SEGURANÇA EM REDES SEM FIO: “AS DUAS FACES DA MOEDA”

Autores: Gabriel dos Santos Silva
Hulley Uziel Deyvison Carneiro Campos
Ícaro de Souza Nogueira
Bruno Henrique Rocha Silva
Bruno Nascimento de Oliveira
Orientador: Msc. Alexandre Monge

E-mail: gabriel93.silva@gmail.com

Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Campus Barreiras.

## 1. Introdução

A revolução da informação vem se tornando cada vez mais forte, trazendo consigo uma crescente onda de facilidades. A sociedade atingiu um quadro de evolução tecnológica tão elevado, onde as chamadas casas do futuro, com televisões e geladeiras, inteligentes e conectadas à internet, já deixaram de assim ser chamadas há muito tempo. Já são assim os lares do presente, e isso tornou a necessidade da existência de milhões de redes para a comunicação entre os mais variados aparelhos muito mais que aparente. Sentar ao ar livre, abrir o *notebook*, ou tirar o *smartphone* do bolso, e acessar a conta do banco para a retirada de um extrato ou realizar compras *on-line* tornou-se cada vez mais presente no cotidiano de muitos.

Levanta-se então a seguinte questão: confiar exageradamente em modos alternativos de conexão, especificamente o de conexão sem fio, é realmente o mais adequado quando não se tomam as devidas providências para a segurança?

## 2. Métodos e fundamentação teórica

Por meio de tal questionamento, realizamos um estudo a respeito da relação entre a utilização e a vulnerabilidade das redes *wireless*. Promovemos uma pesquisa entre os discentes do Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Campus Barreiras, a fim de acúmulo de dados, e fizemos destes uma base para a nossa pesquisa.

Com os resultados obtidos por meio de tal pesquisa, encontrou-se uma base consistente o suficiente para sustentar os questionamentos aqui propostos. Em seguida, utilizamos o Backtrack 4, um sistema

operacional baseado em Linux e focado em *forense* de redes (estudo da segurança, organização, e gerenciamento) em nossas pesquisas na tentativa de demonstrar a fragilidade da rede *wireless*.

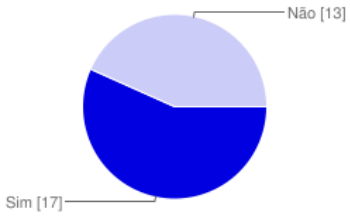


**Figura 1. Utiliza rede sem fio em casa**

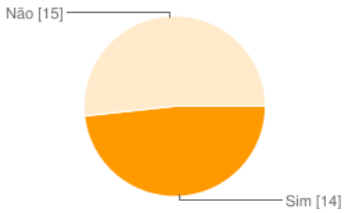


**Figura 2. Usa senha na sua rede?**

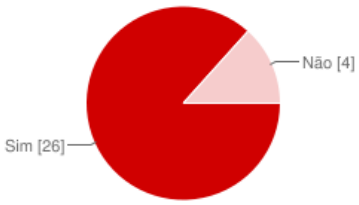


**Figura 3. Já usou rede sem fio em espaços públicos?**

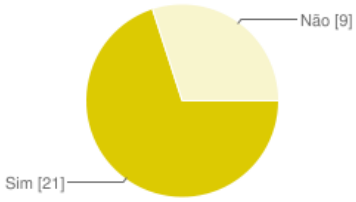


**Figura 4. Já utilizou internet banking ou compras on-line?**

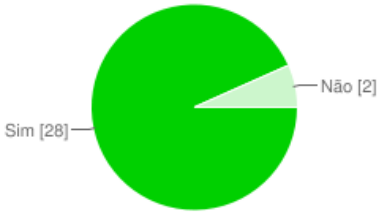


**Figura 5. Preocupa-se com vulnerabilidade dos seus dados?**

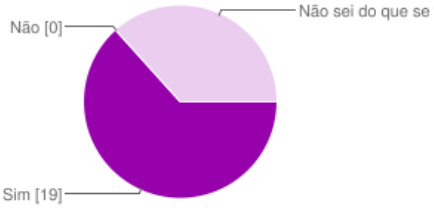


**Figura 6. Considera a criptografia de dados importante?**

## 3. Resultados e Discussão

Percebemos que 57% dos entrevistados utilizam algum tipo de rede sem fio em casa. Destes, apenas 47% protegem a rede com algum tipo de senha. 87% dos entrevistados, ainda, já utilizaram conexões sem fio em locais públicos, 70% já realizaram compras ou acessaram bancos pela internet, 93% se preocupam com a integridade e segurança de suas informações pessoais, porém apenas 63% sabem do que se trata a criptografia dos dados. Com tais dados, é possível perceber a difusão da conexão sem fio - mais da metade dos entrevistados usam wireless em casa, quase todos se preocupam com a integridade dos dados, porém pouco menos da metade utiliza algumas das várias técnicas de proteção existentes. Ao se falar em criptografia, pouco mais de 60% sabe do que se trata. É cada vez mais crescente o número destes usuários, porém acabam não percebendo que a

comunicação muda em praticamente todos os aspectos. As pessoas passam a “abandonar” os fios, mas esquecem de se adequar à nova situação.

Coma utilização do Backtrack 4, em poucos minutos e com cerca de sete linhas de código conseguimos quebrar uma senha do padrão WEP (o padrão considerado mais frágil, e por sua vez mais utilizado, de senhas de redes sem fio). Utilizando outras ferramentas, ainda é possível interceptar pacotes, furar proteções, desconectar estações remotamente, e até mesmo assumir o controle dos clientes da rede. Vale lembra que nenhuma rede é totalmente segura, mas há meios e ferramentas de obter mais segurança e tranquilidade.

## 3. Conclusões

Discutindo e analisando os resultados, percebemos a forte presença das conexões wireless na sociedade. É impossível imaginar a inexistência das conexões sem fio, a própria telefonia móvel, por exemplo, não poderia existir. Isto indica o nível de dependência e de confiança em tal tipo de conexão. As facilidades do uso da conexão sem fio são as mais variadas e irrefutáveis, é impossível questionar tal fato. No entanto, as facilidades de uso são refletidas de maneira diretamente proporcional na exposição dos dados, que literalmente trafegam pelo ar.

Existem diversas maneiras de aumentar significativamente o nível de segurança das redes sem fio, como ocultar o nome da rede, utilizar padrões de criptografia mais sofisticados, e aproveitar de tecnologias empregadas pelos grandes fabricantes de equipamentos, mas é essencial lembrar que não existe nenhuma barreira que seja intransponível. Toda rede pode ser invadida, especialmente uma rede onde as informações passam pelo ar, e é essencial tomar cuidado com tais casos em especial.

Espera-se, então, promover uma discussão detalhada sobre o assunto, promover os riscos da conexão sem fio, os cuidados que devem ser tomados, as diferentes funcionalidades, a vulnerabilidade, e como contornar tais fatores através das diferentes técnicas e métodos de criptografia. A sociedade deve entender que junto com a facilidade e a praticidade vêm outros fatores que devem ser encarados com muito mais seriedade do que são atualmente. Todos os usuários de qualquer rede sem fio devem ser educados adequadamente, o que revela o objetivo de nossa pesquisa.

Palavras-Chave: Wireless, Segurança, Criptografia.