“WIRELESS”: UMA ANÁLISE, NA REGIÃO DE GOIÂNIA, DA SEGURANÇA DOS QUADROS SINALIZADORES DE REDES DO PADRÃO 802.11

"WIRELESS": AN ANALYSIS IN REGION OF GOIÂNIA OF SAFETY OF TABLES NETWORK SIGNALS OF THE 802.11 STANDARD

GERÔNCIO DA ROCHA OLIVEIRA
Especialista em Gestão e Segurança em Redes de Computadores, Universidade Estadual de Goiás (UEG), Campus Trindade.
geroncio1001@gmail.com.

ANTÔNIO CRUVINEL BORGES NETO
Mestre em Engenharia Agrícola e docente da Universidade Estadual de Goiás (UEG) - Campus de Ciências Exatas e Tecnológicas Henrique Santillo (Anápolis - GO) e diretor educacional da Universidade Estadual de Goiás (UEG), Campus de Trindade
antonio@cruvinel.com.br

Resumo: Com a evolução da tecnologia**,** as conexões sem fio foram se popularizando com inúmeras redes sem fio por toda a cidade. Desta forma tornou-se uma questão interessante para a classe acadêmica de Segurança e Gestão de redes de computadores a elaboração de estudos que descrevam as aferições das configurações de transmissão sem fio. Para realização deste artigo será adotada a análise de redes sem fio ativas em uma região pré-determinada de Goiânia. A metodologia adotada será a análise da mensuração de critérios encontrados em sistemas de comunicação de dados via radiofrequência (*wireless*), comumente utilizado em redes de computadores, dos quais estes são classificados inclusive pelo conjunto de normas internacionais IEEE 802.11 e assim determinar alterações nos perfis de configurações através da base de dados histórica elaborada pelo próprio do autor.
Palavras-chave: *Wireless*. Segurança.*Wardriving*

Abstract: With the evolution of technology, wireless connections have become popular with numerous wirelless networks throughout the city. In this way it has become an interesting question for the academic class of Security and Management of computer networks to elaborate studies that describe the measurements of the wireless transmission configurations. For the accomplishment of this article will be adopted the analysis of active wireless networks in a predetermined region of Goiânia. The methodology adopted will be the analysis of the measurement of the criteria found in radiofrequency data communication systems, commonly used in computer networks, of which these are classified even by the IEEE 802.11 international standard set and thus determine changes in the profiles of through the historical database elaborated by the author's own.
Keywords: Wireless. Safety. Wardriving

INTRODUÇÃO

A partir da década de 70 do século XX, deu-se início a informatização da sociedade com o surgimento da microinformática e o estabelecimento do *personalcomputer*(PC). Neste

processo de informatização, que ocorre até os dias atuais, a tecnologia sofreu e sofre mudanças que a tornam mais eficiente permitindo a interoperabilidade uns com os outros.

A interligação destes dispositivos foi possível através do surgimento das redes de computadores com a "grande rede" (*internet*), causando transformações nas práticas sociais, principalmente no costume de produzir e consumir informação. O advento da mobilidade computacional ocorreu com a evolução da comunicação entre os dispositivos que utilizam a técnica de radiofrequência para a transferência de dados. De acordo Leão (2004, p. 18) "esse conjunto de evoluções permitiuque não fosse mais o usuário que se desloque até a rede, mas a rede que passa a envolver os usuários e os objetos numa conexão generalizada"

A adoção de transmissão de dados via radiofrequência trouxe além do benefício da mobilidade e, em muitos casos, proporcionou economia na infraestrutura de comunicação, visto que a mesma poderá não necessitar de passagem de novos cabeamentos, nem de profissionais instalando ou realizando alterações físicas nos edifícios para novos pontos de conexão. Em contrapartida, a área de cobertura de uma rede sem fio, principalmente as com o método de autenticação aberto, pode prover conexão a equipamentos que não se deseja conectados à mesma. Além da má configuração do método de autenticação, facilitando o processo de invasão, há métodos que permitem capturar os dados transmitidos em um espectro da radiofrequência pré-definido. Estes equipamentos podem também nem estar presentes no espaço físico destinado a utilização. Com a rápida expansão das tecnologias de informação e o acompanhamento evolutivo também pelas redes sem fio, sempre haverá a preocupação com a segurança das informações, tanto das transmitidas, quanto das armazenadas.

