REVISTA CIENTÍFICA DE
REDES DE COMPUTADORES
v.1, n.1, p-1-47, abr., 2018

VULNERABILIDADES EM REDES WI-FI

Vulnerabilities in Wi-Fi Networks

Robson Everton Sousa[1]
Edilson Lima Junior[2]

RESUMO

As redes sem fio (wireless) têm oferecido às pessoas facilidades em conecta-se à internet em distancias médias (WLAN). E com isso vem dando mais comodidade aos seus usuários. No entanto, os possíveis ataques por ela sofridos têm oferecido riscos ao usá-la, mas em meio a essas ameaças existem forma de corrigir as falhas que abrem portas aos possíveis atacantes. O que leva as redes a sofrerem ataques é devido à forma como os seus dados são transmitidos, por ondas de rádios que circulam fora dos limites físicos dos ambientes onde são instaladas, e em meio a isso pessoas mal intencionadas utilizam-se desses recursos para tentarem praticar crimes capturando dados sensíveis, como: senhas e números de cartões, informações profissionais, senha de servidores de redes e outras. Para combater essas ameaças os fabricantes juntamente com a 802.11 vêm construindo diversas ferramentas de segurança como WEP, WPA, WPA2 e outras formas de criptografia; autenticação dos usuários com a rede correta; servidores de autenticação e formas combinadas de criptografia e configuração por obscuridade. Contudo, elas apresentam grande vulnerabilidade relacionada à segurança, necessitando de uma análise prévia ao aderir a esta nova tecnologia. Assim sendo, este trabalho visa estudar a segurança, promovendo ferramentas na tentativa de orientar os usuários de como configurar e usar as redes Wi-Fi de forma segura e para isso cita as vulnerabilidades e as formas de configuração mais confiáveis.

Palavras-Chave: Redes Sem Fio, Wireless, Vulnerabilidades, Criptografia.

ABSTRAT

Wireless networks (wireless) have offered to people in facilities connects to the internet at medium distances (WLAN). And with that comes giving more convenience to its users. However, the potential attacks suffered by the applicant have offered risk to use it, but in the midst of these threats are no way to fix the flaws that open doors to possible attackers. Which brings networks to suffer attacks is because of the way your data is transmitted by waves radios circulating outside the physical boundaries of the environments where they are installed, and amid that bad guys use up those resources to try commit crimes capturing sensitive data, such as passwords and card numbers, information professionals, network servers and other password. To combat these threats manufacturers along with 802.11 are building several security tools such as WEP, WPA, WPA2 and other forms of cryptography; authentication of users with the correct network; authentication servers and combined forms of encryption and configuration by obscurity. However, they are highly vulnerable security-related, requiring a previous analysis by adhering to this new technology. Therefore, this work aims to study the security, promoting tools in an attempt to guide users on how to configure and use Wi-Fi networks securely and it cites the vulnerabilities and ways to more reliable configuration.

Keywords: Wireless Networks, Wireless, Vulnerabilities, Encryption.

[1]Técnico em Tecnologia da informação – UFMA - Especialista em Redes de Telecomunicação. Email: robsoneverton26@gmail.com
[2]Técnico em Tecnologia da informação – UFMA - Especialista em informática e Comunicação na Educação. Email: edilsonl@outlook.com

1 INTRODUÇÃO

A motivação para o desenvolvimento deste trabalho é para passar informações referente ao uso de rede Wi-Fi e indicar a melhor forma de uso, nos quesitos configuração- por parte dos profissionais que irão montá-la- e os usuários comum, sem conhecimentos técnicos, que queira monta uma rede sem fio em sua residência, mas lembrando em caso de duvidas não é recomendado que uma pessoa sem conhecimento em segurança em redes sem fio instale uma rede Wi-Fi.

No que toca a vulnerabilidade das redes sem fio é certo que todos gostariam que o conteúdo que transita nas WLANS permanecesse secreto, a salvo de bisbilhoteiros, mas não é bem isso que acontece, devido à transmissão dos sinais ocorrerem através de sinais de radiofrequência, os quais se propagam e podem cobrir áreas com dezenas de metros, de acordo com a potência de seus transmissores e a capacidade de seus receptores permitindo que os sinais de comunicação se estendam além das paredes de uma instituição ou residência possibilitando a captura de informações sensíveis.

