GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA MICROEMPRESA

Autores:

Danielle de Cássia da Silva Malcher Lobato

Daniel da Silva Malcher

Thiago Lobato Rodrigues

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA MICROEMPRESA

RESUMO

Este trabalho apresenta uma análise da infraestrutura de rede sem fio de uma clínica odontológica localizada na cidade de Belém, Estado do Pará. O empreendimento possui uma rede Wi-Fi que apresenta falhas e vulnerabilidades de segurança, o que pode gerar transtornos e prejuízos tanto para a clínica quanto para seus funcionários e clientes. Esta análise tem como objetivo geral aprimorar a segurança da rede sem fio desta empresa, buscando, de maneira mais específica, identificar suas falhas e vulnerabilidades de segurança, implementando, posteriormente, medidas para corrigi-las. Este trabalho foi realizado em diferentes etapas, cumpridos todos seus objetivos a partir de uma metodologia moldada na utilização do *software Shield Test* e do equipamento *Mikrotik Wireless*, que possibilitou a tomada de medidas que objetivam sanar as falhas de segurança encontradas, possibilitando que o estabelecimento atue de maneira mais segura e confiável.

Palavras-chave: Segurança de rede; Internet; Wi-Fi; Vulnerabilidade.

ABSTRACT

This paper presents an analysis of the wireless network infrastructure of a dental clinic located in the city of Belém, Pará State. The enterprise has a Wi-Fi network that presents flaws and security vulnerabilities, which can generate inconvenience and losses for both the clinic and its employees and customers. The general objective of this analysis is to improve the security of the company's wireless network, and, more specifically, to identify its flaws and security vulnerabilities, and then implement measures to correct them. This work was carried out in different stages, fulfilling all its objectives from a methodology modeled on the use of Shield Test software and Mikrotik Wireless equipment, which enabled the taking of measures that aim to remedy the security flaws found, allowing the establishment to act in a more secure and reliable way.

Keywords: Network security; Internet; Wi-Fi; Vulnerability.

1 INTRODUÇÃO

Na década de 60 nasceram os primeiros esboços daquilo que viria a ser uma das grandes invenções do homem no último século, entretanto, em seu princípio básico, a internet possuía objetivos bem diferentes dos atuais, resumia-se à rede de conexão da DARPA, Agência de Projetos de Pesquisa Avançada dos Estados Unidos, que focava na área militar do país, com a intenção de ajudar na sua proteção durante a Guerra Fria, conflito que polarizou o mundo entre os EUA e a União Soviética naquela época (BARROS, 2013).

Dessa época até os dias atuais, o objetivo da internet mudou, o foco agora, ensina Barros (2013), é o entretenimento e o mundo *business* (negócios). Além disso, a pulverização de dispositivos que acessam a rede, como os smartphones, presentes em 99,5% dos lares brasileiros de acordo com Ministério das Comunicações, contribuiu para a popularização e consequente aumento do número de acessos à Grande Rede, assim, hoje é inimaginável pensar em nossas vidas sem redes sociais, e-mails e sites de buscas.

Frente a isso, Castells (2003) afirma que o efeito da Internet no início do século XXI na vida humana é similar ao da eletricidade no início do século XX, ou seja, se o século XX foi moldado pelas diferentes aplicações da energia elétrica, o século XXI será moldado pelas diferentes aplicações da informação, que pode ser obtida de todas as fontes existentes nesse espaço de experiências amplificadas que é a Internet, onde pessoas podem falar com qualquer um a qualquer tempo sobre qualquer coisa.

Segundo o Ministério das Comunicações, 82,7% dos domicílios nacionais possuem atualmente acesso à internet, seja ela móvel (3G ou 4G), cabeada ou sem fio, também conhecidas como Redes *Wireless Fidelity* (Wi-Fi), que possibilita uma grande expansão no uso dos dispositivos móveis, fornecendo, dentre suas principais características, maior mobilidade (TANEMBAUM, 2003).

Por essa mobilidade, a conexão sem fio se tornou tão importante ao ponto de que salas de conferências, aeroportos, hotéis, bares, restaurantes e até consultórios médicos/odontológicos passaram a oferecê-la como diferencial aos seus clientes, possibilitando-os de acessar a internet a partir de seus dispositivos móveis (RUFINO, 2005), além disso, complementa Kotler (2003), a internet oferece novas possibilidades para as empresas conduzirem seus negócios com mais eficiência.

