.

***Keywords*:** Information. Protocols. Data. Threat. Security.

LISTA DE ILUSTRAÇÕES

Figura 1 – Proposta de novo modelo para Segurança da Informação 00
Figura 2 – Gerenciamento de Mudanças (GMUD) 01
Figura 3 – Versões do SSL/TLS 02
Figura 4 – 50 maiores vazamentos do conjunto de 50.664 e-mails.....03
Figura 5 – Ambiente configurado para realizar o ataque MITM.....04

LISTA DE ABREVIATURAS E SIGLAS

HTTPS	Hyper Text Transfer Protocol Secure
SSH	Secure Shell
VPN	Virtual Private Network
DDoS	Distributed Denial-of-Service
NBR	Norma Brasileira
SSL	Security Socket Layer
TLS	Transport Layer Security
IP	Internet Protocol
SBCOPENLIB	Biblioteca Digital da Sociedade Brasileira de Computação
GSI/PR	Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República
CID	Confidencialidade Integridade Disponibilidade
SI	Segurança da Informação
PSI	Políticas de Segurança da Informação
GMUD	Gestão de Mudanças
BAD	Botnet Activity Detection
DoS	Denial of Service
C&C	Command & Control
NSA	National Security Agency
FBI	Federal Bureal Investigation
NGFW	Next Generation Firewall
DLP	Data Loss Prevention
SQL	Structured Query Language
MITM	Man-in-the-Middle
ARP	Address Resolution Protocol
DNS	Domain Name System
TCP	Transmission Control Protocol
LGPD	Lei Geral de Proteção de Dados

SUMÁRIO

1. INTRODUÇÃO.....13
2. SEGURANÇA DA INFORMAÇÃO E SEUS CONCEITOS ATUAIS.....14
3. TÉCNICAS APLICADAS EM SEGURANÇA DA INFORMAÇÃO.....19
4. VAZAMENTO DE DADOS E AMEAÇAS CONSTANTES.....24
5. CONSIDERAÇÕES FINAIS.....29
REFERÊNCIAS.....30

1. INTRODUÇÃO

Essa pesquisa discorreu sobre a segurança da informação pois é considerada um dos pilares essenciais de uma empresa que preza por privacidade e integridade dos seus clientes e colaboradores. Uma rede de computadores sem cuidado ao mundo digital está vulnerável e qualquer tipo de atrocidade virtual.

Um assunto muito visado e necessário, pois, a segurança demanda estudos e mais desenvoltura para adquirir um grau ideal em ambientes diversos, a implementação correta de medidas de segurança tornam cada vez mais seguro um sistema e entender como ataques cibernéticos acontecem e analisar a forma que normalmente os criminosos utilizam.

O ponto focal apresentado nesse trabalho foi entender que apesar de várias evidências e análises dos autores da área há ainda um certo tipo de receio de que uma falha de segurança pode as vezes não ser realidade para quem lida com informação sigilosa, as ameaças cibernéticas seriam uma realidade para pessoas e empresas do ramo?

O objetivo principal deste trabalho foi em torno da tecnologia existente envolvida em cybersecurity e possuiu como objetivos secundários a importância de saber o que realmente significa segurança da informação, sempre lembrar o leitor deste trabalho que nenhum sistema é cem por cento seguro de falhas e compreender algumas das técnicas usadas no ramo de segurança da informação.

O método de pesquisa aplicado no desenvolvimento deste trabalho foi uma revisão de literatura sendo ela apoiada por dissertações, artigos científicos e livros do período de 2002 a 2022, como, Edison Luiz Goncalves Fontes (2010), Luiz Paulo Lopes dos Santos (2018), Diego Kreutz (2020) e Filipe José Teixeira Dias (2018), entre outros. O maior número de publicações pesquisado sobre o assunto foi do autor Dias através do seu estudo sobre Segurança dos Protocolos SSL/TLS. Pesquisado também informações sobre o assunto no artigo Avaliação de Proteção contra Ataques de Negação de Serviço Distribuidos (DDoS) utilizando Lista de IPs Confiáveis de Luis Oliveira et al. (2007), através do site Biblioteca Digital da Sociedade Brasileira de Computação -- SBCOPENLIB. As palavras-chave mais utilizadas para pesquisa no site do Scholar Google foram: “cybersecurity”, “segurança da informação”, “protocolos de segurança”, “proteção na internet”, “ataques cibernéticos” e “vazamento de dados”.

2. SEGURANÇA DA INFORMAÇÃO E SEUS CONCEITOS ATUAIS

A vida cotidiana praticamente se resume a dados, sejam eles sigilosos ou não, a segurança da informação se resume ao conceito de proteger os dados, principalmente os sigilosos, sejam eles de grandes corporações ou de pessoas físicas, o conceito de segurança da informação se estende ao conceito de segurança cibernética, Regulamento de Segurança Cibernética (2021).

De acordo com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a segurança cibernética é citada como “ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade.

A palavra segurança e informação precisam andar lado a lado para que a estrutura da Confidencialidade, Integridade e Disponibilidade (CID) não sejam quebradas ou afetadas por um incidente cibernético, Cassio Bastos Alves (2010).

Um termo citado constantemente seria de que informação é a mesma coisa que dinheiro ou se não mais valorizado. Assim, foi mencionado que “Toda informação tem um valor para a organização, para a concorrência e para o mercado em que ela atua” (FONTES, 2006, p. 49). É necessário garantir sempre que a informação de um sistema seja condizente com o termo CID e aos conceitos citados acima sobre segurança da informação.

O conceito simples de segurança da informação traz um conglomerado de dados que quando analisados e sequencialmente tratados conseguem levar algum significado em um determinado contexto (TORRES, 2015, P.9).

Através da implementação da segurança da informação muitos empresários e pessoas podem se proteger e com isso não acontecendo incidentes como vazamentos de dados cruciais, a Segurança da Informação (S.I) é definida por uma execução de práticas e conceitos elaborados através de ações determinadas por políticas de segurança da informação (PSI), (TORRES, 2015, P.10).