Para que uma rede seja utilizada corretamente é necessário configura-la seguindo critérios de seguranças que são, considerados, fundamentais ao implementar-se uma rede sem fio. Diferentemente dos sistemas cabeados, para que a segurança seja afetada, o atacante deve estar conectado fisicamente a um ponto lógico da rede. Já, no contexto das redes sem fio a proteção do sistema deve ser feito através da implementação de protocolos de segurança.

Os protocolos de criptografia de dados mais utilizados são: WEP, WAP, WPA2, cada um deles com seu respectivo grau de segurança. O WEP já não é recomendado por possuir diversas vulnerabilidades; já o WPA tem um grau de segurança mais elevada que o WEP, mas sua segurança já foi superada por alguns métodos de quebra de criptografia o que o levou a ser tão vulneral quanto o WEP; Já em se tratando de WPA2, que é considerado um dos protocolos de segurança mais seguros, quando combinado com outras técnicas de segurança, são os mais recomendados em redes sem fio.

“O WPA puro é um esquema intermediário que implementa um subconjunto do 802.11i. ele deve ser evitado em favor do WPA2”. (TANENBAUM,2012).

2 METODOLOGIA

A metodologia utilizada foi à pesquisa descritiva, com abordagem qualitativa. A pesquisa descritiva é aquela em que se observa, registra, analisa e correlaciona fatos ou fenômenos sem manipulá-los.

Segundo Hori (2010) a abordagem qualitativa tem como principais características: Busca descrever significados que são socialmente construídos, e por isso é definida como subjetiva; tem características não estruturadas, é rica em contexto e enfatiza as interações; Através da coleta de dados qualitativos, obtêm-se respostas que são semiestruturadas ou não estruturadas; as técnicas de análise são indutivas, orientadas pelo processo, e os resultados não são generalizáveis.

A pesquisa foi realizada mediante o levantamento bibliográfico em livros, trabalhos acadêmicos, sites e portal de segurança da informação, buscando artigos e resoluções descritivas sobre segurança em Redes de computadores, principalmente Redes sem Fio. O levantamento bibliográfico foi a principal fonte de dados para fundamentação teórica no intuito de descrever as possíveis consequências de uso inadequado das redes sem fio e concomitante, o levantamento de alterna-

tivas de segurança.

3 REFERENCIAL TEÓRICO

As redes de computadores estão presentes no dia a dia das pessoas de uma forma que seria inimaginável viver sem elas. Por meio das redes de comunicações os indivíduos têm a oportunidade de se comunicarem com pessoas distantes, estudar, trabalhar, resolver os mais diversos problemas e muitas outras situações que hoje são indispensáveis para a demanda da humanidade.

Segundo, Mendes 2007, as redes vêm se tornando, a cada dia, um recurso indispensável para as pessoas e a internet é a principal responsável pelo aumento das redes de comunicações, entretanto, é importante conhecer as vantagens e desvantagens do uso dessas tecnologias que constantemente sofrem ataques com intuito de se obter acesso indevido.

Uma ameaça consiste em uma possível violação da segurança de um sistema. Algumas das principais ameaças ás áreas de computadores são: destruição de informação ou de outros recursos; modificação ou deturpação da informação; roubo, remoção ou perda de informação ou de outros recursos; revelação de informação; interrupção de serviços.

3.1 Tipos de Redes sem Fio

As LANs sem fios, foco do nosso estudo sugiram com objetivo de conectar dispositivos móveis sem precisar conectá-los via cabos. Com isso as pesquisas na área foram se intensificando e proporcionou em bons resultados na criação e expansão das redes sem fios resultando em diversas tecnologias capazes de transmitir dados via ondas de rádios.

Antes de começarmos a falar de redes 802.11, vamos primeiro apresentar as demais formas de comunicação sem fio. Como sabemos existem várias tecnologias para se montar uma rede sem fio, temos o infravermelho para a transmissão de dados entre computares, apesar de ser o precursor, apresenta uma grande desvantagem que são as baixas taxas de transmissão, curto alcance (1 metro) e necessitam de campo de visão entre o emissor e o receptor, sem que haja nem um obstáculo.