Em ambientes corporativos, as redes sem fio são cada vez mais utilizadas como um auxiliar precioso para as LANs (*Local Area Networks*) convencionais, seja por prover vantagens econômicas, seja por prover mobilidade aos usuários e facilidade de instalação (DUARTE, 2003). Entretanto, alerta Grégio (2005), o meio não-guiado por onde as informações destas redes trafegam, usando ondas de rádio, é extremamente inseguro, uma vez que os dados estão suscetíveis à escuta e a ataques diversos.

Apesar disso, grande parte das pequenas empresas não se preocupam com a segurança de sua rede, uma vez que, segundo Oliveira (2021), essas são alvo de 43% dos ataques cibernéticos. Isso ocorre, especula-se, devido à falta de conhecimento dos empresários acerca dos riscos ou ao limitado fluxo de caixa que a maioria dessas empresas possui, o que torna improvável que uma empresa de pequeno porte tenha uma equipe de segurança de TI dedicada, capaz de responder rapidamente a esses ataques.

Assim, redes de pequenas empresas se tornaram um alvo fácil para pessoas mal intencionadas, desejosas em comprometer sistemas e/ou roubar informações sigilosas, pois, disponibilizam inúmeros atrativos como dificuldade na identificação da origem exata do ataque, imaturidade das opções e protocolos de segurança para esse tipo de tecnologia, facilidade em obter acesso à rede guiada através de uma conexão de rede sem fio e, principalmente, a falta de conhecimento técnico da maioria dos usuários adeptos desta tecnologia (DUARTE, 2003).

Levando tal fato em consideração, este estudo concentra-se em uma microempresa que atua no mercado odontológico, um consultório localizado na cidade de Belém no Estado do Pará, e busca, a partir de uma análise de segurança de sua rede de internet sem fio, tomar medidas que sanem suas possíveis falhas e vulnerabilidades e que, ao mesmo tempo, demandem nenhum ou pouco investimento, com a finalidade de se criar um ambiente de rede mais seguro para usuários e clientes e que, concomitantemente, sejam compatíveis com a realidade financeira da empresa.

1.1 OBJETIVOS

1.1.1 OBJETIVO GERAL

Aprimorar a segurança da rede sem fio de uma clínica odontológica.

1.1.2 OBJETIVOS ESPECÍFICOS

- Analisar a infraestrutura de rede sem fio, identificando possíveis falhas e vulnerabilidades de segurança;
- Executar ações e melhorias que sanem as falhas e vulnerabilidades encontradas.

1.2 PROBLEMA

Analisando o sistema de rede utilizado pela clínica odontológica foco deste estudo, verificou-se que a mesma utiliza um do tipo WLAN (4 (802.11n)), com um modem e um roteador transmissor de Wi-Fi, utilizando o nome de usuário e senha do roteador padrão de fábrica, tudo isso disponibilizando a rede sem fio livremente (sem senha) para todos os clientes e funcionários (usuários).

Foi verificado, também, que o estabelecimento não possui um sistema de banco de dados seguro para armazenamento das informações dos clientes, uma vez que as mesmas ficam armazenadas livremente no computador da empresa e a mesma não utiliza nenhum *software* ou *hardware* de proteção de rede.

Destarte, ao fim dessa análise inicial, constatou-se os seguintes problemas:

- Utilização de SSID, nome de usuário e senha do roteador padrão de fábrica, o que facilita, consideravelmente, que pessoas mal-intencionadas tenham acesso às informações da clínica odontológica, de seus funcionários e clientes;
- Não possui proteção de Aps e/ou *hardwares* de rede, aumentando a exposição dos dados confidenciais guardados pela empresa;
- Compartilhamento livre (sem senha) da rede Wi-Fi com os colaboradores e clientes, fato esse que, somado aos demais problemas encontrados, enfraquece, sobremaneira, a segurança da rede sem fio do estabelecimento.