Figura 1 – Proposta de novo modelo para Segurança da Informação

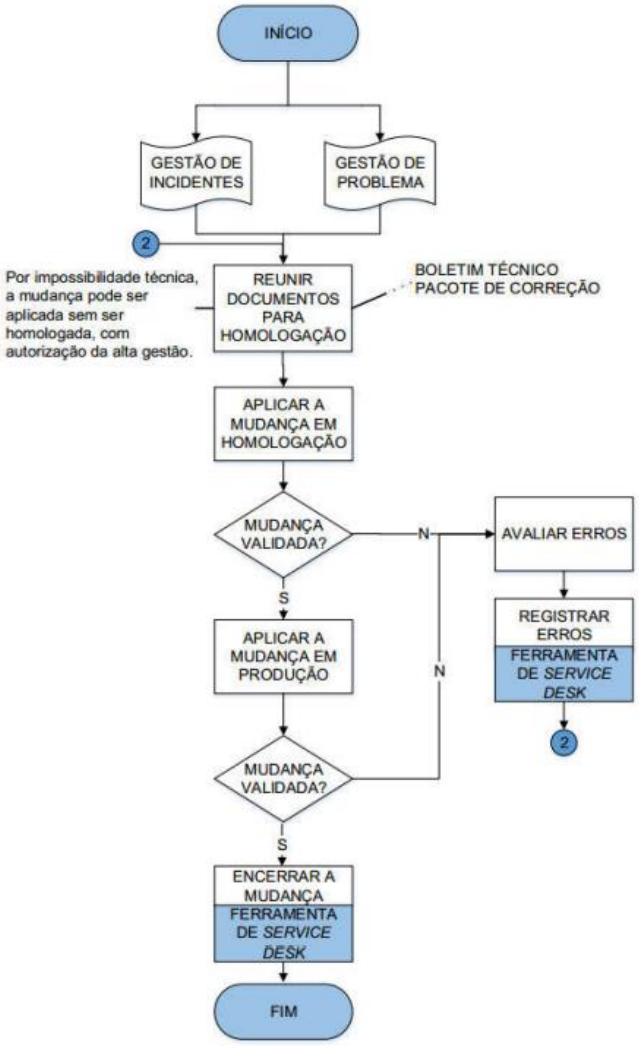
Fonte: Elaine (2008, p. 43)

A Figura 1 representa o fator humano que na maioria das vezes se torna o tornozelo de Aquiles de muitas empresas, afetando um sistema inteiro de rede de computadores ou literalmente a operação completa daquele ambiente. Em redes de computadores e sistemas empresariais diversos há a necessidade constante de treinamento pessoal e da equipe como um todo, não há sentido em investir puramente em ferramentas de última geração para proteção dos seus ativos sendo que basta um engenheiro social ligar no setor alvo e conseguir praticamente o acesso completo a uma parte de sua infraestrutura que estava totalmente “protegida”. “Todos que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadados a sofrer da chamada ilusão da segurança”, segundo MITNICK e SIMON (2003).

Políticas de segurança, planejamento de mudanças e treinamento de colaboradores são vários conceitos atuais que englobam o termo segurança da informação. Uma empresa sem normas de segurança e padrões implementados em projetos estará cada vez mais perto de um incidente ao triangulo base denominado CID. Assim afirma, “As políticas de segurança da informação são, via de regra, apresentadas como códigos de conduta aos quais os usuários dos sistemas computacionais devem se adequar integralmente.” (MARCIANO e LIMA-MARQUES, 2006).

Planejamento de mudanças é um conceito relativamente ligado ao tema segurança da informação, que faz parte também de políticas de segurança englobadas em rede de computadores. Também conhecida por Gestão de Mudanças (GMUD) normalmente aplicado ou regulado pelo setor de governança de uma empresa responsável por promover, atualizar e executar as diretrizes (FREITAS, 2017, p. 68).

Figura 2 – Gerenciamento de Mudanças (GMUD)



Fonte: Pablo Gulias Rufino de Freitas (2017, p.68)

De acordo com a Figura 2 apresentada é notório uma certa relação de segurança do processo que conecta ao conceito de segurança da informação,

nenhuma mudança acontece na empresa sem o aval de um comitê preparado para entender a demanda e aprovar ou não essa mudança. (FREITAS, 2017, p. 68)

Segundo o próprio Freitas (2017, p.68) há as validações dos processos apresentados nessa figura que consistem em garantir a entrega de qualidade daquela mudança e que não haja impacto na operação em produção.

Como observado anteriormente nas várias citações dos autores, a segurança da informação engloba um aspecto geral em torno de segurança de dados, segurança do processo e segurança comportamental. Toda essa magnitude de conceitos é aplicada diretamente ao funcionamento ideal de uma rede de computadores, totalmente escalável e transversal, pois o termo computadores pode ser visto até de uma forma virtualizada, um conceito usado e aplicado em redes corporativas. (GHANNOUM; RODRIGUES,2018).

A apresentação ao mundo do conceito de virtualização de computadores gerou uma demanda enorme de novos conhecimentos e novas técnicas de funcionamento de uma operação inteira de uma empresa, aquilo antes chamado redes de computadores também pode ser chamado de redes de computadores virtualizados. Segundo Lopes et al. (2009 apud HANSEN, 2016, p. 91) existem diversas topologias de redes, mas o modelo de rede cliente/servidor se destaca em relação aos outros.

Computadores virtualizados podem ser denominados máquinas virtuais:

> Basicamente, as máquinas virtuais podem ser implementadas como uma aplicação de um sistema operacional e executarem em modo usuário, ou serem uma camada de software posicionada entre o hardware da máquina e o sistema operacional. (ALEXANDRE CARISSIMI, 2016, p. 175).

Como toda tecnologia nova, há seus novos recursos. Há quatro conceitos de virtualização que podem ser aplicados no tema de segurança de informação (LAUREANO; MAZIERO, 2008):

- Isolamento: Todo ambiente virtual precisa de uma divisão entre a camada real do hardware e os sistemas hospedados, diga-se máquinas virtuais. Com isso aplicado há uma camada de segurança que faz parte da tríade CID, provendo assim a confidencialidade dos dados (LeVasseur et al. 2004).

- Controle de recursos: Com o hipervisor (monitor de máquinas virtuais) é possível adquirir informações sobre acessos e registros de qualquer modificação no sistema ou em alguma máquina virtual em específico (Dunlap et al., 2002).

- Inspeção: O hipervisor tem uma capacidade de análise de informações das máquinas virtuais podendo elas serem um laboratório para estudos de vírus, técnicas de invasão atuais, praticamente um ambiente de laboratório (Laureano et al., 2007).

- Encapsulamento: Antes de realizar algum procedimento considerado perigoso ou com um nível de mudança drástica àquela máquina virtual pode ser feito um ponto de restauração para caso aconteça algo ser feito o rollback, praticamente um backup do estado da máquina antes das próximas alterações (XU, 2005).