Temos também, considerada, como rede sem fio a tecnologia Bluetooth, que seguiu um caminho de desenvolvimento diferente da família 802.11 essa tecnologia opera na topologia Ad-Hoc em frequência de 2,4 GHz dando possibilidade de transmissão em curta distância entre telefones sem fio, celulares, impressoras, PDAs, notebooks, fax, teclado, ou seja, qualquer aparelho digital que use um chip Bluetooth. O objetivo principal do Bluetooth é simplesmente simplificar a comunicação e a sincronização entre esses dispositivos eletrônicos que hoje utilizam cabos para conectarem e sincronizarem entre si. (MENDES, 2007)

A tecnologia 802.11 que também é conhecido como Wi-Fi, mais vale lembrar que Wi-Fi e IEEE 802.11 não são a mesma coisa. Wi-Fi é uma marca registrada da aliança Wi-Fi, um grupo formado por diversos fabricantes. Para que um equipamento receba o nome Wi-Fi, o mesmo deve passar por uma série de procedimentos que o certifique como pertencente a esse grupo. (TORRES, 2014) Como foi comentado existem diversas formas de se utilizar redes sem fio, mas como objetivo, aqui, é tratar de vulnerabilidades em redes sem fio e especificadamente no padrão Wi-Fi, vamos nos ater em comentar somente essa tecnologia.

3.2 Wi-Fi (IEEE 802.11) – Redes Lan Sem Fio

Esta arquitetura de rede não faz uso de cabos de cobre nem fibra óptica. Os seus sinais são transmitidos entre os dispositivos que possui uma placa de rede sem fio através de ondas eletromagnéticas.

As redes no padrão 802.11 usam uma topologia lógica de barramento, que controla o acesso dos dispositivos a ela conectado, através de um sistema semelhante ao CSMA/CD das redes Ethernet. Esse barramento quando utilizado em redes sem fio é chamado CSMA/CA (Carrier Sense With Multiple Access and Collision Avoidance – algo como Sensor de portadora com Acesso Múltiplo. (CARVALHO,2013)

Para o funcionamento dessas redes é necessário que os seus dispositivos sejam dotados de placas de redes sem fio possuidoras de uma antena para transmitir e receber os sinais das outras placas em vez de conectores de Rj- 45, presentes em placas Ethernet. As redes sem fio IEEE 802.11 em sua grande maioria são apresentadas como cliente servidor

3.3 Sub -Padrões Wi-Fi 802.11

Mendes (2007), afirma que toda tecnologia necessita de um padrão para seguir, as redes Wi-Fi utilizam o padrão 802.11. Essa tecnologia refere-se às especificações desenvolvidas pelo Institute of Electrical and Electronics Engineers (IEEE) para redes sem fio, com intuito de evitar que cada fabricante produza um equipamento diferente, o que gera incompatibilidade.

Dentro do padrão IEEE 802.11, há diversos sub padrões desenvolvidos, entre eles podemos destacar alguns, como: o 802.11b: o padrão de rede Wi-Fi mais antigo usando uma frequência de 2,4 GHz e transmitindo dados a 11Mbp; o 802.11g: também utiliza a faixa de frequência de 2,4GHz e transmitindo dados em até 54 Mbps; o 802.11a: utilizada a faixa 5GHz para transmitir a 54Mbps. É um padrão pouco usado no Brasil; e o 802.11n: realiza transmissão da ordem de 300Mbps e usando duas faixas de frequência possíveis (2,4 GHz e 5 GHz) para que os equipamentos desse sub padrão possam se comunicar com todos os demais sub padrões.

3.3.1 Infraestrutura ou Cliente/Servidor

O modo infraestrutura ou cliente servidor, podemos dividi-lo em dois módulos: um básico voltado para usuários de ambientes domésticos ou para empresas de pequeno porte; ou em um modulo mais avançado, voltado para instituições de grande porte.

