PATRYCIA BARBOSA ZUCATELLI
VICTOR OLIVEIRA CALIMAN

FALHAS DE SEGURANÇA: Métodos de proteção cibernética para falha baseada no Flash Player 18

Ji-Paraná – RO.
2022

PATRYCIA BARBOSA ZUCATELLI
VICTOR OLIVEIRA CALIMAN

FALHAS DE SEGURANÇA: Métodos de proteção cibernética para falha baseada no Flash Player 18

Trabalho de Conclusão de Curso apresentada à Banca Examinadora do Centro Universitário São Lucas de Ji-Paraná, como requisito de aprovação para obtenção do Título de Bacharel no curso de Sistemas de Informação.

Orientador: Prof. Esp. José Rodolfo Milazzotto Olivas.

Ji-Paraná – RO.
2022

Dados Internacionais de Catalogação na Publicação - CIP

Z94f Zucatelli, Patrycia Barbosa.

Falhas de segurança: métodos de proteção cibernética para falha baseada no Flash Player 18. / Patrycia Barbosa Zucatelli ; Victor Oliveira Caliman. – Ji-Paraná, 2022.
37 p.

Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) – Centro Universitário São Lucas Ji-Paraná, 2022.

Orientador: Prof. Esp. José Rodolfo Milazzotto Olivas

1. Segurança da informação. 2. Vulnerabilidades. 3. Falhas de segurança. 4. Proteção contra os ataques cibernéticos. I. Caliman, Victor Oliveira. II. Olivas, José Rodolfo Milazzotto. III. Título.

CDU 004.056.53

Ficha Catalográfica Elaborada pelo Bibliotecário Giordani Nunes da Silva CRB 11/1125

RESUMO

A quantidade de crimes no Brasil tem aumentado rapidamente, boa parte deles estão evoluindo junto à tecnologia. Neste trabalho de conclusão de curso abordou-se os principais tipos de golpes e artefatos usados, como também algumas normas, recursos e meios para reduzir e proteger-se dos ataques cibernéticos, dos roubos, das adulterações e da destruição de dados essenciais. O presente trabalho tem como objetivo relatar os principais pontos sobre o tema, do mesmo modo que visa criar um ponto de partida de estudo. Será explorado alguns tipos de vírus e os seus aspectos, as falhas de segurança e vulnerabilidades. Para refletir sobre os perigos serão citados alguns casos de grandes empresas que tiveram problemas com invasões, assim como, algumas formas de proteger-se e reduzir riscos, explorando os programas utilizados e normas aplicadas para sanar essas vulnerabilidades. Será abordado as medidas de proteções básicas e avançadas contra os ataques cibernéticos destacando as maiores empresas que trabalham para oferecer aos usuários segurança cibernética.

Palavras-chaves: Segurança da informação. Vulnerabilidades. Falhas de segurança. Proteção contra os ataques cibernéticos.

ABSTRACT

The number of crimes in Brazil is increasing rapidly, most of them are evolving with technology. In this course conclusion work, will be adress the main types of scams and artefacts used, as well as some rules, resources and means to reduce and have protection against cyber-attacks, theft, tampering and destruction of essential data. The present work aims to report the main points on the subject, in the same way that it aims to create a starting point for related studies. Some types of viruses and their aspects, security flaws and vulnerabilities will be explored. To reflect on the dangers, some case studies of large companies that had problems with invasions will be mentioned, as well as some ways to get protection and reduce risks, exploring the programs used and standards applied to mitigate these vulnerabilities. Basic and advanced protection measures against cyber-attacks will be addressed, highlighting the largest companies that work to provide users with cyber security.

Keywords: Information security. Vulnerabilities. Security flaws. Protection from cyber-attacks.

SUMÁRIO

1 - INTRODUÇÃO 8
1.1– Problematização 8
1.2– Objetivos 9
1.2.1- Objetivo Geral 9
1.2.2- Objetivos específicos 9
2 - REFERENCIAL TEÓRICO 10
2.1 - Informação como recurso e bem da empresa 10
2.2 - Segurança da Informação 10
2.3 - Falhas de Segurança, seus Principais Problemas e Vulnerabilidades. 12
2.4 – O que são Falhas de Segurança. 12
2.5 – Problemas de Segurança. 13
2.6 – Vulnerabilidade 14
2.7 – PRINCIPAIS ATAQUES A SEGURANÇA DA INFORMAÇÃO 15
2.7.1 – Por negação de serviço. 15
2.7.1.1 – Consumo de Largura de Banda 15
2.7.1.2 – Consumo de Recursos 16
2.7.1.3 – Falhas de Programação 16
2.7.1.4 – Ataques de Sistemas de Nome de Domínios (DNS) ou Roteamento: 16
2.7.2 - Ataque Smurff 17
2.7.3 - Ataque INUNDAÇÃO SYN 17
2.7.4- ATAQUES DdoS 18
2.7.5 – Esgotamento do TCP 18
2.7.6 – Nas camadas de aplicativos 18
2.7.7 – Volumétricos 18
2.8 - Tipos de Malware 19
2.8.1 - VÍRUS 19
2.8.2 - PHISHING 20
2.8.3 - BOT E BOTNET 21
2.8.4 - SPYWARE 21
2.8.5 - CAVALO DE TROIA (TROJAN) 23
2.8.6 - WORM 24

2.9 – SEGURANÇA CIBERNÉTICA – SE PROTEGENDO DE ATAQUES CIBERNÉTICOS 24
2.9.1 - Segurança Cibernética. 24
2.9.2 – Medidas básicas para se proteger de invasões cibernética. 25
2.9.2.1 – Antivírus 25
2.9.2.2 – Evitar Acessos em Redes Abertas 26
2.9.3 – Vazamento de empresa hackeada revela grave vulnerabilidade no Flash 27
3-MATERIAIS E MÉTODOS 30
4 – RESULTADOS E DISCUÇÕES 31
5 - CONCLUSÃO 32
6-REFERÊNCIAS 33

1 – INTRODUÇÃO

Sabe-se que a informação deve chegar ao destino de forma rápida, eficaz e segura, mas não deve se desprezar a segurança e integridade dos dados fornecidos, a tecnologia digital se expandiu rapidamente e esse crescimento rápido se deve a popularização da tecnologia em todas as camadas sociais e econômicas, mas esse crescimento desordenado trouxe brechas que são exploradas por indivíduos com intenção de roubar, alterar e até mesmo destruir dados, na nova geração é possível vivenciar experiências diariamente, entretanto, essas experiências podem deixar de ser maravilhosas e se tornem um pesadelo para os usuários finais e empreendedores. As falhas de segurança podem ser reduzidas através de implementações de normas, conscientização dos riscos que essas falhas possuem, manutenções periódicas, estudo aprofundado de casos distintos e compreensão dos possíveis cenários no cotidiano da vida particular ou no âmbito profissional. Assim, objetiva-se abordar a temática das várias falhas de segurança e os meios que os usuários e empreendedores podem usar para restringir os acessos indesejados e reduzir as vulnerabilidades.

Também conhecida pelo termo Sociedade da Informação, a globalização representa uma formação ainda em expansão caracterizada pelo seu dinamismo, pois, as tecnologias usadas atualmente sempre estão em processo de evolução.