O mundo da segurança da informação é baseado, sustentado e alimentado por esses conceitos atuais de virtualização. Um sistema operacional usado no mundo de profissionais de segurança da informação seria o Linux, através desse sistema de código aberto existem muitas possibilidades de estudos, aplicações e até simulações do mundo real, utilizado em testes de penetração autorizados previamente pela empresa que contratou o serviço para identificar se existe alguma vulnerabilidade a ser corrigida (SANTOS, 2015, P. 16). Segundo Santos (2015) a distribuição oferece recursos suficientes para que empresas de pequeno e médio porte encontrem as vulnerabilidades que seus sistemas podem apresentar.

Há uma relação de segurança, desempenho, processo e tecnologias novas, onde um sempre precisa estar alinhado com o outro, os conceitos atuais de segurança da informação englobam um aspecto homogêneo de todos esses tópicos e citações mencionadas acima (MAYER; FAGUNDES, 2010).

3. TÉCNICAS APLICADAS EM SEGURANÇA DA INFORMAÇÃO

É notório que existem várias técnicas das mais simples a até aquelas mais avançadas que necessitam de um conhecimento vasto e experiencia na área de cyber segurança. As principais ameaças virtuais são muito extensas, mas há quatro tipos delas bem comuns:

- Malware: Capaz de infectar um dispositivo ou até uma rede complexa de computadores comprometendo o funcionamento operacional e derrubando os pilares CID.
- Phishing: Comumente usados em ataques fraudulentos principalmente quando o meio de comunicação usado é o e-mail onde o criminoso consegue ludibriar a vítima com ofertas, links maliciosos com malware e tantas outras coisas.
- DDoS: Ataques que consistem em derrubar um dos pilares essenciais do CID, a Disponibilidade. Com esse tipo de técnica aplicada de forma conjunta e sistemática um grupo de pessoas ou até uma pessoa consegue derrubar um sistema ou site apenas com conhecimentos técnicos e desenvoltura social.
- Zero-day: Um dos meios mais perigosos de ataque pois é aquela falha descoberta recentemente em algum sistema, aplicação ou na rede de uma empresa. Várias empresas ocorreram em vazamento de dados por causa dessas falhas.

O conceito de um malware na prática é definido segundo Silva (2004, p.30) quando um vírus denominado trojan se instala no sistema coletando senhas digitadas com logs de endereço IP e depois enviando para um servidor destino onde se encontra o criminoso do outro lado.

Esse criminoso é normalmente chamado de hacker pois seria aquela pessoa que tem muito conhecimento da tecnologia capaz de se beneficiar em prol da falha da outra pessoa. Ele adquiriu um certo tipo de informação e com ela define o que fazer, mas muitas vezes se volta para o lado criminoso.

Há um conceito quase parecido com hacker, mas que na verdade seria o Cracker, segundo Oliveira (2006, p.49) a intenção do cracker é destruir, conseguir sempre algo para benefício próprio e caso não fique satisfeito ele irá prejudicar ainda mais a vítima sempre olhando para o lado individualista e criminoso do ser.

A definição de Phishing é bem escrita segundo Gomes (2009, p.1) é um termo usado para descrever ataques informáticos. Através de e-mail seu atacante consegue adquirir informações muitas vezes importante que através de conhecimento técnico consegue aplicar os dados obtidos para um benefício próprio ou conduzir a vítima a lhe dar mais acessos específicos ao sistema atacado.

Ataques usando DDoS (Distributed Denial-of-Service) normalmente quando não mitigados causam estragos e as vezes parada total do serviço ou aplicação alvo. Como dito por Oliveira et al. (2007) “Estes ataques são caracterizados pelo envio indiscriminado de pacotes e requisições a um determinado alvo, visando degradar a qualidade ou tornar completamente indisponíveis os serviços oferecidos pela vítima.

Um DoS feito de forma distribuída, ou seja, tornando um DDoS é capaz de derrubar muitas técnicas de defesas de várias empresas e ou sistemas. A internet a todo momento é inundada de requisições e ataques desse tipo. Existem vários websites capazes de rastrear movimentações maliciosas e duvidosas em tempo real e um deles seria o cybermap.kaspersky.com que com maestria consegue nos apresentar uma técnica comum utilizada em ataques de negação de serviço (DoS). O site consegue mapear o BAD (Botnet Activity Detection) que consegue demonstrar vários dados e informações acerca de redes infectadas por Botnet e servidores C & C (Command e Control) e a fonte desses dados fazem parte da arquitetura de proteção DDoS do produto Kaspersky.

É perceptível notar que quanto mais técnicas surgem de ataque, mais técnicas de defesas precisam ser desenvolvidas para parear a batalha. É uma guerra constante travada vinte e quatro horas por dia na internet.

É fato que a maioria dessas técnicas usam muitas vezes a internet oculta denominada deep web ou dark web, um dos objetivos principais de criminosos usarem essa internet se deve ao fato de ser quase sempre um acesso anônimo, ou seja, você mantém sua identidade oculta assim como é a rede da deep web. O rastreamento em troca de informações praticamente não é executado como na surface web que na verdade é a internet que a maioria da população conhece. A dark web é praticamente

uma faca de dois gumes, como diz SANTOS (2013) “Na Deep Web quem escolhe o que buscar depende de cada um, se a pessoa buscar
conteúdo criminoso ela vai encontrar”.

A deep web apesar de ser dita como não rastreável e totalmente anônima acaba entrando em um pouco de contradição pois órgãos governamentais com suas policias federais estão sempre tentando encontrar criminosos de alto escalão através de ferramentas exclusivas de instituições como NSA e FBI, um caso famoso seria do website Silk Road que vendia drogas através da deep web que foi derrubado através de técnicas não reveladas pelo FBI e uma conhecida no mundo da informação da segurança, engenharia social.

De acordo com SANTOS (2018) “Dois clientes do site ameaçaram divulgar informações sobre seus usuários. Aliás, um deles era ex-funcionário do Silk Road.” Com isso dito é notório que engenharia social é uma das técnicas mais perigosas aplicadas na área de segurança da informação.

A engenharia social é citada por Rosa et al. (2012) “[...]é a aplicação de conhecimentos empíricos e científicos de um modo sociável de acordo com as necessidades humanas para obter informações. Muitas vezes aplicada de forma simples e nada ofensiva, um exemplo comum é quando uma pessoa com intenções secundarias liga para uma atendente de alguma empresa solicitando algum tipo de informação até então sem valor para a atendente, mas com muito mais valor técnico para quem ligou.

