Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**SEGURANÇA NA WEB**

Prof.º Denilce Veloso

Disciplina: Programação Web

Márcio Aurélio da Silva Calixto  0030482023004

Sorocaba

Agosto/2022

**1 Introdução**

A sociedade cada dia está mais próxima de ser totalmente desenvolvida tecnologicamente. A internet vem trazendo as informações para perto de cada um, auxiliando em diversos problemas que o ser humano tem a enfrentar. Isso é muito bom e proveitoso, porém, assim como fora dela, na internet também existem diversos problemas que atrapalham a vida de seus usuários, entre eles a falta de segurança.

A segurança na web é um tema a ser discutido e sempre lembrado quando for necessário acessar qualquer site, afinal, devido aos algoritmos e todas as formas de se obter informação, é muito difícil “sair” de lá sem deixar algum dado importante seu lá dentro, ou ainda trazer algo de mal para o seu dispositivo de acesso, e é aí que está o perigo.

Hoje, com tantas formas de ataque, surgiram também várias formas de proteção. Vejamos algumas delas ao decorrer desta pesquisa.

**2 O que é a Segurança na Web?**

Como o próprio nome já diz, o termo especifica sobre as formas de como se proteger dentro da Internet. O estudo desse termo discorre sobre o comportamento dos usuários na rede, as formas que os algoritmos agem para conseguir informação, e como os hackers agem para conseguir roubar os dados de quem acessa determinados sites. Dentre as ameaças encontradas na web, podemos citar as três mais comuns:

Hackeamento, que ocorre quando usuários acessam outras máquinas que não são as suas, sem permissão do administrador;

Vírus (malware ou software malicioso), que conseguem danificar dados e/ou tornar sistemas vulneráveis a outros possíveis vírus e ataques;

Roubo de identidade, onde criminosos roubam a identidade de usuários ou empresas que estão inseridas na rede.

Estas são as formas mais comuns de ataque às redes. Vejamos estas, e ainda outras formas de ataque com mais profundidade:

**2.1 Phishing**

O Phishing é a forma mais antiga e popular de ataque na internet. Conhecida popularmente na década de 90, o phishing nada mais é que um e-mail, aparentemente relevante, enviado a algum usuário, com intuito de fazer o mesmo enviar dados pessoais ou baixar algum malware sem que perceba, correndo grande risco na rede.

**2.2 Hackeamento e Softwares de Acesso Remoto**

Está forma, como já especificada anteriormente, ocorre quando usuários mal-intencionados invadem as máquinas de outrem sem permissão. Aqui o principal tema é uma das formas que eles utilizam, que são os Softwares de Acesso Remoto, onde pode-se acessar uma máquina através de outra. Geralmente, esses softwares fazem com que as máquinas fiquem vulneráveis (sendo o serviço do software esse mesmo de liberar o acesso à outro usuário), correndo o risco de algum outro usuário invadir a máquina referida.

**2.3 Malware e malversiting**

Estes dois termos em inglês servem para definir os vírus que os computadores estão vulneráveis, quando desprotegidos. Especificamente falando, o Malware é o nome do vírus em si mesmo, enquanto o Malversiting diz sobre os anúncios encontrados na web e que podem ser de grande ajuda para os hackers disseminarem os vírus.

**2.4 Ransomware**

Esse é um tipo específico de vírus, onde ele, quando invade seu computador, bloqueia você de utilizar a máquina ou de acessar certos arquivos, enquanto você não “pague” pelo resgate da máquina. O ransomware é basicamente um sequestro, e ultimamente diversos hackers estão utilizando a nova criptomoeda, BitCoin, para pedir os resgates.

**2.5 Botnets**

Basicamente, os usuários desse tipo de ataque fazem com que um determinado conjunto de máquinas façam o serviço que ele faria. Quando certa máquina é acometida com esse ataque, ela começa a ser controlada pelo proprietário do botnet e realiza ataques na rede.

**3 Formas de Proteção**

Para todos os tipos de ataque, existem diversas formas de proteção. Algumas delas servem até para mais de um tipo de ataque. Vejamos algumas delas:

**3.1 Autenticação Multifatorial**

Essa forma de proteção trabalha em um usuário utilizar mais de uma forma de identificação na web. Sempre que ativada, ela dispara um pedido de senha, desbloqueio de impressão digital, perguntas pessoais sobre o usuário, afim de que somente ele tenha acesso à essas informações, impedindo de que alguém se passe por ele.

**3.2 FireWall**

Os FireWalls ajudam as máquinas criando como que uma espécie de barreira na rede, impedindo o tráfego de dados que possam atacar a máquina e atrapalhar o seu desempenho. Ele auxilia tanto na performance da máquina quanto na proteção de malwares e outros ataques.

**3.3 Senhas fortes**

Ter uma senha padrão hoje em dia é muito inseguro, mas sendo uma senha forte, sendo ela de difícil decodificação, auxiliará muito o usuário a proteger suas contas na rede. Ter um bom gerenciador de senhas também é muito importante, pois quanto mais segura a senha estiver, menos chance de ser descoberta.

**3.4 Programa de Segurança**

Há muitos softwares que foram criados para auxiliar na segurança. Basicamente, os mesmos têm formas de notificar o usuário quando há algo de errado em seu dispositivo, ou também quando o usuário está acessando algum site que pode trazer riscos à sua máquina.

**4 Conclusão**

É evidente que se manter seguro na rede não é nada fácil, mas o ser humano necessita do sentimento de segurança, pois o instinto dele mesmo anseia por viver uma vida sem riscos. A verdade é que o ser humano mesmo colabora para que avance para uma sociedade mais segura e livre de riscos. As formas de estar seguro fisicamente estão aí, agora é hora de trabalharmos nas formas de segurança tecnológicas, pois todos estamos inseridos em dois mundos, o físico e o tecnológico!

**5 Referências**

https://www.kaspersky.com.br/resource-center/definitions/what-is-internet-security