Tais evoluções tecnológicas influenciam diretamente no comportamento cultural, econômico e social de uma sociedade, sendo uma fonte interminável de produção de novos conhecimentos que estão enraizadas cada vez mais na sociedade, denominando-se de “Sociedade do Conhecimento”.

Milhares de pessoas de diferentes países e culturas conectaram-se umas com as outras através da internet, devido a isto, as pessoas se tornaram vulneráveis a crimes e golpes cibernéticos que podem causar danos financeiros, vazamento de dados dos clientes e informações sigilosas.

1.1 – Problematização

O processo de evolução tecnológico tem promovido o desdobramento dos crimes, conforme as tecnologias avançam os golpes acabam sendo criados ou reciclados, na era da informação, não é necessário ser um programador para cultivar

e aplicar golpes e invasões, apenas adquirir um algoritmo, um processo ou ferramentas necessárias. Tem sido cada vez mais comum o surgimento dos golpes e o número de vítimas têm crescido de forma alarmante. Uma pessoa que sofreu o golpe pode acabar expondo seus dados ou até mesmo expor as informações da empresa onde trabalha. Esse trabalho busca utilizar os conhecimentos obtidos para reduzir as vulnerabilidades e proteger as informações dos acessos não autorizados, sejam eles empresariais ou pessoais.

1.2 – Objetivos

Nesta seção serão apresentados os objetivos gerais e específicos definidos para este trabalho.

1.2.1 - Objetivo Geral

Com base nas técnicas, ferramentas e conteúdos, pretende-se apresentar um estudo sobre as falhas de segurança, vírus, métodos usados para atingir empresas e usuários e formas que são empregadas para obter informações sigilosas.

1.2.2 - Objetivos específicos

- Apresentar a variedade de métodos usados para obter informações sigilosas.
- Informar os métodos e ferramentas usados para prevenir-se e evitar vazamentos de informações pessoais ou empresariais.
- Levantar as informações sobre a falha de segurança do Adobe flash exposta em 2015 da versão 9 até 18.0 .0.194 e informar sobre o risco que o usuário final sofria.

2 - REFERENCIAL TEÓRICO

2.1 - Informação como recurso e bem da empresa

A crescente evolução tecnológica constitui oportunidades na sociedade, os dados comuns que antes eram menosprezados e apenas tratados como informações básicas, passaram a ter um valor incalculável para as empresas, permitiram tratar, quantificar, calcular e até mesmo prever situações.

Os dados passam a formar informações para empresas e a informação começa a ter valor, o conceito de informação pode ter variações, mas segundo ZORRINHO (1995, p. 32),

> "é um processo que visa o conhecimento, ou, mais simplesmente, informação é tudo o que reduz a incerteza. (...) Um instrumento de compreensão do mundo e da ação sobre ele",

A informação passa a ter não só um valor simbólico, mas toma a forma de um ativo importante para a gestão e o crescimento do negócio.

De acordo com a ISO/IEC 27001:2005 um ativo, é "qualquer coisa que tenha valor para organização". O bem da empresa pode tomar várias formas no conceito da informação como, por exemplo, contratos, acordos, documentação de sistemas manuais para os usuários, trilhas de auditorias, Banco de dados, cadastros, e no caso de algumas instituições financeiras até o sigilo bancário.

Compreendendo sobre as responsabilidades dos ativos, deve-se conceber uma classificação apurada com base na importância, criticidade, sensibilidade e o valor que possui para o negócio. Como resultado, será possível definir termos adequados para a proteção. (ABNT NBR ISO/IEC 27002: 2005)

2.2 - Segurança da Informação

Segurança da Informação é um tema abrangente, bastante debatido por estudiosos, pois trata-se de informações pessoais ou corporativa sistematizadas, que quando lançado na rede e lido ou distribuído de forma maliciosa pode causar transtornos à vítima.

Existem vários autores diferentes que dissertam sobre o assunto, vejamos algum deles:
Para Alves, a Segurança da Informação:

> “Visa proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios”. (2006, p. 15)

Entende-se que a informação é uma ferramenta de continuidade das operações da empresa, sem as informações não seria possível consultar preços rapidamente, verificar o estoque ou até mesmo fidelizar o cliente com cadastros e promoções direcionadas, todos esses aspectos visam agregam valor para a empresa.
Sêmola define Segurança da Informação como:

> “Uma Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”. (2003, p. 9)

Compreende-se que devido à informação ter valor real para empresa como ativo, deve-se dedicar uma área específica para protegê-la, pois a indisponibilidade pode causar a paralização da empresa e o acesso e alteração do conteúdo dos dados podem causar perda irreparável na imagem da empresa e prejuízos por estarem trabalhando com informação corrompida.
Para Ferreira, a Segurança da Informação:

> “Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades.“ (2003, p.162).

Em outras palavras, segurança da informação tem como objetivo proteger e assegurar-se que não haja interferências no ambiente da organização e o responsável por ela deve usar de todos os meios para garantir a estabilidade do negócio para que possa ser atingido um bom retorno dos investimentos e evitar as perdas.

Temos também a definição dada pela padronização mundial formada pela ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) Segurança da Informação é:

> "Como uma proteção das informações contra uma ampla gama de ameaças para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidade comerciais". (ISO/IEC 27001:2005)

Percebe-se que a segurança da informação deve agir como um escudo contra todos os meios que possam significar riscos para as informações da instituição, e que deve ser capaz de reduzir os detrimentos do negócio.

Além das definições dadas pelos autores e pela padronização mundial, temos o conceito criado pela norma ISO/IEC 17799, onde diz que a proteção da informação é vital, sendo caracterizada pela trilogia CID - Confidencialidade, Integridade e Disponibilidade.

2.3 - Falhas de Segurança, seus Principais Problemas e Vulnerabilidades.

Neste capítulo, será abrangido o tema Falhas de Segurança, seus principais problemas e suas vulnerabilidades.

2.4 – O que são Falhas de Segurança.

> "Uma violação de segurança é qualquer incidente que resulte em acesso não autorizado a dados, aplicativos, redes ou dispositivos de computador. O resultado é que as informações são acessadas sem autorização. Normalmente, isto ocorre quando um intruso é capaz de burlar os mecanismos de segurança." (kaspersky).

Em outros termos, qualquer acesso de informação confidencial ou sigilosa para o proprietário por meio provido de acesso não autorizado é uma violação da segurança onde o intruso conseguiu burlar os mecanismos proteção.

2.5 – Problemas de Segurança.

No que se refere a problemas de segurança, existem inúmeros fatores que ocasionam a perda e/ou violação de dados, como: má operação do sistema ou quando sua segurança está sofrendo ameaça, desastres, falhas, risco e vulnerabilidade.

Em uma rede empresarial, as ameaças são mais nítidas em um sistema, visto que as empresas utilizam recursos de telecomunicações para interligarem seus sistemas em vários setores, através de intranets[1] e extranets[2], com isto há uma grande exposição de ameaças, uma vez que todo o sistema da empresa está ligado à rede de internet, onde várias pessoas tentarão ter acesso às informações mesmo sem autorização, se houver brechas na segurança do sistema ele poderá ser invadido.