O modulo mais básico classificado como Basic Service Set (BSS). Nesse modo de operação a rede é comandada por um ponto de acesso, também conhecidos como “roteadores de banda larga”. Para que os computadores que estão na rede sem fio possam ter acesso a uma rede maior (rede da empresa ou internet), o ponto de acesso precisa estar conectado à rede através de cabos. Neste modo de operação a rede recebe um nome que é configurado pelo administrador da rede. Quando as estações desejam se associar ao ponto de acesso é necessário saber o nome da rede (SSID), e se exigido, a senha para autenticação. Esse tipo de rede também recebe um identificador aleatório de 48 bits (seis octetos) usando o mesmo padrão de endereçamento MAC, chamado BSSID. (TORRES, 2014)

No modo mais avançado de infraestrutura de redes sem fio (padrão 802.11) entra em ação a Ex-

tended Service Set (ESS) uma rede sem fio que possibilita a cobertura de grandes locais. O funcionamento dessa rede se dá utilizando vários pontos de acesso formando uma rede com o mesmo SSID possibilitando ao usuário maior área de cobertura, lhe garantindo maior conectividade com a rede mesmo estando em movimento. O usuário pode sair do alcance de um ponto de acesso e logo em seguida entra no alcance de outro, com isso aumentando o poder de mobilidade durante a conexão com a rede. Para que essa mobilidade ocorra de forma segura é necessário que o administrador da rede configure os seus pontos de acesso de forma idêntica, apenas respeitando configurações que possam causar conflito entre os pontos de acessos. Outro ponto crucial na elaboração do projeto dessas redes é respeitar o limite de interseção de no mínimo 10% na área de cobertura dos pontos de acesso.

Existe uma semelhança entre funcionamento da ESS com a telefônica celular (no caso dos telefones celulares a área de cobertura das antenas é chamada célula que o usuário pode transitar de uma célula para outra sem a perda da conexão). (TORRES, 2014)

3.4 Técnica de invasão

As pessoas que se utilizam de brechas nas configurações de redes sem fio geralmente utilizam-se de um planejamento para obter uma invasão bem-sucedida, portanto é necessária uma sequência de procedimentos que possibilitem ao atacante precisão. Existe uma serie de ferramentas e procedimentos como: o mapeamento da área a ser atacada, um dispositivo dotado de placa Wi-Fi, levantamento de quais programas serão necessários para varredura da rede e quebra da criptografia adotada.

A maioria dos mapeamentos, captura de trafego e ataques são feitos com programas especializo, devido às peculiaridades presentes nos subpadrões das redes sem fios (802.11b; 802.11; 802.11g e outros). Essas ferramentas são especializadas e podem ser encontradas de forma gratuitas. (RUFINO, 2015)

O Kismet é uma das ferramentas utilizadas para vários fins em relação a exploração de redes sem fio. Tal ferramenta é considerado bastante robusta em relação a muitos outros programas similares, números de chipsets suportados entre outras características. (RUFINO, 2015)

3.4.1 Utilização do kismet em exploração de redes WLAN (802.11)

Esse programa é bastante utilizado para identificação das redes sem fio em uma determinada localidade. Durante o mapeamento da área, os principais dados levantados pelo Kismet, são: Nome da rede (SSID); Nível de sinal; Existência de criptografia (WEP); Canal utilizado; Informações sobre clientes conectados; Endereço MAC dos participantes (concentradores inclusive); bloco de endereço IP utilizado; quantidade de pacotes transmitidos; padrão utilizado (802.11 a/b/g). (RUFINO, 2015).