Através dessas técnicas sociais de persuasão muitos criminosos praticam e conseguem obter resultados devastadores para várias empresas e pessoas. Lembrando que dados e informações são coisas muito valiosas, quanto mais dado um cracker consegue adquirir talvez mais longe ele irá chegar.

Citando outro exemplo de engenharia social comum e até muitas vezes despercebido de acordo com Viana et al. (2018) um pen-drive é encontrado por um funcionário no chão e esse mesmo funcionário acaba levando o pen-drive para a empresa e inserindo o mesmo em algum computador ou dispositivo com acesso a internet e com acesso direto a rede interna do local. Algo inconcebível em segurança da informação seria colocar qualquer pen-drive duvidoso em algum dispositivo principalmente se esse for de propriedade da empresa onde a pessoa trabalha. É por isso que muitas vezes várias empresas conseguem adotar políticas de permissões de

usuários em que um simples controle de acesso talvez possa impedir uma invasão partindo de dentro da empresa.

Uma técnica utilizada em segurança da informação para impedir que muitas vezes esses fatos aconteçam é quando uma empresa contrata um serviço profissional em testes de segurança, denominados Pentesters que significa testadores de invasões ou melhor dizendo de forma não literal, profissionais de cibersegurança.

Amplamente utilizado em várias empresas, a técnica de testar se sua infraestrutura está completamente segura é uma estratégia preventiva, é a empresa realizando um processo de “prevenção de acidentes”, mas na parte lógica e estruturada de redes.

Um dos principais protocolos recomendados em segurança de website seria a implementação do HTTPS como diz KREUTZ (2020) “O HTTPS é essencial para garantir a segurança das comunicações que utilizam o protocolo HTTP na Internet.” Através de um website sem o protocolo de segurança implementado uma equipe contratada de pentesters consegue facilmente derrubar a integridade e a confidenciabilidade daquele sistema.

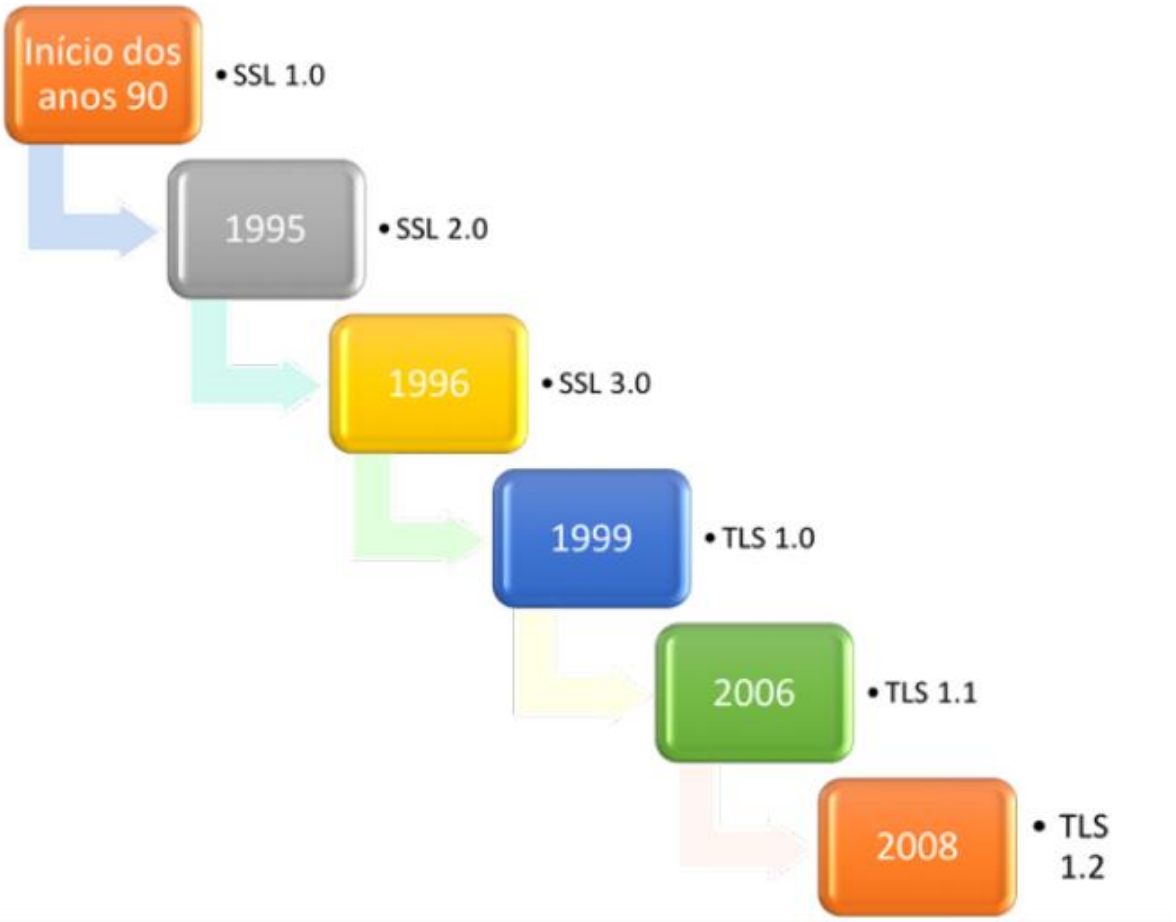
Segundo Gaspar (2021) “O protocolo https é uma forma de proteger a comunicação entre dois sistemas, como servidor e navegador. Ele permite o trânsito de dados confidenciais, como números de cartão de crédito, informações bancárias e credenciais de login.”

Muitas vezes protocolos de segurança conseguem mitigar ataques que normalmente poderiam ser evitados, a implementação do HTTPS em servidores web é praticamente obrigatório, com o tempo várias técnicas de invasão são implementadas assim como várias implementações de segurança são atualizadas.

A segurança aprimorada dos protocolos de criptografia que compõe o funcionamento do HTTPS precisou se atualizar com o tempo, citando DIAS (2016) “A confidencialidade e a integridade dos dados são um requisito fundamental aquando o envio de informação sensível e ao longo dos tempos, os protocolos SSL/TLS sofreram atualizações”.

O protocolo SSL (Security Socket Layer) foi um dos primórdios na segurança web, com ele se iniciou o passo para uma maior integridade dos ambientes expostos na rede.