Vejamos exemplos de empresas que tiveram seu sistema de segurança invadido no ano de 2020:

- iFood – Brecha de segurança expõe dados do aplicativo;
- EasyJet – Ciberataques expõe dados de 9 milhões de clientes;
- Natura – 50 mil clientes Natura têm informações vazadas na web;
- Samsung – Falha de segurança permite invasão de celulares Galaxy desde 2014;
- Zoom – Problemas de privacidade e invasões na plataforma de videoconferências;
- Nubank – Dados de correntistas do Nubank estavam disponíveis no Google.

No ano de 2022, as linguagens de programação PHP e Python tiveram seus repositórios comprometidos, devido a invasão de dois hacks, com isto, o pacote ‘ctx’ foi modificado com a finalidade de roubar dos seus usuários (desenvolvedores) as variáveis do ambiente de programação. Segundo o pesquisador indiano Somdev Sangwan (@s0md3v no Twitter) “o código malicioso envia todas as variáveis de ambiente para um aplicativo heroku, provavelmente minerando as credenciais da AWS”.

[1] Intranet é uma rede de computadores utilizada para comunicação interna da equipe de uma corporação.
[2] Extranet é uma rede virtual privada para trabalhar de forma segura, compartilhar informações ou integrar operações com equipes externas, como clientes, fornecedores e parceiros.

Em uma rede doméstica as ameaças também podem ser encontradas com facilidade, através de uma rede wireless[3] não privada, com isto, qualquer indivíduo pode acessar a rede e navegar, com más intenções, ele pode invadir a rede e causar dados ao proprietário, proporcionando-lhe transtornos, tendo em mãos o endereço MAC[4] de seus dispositivos.

Tanto empresas quanto usuários domésticos usam a internet no dia a dia, pois ela se tornou uma ferramenta essencial para o mercado de trabalho e para momentos de lazer, todavia, ao acessá-la, os dispositivos eletrônicos ficam expostos a rede, e não tendo uma proteção eficaz os dados pessoais ficam aos olhos de todos, o que causa risco para o usuário, já que pessoas mal intencionadas podem querer se passar pelo dono da rede e usando da identidade alheia cometem crimes como, sequestro, estelionatário e dentre outros.

Hodiernamente[5], mais da maioria das empresas estão informatizadas e possuem um sistema de gerenciamento eletrônico de suas atividades diárias, apesar disto, muitos softwares auxiliares das atividades e tomadas de decisões podem apresentar vulnerabilidades em relação aos sistemas manuais. (Kelvin Zimmer, 2022)

2.6 – Vulnerabilidade

A vulnerabilidade de um sistema é ocasionada pela falha que ele possui, provocando instabilidade das informações, quebra de sigilo e alterações sem permissão, encadeando vários fatores, como falta de manutenção, falta de treinamento, falha nos controles de acesso, insuficiência de proteção de uma área ameaçada.

As vulnerabilidades podem ser classificadas nas seguintes categorias:

- **Tecnológica:** aqui, as redes de computadores e os dispositivos sofrem ameaças por vírus, por hacker/cracks; ou seja, todas atividades que são interligadas a tecnologia.
- **Física:** tem relação com o ambiente que os computadores e periféricos estão guardados/armazenados ou sendo usados. Como exemplo: falta de energia, sem proteção para mudanças climáticas, dentre outros.

[3] Rede sem fio – Wi-Fi.
[4] MAC - Identificador único atribuído a uma interface de rede – funciona como um CPF dos dispositivos.
[5] O mesmo que nos dias atuais.

- **Humanas:** aqui, existem vários fatores que influenciam, como características psicológicas, socioculturais e emocionais que variam de indivíduo para indivíduo; temos como exemplo, falta de qualificação, ambiente organizacional inapropriado e falta de treinamento.

As falhas mais comuns que ocorrem na segurança de um sistema são ocasionadas pela falta de gerenciamento dos acessos efetuados, backups desatualizados, inexistência de uma política de segurança formalizada, falta de treinamento e informativos aos usuários de como explorar com segurança os recursos tecnológicos, entre outros. (Hugo Bär, 2021)

2.7 – PRINCIPAIS ATAQUES A SEGURANÇA DA INFORMAÇÃO

2.7.1 – Por negação de serviço.

Este tipo de ataque se dá quando um indivíduo usa uma máquina para realizar várias requisições a um computador e/ou servidor, com má intenções, causando uma sobrecarga nos sites deixando-o indisponível para os usuários; ele também é conhecido como Denial of Service (DoS).

Estes ataques são os mais comuns devido à sua facilidade de execução, segundo McClure, Scambray e Kurtz eles podem ser categorizados em quatro categorias básicas. (Mcclure, J. et al. 2000)

2.7.1.1 – Consumo de Largura de Banda:

Mesmo sendo considerado pouco complexo, este ataque consome toda largura de banda existente, podendo acontecer dentro da rede ou remotamente. Uma das formas de ataque é quando o atacante usa uma conexão de rede maior que a rede que está sendo atacada. Outra forma de ataque é quando o atacante domina diversos hostes para expandir o ataque, saturando a conexão de banda da rede atacada; esta segunda forma também é conhecida como Ataque de Negação de Serviço Distribuído, ou Distributed DoS (DDoS). (Mcclure, J. et al. 2000)

2.7.1.2 – Consumo de Recursos:

Este ataque tem por finalidade malgastar[6] todo o recurso de um sistema (memória, espaço de armazenamento, CPU) sobrecarregando-os até seus limites de capacidades e tornar o sistema incapacitado de processar, deixando-os deterioráveis. (Mcclure, J. et al. 2000)

2.7.1.3 – Falhas de Programação:

Softwares são programas pré-estabelecidos para executarem uma determinada tarefa, com a finalidade de solucionar problemas, e/ou outras situações que mais se identificam com o usuário/cliente; todavia, todo software possui brechas (falhas) em sua programação, que ao serem descobertas por pessoas mal intencionadas podem gerar um prejuízo ao usuário, até mesmo processadores podem possuir falhas de programações, caso uma determinada instrução ou informação não esteja programada poderá exaurir os recursos de um sistema. (Mcclure, J. et al. 2000)

2.7.1.4 – Ataques de Sistemas de Nome de Domínios (DNS[7]) ou Roteamento:

Neste tipo de ataque a tabela de endereços do DNS é alterada e a rede fica incapacitada de descobrir quais os endereços estão sendo requisitados pelos hosts[8], ou então informa endereços falsos ou errados. No ataque a tabela de roteamento, uma rede específica é alterada possibilitando que algumas falhas nos protocolos como RIP[9] e BGP[10] sejam exploradas. (Mcclure, J. et al. 2000)

---

[6] O mesmo que desperdiçar.

[7] Sigla que em inglês significa "Domain Name System. "

[8] Hosts é uma palavra em inglês que na Língua Portuguesa significa hospedeiro, ou seja, hosts é um servidor que hospeda sites.

[9] O protocolo RIP é um padrão que serve para troca de informações entre os gateways (um nó de rede equipado para interfacear com outra rede que usa protocolos diferentes) e hosts de roteamento.

[10] BGP é um protocolo de roteamento entre sistemas independentes, desenvolvido para o uso dos roteadores fundamentais para a Internet.