O processo de captura de trafego utilizando o Kismet releva diversas informações que circulam na rede. Esses dados coletados são armazenados em um arquivo com extensão. dump, mas também existe a possibilidade de ser visto em tempo real por um possível atacante. Essa funcionalidade é particularmente útil em redes sem criptografia, quer nativa (WEP, WPA e etc.). A captura das informações que circulam na rede tem como principal finalidade obter informações sensíveis, como: senha de acesso a servidores externos, entre outras possibilidades. (RUFINO,

2015)

3.5 Tipos de ataque

3.5.1 Fake AP

Dos inúmeros problemas relacionados a redes sem fio, o Fake AP é só mais uma ferramenta de ataque a redes sem fio. A finalidade dessa ferramenta é de tentar se interpor entre o dispositivo e o ponto de acesso legítimo ou tentar se fazer por esse ponto de acesso. Durante a associação do dispositivo e o ponto de acesso falso são capturados dados que trafegam na rede (senhas, números de cartão de crédito e outras informações sensíveis). (RUFINO, 2015)

Essa forma de explorar redes sem fio, só ganha força por ter a possibilidade de convencer o cliente que realmente está associado ao concentrador correto, para que isso ocorra são utilizadas várias alternativas como: receber conexões em um canal específico; usar SSID específico; utilizar um endereço MAC específico ou o padrão de um determinado fabricante; usar uma determinada chave WEP; permitir configuração de potência de saída.

Apesar de o Fake AP utilizar dessas artimanhas o mesmo possui limitações estruturais para convencer o cliente de que ele estar conectado à rede certa, isso ocorre pelo fato de não existir relação com os concentradores legítimos, no sentido de redirecionamento do trafego para o concentrado oficial depois de capturar a informação desejada e com isso facilitando que o cliente perceba que existe algum problema na rede.

3.5.2 Escuta de trafego

A escuta de tráfego é um dos principais meios de os invasores de redes (seja ela cabeada ou sem fio) planejarem e invadirem redes de computadores. Os alvos mais fáceis de serem atacados são as redes que transmitem dados sem cifragem ou com criptografia fraca, no caso da última existem vários programas com capacidade para quebrar a criptografia. (RUFINO, 2015).

3.5.3 Ataque Homem-no-meio

Esta forma de ataque é conhecida por homem do meio por ser feito a um concentrador que está posicionado no meio de uma conexão de rede sem fio. Normalmente este ataque é feito clonando-se um concentrador já existente ou criando outro para interpor-se aos concentradores oficiais, recebendo assim as conexões dos novos clientes e as informações transmitidas na rede (RUFINO, 2007).

3.6 Métodos de Defesa

Existe alguns métodos de defesa por obscuridade que possibilitam um certo grau de segurança a redes sem fio, mas esses métodos não possibilitam segurança total a rede. Pois existem vários programas computacionais que possibilitam revelar informações que estão criptografadas ou ocultas.

3.6.1 Configuração do concentrador

3.6.1.1 Desabilitar a difusão do SSID.

Desabilitar essa função é uma das principais recomendações de qualquer manual de segurança em redes sem fio. Por meio dessa configuração, os administradores de redes tentam evitar que pessoas externas à rede saibam o nome da mesma e tente acessá-la. Essa forma de configuração por obscuridade tenta impedir que pessoas más intencionadas venham fazer uso da rede para fins ilícito. (RUFINO, 2015)

Essa técnica resulta eficiência quando combinada com outras técnicas subjetivas. Essa configuração tem se mostrado quase que inócua, visto que existem possibilidades de ataques que não necessitam conhecer o nome da rede. Pois o simples fato de escutar o trafego da rede já oferece subsídios para o atacante obter o nome e outros dados da rede, já que essas informações passam em claro pela rede em vários momentos, como: beacons, busca por concentrador ativo; resposta à busca por concentrador; requisição de associação; requisição de reassociação. (RUFINO, 2015)

3.6.1.2 Modificando o nome ESSID-padrão

Essa configuração tenta impedir que o ponto de acesso tente difundir o ESSID-padrão que geralmente vem configurado com o nome do fabricante e modelo, sendo essas duas informações essenciais para um atacante realizar seus ataques.

> Esse procedimento também tende a ser categorizado como segurança por obscuridade, porem o problema com esta categoria existe apenas quando toda a segurança é baseada somente na obscuridade, ou seja, o atacante em princípio não pode promover um ataque bem-sucedido, porque desconhece algumas características do alvo, portanto se, ou quando ele tiver essa informação, o alvo estará completamente vulnerável. (RUFINO, 2015)

Apesar de os administradores de redes modificarem os nomes das redes não se tem garantia de que não descobriram as informações básicas do ponto de acesso. Pois essas medidas não são suficientes para conter as inúmeras ameaças que rodeiam as redes sem fio. Outra possível falha que ocorre ao se renomear um ponto de acesso é quando se coloca o nome do ponto de acesso associado ao nome do proprietário da rede (nome da empresa, ao o nome pessoal). A coleta desses dados possibilita aos atacantes saberem quais os tipos de dados podem circular na rede.