Figura 3 - Versões do SSL/TLS



Fonte: Dias (2016, p. 10)

Analisando a Figura 3 é perceptível a necessidade de evolução dos protocolos, à medida que o tempo passou foi necessário até a mudança de nomenclatura da tecnologia. Na imagem não consta, mas existe também o TLS (Transport Layer Security) 1.3 considerado o mais seguro e com vulnerabilidades quase não conhecidas.

Os protocolos citados acima são integrados com a ideia básica de criptografia, você tem uma chave e o outro lado da comunicação tem outra chave que só funciona quando a sua chave em específico bate com a original, tudo acontece de forma instantânea e transparente.

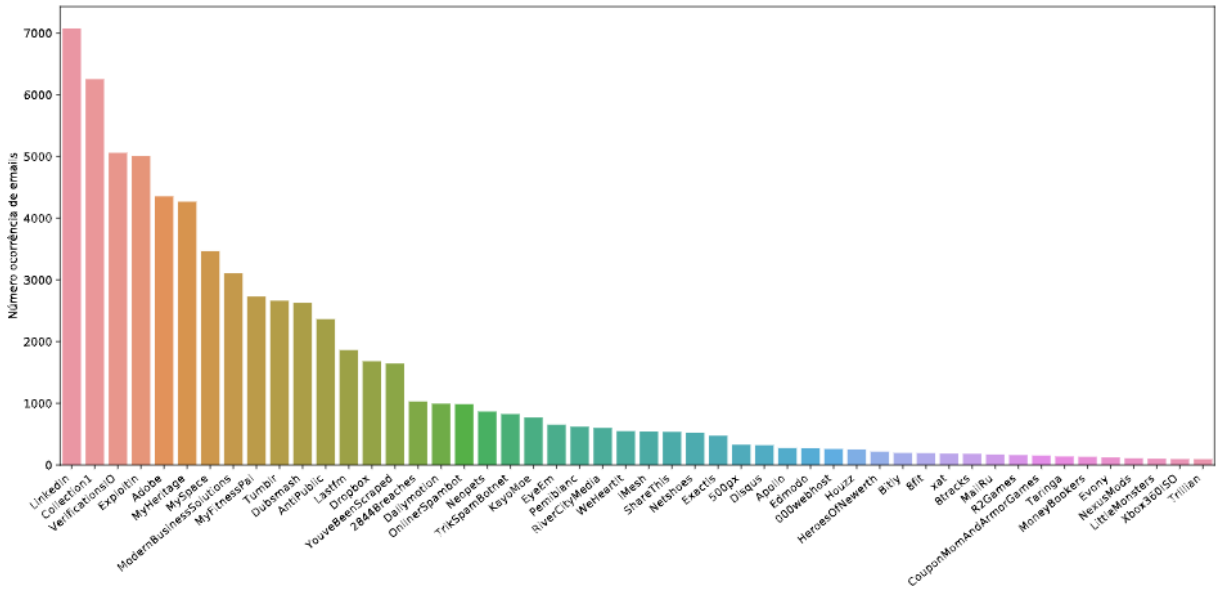
É importante mencionar que apesar de todos os protocolos de segurança citados, nenhum sistema é cem por cento seguro!

4. VAZAMENTO DE DADOS E AMEAÇAS CONSTANTES

A percepção de segurança é bem superficial, a sensação quando algo que não devia acontecer acontece é desafiadora, existem diversas ameaças virtuais que tem a capacidade de realizar um estrago jurídico e de valor de dados sem precedentes.

A capacidade de proteção dos dados muitas vezes não é compreendida ou investida, de acordo com Castro et al. (2019) “Infelizmente, os dados dos usuários nem sempre são tratados e armazenados levando em consideração aspectos de segurança e privacidade.” A pessoa que tem seus dados violados muitas vezes não fica sabendo e quando sabe já é tarde demais. Mostrando em gráfico, é perceptível a quantidade assustadora de pessoas que tem seus e-mails expostos na internet:

Figura 4 - 50 maiores vazamentos do conjunto de 50.664 e-mails



Fonte: Castro et al. (2019, p. 3)

Mostrado os dados da Figura 4 pode-se concluir que o nível de vazamento de dados das empresas é assustador e perceptível. A sensação de insegurança é tão grande que existe um site para descobrir se os seus dados foram vazados ou não, nele você consegue inserir o seu e-mail e descobrir se ele foi compartilhado em algum vazamento de dados de alguma empresa que continha suas informações no banco de dados dela.

Com ferramentas e mecanismos de segurança conseguimos descobrir se algum dado pessoal ou até empresarial ou governamental foi vazado. Conseguimos através do Avast Hack Check que notifica por email os usuários quando suas senhas, utilizadas nos mais diversos tipos de sites e sistemas online, são vazadas Castro et al. (2019). Outra ferramenta comum é chamada de Have I Been Pwned, ou seja, traduzindo de forma literal, “eu fui humilhado?” sabendo assim se seu e-mail ou senha foi exposta para a internet de forma indevida.

Ameaças virtuais se tornaram cada vez mais reais e com isso técnicas de proteção a essas ameaças foram desenvolvidas para acompanhar o processo, por exemplo o dispositivo denominado firewall criado com a função de impedir comunicação indevida da rede externa com a rede interna (ZOREK; FONTANA, 2022).

Segundo Maneca (2015) devido à complexidade dos sistemas de ataques cibernéticos o firewall tradicional já não basta para proteções eficazes, nos últimos tempos foi usado de forma essencial, mas é preciso um foco total na parte de segurança, com isso foi criado o Next Generation Firewall (NGFW).

A aplicação do NGFW foi necessária devido a ameaças internas, ou seja, além das ameaças externas que o firewall tradicional normalmente conseguia subtrair. Tornou-se cada vez mais necessário a vigilância da rede interna para evitar ataques como engenharia social ou até permissões concebidas indevidamente ao usuário (MANECA, 2015, P. 1).