2.7.2 - Ataque Smurf

Embora seja um ataque mais fácil é o pior dentre eles. Inicialmente, este ataque é feito através de um comando ping[11] que são programados para serem enviados ao endereço de broadcast[12] de uma rede. O endereço originário do pacote ICMP[13] é disfarçado passando a usar um IP[14] inautêntico (chamado de IP spoofing[15]). Neste caso, os protocolos são alterados e o IP de origem é modificado para o IP da vítima. E assim, todos os resultados dados ao ping são enviados somente para um host, acabando rapidamente com toda banda largar disponível do usuário vítima. (Cloudflare)

2.7.3 - Ataque INUNDAÇÃO SYN

O ataque acontece através de envios de requisições SYN[16] ao protocolo TCP, em uma velocidade muito superior que a capacidade de resposta do servidor que está sendo alvo, para isto as requisições fazem uso de IPs[14] falsos, ou seja, os endereços são modificados, esta técnica é denominada IP Spoofing[15]. Através desta tática de ataque o servidor envia resposta SYN-ACK[17] para caminhos inexistentes, sem tráfegos de informações e fica aguardando a resposta ACK, entretanto nunca receberá as respostas esperadas, pois, o destino não existe. Com isto o servidor terá várias conexões semiabertas até alcançar seu limite de capacidade, bloqueando o atendimento para novas requisições.(Cloudflare)

---

[11] Ping – sigla de “Packet Internet Network Grouper”, funciona como um Procurador de Pacotes da Internet; é um comando que serve para testar a conectividade entre equipamentos de uma rede.

[12] Broadcast é um endereço lógico onde todos os dispositivos conectados a uma rede de comunicações de acesso múltiplo, ou seja, uma mensagem enviada para um endereço de broadcast pode ser recebido por todos os hospedeiros conectados à rede.

[13] Sigla em inglês que significa “Internet Control Message Protocol” (na Língua Portuguesa significa Protocolo de Mensagens de Controle da Internet).

[14] IP - Protocolo de Internet - é um protocolo de comunicação usado entre todas as máquinas em rede para encaminhamento dos dados.

[15] IP spoofing - é um ataque que consiste em mascarar pacotes IP utilizando endereços de remetentes falsificados.

[16] Assim que o usuário começa uma conexão TCP com um servidor, ambos trocam uma série de mensagens, que geralmente tem os seguintes caminhos: O usuário requisita uma conexão enviando um SYN (synchronize) ao servidor, este servidor confirma esta requisição enviando um SYN-ACK (acknowledge) de volta ao usuário.

[17] Serviço da máquina-alvo com SYN/ACK indicando que a porta se encontra ouvindo, através de um serviço que está sendo utilizado.

2.7.4- ATAQUES DdoS

"Distributed Denial of Service" (DdoS), que traduzido para o Português é denominado Ataque Distribuído de Negação de Serviço, tem a finalidade de tornar os serviços oferecidos pelo servidor inacessíveis para os clientes legítimos no momento em que se esforça para processar o tráfego gerado pelo ataque. (Cloudflare)

Os DdoS são desenvolvidos por rede de computadores de máquinas contaminadas (também conhecidas como máquinas zumbi) que proporcionam ataques organizados a um determinado alvo. (Cloudflare)

2.7.5 – Esgotamento do TCP[18]

A intensão deste ataque é arruinar as conexões, acabando com os limites suportados por cada dispositivo, tem como principais alvos balanceadores de carga, servidores web e firewalls. (Cloudflare)

2.7.6 – Nas camadas de aplicativos

O alvo deste ataque são as falhas e/ou vulnerabilidades de um servidor ou aplicativo; comprometendo o funcionamento de suas aplicações. (Cloudflare)

2.7.7 – Volumétricos

A finalidade deste ataque é sobrecarregar uma largura de banda local enviando um imenso volume de tráfego de informações. São realizados por intermédio de botnets[19], onde vários computadores são afetados e monitorados por hackers/cracks. (Cloudflare)

---

[18] Protocolo de Controle de Transmissão - responsável pela entrega dos dados quando o endereço IP é encontrado.

[19] Botnets são números de dispositivos conectados à Internet, uma rede de bots pode ser usada para executar ataques DDoS, roubar dados, enviar spam e permitir que o invasor acesse a conexão de um dispositivo.

2.8 - Tipos de Malware

Malwares são programas de computadores maliciosos que invadem outros sistemas de computadores sem que o usuário perceba, com a finalidade de causar prejuízo ou roubar informações. Algumas atuações do Malware podem comprometer as funcionalidades do computador explorando as vulnerabilidades que existem nos softwares instalados, infecção de mídias removíveis como pendrives, acesso a páginas da web mal-intencionadas, fazendo o uso de navegadores vulneráveis, envio de mensagens eletrônicas infectadas por vírus, dentre outros, vejamos alguns tipos de Malware:

2.8.1 - VÍRUS

São programas de computadores maliciosos que tem o objetivo de infectar o sistema causando impedimentos em seu funcionamento, desempenhando ações indesejadas pelo usuário; para ser ativado na máquina um programa hospedeiro já contaminado necessita ser executado.

Mídias removíveis, como pendrives, são os principais meios de expansão dos vírus.

Segundo a cartilha CERT BR[20], os vírus mais comuns são:

> • **Vírus propagado por e-mail:** "recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador". (Cert.br).

Esse tipo de vírus tem com objetivo se propagar nas caixas de e-mail, após infectar os computadores ele transforma a máquina em um servidor de correspondência eletrônica para se expandir para os contatos da vítima. Ele se caracteriza por seu meio de disseminação, entretanto pode acabar sendo usado para levar outros tipos de códigos maliciosos como programas espiões para as máquinas.

[20] Disponível em: <CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para Internet. 2017> acesso em 23 de abril de 2022.

> • **Vírus de script:** “escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador web e do programa leitor de e-mails do usuário”. (Cert.br).

Esse tipo de vírus é construído através de linguagens script, são usados para injetar códigos maliciosos em programas com vulnerabilidades para tomar o controle, monitorar e eventualmente invadir roubar informações.

> • **Vírus de macro:** “tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros) ”. (Cert.br).

Também conhecido como macro vírus, é um código maliciosos geralmente em visualbasic, que é a linguagem de programação do que geralmente é alvo como o pacote da Microssoft Office.

> • **Vírus de telefone celular:** “vírus que se propaga de celular para celular por meio da tecnologia Bluetooth ou de mensagens MMS (Multimedia Message Service). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares”. (Cert.br).

Esse tipo de vírus tende a infectar pessoas que aceitam arquivos de procedência duvidosa e pode ser usado para adquirir a lista de contatos do alvo, o que permite até mesmo a aplicação de golpes via ligação.

2.8.2 - PHISHING

Este ataque é feito através de envios de mensagens eletrônicas com o objetivo de enganar o usuário se passando por empresas oficiais e verdadeiras, o

invasor utiliza técnicas de engenharia social para atrair as vítimas com publicidades, serviços e imagens de assuntos atuais em destaque.

2.8.3 - BOT E BOTNET

A finalidade deste malware é reter as informações sigilosas dos usuários como senhas de bancos, números de cartões de crédito, dentre outros. Este programa procura as vulnerabilidades e falhas nos sistemas e softwares instalados nas máquinas de computadores com o intuito de explorá-los remotamente.