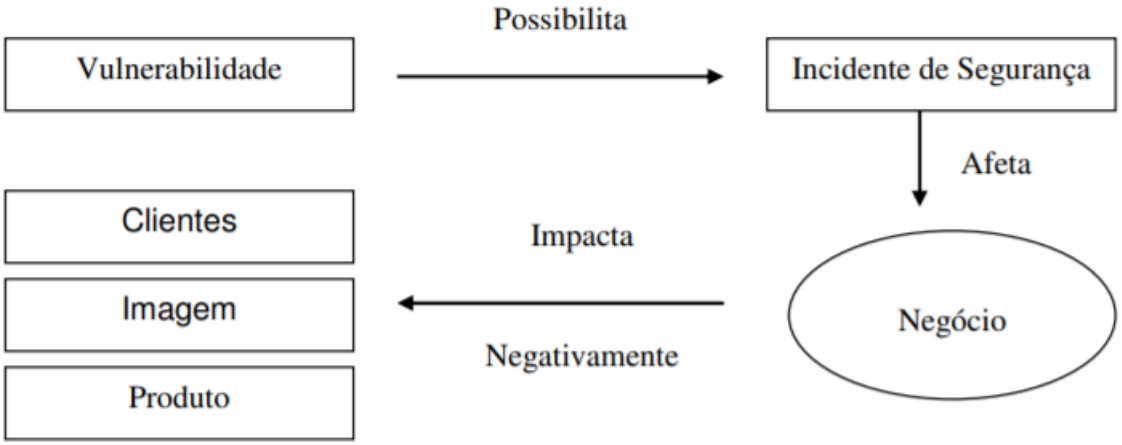
1.3 JUSTIFICATIVA

Como exposto no tópico anterior, a clínica odontológica foco deste estudo possui graves falhas e vulnerabilidades na sua rede de internet sem fio. Tal situação, consequentemente, escancara as portas para que pessoas mal-intencionadas (*hackers*) se aproveitem dessas brechas de segurança para roubar dados e informações sigilosas da própria

clínica, de seus funcionários e de seus clientes, podendo gerar constrangimentos e prejuízos de ordem financeira para as vítimas, além de processos de ordem judicial contra a empresa.

Moreira (2001) esclarece que vulnerabilidades possibilitam o surgimento de incidentes de segurança e que esses, por sua vez, afetam o negócio da empresa causando impactos negativos para todos os envolvidos no processo, inclusive para a imagem do estabelecimento, a figura abaixo ilustra essa situação:

Figura 1 – Impacto dos incidentes de segurança para empresas



Fonte: Moreira (2001).

Frente a topo exposto, e considerando que 60% das pequenas empresas fecham as portas após sofrerem um ataque em sua rede (OLIVEIRA, 2021), este estudo se justifica pela sua intenção de evitar, além da falência da empresa em questão e consequente desemprego de seus funcionários, que pessoas inocentes tenham seus dados pessoais e bancários expostos de forma a lhes causarem algum tipo de dano.

2 METODOLOGIA

Neste artigo, a metodologia de estudo empregada é o estudo de caso, através da análise experimental com o levantamento das vulnerabilidades existentes na infraestrutura de rede sem fio e das técnicas de invasão utilizadas para aproveitar estas brechas da segurança que podem ser observadas no sistema utilizado pela clínica odontológica.

Conforme descrito por Gil (apud SILVA, 2009), considera-se pesquisa experimental o ato de se determinar um objeto de estudo, verificando as variáveis que são capazes de inferi-lo, tendo ainda controle e observação dos efeitos que ela produz no objeto.

Em um primeiro momento se realizou o levantamento das problemáticas que o sistema de rede sem fio da clínica apresenta. Tais informações foram aferidas através da observação in loco com a utilização do Shield Test, software que mede a suscetibilidade da rede à infecção e avalia os níveis de defesa existentes contra ataques potenciais.