Segundo o relatório de Martinhão:

> As conexões Wi-Fi estão presentes em 79% dos domicílios brasileiros com acesso à Internet, o que representa um crescimento de 13 pontos percentuais em relação à edição de 2014. Além disso, 56% dos usuários afirmam ter utilizado a Internet na casa de outra pessoa (amigo, vizinho ou familiar), fazendo deste local de acesso o segundo mais popular(MARTINHÃO, 2016, p. 129).

Considerando a preocupação com segurança em computadores que envolvam redes conectadas à internet, criou-se, há 15 anos o Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil – CERT. Br. Sua principal função é atuar "como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato"(CERT. BR 2016).

As estatísticas disponibilizadas pelo CERT. Br indicam que no decorrer dos anos houve um crescimento nos incidentes reportados ao centro, como demonstrado abaixo na Figura 1.

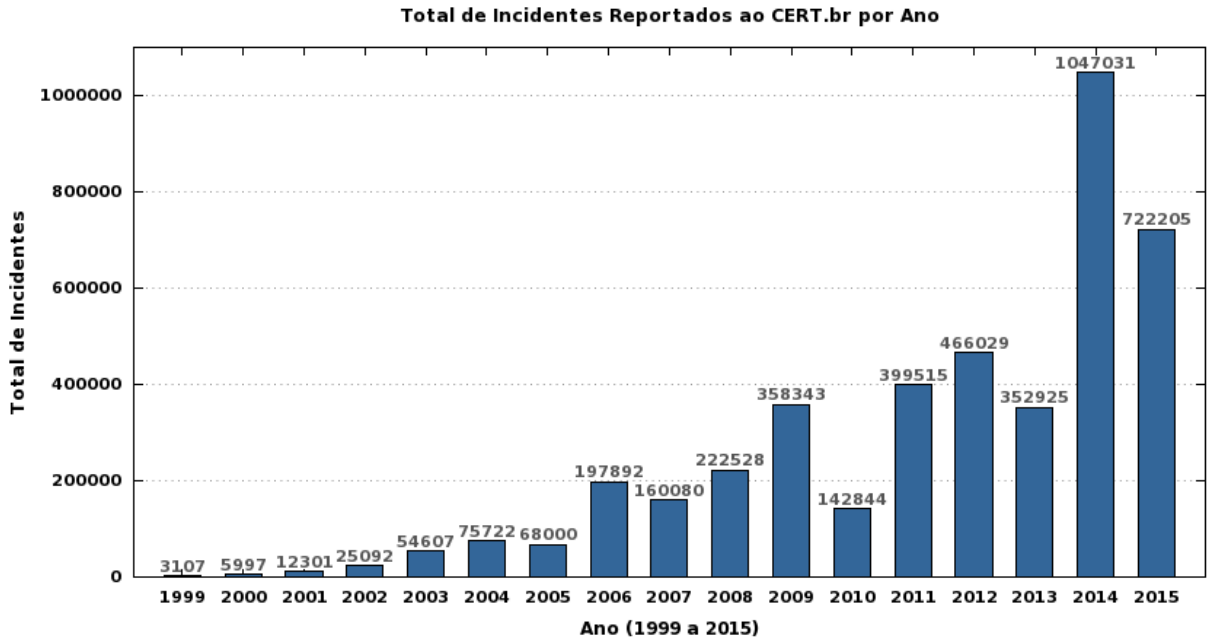

Figura 1: Total de Incidentes Reportados ao CERT. Br por Ano
Fonte: https://www.cert.br/stats/incidentes/.