Ele também pode ser chamado de spam zombie[21], onde o bot instalado transforma em servidor de e-mails para o envio de spam.

Conforme a cartilha Cert BR:

> "Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores." (Augusto, H.).

Os bots são de grande risco tanto para os sistemas empresariais quanto para usuários domésticos, pois este malware pode inutilizar serviços e roubar dados valiosos causando muitos danos financeiros ao cliente.

2.8.4 - SPYWARE

É um programa criado para monitorar as tarefas que são realizadas pelo sistema e enviar as informações capturadas para terceiros, podendo ser usado de duas formas, a primeira é a forma legítima, onde o próprio dono ou com seu consentimento instala o software em seu computador pessoal para averiguar se outras pessoas estão usando sua rede de forma abusiva ou não autorizada; a segunda é a forma maliciosa, onde as ações executadas comprometem a privacidade do usuário ameaçando a segurança do computador e as informações como conta de usuário e senhas são repassada para terceiros mal intencionados.

[21] Os computadores infectados por códigos maliciosos, capazes de transformar o sistema do usuário em um servidor de e-mail para envio de spam, são chamados de Spam Zombies.

Segundo a cartilha Cert BR, existem tipos de Spyware sendo eles: Keylogger, Screenlogger e Adware, vejamos suas definições:

> “**Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.” (Cert.br).

Compreende-se que a função primária do código malicioso é monitorar as teclas pressionadas, tendo como gatilho o acesso a páginas já definidas pelo invasor, como contas de bancos, redes sociais, contas de e-mail’s entre outros.

> “**Screenlogger:** similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelo usuário sem teclados virtuais, disponíveis principalmente em sites de Internet Banking." (Cert.br).

Nesse caso específico a função é monitorar onde ocorre os cliques do mouse depois de acessar páginas alvo sites de bancos quando for acessar as contas de bancárias, um dos modos para evitar ter as teclas clicadas gravadas é usar o teclado virtual, mas para burlar isso o método de ação do vírus mudou para armazenar onde era clicado.

> “**Adware:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.” (Cert.br).

Esse tipo de código tem como finalidade executar automaticamente sem a permissão do usuário e mostrar para os usuários propagandas e anúncios, ele analisa os principais sites que são acessados e fazem esse marketing dos produtos

pertinentes ao conteúdo acessado, entretanto devido sua facilidade e grande propagação também é usado de forma maliciosa, direcionando para golpes.

2.8.5 - CAVALO DE TROIA (TROJAN)

A denominação deste malware é uma analogia feita ao cavalo de madeira usado pelos gregos ao invadirem Tróia, no famoso episódio da guerra de Tróia, devido à genialidade que os gregos usaram para invadirem seus inimigos sem serem descobertos.

No Sistema Operacional de um computador os trojans são backdoors[22] sendo aplicados para abrir brechas para atacantes invadirem o sistema sem serem descobertos pelo usuário, normalmente vem disfarçado de programas ou arquivos como músicas ou jogos; utilizam as portas TCP ou UDP[23] para estabelecer conexões externas e assim facilitar o acesso ao prompt[24] de comando. (Kaspersky)

Existem diferentes tipos de Trojans, vejamos alguns:

- **Trojan Backdoor**: possibilita o acesso remoto dos invasores ao computador, pois possuem backdoors;
- **Trojan Banker ou Bancos**: reuni os dados bancários do usuário, por intermédio do programa spyware, que são acionados quantos se acessa os sites de Internet Banking[25].
- **Trojan Clicker:** encaminha a navegação do usuário para sites selecionados, com a finalidade de aumentar a quantidade de acessos a estes sites ou apresentar propagandas indesejadas.
- **Trojan Proxy:** com a instalação de um servidor proxy, o computador pode ser utilizado para navegações anônimas e envios de spam.

---

[22] Em um sistema de computador ou software backdoor é uma porta de acesso não documentada que permite ao administrador entrar no sistema.

[23] "User Datagram Protocol" um protocolo simples da camada de transporte.

[24] Prompt de Comando é um interpretador de linha de comando no sistema operacional criado pela IBM (International Business Machines Corporation - tradução: Corporação Internacional de Máquinas de Negócios) e de sistemas baseados no Windows.

[25] Internet banking é um aplicativo - para smartphones ou computadores, onde é possível acessar uma área dentro do site do banco que a pessoa seja correntista com o intuito de realizar transações sem precisar ir à agência, como por exemplo: consulta de saldo, fazer transferências, visualizar extratos, fazer pagamentos de boletos e faturas, PIX, entre outros.

- **Trojan Spy:** instala programas spyware e os utiliza para capturar dados sigilosos do usuário, como senhas e números de cartão de crédito, enviando essas informações ao atacante. (Kaspersky)

2.8.6 - WORM

Os Worms se diferem dos vírus devido a sua forma de propagação, visto que, não necessitam de outros programas para serem executados, ele se propaga automaticamente pelas redes fazendo cópias de si mesmo entre os computadores de forma muito rápida.

O Worms, na maioria das vezes, contamina o Sistema Operacional silenciosamente, sendo assim, o usuário não percebe que seu computador está infectado, só notando tal feito quando ocorrem anormalidades nas funcionalidades do sistema.(Martins, E.)

2.9 – SEGURANÇA CIBERNÉTICA – SE PROTEGENDO DE ATAQUES CIBERNÉTICOS

Neste capítulo será abordado as medidas básicas e avançadas de Segurança Cibernéticas, com a finalidade de orientarmos o leitor, usuários de redes de internet a se protegerem de ataques cibernéticos, resguardando seus dados e informações.

2.9.1 - Segurança Cibernética.

Schultz alega que a segurança cibernética é um ramo da segurança da informação que tem como objetivo prevenir os ataques realizados por sistemas maliciosos que se aproveitam de falhas sistêmicas para invadir dispositivos, roubando, manipulando e tornando indisponível uma série de dados ou arquivos. Assim, segurança cibernética envolve a prevenção e proteção no que tange ao ciberespaço[26] e a segurança da informação envolve a prevenção e proteção contra

[26] Espaço das comunicações por redes de computação.

todo tipo de risco, seja físico ou digital, controlando acessos de pessoas a locais, permissões para acessos de arquivos, entre outros. (Schultz, F.)

2.9.2 – Medidas básicas para se proteger de invasões cibernética.

2.9.2.1 – Antivírus

Antivírus são programas com a finalidade de detectar algum vírus no computador e eliminá-lo, garantindo que a redes e/ou outros programas instalados no dispositivo seja infectado por um malware malicioso. (GD. Solution)

Existem três formas básicas de matar o vírus, vejamos:

Antivírus Descontaminadores: tem a função de limpar, descontaminar o sistema já infectado pelo vírus eliminando os programas maliciosos que estão instalados na máquina. (GD. Solution)

Antivírus identificadores: tem a função de realizar o rastreamento das sequencias de códigos específicos associados ao vírus, desta forma, identifica programas maliciosos que afetam a integridade e funcionalidades do sistema. (GD. Solution)

Antivírus Preventivo: é inserido na memória do computador, tem a função de monitorar as funções do sistema; e ao ser detectado uma possível contaminação ele envia uma mensagem de aviso antecipadamente ao usuário. (GD. Solution)

Melhores antivírus gratuitos para a proteção de computadores pessoais ou empresariais:

- **Sophos Home Free**

O Sophos tem como base a segurança empresarial, esta versão gratuita garante proteção idêntica aos seus produtos empresariais, possibilita a proteção remota de até 3 aparelhos eletrônicos; possui uma boa proteção contra phishing e conta com um excelente recurso para bloqueios de URLs maliciosos; tem como diferencial um gerenciamento remoto que assegura proteção aos dispositivos e seus dados mesmo que eles estejam distantes. (Belcic, I.)

