Ciber Segurança

Escola secundária de ílhavo

Aveiro, 28-11-2023

Trabalho realizado pelo aluno uziel , da turma 12 E , sob orientação do Professor, Sérgio Heleno, no ano letivo 2020/2021.

1 Introdução

Este trabalho surgiu no âmbito de Redes de Comunicação/FCT com a finalidade de aprender mais sobre a segurança na Internet. Trabalho realizado em fevereiro de 2021 na cidade de Esmoriz.

2 O que é a CiberSegurança

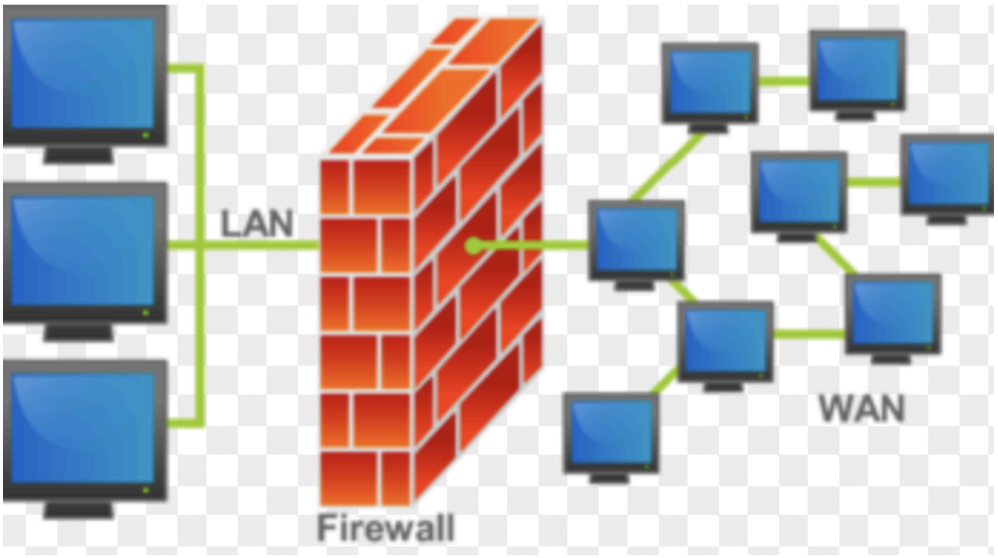
Segurança de rede é a prática de proteger uma rede de computadores contra intrusos, sejam eles invasores direcionados ou malware oportunista.

3 O que é a Darkweb

refere-se a servidores de rede disponíveis na Internet, acessíveis somente através de ferramentas, configurações ou autorizações específicas que dão um elevado nível de anonimato tanto a quem publica os conteúdos como a quem os consulta.

4 O que é uma Firewall

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.



5 O que é um router

Geralmente, um router é um dispositivo que fornece Wi-Fi. Envia informação da Internet para os seus dispositivos pessoais, como um computador, um telemóvel ou um tablet. Estes dispositivos ligados à Internet de sua casa constituem a sua rede local (LAN).

6 O que é um switch

Um switch de rede é um equipamento que permite que dois ou mais dispositivos de TI, como computadores, comuniquem-se entre si. A conexão de vários dispositivos de TI em conjunto cria uma rede de comunicações. Computação, impressão, servidores, armazenamento de arquivos, acesso à Internet e outros recursos de TI podem ser compartilhados por toda a rede.

7 O que é um antivírus

Antivírus é um software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e worms. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário.

8 Tipos de Hacker

Diferentes tipos de cibercriminosos: White hat, black hat, gray hat e muito mais. Os hackersusam suas habilidades para burlar a segurança digital e acessar informações restritas. Embora os hackers geralmente sejam criminosos, existem vários tipos de hackers, e nem todos são mal-intencionados.

8.1 O que é um Hacker

é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programase redes de computadores. *Hackers* podem ser motivados por uma infinidade de razões — como lucro, protesto, vaidade, curiosidade, patriotismo, espírito competitivo, coleta de informações, recreação[ou para avaliar as fraquezas do sistema e auxiliar na formulação de defesas contra *hackers* em potencial. *Hackers* que usam seu conhecimento para fins ilegais são chamados *crackers*.