Este trabalho tem como objetivo analisar o comportamento das redes sem fio em uma região da cidade de Goiânia – GO, nos quesitos de autenticação de rede, criptografia, canal de utilização e informações presentes no SSID (nome da rede). Especificamente, quantificar os canais, em que operam a fim de identificar quais será mais utilizado, quantas redes que não utilizam de criptografia e quais foram às mudanças nas configurações dos radiotransmissores analisados em 2014.

A metodologia empregada para a realização deste trabalho consistiu nos seguintes passos:

Utilizou-se a base de dados do autor tinha para estabelecer a rota percorrida em 2014. A base de dados continha 7084 dados de redes sem fio que, além de ser a base para restabelecer a rota percorrida, são base para as analíticas sobre alterações. No estabelecimento da rota a ser percorrida, organizou-se os dados pela data da captura e baseado na fórmula de *Haversine* para o cálculo da distância entre os pontos[1]:

[1]O autor tinha 89,7% da base de dados utilizada do trabalho apresentado em 2014.

$$DistânciaAB = 637100 * ACOS(COS(PI() * (90 - LatitudeB)/180) * COS((90 - LatitudeA) * PI()/180) + SEN((90 - LatitudeB) * PI()/180) * SEN((90 - LatitudeA) * PI()/180) * COS((LongitudeA - LongitudeB) * PI()/180))$$

Após os resultados das distâncias entre os pontos, foi realizada uma comparação no qual apresenta os pontos com a distância maior ou igual a 150 metros, definindo em um mapa de "*checkpoints*[2]" para ser percorrido. O resultado foi exportado para um GPS[3] para então realizar a captura das redes nestes locais (figura 2).

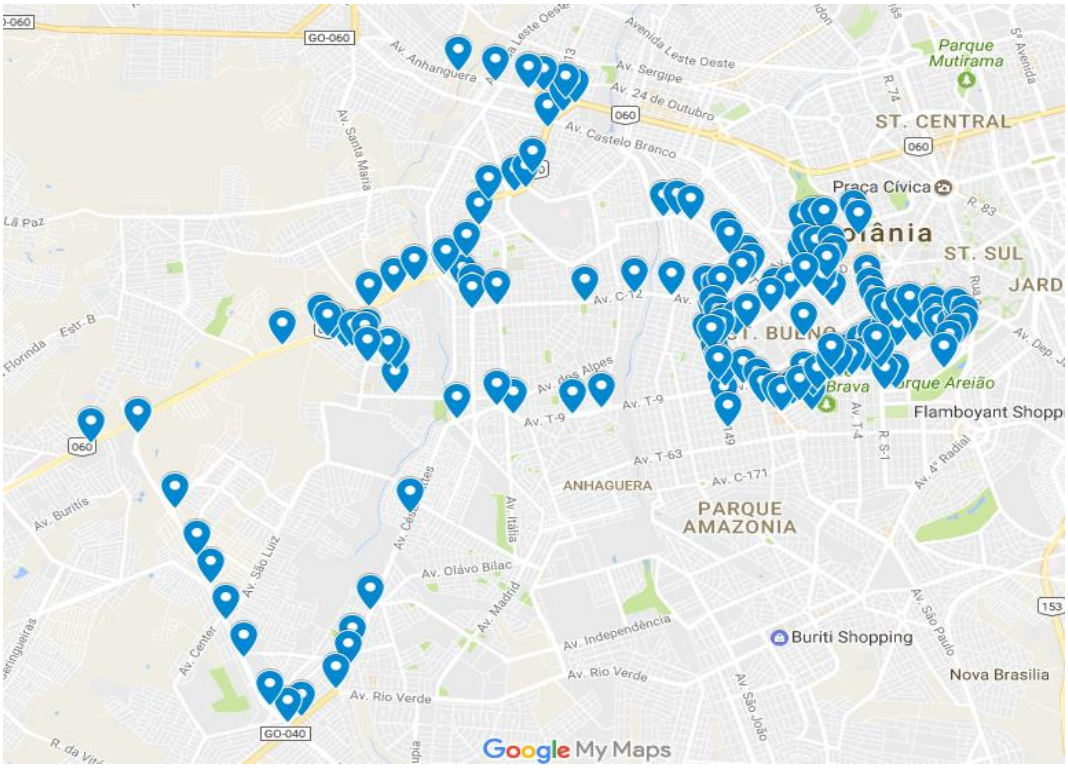

Figura 2: Mapa de "checkpoints" para realizar a mesma rota de 2014.
Fonte: Google MyMaps