- **Avast Free Antivírus**

De fácil compreensão e manuseio, o Avast Free faz verificações de segurança de rede, seu navegador web é seguro, e possui várias outras funcionalidades que

auxilia na proteção dos computadores como o modo Não Perturbe, que tem a finalidade de bloquear pop-ups de anúncios indesejados e suspeitos e averigua o comportamento dos aplicativos garantindo a proteção do dispositivo a qualquer pequeno sinal de malware. (Belcic, I.)

- **AVG Antivírus FREE**

O AVG faz uma varredura no sistema buscando Malwares ocultos, desde vírus até softwares maliciosos como os spywares[27] e ransomwares[28]; também procura se alguma URL é maliciosa, faz buscas de navegadores indesejáveis e detecta problemas de desempenho no PC[29]; possui a função de destruição de dados, onde apaga todos os dados sigilosos do usuário evitando que os mesmos fiquem expostos na web[30]. (Belcic, I.)

- **Microsoft Windows Security**

Este aplicativo de antivírus ultimamente já vem integrado ao Windows 10, ele detecta Malwares, está se aprimorando na proteção de phishing e bloqueio de RLs maliciosas; vem melhorando seu desempenho a cada atualização. (Belcic, I.)

2.9.2.2 – Evitar Acessos em Redes Abertas.

Atualmente é muito comum que ao chegar em um determinado ambiente as pessoas procurem uma rede Wi-Fi aberta para se conectarem a internet, evitando assim de gastarem seus dados móveis deixando-o para usá-lo somente em locais que não possuem uma rede Wireless disponível; todavia, este tipo de comportamento pode ser arrisco para a segurança dos dados que estão armazenados em seus dispositivos, visto que, é bastante comum que hacker/cracker[31] crie uma rede aberta falsa com nome de locais públicos com excelentes conexões com a finalidade de atrair diversas pessoas e quando o usuário conecta em um ponto de acesso falso, seus dados poderão ser vistos e enviados

[27] **Spywares** são tipos de Malwares que tentam se esconder para registra secretamente informações e rastreia suas atividades online em computadores ou dispositivos móveis.
[28] **Ransomwares** são tipos de Malwares que sequestra dados, realizados por meio de criptografia, tendo como refém arquivos pessoais da vítima e cobra em criptomoedas pelo resgate para restabelecer o acesso a estes arquivos, tornando praticamente impossível fazer o rastreamento do criminoso.
[29] PC – Computador pessoal ou restrito a um pequeno grupo de indivíduos.
[30] Rede mundial de computadores.
[31] Quando um indivíduo invade um sistema para fazer o bem ele é denominado hacker, a partir do momento em que ele usa os dados coletados pela invasão para praticar ações maliciosas, causando danos irreparáveis ao usuário ele recebe uma nova nomenclatura e passa a ser denominado como um cracker.

aos hacker/cracker que poderão usá-los de forma maliciosa, podendo causar danos irreparáveis ao usuário.

Para se proteger dos invasores de redes abertas falsas é necessário tomar algumas medidas, tais como:

Fazer uso de uma VPN[32] - Uma conexão de rede virtual privada comumente usada por redes empresariais, é bastante recomendada por possuir uma criptografia de ponta que protege os dados do usuário, desta forma, quando um cracker tem acesso a eles, primeiro irá precisar discriptografá-lo e isso faz com que ele desista da invasão. (Kaspersky).

Fazer uso de conexões SSL[33] **–** É uma forma de proteção de rede mesmo que ela não seja privada; pois, tem a função de criptografar os dados do usuário. Uma boa maneira de saber se um site possui SSL é observando sua URL[34], se a URL possuir um cadeado ao lado de um https[35] o site é considerado seguro.(Martins, E.)

Desativar o compartilhamento de dados – Ao acessar uma rede aberta evite deixar ativado ou ativar o compartilhamento de dados dos Smartphones[36] ou outros dispositivos eletrônicos, desta forma seus dados estarão seguros de uma invasão cibernética. (GEIB, T.H.)

2.9.3 – Vazamento de empresa hackeada revela grave vulnerabilidade no Flash

Segundo Gabriela Garcia da exame, a falha permitia que invasores controlassem e monitorassem remotamente as máquinas.

> "A empresa de spyware Hacking Team foi invadida no começo da semana, vazando 400 GB de arquivos confidenciais e códigos fontes. Além de documentos mostrando que a empresa italiana prestava serviços para ditaduras, os arquivos mostram que a Hacking Team explorava graves vulnerabilidades em softwares bastante populares." (Gabriela Garcia, exame).

[32] Abreviação de Virtual Private Network.
[33] Protocolo de Internet padrão para servidores e navegadores.
[34] Uniform Resource Locator – Em português significa Localizador Padrão de Recursos - é o endereço de um recurso disponível em uma rede.
[35] Camada adicional de segurança que utiliza o protocolo SSL/TLS.
[36] Smartphones são celulares que combinam recursos de computadores pessoais.

Segundo o site The Register, os documentos vazados revelaram que havia duas falhas de vulnerabilidades desconhecidas que afetavam o Adobe Flash e um driver de fontes do Adobe no Windows.

> “A Hacking Team descreve a falha no programa da Adobe como "a mais bela vulnerabilidade no Flash dos últimos quatro anos", sugerindo que a empresa poderia estar usando o bug para praticar spyware há algum tempo. Os documentos mostram que a Hacking Team usou essa vulnerabilidade para instalar malwares que monitoravam e controlavam remotamente outros PCs.
>
> A falha permitia que invasores executem códigos na máquina da vítima por meio de um site. A falha afeta as versões do software para Windows, OS X e Linux, e pode ser usada contra navegadores como o Internet Explorer, Mozilla Firefox, Google Chrome e o Safari, da Apple.
>
> A outra falha afeta um driver de fontes da Adobe no Windows. Todas as versões de 32-bit e 64-bit do Windows são afetadas pelo bug, desde o Windows XP até a versão 8.1 do sistema operacional, segundo os pesquisadores.
>
> A vulnerabilidade permite que invasores aumentem o nível de privilégios que possuem em uma máquina para o grau de administrador, e deveria seria usada simultaneamente à vulnerabilidade no Flash.
>
> "Acreditamos que o risco é limitado para os consumidores em geral, já que, sozinha, essa vulnerabilidade não pode permitir que um adversário tome controle de uma máquina", afirmou um porta-voz da Microsoft ao site *The Verge*. "Encorajamos os clientes a aplicar a atualização da Adobe e estamos trabalhando em uma correção." (Gabriela Garcia, exame).

