UEaD SL Universidade, EaD e Software Livre 2020 | 1°Semestre
CON SCIÊNCIAS UEADSL 2020 / 1° a 7 de junho

SEGURANÇA NA INTERNET: PROBLEMAS E SOLUÇÕES PARA O USUÁRIO COMUM

Samuel Guimarães Espínola[1], Letícia Cerqueira Menezes Cruz[2]

CEFET-MG Eletroeletrônica

Resumo ou descrição abreviada: O intuito do artigo é mostrar que a rede não é segura como parece ser. Sabendo da existência de pessoas mal intencionadas na internet e que se tornou possível adulterar conversas, compras, invadir sistemas e transmitir vírus; a necessidade da segurança se fez grande. Nesse artigo explicamos alguns conceitos da área e concluímos que não se é possível estar completamente seguro, no entanto mostramos boas medidas protetivas.

Palavras-chave: Segurança, Internet, Medidas Protetivas.

1. A segurança na Internet realmente existe?

Quando o assunto é segurança *on-line*, muitas vezes pensamos que estamos completamente seguros devido aos sistemas de segurança que usamos, como antivírus e *firewalls*. Entretanto, na realidade essas mensagens de “Você está totalmente seguro” que recebemos dão uma falsa sensação de segurança na rede.

De acordo com a pesquisadora Georgia Weidman, de uma forma geral, existem dois tipos de hackers utilizando-se da ética como método de comparação. Seriam eles os “White Hats” e os “Black Hats”. White hats são os hackers éticos e Black Hats são os hackers não-éticos. Tendo em vista este conceito podemos explicitar de forma mais simples como funciona a área da segurança da informação que se tornou tão importante nos dias de hoje. A ética contribuindo como uma classificação torna esse ramo muito mais relevante, já que antigamente o termo

hacker era sempre designado pela mídia a todo aquele que praticava o ciberativismo.

O que seria essa “ética” na nossa classificação que diferencia um hacker de outro? O hacker ético é aquele que defende o conhecimento em prol de todos, ou seja, ele não utiliza seus conhecimentos para prejudicar outras pessoas ou companhias. Já o hacker não-ético é aquele que utiliza o seu conhecimento em prol de seu próprio bem, isto é, sempre que encontra uma vulnerabilidade em um sistema, ele abusa dela para obter informações de outras pessoas e utiliza esse conhecimento como uma forma de “poder”.

Sabendo disso, devemos entender que, como esses hackers trabalham no seu dia a dia em empresas digitais, redes sociais e sistemas, todos têm suas medidas de segurança, normalmente as melhores disponíveis. Mesmo quando uma empresa já adquiriu tudo o que há de melhor no mercado ela não está totalmente segura. Para prevenir-se de futuros problemas de segurança a empresa se abre para que qualquer indivíduo que encontrar uma falha em seus sistemas possam reportar e receber uma compensação pelo seu trabalho, o chamado “*Bug Bounty*”. Empresas como Facebook, Instagram, Microsoft e Google têm esses programas vigentes e com regras específicas para serem seguidas, e a quebra de qualquer uma dessas regras implica seriamente no pagamento do programa de recompensa.

Já estabelecido o conceito dos “*White Hats*”, lado bom dos hackers, analisemos agora o universo dos *Black Hats*, algo que poderia ser traduzido como “o lado mal dos hackers”. Enquanto para o *Black Hat* só necessita de encontrar uma falha para colocar o sistema inteiro em colapso, o *White Hat* precisa encontrar todas as falhas para se defender dos atacantes. Para os hackers não-éticos, existem diversas ferramentas que podem ser utilizadas para encontrar fragilidades em um sistema, e a maior delas é a falha humana.

Ao contrário do que se leva a entender, a falha humana é sim a maior fragilidade de um “*firewall*”. Conforme mencionado anteriormente, empresas compram todos tipos de *software* de segurança para se manterem seguras e longe de problemas, porém a falta de treino de um funcionário pode comprometer toda

uma empresa e existe uma classificação especial para esses tipos de ataques, de modo que veremos no próximo tópico.

2. O que é a Engenharia Social?

Engenharia Social, de acordo com o site de segurança digital *"We live Security"* (2020), refere-se à manipulação psicológica de pessoas para se obter acesso a informações delicadas ou até mesmo ações. Ela é utilizada em muitos setores da SI e é independente de sistemas computacionais. Nela, o elemento mais vulnerável é o ser humano e, por não ser exclusiva da área de Informática, também é utilizada para explorar falhas humanas em organizações físicas ou jurídicas as quais operadores do sistema de segurança possuem poder de decisão total ou parcial sobre o sistema, seja ele físico ou virtual. Como se pode imaginar, essa técnica envolve a Informática da mesma forma que a Psicologia, visto que para uma boa análise usa-se leitura fria, linguagem corporal e leitura quente. Leitura fria é um conjunto de técnicas para manipular pessoas fazendo com que elas se comportem de uma nova maneira, e isso tudo sem nenhuma informação prévia da vítima, já na leitura quente é utilizado um conhecimento básico sobre a vítima, normalmente adquirido por meio fraudulento.