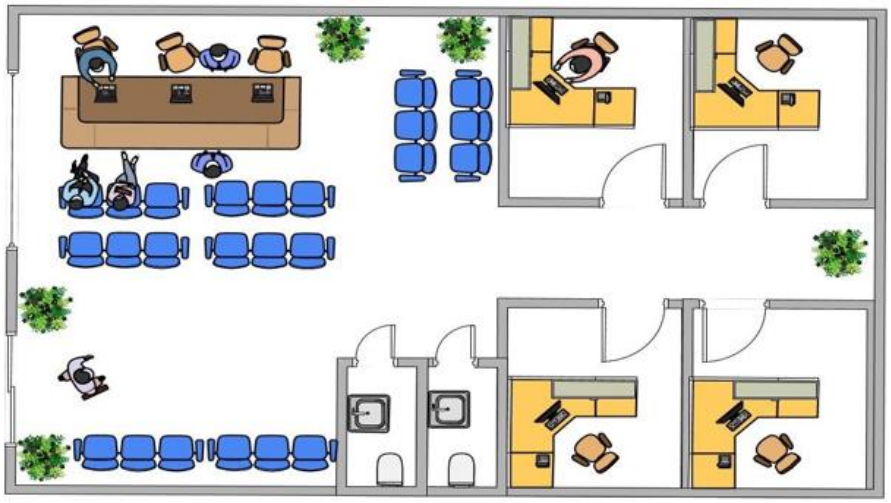
Por fim, foi utilizado o equipamento Mikrotik Wireles para a resolução das problemáticas em modo geral.

3 ESTUDO DE CASO

3.1 CARACTERIZAÇÃO DA EMPRESA

A Clínica Odontológica estudada se localiza em uma rodovia de grande movimentação na cidade de Belém, Estado do Pará, em um bairro de classe média caracterizado como residencial e comercial, onde desde 13 de janeiro de 2020 oferece diversos serviços odontológicos a seus clientes. O empreendimento é considerado uma microempresa, contando, além do gerente, com apenas 11 colaboradores, dentre os quais 7 são profissionais da área de saúde bucal (dentistas e protéticos), 3 são recepcionistas e 1 responsável pelos serviços gerais. A figura 2, abaixo, elucida a estrutura física da clínica:

Figura 2 - Planta baixa da clínica odontológica



Fonte: Autoria própria**.**

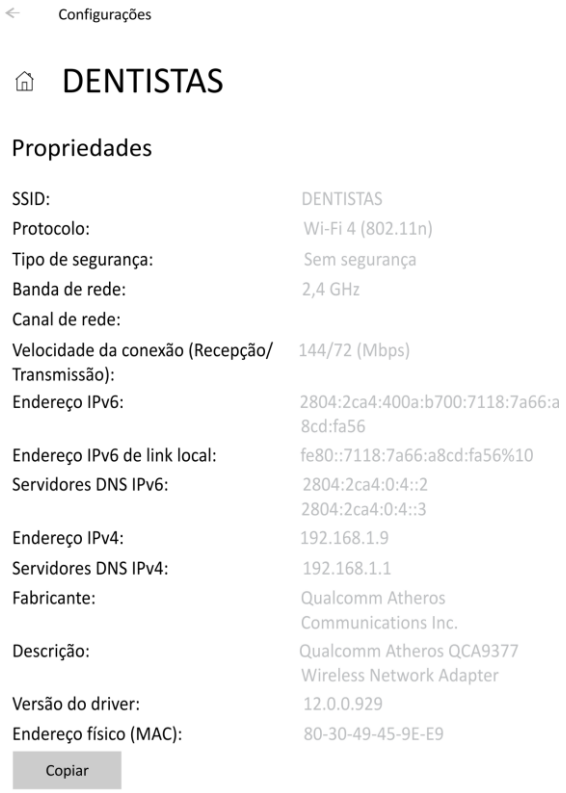
Como já mencionado no item 1.2, a rede sem fios da clínica odontológica estudada possui graves falhas de segurança e vulnerabilidades que colocam dados sigilosos da própria empresa, dos seus funcionários e de seus clientes expostos à pessoas mal intencionadas (*hackers*). A figura 3, abaixo, mostra qual roteador é utilizado pelo empreendimento:

Figura 3 – Roteador utilizado na clínica odontológica

Fonte: Acervo próprio.