O equipamento utilizado para captura dos dados foi um *smartphone* com a aplicação *Wigle*[4]instalada. A adoção do *smartphone* tem o propósito nesta metodologia, de utilizar ferramentas para análise das redes sem fio que estão ao alcance da maioria da população, tendo este tornado de uso comum a maioria das pessoas e que não fosse utilizada nenhuma técnica de antenas nas quais possibilitem maior ganho dos sinais. O equipamento escolhido, além de prover portabilidade, a interface de rede opera sobre os padrões da IEEE 802.11

[2]Pontos de controle
[3] Global Positioning System, que em português significa: "Sistema de Posicionamento Global"
[4] Disponível em: https://wigle.net/

A análise consiste em verificar as informações das redes sem fio, de forma não invasiva a rede. Ou seja, informações transmitidas pelo espectro de radiofrequência que são os metadados, informações não criptografadas que os originadores dos sinais disponibilizam para que os outros dispositivos possam localizar, para então realizar as atividades de autenticação, sincronização e assimilação à rede.

Segundo o autor Rufino para uma rede sem fio existir, deverá operar em uma radiofrequência:

> O espectro de radiofrequência é dividido em faixas, que são intervalos reservados, normalmente, para determinado tipo de serviço, definido por convenções internacionais e/ou por agências reguladoras. Uma faixa é, em geral, subdividida em frequências menores, para permitir a transmissão em paralelo de sinais diferentes em cada uma delas. Essas frequências menores (ou subfrequências) são chamadas de canais, que já fazem parte do nosso dia a dia o bastante tempo, como os canais de rádio (AM/FM) e televisão(RUFINO, 2011, p. 20).

O primeiro resultado obtido é relacionado à análise dos equipamentos operantes na faixa de 2,4 GHz, que totalizaram 95% das amostras. Foram encontrados 10.152 nestas condições e 50,39% destes estavam, no momento, operando nos canais 1, 6 e 11. Estes canais geralmente são configurados pelos os fabricantes e provavelmente não foram alterados pelos configuradores das redes. No quesito de segurança, o fato de vários equipamentos transmitindo na mesma frequência pode ocasionar a interferência, que:

> [...] de um ponto de vista de radiofrequência ocorre quando um receptor ouve dois sinais diferentes na mesma frequência ou próxima. A interferência faz com que os sinais de rádio frequência sejam distorcidos. Em LANs sem fio, essa interferência pode ter um impacto severo na qualidade do sinal recebido por um dispositivo sem fio. Este sinal distorcido ou corrompido irá diminuir a quantidade de dados que um dispositivo pode efetivamente receber, causando assim a perca de dados(BARTZ, 2012, 188).

A segunda análise quantificou os fabricantes. Para identificar o fabricante, utilizou-se de API dos sites macvendors.com/api e do www.macvendorlookup.com que ao passar o endereço MAC através do método GET, a aplicação do site processa a informação, resolvendo os 24 primeiros bits e retornando o registro do fabricante junto a IEEE. Feito isso, a análise amostral dos fabricantes nos dá indícios de onde direcionar os esforços para realizar uma tratativa ou exploração de vulnerabilidade do equipamento, podendo aumentar as chances de sucesso.