8.2 White Hats

Entre os profissionais de **otimização de mecanismo de pesquisa** (SEO), o SEO white hat diz respeito às estratégias, práticas e táticas de otimização focadas nas pessoas. Refere-se a qualquer técnica que aprimore a classificação em uma página de resultados de mecanismo de pesquisa (SERP) e siga as regras e políticas dos principais mecanismos de pesquisa, como o Google. Por exemplo, as técnicas de SEO white hat incluem o uso de palavras-chave relevantes e análise de palavras-chave, oferecendo serviços e conteúdo de alta qualidade para os usuários, carregamento rápido do site e navegação fácil.

8.3 Gray Hats\ Black Hats

9 Tipos de Malware

- Vírus. Um vírus geralmente vem como um anexo numa mensagem de correio eletrónico que contém uma carga de vírus ou a parte do **malware**que executa a ação maliciosa. ...
- **Ransomware**. ...
- Scareware. ...
- Worms. ...
- Spyware. ...
- Troianos. ...
- Adware. ...
- **Malware** sem ficheiros.

9.1 O que é o Malware

Malware é qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores.

9.2 Spyware

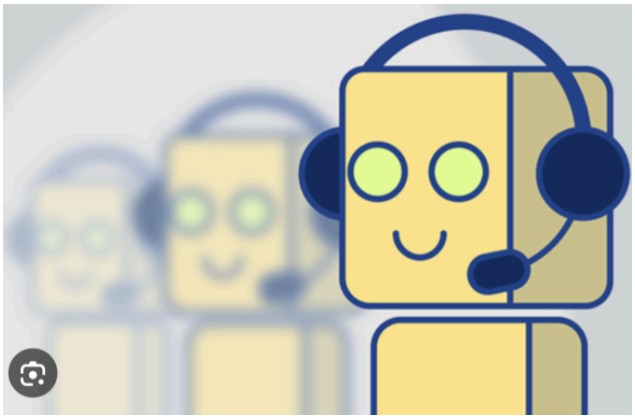
Spyware é um tipo de malware que é utilizado para "espiar" o seu computador ou dispositivos com a intenção de recolher dados pessoais, tais como e-mails, passwords, histórico e números de cartão de crédito, e a capacidade de passar esta informação a terceiros através da Internet.

9.3 Adware

O adware é software indesejado concebido para provocar o aparecimento de anúncios no seu ecrã, a maioria dentro de um browser. Alguns profissionais de segurança veem-no como precursor do mais moderno PPI (programa potencialmente indesejável). Normalmente, utiliza um método discreto para se disfarçar como se fosse legítimo ou apanha boleia de outro programa para enganar os utilizadores para que o instalem em PCs, tablets ou dispositivos móveis.

9.4 Bot

Bots de computador e bots de internet são essencialmente ferramentas digitais e, como qualquer ferramenta, podem ser usados tanto para o bem como para o mal.



9.5 Ransomware

Ransomware é um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como reféns arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos.

9.6 Scareware

Scareware é um software malicioso que engana os usuários, levando-os a visitar sites infestados de malware.

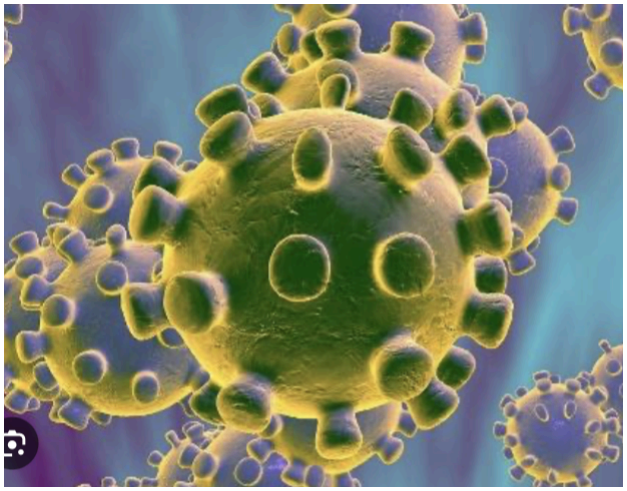
9.7 Rootkit

Rootkit

Conjunto de programas que permite assegurar e manter a presença de um invasor em um computador comprometido.