A pronúncia da Hacking Team quanto à falha ser a mais bela desde os últimos quatro anos, leva a acreditar que eles a exploravam instalando programas espiões, os documentos usou a vulnerabilidade para instalar malwares que monitoravam e controlavam os computadores das vítimas.
Segundo o The Register,

> “As falhas de segurança são usadas para injetar código malicioso em PCs; esse código instala ferramentas de vigilância para monitorar cada movimento do usuário e controlar remotamente suas máquinas pela internet. Pelo que vimos até agora, dentro do código-fonte vazado está um exploit do Adobe Flash para o qual não existe patch: ele pode ser usado

> contra o Internet Explorer, Firefox, Chrome e Safari, e afeta o Flash Player 9 até a versão mais recente, 18.0 .0.194 . Uma exploração de prova de conceito usa a falha para abrir o calc.exe no Windows, provando que um arquivo Flash malicioso baixado da Internet pode executar código arbitrário no computador da vítima. A Hacking Team o descreve como "o bug do Flash mais bonito dos últimos quatro anos" em sua documentação interna." (Chris Williams, The Register).

Entende-se que a falha de segurança foi explorada como porta de entrada para a injeção dos códigos maliciosos nos computadores, através disso foi possível instalar programas que vigiam e monitora cada uma das ações da vítima, sendo possível até mesmo controlar remotamente as máquinas, vários navegadores de internet eram afetados por essa lacuna na segurança da aplicação, como por exemplo: Firefox, internet Explorer, Google Chrome e Safari.

3 – MATERIAIS E MÉTODOS

Trata-se de uma pesquisa bibliográfica integrativa sobre as diversas falhas de segurança, meios utilizados para explorar as falhas, normas para redução de vulnerabilidades e restrições de acessos não autorizados.

Para tanto, buscou-se as normas orientações e normas descritas na família da ISO2700, doutrinas usadas, artigos científicos que tratassem sobre a temática em todo Brasil e disponibilizados fisicamente nas plataformas online de pesquisas, tais como acervos online, livros, Google Scholar, tendo sido usado às palavras-chaves nas buscas online, tais como “ISO27000”, “ISO27001”, “segurança da informação”, “vulnerabilidades”, “normas de segurança da informação”, “redução de riscos cibernéticos”.

Foram utilizadas duas matérias publicadas pela exame e theregister. Após compreender as falhas expostas, houve capacidade de entender o método de invasão a qual os usuários estavam expostos para que seja elaborada uma orientação de como se proteger e evitar que os dados sejam vazados ou monitorados.

4 – RESULTADOS E DISCUÇÕES

O presente trabalho trouxe as principais formas e normas de proteção a ataques cibernéticos para que o usuário possa compreender e pôr em prática com o objetivo de proteger seus dados informativos de vulnerabilidades sistemáticos e brechas de falhas de segurança.

Através do conteúdo colhido é possível compreender a extensão dos danos e das formas de expansão que os vírus ou hackers podem atingir. Entende-se que grandes empresas podem acabar sofrendo invasões e também expondo os usuários finais as invasões como no caso reportado pela The Register e exame.

O usuário acaba sendo o maior responsável e interessado na segurança das suas informações, entretanto acaba negligenciando quando adere a programas com longos históricos de vulnerabilidades. Mesmo usando eles deve se manter atento as atualizações, uma outra forma de proteger os dados é ficar de olho nas notícias e reportagens sobre as vulnerabilidades que estavam sendo exploradas, caso o mesmo tenha essa brecha no computador é necessário a remoção imediata, se suspeitar que tenha sido afetado, o pc deve ser examinado por um técnico ou até mesmo formatado o mais rápido possível.

5 - CONCLUSÃO

Em suma, frente a todos os tópicos abordados é perceptível que independente de ser pessoa física ou jurídica, é necessário conhecer sobre os princípios abordados e traçar uma estratégia coerente, clara e objetiva, usando programas como o antivírus para evitar infecções de vírus já analisados anteriormente, evitar abrir e-mails de origens desconhecidas ou não solicitadas, bem como, na ocasião de ser uma empresa de médio ou grande porte dar preferência ao uso de normas como a ISO/IEC27001 para padronizar e abranger os pontos mais críticos e evitar que dados sensíveis sejam acessados por pessoas não autorizadas com o intuito de prejudicar moral e financeiramente os portadores dos dados, conclui-se também, que o despreparo das pessoas responsáveis pela segurança da informação ou até mesmo dos usuários finais pode permitir a abertura de brechas no sistema, culminando na infecção de códigos maliciosos. Compreende-se também que o usuário final possui grande responsabilidade sobre os próprios dados, mas acaba negligenciando ao usar a máquina de forma descuidada e instalando tudo que acreditar serem necessários para usa-la, os mesmos devem se manter atentos as matérias e reportagens nos sites de notícias a fim de se manter informado sobre eventuais vulnerabilidades ou falhas de segurança que possam ocorrer em empresas que possuem seus dados ou que fornecem os sistemas em seu PC, caso sejam apenas nos aplicativos o dono deve buscar um técnico para examinar o computador para tomar as providências necessárias.

6-REFERÊNCIAS

ALVES, Gustavo Alberto. Segurança da Informação: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna Ltda, 2006. BRASIL. Ministério da Integração. Plano de Contingência. Disponível em: < http:// www.mi.gov.br/orientacoes-para-elaboracao-de-um-plano-de-contingencia> Acesso em: 23 abr. 2022

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2005 Tecnologia da informação: técnicas de segurança. Rio de Janeiro, 2006.

Augusto, H. Códigos maliciosos (Malware), 2021 Disponível em: <https://sac.educacao.go.gov.br/ajax/common.tabs.php?_target=/front/knowbaseitem.form.php&_itemtype=KnowbaseItem&_glpi_tab=KnowbaseItem$1&id=87&item_itemtype=&item_items_id=#:~:text=Bot%20%C3%A9%20um%20programa%20que,em%20programas%20instalados%20em%20computadores.> Acesso em: 18 jun. 2022

BÄR, Hugo Entenda o que são vulnerabilidades, as mais recorrentes e os mecanismos de segurança da informação para evitá-las, 2021, Disponível em: <https://tripla.com.br/entenda-o-que-sao-vulnerabilidades/> Acesso em:12 jun. 2022

BEAL, Adriana. Segurança da Informação. Princípios e Melhores práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo. Atlas, 2005 – Reimpressão 2008.

Belcic, I. publicado em 18/12/2020 <https://www.avast.com/pt-br/c-best-free-antivirus-software> Acessado em: 19/06/2022

CANALTECH, O que é DoS e DDoS <https://canaltech.com.br/produtos/O-que-e-DoS-e-DDoS/> acesso em 13 de fevereiro de 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE. INCIDENTES DE SEGURANÇA NO BRASIL – Cert.br. Cartilha de Segurança para internet. Disponível em:< http:// cartilha.cert.br/glossário> Acesso em: 08 abr. 2022.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para Internet. 2017> acesso em 23 de abril de 2022.