Na figura 3 os canais mais utilizados na faixa 2,400 - 2,4835 GHz relata quantitativamente essa utilização de espectro. São:

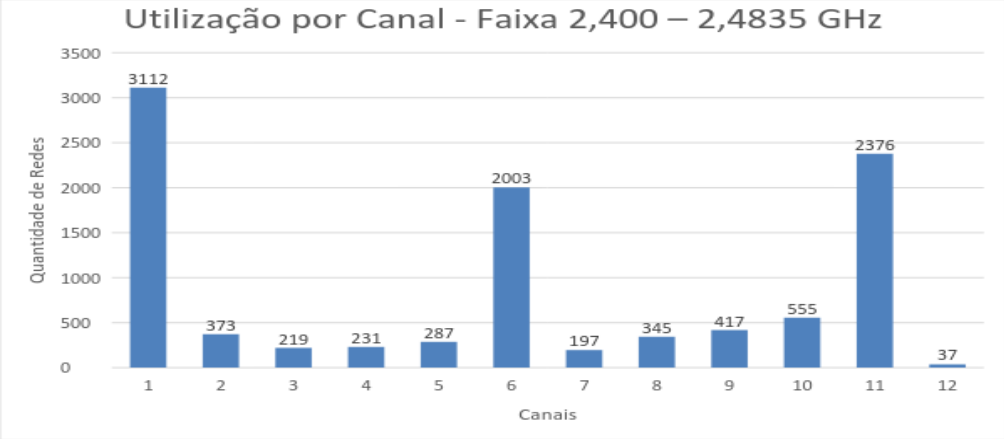

Figura 3: Canais mais utilizados na faixa 2,400 - 2,4835 GHz
Fonte: Autores (2016)

Cruzando essas informações com a base de dados de www.cvedetails.com/[5], foram correlacionados a seguir os dez fabricantes que tiveram maior percentual no ambiente amostral estudado, como será demonstrado na figura 4.

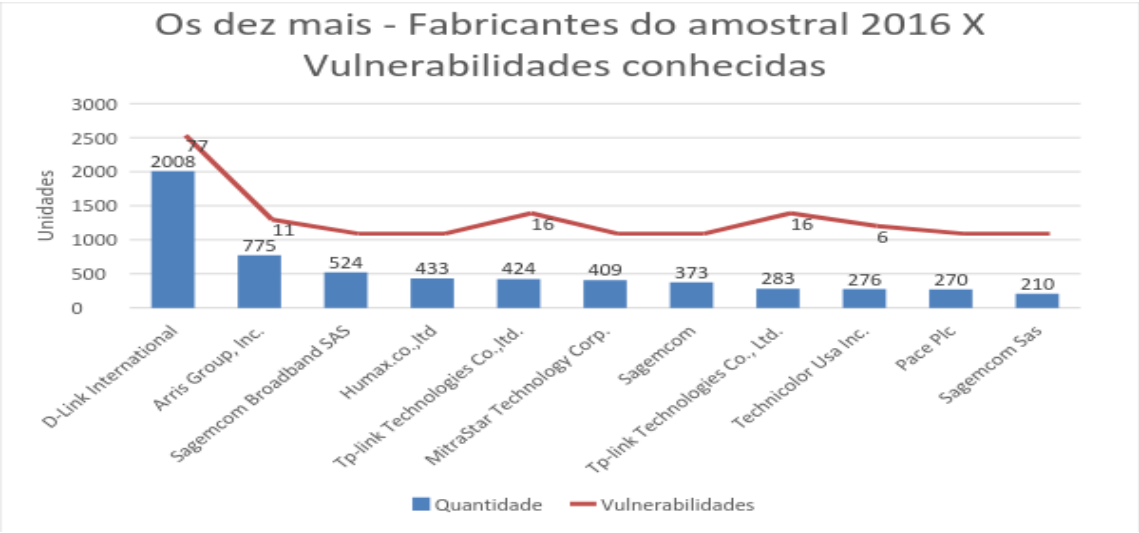

Figura 4: Os dez mais - fabricantes do amostral 2016 x Vulnerabilidades conhecidas
Fonte: Autores (2017)

O padrão IEEE 802.11 requer que uma estação que estabeleça sua identidade antes de enviar quadros. A autenticação ocorre toda vez que a estação se assemelha à rede. Os métodos se resumem basicamente em dois modos: autenticação aberta – não há uma senha (chave) para autenticar as estações à rede e todo o tráfego é descriptografado, facilitando a captura dos