3.6.1.3 Substituição do endereço MAC

É recomendável a substituição do endereço MAC, pois esse endereçamento está associado ao fabricante e com isso possibilitam aos atacantes obterem informações para um possível ataques a rede.

Essa mudança não gera transtorno ao usuário e, por outro lado, evita a identificação imediata do fabricante por parte de um possível atacante. Mas esta ação por si só não garante a segurança de uma instalação, portanto deve ser combinada com outras medidas para obter um ambiente com a segurança mais próxima da ideal. (RUFINO, 2015)

3.6.1.4 Desabilitar acesso ao concentrador via rede sem fio.

A maioria dos concentradores oferecem acesso via HTTP e TELNET, e como esses dois protocolos não oferecem criptografia, é recomendado desabilitar essas opções do lado da rede sem fio, para evitar que os pacotes com usuário e senha sejam capturados por um possível atacante. Essa alternativa deixa aos cuidados da rede cabeada o acesso ao concentrador, desde que a mesma seja dotada de mecanismo de proteção que possibilite monitorar e autenticar os usuários restringindo o acesso ao concentrador. (RUFINO, 2015)

3.6.1.5 Defesa dos equipamentos clientes

Devem ser levadas em consideração a defesa do cliente que possui duas situações a serem consideradas, uma diz respeito à inviolabilidade de comunicação, dados e equipamentos do usuário e a outra precaução é evitar que atacantes cheguem ao equipamento do usuário revele chaves e outras informações que de acesso à rede com as credenciais capturadas da máquina do cliente. (RUFINO, 2015)

3.6.1.6 Desabilitar comunicação entre os clientes

A funcionalidade dessa configuração é evitar o acesso de um cliente a outros ligados ao mesmo concentrador, função conhecida como PSPF (Publicly Secure Packert Forwarding), em que há separação física do trafego, este método não evita a captura do trafego, portanto, como medida isolada, não garante a privacidade do usuário.

3.7 Segurança em Redes Wi-Fi Grátis

Um grande problema de usar redes Wi-Fi grátis ocorre geralmente por falta de criptografia na transmissão dos dados ou quando está, a senha é conhecida. Assim, qualquer hacker “escutando” o tráfego da rede pode sniffar a rede capturando as informações por ela trafegada, tais como logins e senhas de acesso a sites e serviços. Apesar de alguns utilizar o protocolo https para o tráfego de informações sensíveis, que criptografa os dados saindo do seu computador, mas não é recomendável contar só com essa medida de segurança.

4 CONSIDERAÇÕES FINAIS

O processo de manter uma rede Wi-Fi segura é algo muito intenso devido à comunicação ser por meio de sinais de rádio, não tendo a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Devido a isto, os dados trafegados podem ser interceptados por qualquer pessoa próxima possuindo programa especifico, como o Kismet, e um equipamento com placa de redes sem fio (por exemplo, um notebook ou tablet).

Apesar de IEEE 802.11 e fabricantes desenvolverem ferramentas que permitem segurança nas redes sem fio. Existem também pessoas mal intencionadas que estão sempre atentas para explorar as vulnerabilidades da rede através de ferramentas de ataques. Vale lembrar que as falhas de segurança nessas redes quando descobertas devem ser urgentemente corrigidas para evitar que pessoas de má índole tenha acesso aos dados que trafegam na rede.

É essencial que os gerentes de redes e os usuários estejam atentos às recomendações de segurança, tanto em ambientes corporativos, quanto em ambientes domésticos, sendo este caso o mais vulnerável porque se acredita que ninguém está interessado em dados de redes domesticas.