Complementando, a figura 4, a seguir, aclara a configuração da rede sem fio utilizada pela clínica odontológica alvo deste estudo, evidenciando o que foi anteriormente relatado, que a rede Wi-Fi da empresa é livre para todos (sem segurança), ou seja, não é necessária a utilização de senha para acessá-la:

Figura 4 - Configurações do roteador utilizado na clínica odontológica



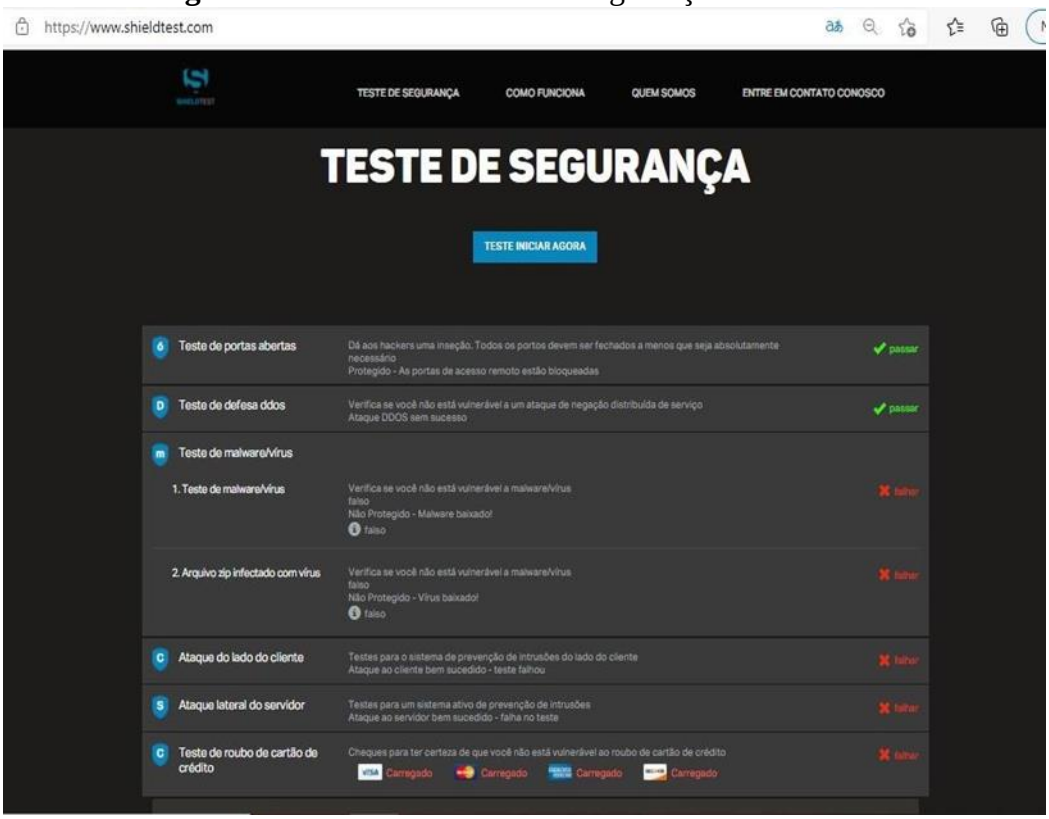
Fonte: Roteador FiberHome.

Após analisar as configurações da rede sem fio da empresa estudada, executou-se um teste de segurança utilizando o *software Shield* Test, que mede a suscetibilidade de determinada rede à infecção e avalia os níveis de defesa existentes contra ataques potenciais, enviando amostras de *malware* transmitidos pelo servidor da ferramenta para realizar uma autoavaliação, possibilitando analisar os seguintes itens:

- Teste de portas abertas;
- Teste de Defesa DDOS;
- Teste de *malware*/vírus;
- Teste de roubo de dados.

Torna-se necessário destacar que, ao finalizar as análises no *Shield Teste*, os dados são removidos do *software*, não fornecendo risco ao sistema que é avaliado, tornando está uma plataforma legitima e segura. Dito isso, ao final do teste, obteve-se o resultado explicitado na figura 5, a seguir:

Figura 5 – Resultado do teste de segurança de rede Wi-Fi



Fonte: *Shield Test*.