[5] "www.cvedetails.com fornece uma interface web fácil de usar para os dados de vulnerabilidade CVE. Você pode procurar fornecedores, produtos e versões e exibir entradas CVE, vulnerabilidades, relacionadas a eles. É possível exibir estatísticas sobre fornecedores, produtos e versões de produtos." (https://www.cvedetails.com/ 2016)

dados - e autenticação utilizando chave pré-compartilhada – nesse método, compartilha-se de forma não prevista pela IEEE 802.11 a chave de acesso à rede. A chave, além de garantir o acesso à rede pelas estações, é utilizada no algoritmo que embaralha os dados, protegendo-os dos bisbilhoteiros.

Ao analisar os meios de autenticação, obtivemos o percentual do tipo de criptografia utilizado nas transmissões das redes sem fio analisadas. O resultado demonstra que a maioria absoluta (94,19%) tende a se preocupar em proteger o meio de transmissão. Em outra via, 5,81% dos transmissores analisados não utilizam criptografia, tornando as informações transmitidas mais vulneráveis e passíveis de captura (figura 5).

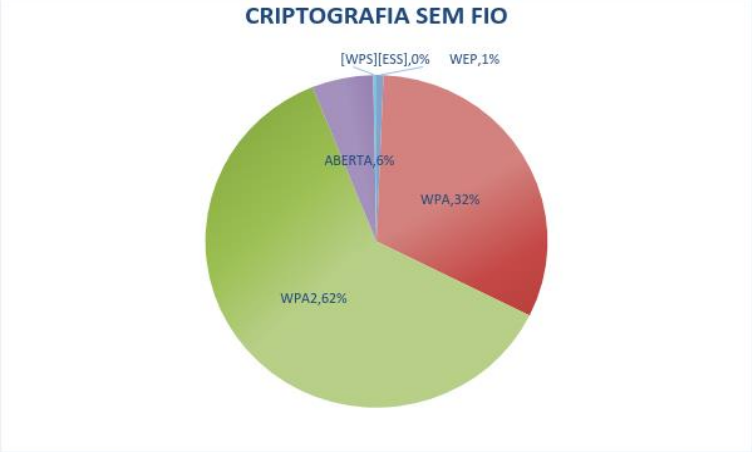

Figura 5: Percentual da criptografia sem fio das amostras
Fonte: Autores (2017)

No aprofundar da análise, 461 das redes abertas (74,75%) detinham do SSID's "Oi WiFi", "Oi WiFi Fon" e "OI_WIFI_FON".

Sabe se que esses SSID são pertencentes a uma rede distribuída, de concentradores sem fio,pertencentes à operadora de telefonia Oi, a qual comercializa o acesso à internet. Os demais pertenciam a outros dispositivos, como celulares, concentradores (*accesspoint* ou roteadores) e impressoras.

Foram comparados também os dados entre as bases de dados de 2014 e 2016, utilizando o endereço MAC, o qual é físico e imutável por padrão, como item chave na pesquisa e identificação dos aparelhos. Resultou-se na localização de 519 equipamentos, e, destes,comparou-se possíveis alterações no nome visível da rede sem fio (SSID), no método de autenticação e também sobre o canal em que operam.

Como decorrência da análise, observou-se que 64% dos radiotransmissores estudados tiveram o nome da rede (SSID) alterado. Do total, 69% alteraram o tipo de criptografia

utilizado, sendo que 5 dos 519 deixaram de utilizar criptografia e 98% alteraram o canal em que operavam (figura 6).