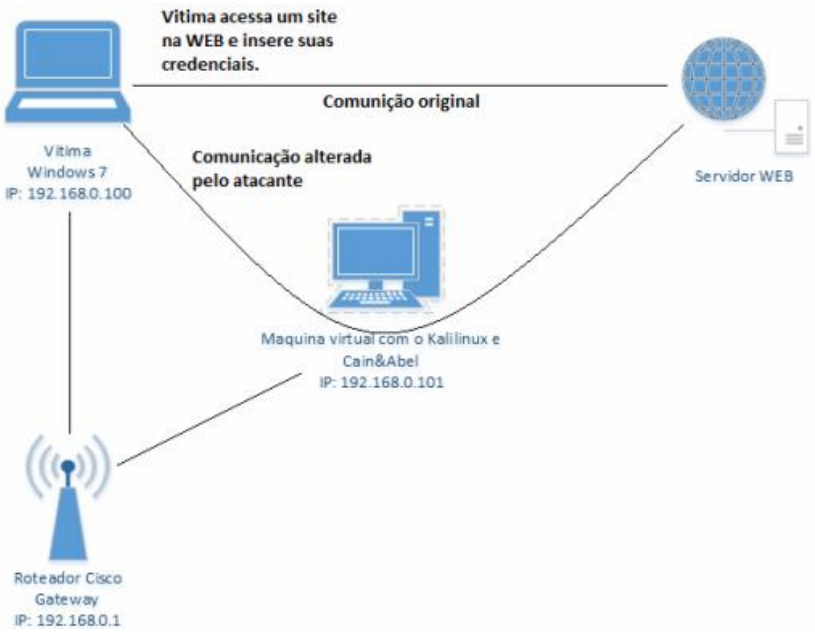
O conjunto de técnicas NGFW é tão extenso que um firewall como o da fabricante Fortinet conta com os mais diversos tipos de proteção e tecnologias capazes de mitigar ameaças constantes em qualquer sistema ou rede computacional. Segundo Fortinet (2021) seus firewalls contém: Secure Hybrid Multi-Cloud, Prevent Lateral Spread, Manage Vulnerabilities, Protect Users, Secure Hyperscale e Secure Industrial and OT Environments. São tecnologias que previnem vulnerabilidades através da sua rede conectada na nuvem, mitigação de ameaças internas que impedem o seu lastro pela rede interna, proteção contra vulnerabilidades não conhecidas, proteção a riscos constantes de vírus tanto da rede externa quanto na rede interna entre diversos outros tipos de proteções que tentam ao máximo barrar as ameaças constantes do mundo cibernético (FORTINET, 2022).

Com a definição do firewall tradicional e o Firewall NGFW é importante salientar que ambos trazem a definição de segurança, mas a ideia por trás do NGFW é tentar alcançar a excelência se tratando de vulnerabilidades recentes.

A prevenção do Firewall NGFW da Fortinet em relação a vazamento de dados funciona através da inspeção do módulo DLP que fiscaliza e monitora os pacotes de redes trafegados na rede interna onde está instalado, caso haja dados considerados maliciosos ao mesmo tempo é feito o bloqueio e ainda dá a possibilidade de verificar como tudo aconteceu através de logs (FACHINELLI; AHLERT, 2019).

Através de mecanismos do mundo cibernético é possível uma extração de dados por meio de alguma vulnerabilidade explorada, uma ameaça constante e explorada de forma recorrente é denominada SQL Injection, que por meio de inserção de códigos voltados para a aplicação do banco de dados é possível extrair algum tipo de informação ou até burlar uma das técnicas mais cruciais na proteção de um sistema, a autenticação do usuário (COSTA et al., 2018). Uma injeção SQL bem executada pode levar a um vazamento de dados irreparáveis ao sistema.

Figura 5 – Ambiente configurado para realizar o ataque MITM



Fonte: Botti et al. (2015, p. 9).

Uma outra ameaça enfrentada corriqueiramente no ambiente cibernético é chamada de Man In The Middle (MITM) abordada na Figura 5 em que nem sempre

o dado que sai do ponto A chega da forma idônea ao ponto B, as vezes ela até chega, mas com dados adulterados (BOTTI et al., 2015).

É possível citar um exemplo de MITM fora das redes em uma situação hipotética quando um carteiro recebe uma carta, mas antes de transmiti-la ele faz a leitura da mesma ou até substitui seu conteúdo, ou seja, adulterando a mensagem original (GANGAN, 2015, P.3).

Existem quatro principais causas para ocorrer o ataque de MITM segundo Gangan (2015), sendo eles:

- ARP Cache Poisoning
- DNS Spoofing
- Session Hijacking
- SSL Hijacking

O envenenamento de cache do protocolo ARP pode ser facilmente atacado quando um computador A tenta comunicar com outro computador B e começa a trocar informações, pois o protocolo ARP se trata de como os dispositivos devem se comunicar, com uma tabela de identificação de cada dispositivo que se atualiza constantemente, se existe um intermediador externo com capacidade de alterar quem é o dispositivo A ou B, ele consegue gerar uma informação falsa conseguindo assim captar a mensagem trafegada entre os dispositivos (GANGAN, 2015, P.3).

Uma ameaça recorrente do MITM se refere ao DNS Spoofing em que o atacante consegue realizar uma resposta ao dispositivo atacado de forma adulterada e quando a vitima realiza uma conexão com algum site legitimo na verdade por causa desse ataque a vitima foi desviada ou redirecionada para o site do atacante onde o mesmo tem controle totalmente da aplicação, causando assim vazamento de dados pois toda informação inserida naquele site na verdade estará indo para o agente principal do MITM (GANGAN, 2015, P.4).

A transmissão do pacote de dados por uma rede é definida pelo Transmission Control Protocol (TCP) que permite estabelecer a conexão, transferir as informações e finalizar aquela comunicação, esse processo é denominado de 3-way handshake. Quando é feito uma interceptação dessa comunicação através do sequestro de

sessão dessa comunicação principal há então a captura de informações (GANGAN, 2015, P.5).

Sobre a quarta ameaça denominada sequestro de SSL é notório a capacidade de quebra de segurança e confidenciabilidade de um sistema, segundo Silva (2019) essa ameaça é utilizada para roubo de informações em comunicações HTTPS entre cliente e servidor, quando o cliente tenta abrir um site em HTTP normalmente nas configurações do web server existe um certo tipo de redirecionamento para HTTPS e seria através desse redirecionamento que a interceptação ocorre ocasionando todo o processo de MITM pois o atacante estaria interceptando as mensagens antes de chegar ao servidor web legitimo.

O desenvolvimento de uma ameaça normalmente depende de outra já explorada, uma situação A só chega em B através da falha número um da situação A, ou seja, apenas uma brecha de segurança pode levar a várias outras segundo Silva (2019) uma interceptação SSL é conduzida através do envenenamento do protocolo ARP conseguindo assim uma abordagem total do ataque inicial.

Ameaças cibernéticas deixam rastros e para uma possível análise inicial é comum identificar alguns aspectos segundo Aquilina et al. (2008, p.285) quando a origem de um processo sendo executado no computador levanta suspeitas ou quando o processo não é conhecido ou quando algum arquivo conhecido pelo sistema está localizado em lugar diferente do normal ou na etapa final quando um processo já foi classificado como possível ameaça e depois é categorizado em outras etapas de análise do sistema alvo.