9.8 Vírus

Vírus são pequenos agentes infecciosos, a maioria com 20-300 nm de diâmetro, apesar de existirem vírus gigantes de, que apresentam genoma constituído de uma ou várias moléculas de ácido nucleico, as quais possuem a forma de fita simples ou dupla



9.9 Trojan horse

Cavalo de Troia é um tipo de malware que, frequentemente, está disfarçado de software legítimo. Eles podem ser empregados por criminosos virtuais e hackers para tentar obter acesso aos sistemas dos usuários.

9.10 Worm

Em computação, worm ou computer worm é um programa independente, do tipo malware, que se replica com o objetivo de se espalhar para outros computadores.

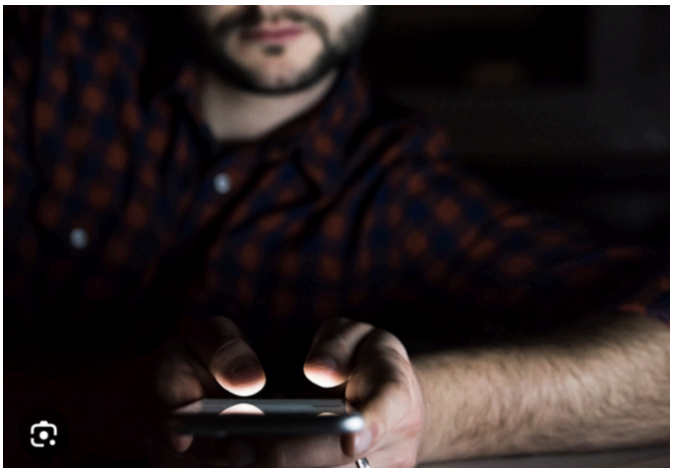
10 Engenharia Social

10.1 O que é a engenharia social

Engenharia social é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Além disso, os hackers podem tentar explorar a falta de conhecimento do usuário. Graças à velocidade da tecnologia, muitos clientes e funcionários não percebem o verdadeiro valor dos dados pessoais e não sabem exatamente como proteger essas informações.

10.2 Pretexting

Traduzido de inglês-Pretexting é um tipo de ataque de engenharia social que envolve uma situação, ou pretexto, criada por um invasor para atrair uma vítima para uma situação vulnerável e induzi-la a fornecer informações privadas, especificamente informações que a vítima normalmente não forneceria fora do contexto do pretexto.



10.3 Tailgating

Traduzido de inglês-Tailgating é a ação de um motorista dirigindo atrás de outro veículo sem deixar distância suficiente para parar sem causar uma colisão se o veículo à frente parar repentinamente.

11 Segurança

11.1 Segurança do posto de trabalho

Segurança do Trabalho (ST) é um conjunto de medidas de prevenção adotadas para proteger os colaboradores de uma empresa e reduzir riscos de acidentes de trabalho e doenças ocupacionais. A ST visa proporcionar um ambiente de trabalho saudável para que as tarefas laborais sejam realizadas da melhor forma possível.

11.2 Segurança de email

A segurança de e-mail é a prática de proteger comunicações e contas de e-mail contra o comprometimento, perda ou acesso não autorizado. As organizações podem melhorar a sua postura de segurança de e-mail ao estabelecer políticas e utilizar ferramentas para proteger contra ameaças maliciosas, como malware, spam e ataques de phishing. Os cibercriminosos definem como alvo o e-mail porque é um ponto de entrada fácil para outras contas e dispositivos e depende, em grande parte, do erro humano. Basta um clique mal orientado para causar uma crise de segurança numa organização inteira.

12 Conclusão

Com a realização deste trabalho fiquei a saber um pouco mais sobre cibersegurança, segurança no trabalho e email e muitas definições

Tive dificuldade em encontrar algumas definições.