Chris Williams, Theregister. ASSASSINO! Adobe Flash, vulnerabilidades de dia zero do Windows vazam da invasão da Hacking Team, 2015, Disponível em: <https://www.theregister.com/2015/07/07/hacking_team_zero_days_flash_windows_kernel/ >Acessado em: 19/06/2022

Ciso Advisor, Ataque ao php e python para roubo de credenciais AWS, 2022 Disponível em: <https://www.cisoadvisor.com.br/ataque-ao-php-e-python-para-roubo-de-credenciais-aws/> acesso em 27 de maio de 2022.

Cloudflare, Central de Aprendizagem Referências da Cloudflare sobre segurança cibernética e como a internet funciona. <https://www.cloudflare.com/pt-br/learning/> Acesso em: 12 jun. 2022

Comitê técnico: ISO/IEC JTC 1/SC 27 Segurança da informação, segurança cibernética e proteção da privacidade, International Standart *ISO/IEC27000,* 5ª Edição, https://standards.iso.org/ 2018.

FERREIRA, Fernando N. F. Segurança da Informação. Rio de Janeiro: Ciência Moderna. 2003.
FONTES, E. Segurança da Informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

Gabriela Garcia, 2015, Disponível em: <https://exame.com/tecnologia/vazamento-de-empresa-hackeada-revela-grave-vulnerabilidade-no-flash/>Acessado em 19 Jun. 2022.

GCF Aprene Livre, O que são antivirus<https://edu.gcfglobal.org/pt/virus-e-antivirus/o-que-sao-antivirus/1/> Acesso em 16 de maio de 2022.

GD SOLUTIONS, quais são os 13 tipos de antivírus e como escolher o melhor, 2021 Disponível em: <https://gdsolutions.com.br/tipos-de-antivirus/> Acessado em: 19/062022

GEIB, T.H. Como desativar o compartilhamento de arquivos no windows 10 , 2020 Disponível em:<https://www.lumiun.com/blog/como-desativar-o-compartilhamento-de-arquivos-no-windows-10/#:~:text=Desativar%20o%20compartilhamento%20de%20arquivos%20%C3%A9%20uma%20forma%20de%20proteger,os%20dados%20e%20arquivos%20remotamente.&text=Certifique%2Dse%20de%20que%20voc%C3%AA%20n%C3%A3o%20precisa%20dos%20compartilhamentos.>Acessado em: 19 jun. 2022

Governo Federal, 2020, Disponível em: <https://www.gov.br/fundaj/pt-br/centrais-de-conteudo/noticias-1/4-codigos-maliciosos-malware#:~:text=V%C3%ADrus%20de%20telefone%20celular%3A%20v%C3%ADrus,arquivo%20infectado%20e%20o%20executa.>Acesso em 18 jun. 2022

Governo Federal, CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para Internet. 2017, Disponível em: <https://www.gov.br/fundaj/pt-br/centrais-de-conteudo/noticias-1/4-codigos-maliciosos-malware#:~:text=V%C3%ADrus%20de%20telefone%20celular%3A%20v%C3%ADrus,arquivo%20infectado%20e%20o%20executa.> acesso em 23 de abril de 2022

GRUPO TPS <https://tps.com.br/as-19-principais-empresas-de-ciberseguranca-conhecidas-em-2021/#:~:text=Resultado%20sobre%20empresa%20de%20ciberseguran%C3%A7a&text=Al%C3%A9m%20disso%2C%20as%20melhores%20empresas,nuvem%20e%20seguran%C3%A7a%20de%20endpoint> Acessado em: 20 de maio de 2022.

HINTZBERGEN, J. et al. Fundamentos de segurança da informação: Com base na ISO 27001 e na ISO 27002. 3ª Edição. Local de publicação: Brasport Livros e Multimídia LTDA, 2010.

INFORMA BR. Segurança da informação. Norma ISO/IEC 17799:2000. Disponível em:< http://www.informabr.com.br/nbr.htm> Acesso em 13 fev. 2022.

ISFER, A. Quais os riscos de uma rede wifi aberta e como se proteger, Disponível em: <https://www.oficinadanet.com.br/seguranca/28096-quais-os-riscos-de-uma-rede-wi-fi-aberta-e-como-se-proteger> acesso em 18 de maio de 2022.

Kaspersky o que é uma vpn e como funciona, Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn > Acesso em: 18 Jun. 2022

Kaspersky, Disponível em:<https://www.kaspersky.com.br/resource-center/threats/what-is-a-security-breach> Acesso em: 18 Jun. 2022

Kaspersky, Disponível em:<https://www.kaspersky.com.br/resource-center/threats/trojans> Acesso em: 18 Jun. 2022

Martins, E. 2008, Disponível em: < https://www.tecmundo.com.br/antivirus/206-o-que-e-um-worm-.htm#:~:text=Um%20Worm%20%C3%A9%20um%20programa,Internet%20ou%20anexos%20de%20emails.> Acessado em:19/06/2022

Martins, E. O que é SSL, 2009 Disponível em: <https://www.tecmundo.com.br/seguranca/1896-o-que-e-ssl-.htm.>Acessado em: 19/06/2022.

MCCLURE, J et al. Hackers Expostos: Segredos e Soluções para a Segurança de Redes, Local de publicação: Makron / Osborne, 2000

MIRKOVIC, J., PRIER, G. e REIHER, P. Attacking DDoS at the source. 10Th IEEE International Conference on Network Protocols, pags. 312-321, 2002.

Neto, G. 8 melhores antivírus para proteger os computadores da empresa Disponível em: <https://gtrigueiro.com.br/blog/8-melhores-antivirus-gratuitos-para-proteger-os-computadores-da-empresa/> acesso em 16 de maio de 2022

OEA, Organização dos estados Americanos, Manual de suporte sobre risco cibernético para o conselho administrativo Disponível em: <https://www.oas.org/pt/ssm/cicte/docs/POR-MANUAL-DE-SUPORTE-SOBRE-RISCO-CIBERNETICO-PARA-O-CONSELHO-ADMINISTRATIVO.pdf> acesso em 20 de maio de 2022.

SANTOS, F.D. Segurança da informação: vírus ataques e contra medidas, 2018<https://app.uff.br/riuff/bitstream/handle/1/8793/TCC_FILIPE_DOS_SANTOS_DOMINGOS.pdf?sequence=1&isAllowed=y> acesso em 13 fevereiro 2022.

SCHULTZ, F. Segurança Cibernética: o que é e como ser um especialista no assunto. 2020. [Online] Disponível em: https://milvus.com.br/seguranca-cibernetica-o-que-e/. Acesso em: 29/04/2022.

SÊMOLA, Marcos. Gestão da Segurança da Informação. Uma visão executiva. Rio de Janeiro. Elsevier, 2003 – 11º reimpressão.

STALLINGS, Willian. Criptografia e segurança de redes / Willian Stallings; tradução Daniel Vieira, revisão técnica Ákio Barbosa e Marcelo Succi. – 4.ed. – São Paulo: Pearson Hall, 2008. (Título Original: Criptography and Networking Security 4/E)

ZIMMER, K. 10 maiores falhas de segurança de 2020, 2020 Disponível em:<https://www.lumiun.com/blog/10-maiores-falhas-de-seguranca-de-dados-em-2020/> acesso em 18 de maio de 2022.

ZORRINHO, C. Gestão da informação. Lisboa: Editora Presença, 1995. p. 32

.