É importante ressaltar que existem inúmeras formas de um sistema ou uma rede complexa de computadores ser atacada e sofrer com os efeitos como um grande vazamento de dados que ocorre na maioria das vezes que uma ameaça deixa de ser ameaça e se torna uma realidade ou incidente, segundo Sousa (2022) tais ameaças podem causar transtornos e possíveis processos judiciais uma vez que a Lei Geral de Proteção de Dados (LGPD) determina como os dados devem ser tratados e lidados.

5. CONSIDERAÇÕES FINAIS

Com o desenvolvimento desse trabalho foi possível encontrar diversas situações em que uma rede de computadores é vulnerável ao ponto de impactar diversos tipos de operações de um sistema. A criticidade da segurança da informação ser bem implementada demanda cada vez mais urgência e detalhe técnico.

Através do aprendizado conceitual foi possível entender as demandas que circundam o termo segurança da informação, se faz cada vez mais necessário uma abordagem ampla quando se trata de segurança cibernética e normas e boas práticas cada vez mais rebuscadas tentando sempre contornar qualquer problema de falha de segurança

Analisado os protocolos de segurança e técnicas mais usados em segurança da informação no lado do atacante e do lado do defensor no mundo cibernético pois através deles é alcançado um certo tipo de estabilidade virtual por meio da aplicação das diretrizes da segurança da informação e mostrado também algumas técnicas comumente usados por pessoas criminosas.

Apresentado de forma gradual os impactos e ameaças causadas por fatores externos de pessoas com conhecimento técnico avançado em falhas de segurança e como explorara-las e com isso analisado algumas formas que tentam ao máximo mitigar vazamento de dados e tentar conter as ameaças constantes do mundo virtual muito semelhante ao mundo natural, onde existem a presa e o predador.

É notório uma abordagem mais próxima de como ainda assim mesmo com todas as técnicas de segurança e empresas que sempre visam o poder do investimento na defesa de sua infraestrutura acabam sucumbindo a uma grande falha de segurança tornando cada vez mais difícil a procura de profissional qualificado para conter essas falhas e impedir cada vez mais a propagação de vetores maliciosos.

REFERÊNCIAS

FONTES, Goncalves. **Segurança da Informação O usuário faz a diferença:** Books Google, 2010. Disponível em: books.google.com.br/books?id=FyprDwAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false. Acesso em: 10 set. 2022.

SILVA, Elaine. **Cuidado com a engenharia social**: Saiba dos cuidados necessários para não cair nas armadilhas dos engenheiros sociais. [S.l.:s.n.], 2008. Disponível em: monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm. Acesso em: 5 out. 2022.

MARCIANO, João; LIMA-MARQUES, Mamede. **O enfoque social da segurança da informação**. Disponível em: < https://www.scielo.br/j/ci/a/L8CqcznptmQK3jyqGqNpWMQ/?format=pdf&lang=pt/>. Acesso em: 26 set.2022.

FREITAS, Rufino. **SEGURANÇA DA INFORMAÇÃO E QoS NA GESTÃO DE REDES DE TELECOMUNICAÇÕES EM CONFORMIDADE COM ITIL**, 2017. Disponível em: repositorio.sis.puc-campinas.edu.br/bitstream/handle/123456789/15035/ceatec_ppggrt_me_Pablo_GRF.pdf. Acesso em: 10 set. 2022.

GHANNOUM, Rodrigo; RODRIGUES, Fábio. **Virtualização de Servidores: Vantagens e Desvantagens**. Disponível em: < https://www.praxia.ueg.br/index.php/mirante/article/view/7612/5329/>. Acesso em: 27 set.2022.

ALVES, Cássio. **Segurança da Informação vs. Engenharia Social - Como se proteger para não ser mais uma vítima.** Disponível em: < https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm/>. Acesso em: 26 set.2022.

Agência Nacional de Telecomunicações. **Segurança Cibernética**. Disponível em: < https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/>. Acesso em: 26 set.2022.

TORRES, Fábio. **Conceitos e Princípios da Segurança da Informação**. Disponível em: < https://www.academia.edu/download/58865183/Mauricio_Rocha_Lyra_-_Governanca_em_Sistemas_de_Informacao20190411-64661-pjz4gt.pdf/>. Acesso em: 29 out.2022.

MITNICK, Kevin; SIMON, William. **A Arte de Enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da informação. São Paulo: Pearson, 2003.

LOPES, Leo et al. **Utilização de Ambientes Virtualizados para Ensino de Servidores de Redes de Computadores**. Disponível em: < http://ojs.sector3.com.br/index.php/sbie/article/view/6689/>. Acesso em: 12 out.2022.

CARISSIMI, Alexandre. **Virtualização: da teoria a soluções**. Disponível em: < https://www.gta.ufrj.br/ensino/CPE758/artigos-basicos/cap4-v2.pdf/>. Acesso em: 12 out.2022.

LAUREANO, Marcos et al. **Protecting host-based intrusion detectors through virtual machines**. Disponível em: < https://www.sciencedirect.com/science/article/abs/pii/S1389128606002428/>. Acesso em: 30 out.2022.

LEVASSEUR et al. **Unmodified Device Driver Reuse and Improved System Dependability via Virtual Machines**. Disponível em: < https://www.usenix.org/legacy/publications/library/proceedings/osdi04/tech/full_papers/levasseur/levasseur.pdf/>. Acesso em: 30 out.2022.

DUNLAP et al. **ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay**. Disponível em: < https://people.eecs.berkeley.edu/~kubitron/courses/cs262a-F14/handouts/papers/dunlap02.pdf/>. Acesso em: 30 out.2022.

XU, Cheng-Zhong. **Scalable and Secure Internet Services and Architecture**. Disponível em: < https://www.taylorfrancis.com/chapters/mono/10.1201/9781420035209-18/service-migration-recon%EF%AC%81gurable-distributed-virtual-machines-cheng-zhong-xu/>. Acesso em: 30 out.2022.

SANTOS, Andréia. **Análise de Vulnerabilidade em Rede, com Teste de Intrusão Utilizando a Distribuição Kali Linux**. Disponível em: < https://releia.ifsertao-pe.edu.br/jspui/bitstream/123456789/352/1/TCC%20-%20AN%c3%81LISE%20DE%20VULNERABILIDADE%20EM%20REDE%2c%20COM%20TESTE%20DE%20INTRUS%c3%83O%2c%20UTILIZANDO%20A%20DISTRIBUI%c3%87%c3%83O%20KALI%20LINUX.pdf/>. Acesso em: 12 out.2022.