4 ANÁLISE DOS RESULTADOS

Através do teste foi possível verificar que a rede Wi-Fi da clínica se encontra protegida em relação aos testes de portas abertas. Esse resultado é importante, visto que o contrário poderia significar uma exposição maior, aumentando o risco de que estas portas fossem exploradas por *hackers* e intrusos cibernéticos em busca de vulnerabilidades no sistema, o que permitiria a invasão de serviços, podendo resultar na obtenção informações sigilosas da empresa, de seus funcionários e clientes.

Outro resultado positivo foi verificado para o teste de defesa DDOS, mostrando que a empresa não está propícia a ter suas operações interrompidas devido a falhas na rede causadas por terceiros de má fé.

No entanto, resultados negativos também foram verificados, apontando que a clínica se encontra desprotegida em relação aos testes de *malware*/vírus, ataque do lado do cliente, ataque lateral do servidor e teste de roubo de cartão de crédito, assim, pode-se afirmar que

somente possuir antivírus no computador não é garantia de se ter a proteção que a empresa precisa, bem como, o não bloqueio de arquivos zip infectados, a não utilização de IPS e a ausência de um mecanismo DLP deixam vulneráveis os arquivos e informações da empresa, de seus funcionários e clientes.

5 AÇÕES PARA A SOLUÇÃO DOS PROBLEMAS ENCONTRADOS

Como mencionado anteriormente, a clínica odontológica alvo deste estudo é caracterizada como uma microempresa, assim, não possui orçamento disponível para grandes investimentos em equipamentos ou *softwares* de segurança de rede, deste modo, procurou-se executar medidas que sejam eficientes e, ao mesmo tempo, demandem pouco ou nenhum investimento financeiro por parte da empresa. Desta feita, para solucionar as falhas e vulnerabilidades encontradas, as seguintes ações foram tomadas para aprimorar a segurança da rede sem fio do estabelecimento em questão:

1. A aquisição de novos equipamentos, roteador e modem Wi-Fi, para uma conexão que transmita dados de forma rápida, estável e com maior alcance de cobertura;
2. Atribuir um novo usuário e senha do administrador para ter acesso a interface do roteador;
3. Proteger a rede sem fio, a partir da atribuição de uma senha forte para utilização da rede Wi-Fi, ou ocultá-la, de modo que apenas os funcionários poderiam acessar a rede do local;
4. Alterar essa senha periodicamente, com o intuito de dificultar a quebra da mesma;
5. Alterar o endereço de IP (em português, Protocolo de Internet) do roteador, para possibilitar uma segunda rede para um outro equipamento que servirá para o acesso dos clientes, em caso de se optar por ocultar a rede. A mudança de IP é feita para que não haja conflito de IP`s na rede, essa medida também serve para garantir maior segurança.
6. Utilizar um serviço de protocolo de Virtual Private Network (VPN), em português, Rede Privada Virtual, denominação dada para uma forma de interligar a rede da organização, com a característica principal de criar o denominado “túnel virtual” de comunicação que possibilita a interligação das redes de modo seguro,

fazendo o uso de criptografia entre pontos autorizados para a transferência de informações, aumentando a segurança na recepção de dados

Segundo Simões (2013), a implementação da VPN atende a três fatores fundamentais: a confidencialidade, referindo-se a limitar o acesso a informações, geralmente através do uso de criptografia; integridade, assegura que os dados não serão alterados durante uma transmissão e autenticação, verifica se a pessoa com quem se está trocando informações sigilosas é realmente quem deveria ser.

Foi utilizado o equipamento *Mikrotik Wireless* para a resolução das problemáticas em modo geral. O uso do *Mikrotik* tem vantagens de administração de rede e possuem diversas ferramentas que podemos configurar dentro dele, como o servidor o DHCP, a qual podemos configurar a faixa de IP que vai rodar, possibilitando criar uma rede, sub-rede ou uma VLAN, assim, aumentando o nível de segurança da rede devido a faixa de rede estabelecida.

Além disso, esse equipamento também controla os *brodcasts* em colisão de pacotes de rede e possibilita o levantamento do serviço de *firewall*, onde se pode configurar as regras e quais tipos de sites estão disponíveis para o acesso na rede, podendo-se bloquear sites pornográficos, redes socias e outros.