Existem várias recomendações para possuir uma rede Wi-Fi segura. Umas dessas recomendações partem da cartilha de segurança para internet – versão 4.0, que orienta quais os cuidados são necessários para usar redes Wi-Fi com segurança. Algumas dessas recomendações são:

• Habilite a interface de rede Wi-Fi do seu computador ou dispositivo móvel somente quando usá-la e desabilite-a após o uso;

• Use, quando possível, redes que oferecem autenticação e criptografia entre o cliente e o AP (evite conectar-se a redes abertas ou públicas, sem criptografia, especialmente as que você não conhece a origem);

• Evite usar WEP, pois ele apresenta vulnerabilidades que, quando exploradas, permitem que o mecanismo seja facilmente quebrado;

• Use WPA2 sempre que disponível (caso seu dispositivo não tenha este recurso, utilize no mínimo WPA).

Essas indicações são para possuir um nível de segurança aceitável. Já para a configuração das redes doméstica é necessário seguir essas recomendações, assim também nos recomenda a cartilha de segurança para internet:

• Posicione o AP longe de janelas e próximo ao centro de sua casa a fim de reduzir a propagação do sinal e controlar a abrangência (conforme a potência da antena do AP e do posicionamento no recinto, sua rede pode abranger uma área muito maior que apenas a da sua residência e, com isto, ser acessada sem o seu conhecimento ou ter o trafego capturado por vizinhos ou pessoas que estejam nas proximidades);

• Altere as configurações padrão que acompanham o seu AP. Alguns exemplos são:

1. Altere as senhas originais, tanto de administração do AP como de autenticação de usuários;
2. Assegure-se de utilizar senhas bem elaboradas e difíceis de serem descobertas;
3. Altere o SSID (Server Set IDentifier);
4. Ao configurar o SSID procure não usar dados pessoais e nem nomes associados ao fabricante ou modelo, pois isto facilita a identificação de características técnicas do equipamento e pode permitir que essas informações sejam associadas a possíveis vulnerabilidades existentes;
5. Desabilite a difusão (broadcast) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos;
6. Desabilite o gerenciamento do AP via rede sem fio, de tal forma que, para acessar funções de administração, seja necessário conectar-se diretamente a ele usando uma rede cabeada. Desta maneira, um possível atacante externo (via rede sem fio) não será capaz de acessar o AP para promover mudanças na configuração.

• Não ative WEP, pois ele apresenta vulnerabilidades que, quando exploradas, permitem que o mecanismo seja facilmente quebrado;

• Utilize WPA2 ou, no mínimo, WPA;

• Caso seu AP disponibilize WPS (Wi-Fi Protected Setup), desabilite-o a fim de evitar acessos indevidos;

• desligue seu AP quando não usar sua rede.

Em alguns casos, as redes sem fio, principalmente em ambiente domésticos, são instaladas incorretamente não seguindo a determinados níveis de segurança e com isso se tornam vulneráveis à

ação de pessoas mal-intencionadas. Portanto, não é seguro que uma pessoa sem conhecimentos técnicos tente instalar uma rede sem fio, por isso o recomendado é sempre buscar ajuda técnica, isto ajudará a prevenir ameaças e riscos de sua rede ser invadida.

REFERÊNCIAS

Cartilha de Segurança para Internet, versão 4.0 / **CERT.br** – São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CARVALHO, João Antônio. **Informática para concursos**: teoria e questões. Rio de Janeiro. Elsevier, 2013.

MENDES, Douglas Rocha. **Redes de Computadores:** teoria e pratica. São Paulo. Novatec, 2007.

TORRES, Gabriel. **Redes de Computadores**. 2. ed. Rio de Janeiro: Nova Terra, 2014.

RUFINO, Nelson Murilo de Oliveira. **Segurança em redes sem fio:** aprenda a proteger suas informações em ambientes Wi-Fi e bluetooth 4. Ed. São Paulo:
Novatec, 2015.

_____. **Segurança em redes de computadores:** aprenda a proteger suas informações em ambientes Wi-Fi. 2. ed. São Paulo: Novatec Editora, 2007.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores.** Tradução Daniel Vieira. 5. Ed. São Paulo: Pearson Prentice Hall, 2011.