MAYER, Janice; FAGUNDES, Leonardo. **Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação**. Disponível em: < https://sol.sbc.org.br/index.php/sbsi/article/view/14696/14541/>. Acesso em: 30 out.2022.

SILVA, Felipe. **Uma Abordagem Sobre Técnicas de Invasão de Computadores**. Disponível em: < https://ri.unipac.br/repositorio/wp-content/uploads/2019/08/Felipe-Lu%C3%ADs-da-Silva.pdf/>. Acesso em: 12 out.2022.

OLIVEIRA, Roberto. **Tópicos de Segurança da Informação**. Disponível em: < https://books.google.com.br/books?hl=pt-BR&lr=&id=E7C2DwAAQBAJ&oi=fnd&pg=PT4&dq=protocolos+de+seguran%C3%A7a+da+informa%C3%A7%C3%A3o/>. Acesso em: 12 out.2022.

GOMES, Vanessa. **A Engenharia Social e os Perigos do Phishing**. Disponível em: < https://www.proquest.com/openview/98e73333a91d01bced5e59ac0f07081a/>. Acesso em: 22 out.2022.

OLIVEIRA, Luis et al. **Avaliação de Proteção contra Ataques de Negação de Serviço Distribuídos (DDoS) utilizando Lista de IPs Confiáveis**. Disponível em: < https://sol.sbc.org.br/index.php/sbseg/article/view/20926/20752/>. Acesso em: 25 out.2022.

KASPERSKY. **Ciberameaça Mapa em Tempo Real**. Disponível em: < https://cybermap.kaspersky.com/>. Acesso em: 09 out.2022.

SANTOS, Carlos; MARCHI, Késsia. **O Que a Deep Web Pode Oferecer Além da Surf**. Disponível em: < https://www.academia.edu/download/38756570/Carlos_Henrique_Aguiar_dos_Santos.pdf/>. Acesso em: 25 out.2022.

SANTOS, Luiz. **Deepweb: Anonimato?** Disponível em: < http://ebrevistas.eb.mil.br/OC/article/view/1751/1439/>. Acesso em: 25 out.2022.

ROSA, Adri et al. **Engenharia Social**: O Elo Mais Frágil da Segurança nas Empresas. Disponível em: < https://www.revistas.udesc.br/index.php/reavi/article/view/2840/2172/>. Acesso em: 25 out.2022.

VIANA, Mayara; PÉTTA, Wendel. **Vulnerabilidades invisíveis**. Disponível em: < http://ric.cps.sp.gov.br/bitstream/123456789/3285/1/20182S_VIANAMayaraTattielenSilva_OD0578.pdf/>. Acesso em: 25 out.2022.

KREUTZ, Diego et al. **Uma Análise da Utilização de HTTPS no Brasil**. Disponível em: < https://sol.sbc.org.br/index.php/sbrc/article/view/12338/12203/>. Acesso em: 27 out.2022.

GASPAR, Larissa. **O que é HTTPS e quais são suas vantagens?** Disponível em: < https://www.hostgator.com.br/blog/o-que-e-protocolo-https/>. Acesso em: 27 out.2022.

DIAS, Filipe. **Estudo de Segurança dos Protocolos SSL/TLS**. Disponível em: < https://core.ac.uk/download/pdf/302870637.pdf/>. Acesso em: 27 out.2022.

CASTRO, Ariel et al. **Os Meus Dados de Fato Vazaram? Uma Análise de Serviços que Monitoram Vazamentos de Dados na Internet**. Disponível em: < https://sol.sbc.org.br/index.php/errc/article/view/9232/9135/>. Acesso em: 28 out.2022.

ZOREK, Ricardo; FONTANA, Fabiane. **Segurança em Redes: Rede Desmilitarizada com Firewall pfSense e Aker**. Disponível em: < https://www.fag.edu.br/upload/revista/tech-magazine/Artigo%20Ricardo%20Zorek%20.pdf/>. Acesso em: 30 out.2022.

MANECA, Miguel. **Firewalls, A Próxima Geração**. Disponível em: < https://docplayer.com.br/24066383-Firewalls-a-proxima-geracao.html/>. Acesso em: 30 out.2022.

Fortinet. **Next-Generation Firewall (NGFW)**. Disponível em: < https://www.fortinet.com/products/next-generation-firewall.htm/>. Acesso em: 30 out.2022.

FACHINELLI, Mateus; AHLERT, Edson. **Firewall de Próxima Geração - Fortinet**. Disponível em: < http://www.meep.univates.br/revistas/index.php/destaques/article/view/2385/>. Acesso em: 30 out.2022.

COSTA, Pablo et al. **Nível de conhecimento de desenvolvedores sobre segurança em aplicações web: Pesquisa e análise**. Disponível em: < https://sol.sbc.org.br/index.php/ersi-rj/article/view/4661/4578/>. Acesso em: 31 out.2022.

BOTTI, Caio; MARTINS, Márcio. **Análise comparativa entre ferramentas de ataque Main in the middle**. Disponível em: < http://seer.uniacademia.edu.br/index.php/cesi/article/view/517/400/>. Acesso em: 31 out.2022.

GANGAN, Subodh. **A Review of Man-in-the-Middle Attacks**. Disponível em: < https://arxiv.org/ftp/arxiv/papers/1504/1504.02115.pdf/>. Acesso em: 2 nov.2022.

SILVA, Carlos. **Análise de Vulnerabilidades em Redes Wireless: Proposta de Soluções para Ataques do Tipo MITM (Man-in-the-Middle)**. Disponível em: < https://repositorio.uema.br/bitstream/123456789/836/1/TCC_Carlos_Adriano.pdf/>. Acesso em: 2 nov.2022.

AQUILINA, James; MALIN, James. **Malware Forensics Investigating and Analyzing Malicious Code-Syngress**. Disponível em: < https://repo.zenk-security.com/Forensic/Malware%20Forensics_%20Investigating%20and%20Analyzing%20Malicious%20Code-Syngress%20(2008).pdf/>. Acesso em: 2 nov.2022.

SOUSA, Iago. **LGPD na Proteção de Dados dos Clientes de Automação** - Responsabilidade das Empresas nas Hipóteses de Vazamento de Dados. Disponível em: < https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3829/>. Acesso em: 2 nov.2022.