Além do *MItrokit*, foram usados três *access point*, um deles para o uso exclusivo dos clientes (visitantes), o qual fica na área da recepção com limitações em relação ao servidor e aos equipamentos da clínica, como: computadores, impressora e máquinas *wireless* de cartão de crédito.

A figura 6 demonstra a planta da clínica com as melhorias da rede de forma física (estrutural), com equipamentos instalados em lugares corretos para que o sinal *wireless* seja distribuído de forma que fique ao alcance dos dispositivos e trazendo uma transferência de dados rápida e com respostas significativas.

Figura 6 – Planta demonstrativa com as melhorias da rede de forma física (estrutural) da clínica odontológica. 1: área de recepção da clínica; 2: área dos consultórios.

Fonte: Elaboração própria.

5 CONSIDERAÇÕES FINAIS

O acelerado aumento das redes Wi-Fi nos últimos anos se deve, especialmente, à mobilidade propiciada aos usuários, à facilidade de implementação e pela redução dos preços dos seus dispositivos, o que propiciou uma rápida popularização destas redes, tanto em sua implementação coorporativa quanto pessoal (AGUIAR, 2005).

O estudo realizado pôde atestar e comprovar falhas e vulnerabilidades graves presentes na rede Wi-Fi da clínica odontológica alvo deste estudo, abrindo brechas na segurança que permitiriam que pessoas mal intencionadas, os *hackers*, se aproveitassem da situação para roubar dados sigilosos da empresa, dos seus funcionário ou de seus clientes, o que poderia acarretar em sérios problemas de cunho pessoal para vítimas, além de prejuízos financeiros.

É notório, entretanto, que Independente do nível de segurança implementado ou possível de ser adotado em redes sem fio, elas sempre apresentarão riscos e vulnerabilidades (RUFFINO, 2005), por esse motivo, recomenda-se a constante manutenção e monitoração do ambiente sem fio implementado, pois, na maioria dos casos, é utilizada uma simples configuração dos mecanismos básicos de segurança da rede, sem o posterior

acompanhamento do seu estado, assim, cria-se a possibilidade de falhas e vulnerabilidades no ambiente configurado (LACERDA, 2007).

Porém, quando bem projetada, uma rede pode ser tão segura quanto necessário (AGUIAR, 2005), desta feita, com as ações implementadas, este trabalho atingiu todos os seus objetivos específicos e, como isso, foi possível, também, cumprir o objetivo geral: Aprimorar a segurança da rede sem fio de uma clínica odontológica.

REFERÊNCIAS

BARROS, T. Internet completa 44 anos; relembre a história da web. Globo.com, 07 abr. 2013. Techtudo. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html>. Acesso em: 29 jun. 2021.

CASTELLS, M. A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

DUARTE, L.O. Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x. São José do Rio Preto, SP. UNESP / IBILCE , 2003, 55p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

GRÉGIO, A .R .A. Wireless Honeynets: Um Modelo de Topologia para Captura e Análise de Ataques a Redes sem Fio. São José do Rio Preto, SP. UNESP / IBILCE , 2005, 57p. Monografia defendida para obtenção do grau de Bacharel em Ciência da Computação.

GUEDES, A. Censura: Seus diferentes aspectos e a função do bibliotecário. In: Revista do centro sócio econômico. v.2, n. 1, p.67 – 86, 1995.

KOTLER, P. Marketing de A a Z: 80 conceitos que todo profissional precisa saber. Rio de Janeiro: Campus, 2003.

MINISTÉRIO DAS COMUNICAÇÔES. Governo do Brasil, 2021. Disponível em: <https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/acesso-a-internet-cresceu-nos-lares-brasileiros>. Acesso em: 29 jun. 2021.

MOREIRA, N. Segurança mínima: uma visão corporativa da segurança da informação. Rio de Janeiro: Axcel Books, 2001.

OLIVEIRA, H. Os desafios da segurança de TI das pequenas empresas. Linux Solutions, 08 fev. 2021. Disponível em: <https://www.untanglebrasil.com.br/os-desafios-da-seguranca-de-ti-das-pequenas-empresas/>. Acesso em: 30 jun. 2021.

TANEMBAUM, A. Redes de Computadores. 4. Ed. – Amsterdam, Holanda: Vrije Universiteit. 632p.