Segundo os especialistas, Silvio César Roxo Giavaroto e Gerson Raimundo dos Santos, uma técnica muito empregada para aplicar golpes em pessoas leigas é o "*Phishing*", que seria como um clone de um site verdadeiro, possuindo o mesmo código fonte, porém com alguns acréscimos de linhas de código que adicionam, por exemplo, um KeyLogger (ferramenta capaz de salvar todos os caracteres digitados pelo usuário) em seus sites, ou seja, o usuário que acessar uma dessas páginas, se não tiver um *software* de proteção para lhe avisar, ou até mesmo que utilize os *softwares*, mas que não tenha conhecimento aprofundado do que garante a segurança em um site, pode acabar entregando seus dados mais importantes nas mãos de um hacker.

Outra técnica bastante similar é o "*Smishing*", e dessa, grande parte dos

usuários já foi vítima. Um exemplo muito comum são as mensagens SMS que pedem a confirmação de dados de contas bancárias ou até mesmo de algum sorteio. Por meio delas, os oportunistas conseguem convencer o consumidor a acreditar na mensagem, utilizando-se desse pensamento amador do destinatário para poder capturar seus dados.

Uma última técnica vinculada ao roubo de dados do usuário é o "*Vishing*", que é quando o consumidor recebe uma ligação questionando-o acerca de alguns dados que não estão "cadastrados" em uma determinada conta ou serviço e, de forma ingênua, o consumidor acaba por entregá-los ao criminoso a fim de evitar mais problemas, mas sem saber que está sendo enganado.

De uma forma geral a Engenharia Social sempre será usada de forma a colher informações, seja de forma virtual ou real. A melhor forma para se prevenir é sempre tomar cuidado com o que é passado de informação em uma frase ou até mesmo em um clique.

3. Atenção aguçada pode deixar alguém totalmente seguro?

Mesmo um hacker pode acabar sendo "hackeado". Apesar de parecer um pouco irônico que isso aconteça, ainda existem algumas técnicas extremamente avançadas e que demandam um conhecimento muito evoluído até mesmo dos *Black Hats*. Segundo o bacharel em Ciência da Computação pela UNESP, Daniel Moreno, essas técnicas são conhecidas, de forma geral, como "*Spoofing*".

Quando citamos o *Phishing* em sites falsos, por exemplo, devemos pensar que um site pode ter o mesmo domínio que o outro, sendo possível clonar o endereço DNS de um site confiável. Isso ocorre porque quando o DNS *Spoofing* é aplicado ele redireciona as solicitações de um endereço DNS específico da rede para outro endereço, ou melhor dizendo, quando o site "X" é solicitado pelo usuário, o atacante o redireciona para o site "Y", porém com o mesmo endereço de URL na rede, o que faz com que o usuário pense que realmente está no site que deveria

estar, quando na realidade o invasor está no controle da situação.

Além do DNS *Spoofing*, ainda existe o *Caller ID Spoofing*, que é um ataque ainda mais fácil de ser feito do que o primeiro. Ele consiste na troca do ID da ligação: o atacante pode ligar para o celular da vítima passando-se por uma operadora telefônica (com o mesmo número de ramal), o que representa uma falsa credibilidade para a vítima.

Assim como o *Caller ID Spoofing*, também temos o *E-mail Spoofing,* que apresenta a mesma ideia do precedente. Juntamente com a técnica do *Phishing,* é enviado ao usuário um e-mail com um link para que ele o acesse a fim de atualizar algum dado, ou então para que participe de uma “promoção”, sempre algo chamativo e diferente dos ataques normalmente usados, e esses links levam aos domínios de empresas confiáveis, como algum site popular, o que passaria certa credibilidade.

4. Recomendações de Segurança Online

Existem medidas de segurança que tornam a sua navegação bem mais segura e intuitiva, te mantendo longe dos “hackers” mal-intencionados. Algumas delas são:

- Evitar o uso de Redes de Internet Públicas;
- Manter o computador e celular sempre atualizados;
- Instalar (e manter) algum *software* de proteção (antivírus);
- Manter a navegação em sites conhecidos e com certificado de segurança (https);
- Evitar o download de arquivos e programas desconhecidos;
- Sempre desconfiar de alguma mensagem suspeita independente de como a recebeu.

5. Conclusão

Tendo em vista os aspectos observados, conclui-se que não existe uma maneira de se manter totalmente seguro dentro da rede, e que até mesmo os profissionais podem ser invadidos. É crucial ter cuidado para não ser manipulado psicologicamente e passar dados pessoais. Com tantos meios de ser enganado é importante seguir as medidas de segurança, visto que dessa forma, o usuário tem uma navegação tranquila com baixas chances de ser comprometida.

Referências bibliográficas:

GIAVAROTO, Sílvio César Roxo; SANTOS, Gerson Raimundo dos. **Backtrack Linux**: Auditoria e Teste de Invasão em Redes de Computadores. Rio de Janeiro: Editora Ciência Moderna Ltda., 2013.

KHARIS, Hussam. **Python for Offensive PenTest.** Birmingham: Packt Publishing Ltd., 2018.

MORENO, Daniel. **Introdução ao Pentest.** São Paulo: Novatec Editora Ltda., 2015.

MORENO, Daniel. **Pentest em Redes Sem Fio.** São Paulo: Novatec Editora Ltda., 2016.

WEIDMAN, Georgia. **Testes de Invasão.** São Paulo: Novatec Editora Ltda., 2014.