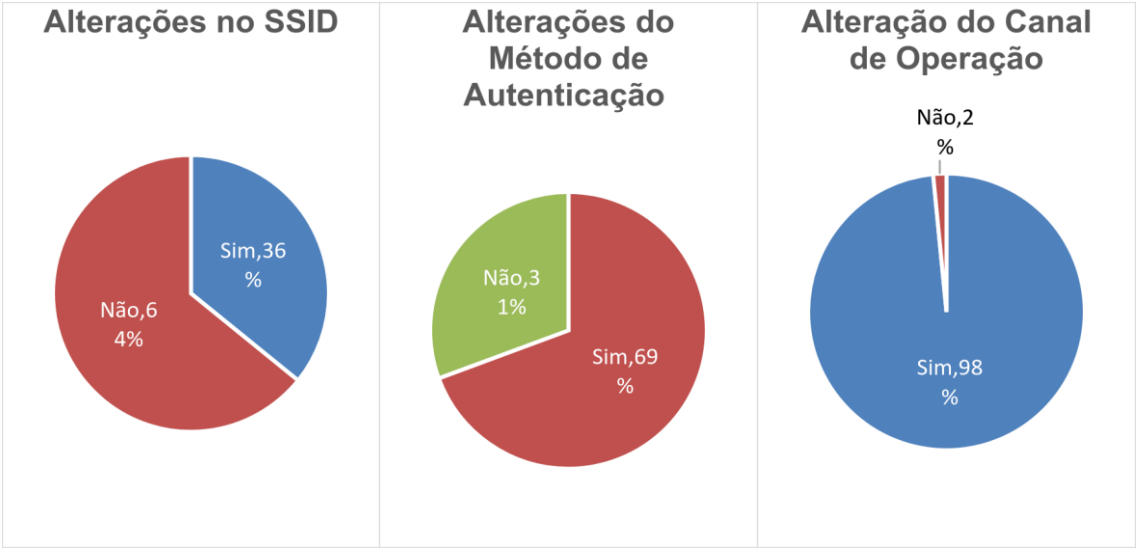

Figura 6: Alterações nas redes encontradas de 2014 a 2016
Fonte: Autores (2017).

Ao observar as alterações de SSID, notou-se uma falha de segurança neste requisito em específico. Percebeu-se nas amostras SSID com informações que facilitariam a identificação do usuário e que poderiam ser utilizadas em engenharia sociais, como por exemplo, redes sem fio com SSID “Net virtuaapt 204” ou “Isabel Ap 202”.

Com considerações finais, pode-se destacar que em uma maioria utilizam os canais de operação configurados pelos os fabricantes, levando-nos a crer que não houve uma análise sob o espectro do local de operação do equipamento.

Este fator, em conjunto com uma alta concentração de equipamentos operantes em um mesmo canal ou com equipamentos que utilizam de amplificadores de frequência, poderá, de fato, causar problemas à segurança da informação nos quesitos de disponibilidade e integridade. Notou-se aimportância, principalmente para gestores de tecnologias de informação, da análise de vulnerabilidades que possam conter nos equipamentos e o risco que poderá acarretar ao negócio. Prova disso está na Figura 4 – Os dez mais - fabricantes do amostral 2016 x Vulnerabilidades conhecidas, que demonstrou que os equipamentos da fabricante D-Link, dentro dos fabricantes com maior reincidência em nosso universo amostral, estão no topo da lista de vulnerabilidades.

Os métodos de autenticação em sua maioria provaramatender requisitos mínimos para a segurança dos dados transmitidos, porém, torna-se preocupante o fato de existiremredes

disponibilizadas sem nem um nível de criptografia. Provou-se também preocupante, o fato de uma operadora de telefonia realizar uma rede distribuída de acesso à *internet* e a mesma ser passível de escutas, por não haver criptografia, podendo permitir capturas de dados sensíveis como cartões de crédito, usuários e senhas de acesso, etc., caso a transmissão destes não sejam tratadas corretamente pelas aplicações.

Das redes possíveis de comparação entre 2014 e 2016, observou-se que, em todos, houve alteração de pelo menos um dos quesitos avaliados (SSID, autenticação e canal de operação. De modo geral, a segurança das redes de computadores sem fio e de suas informações dependem de uma combinação de fatores como o canal de utilização com maior distância entre os dos transmissores vizinhos, métodos de autenticação que garantam a criptografia da transmissão, avaliação de riscos presentes em equipamentos e das informações que não são possíveis de criptografar e que desejem não ocultar, como por exemplo, o SSID.

REFERÊNCIAS

BALOCH, Rafay. **Ethical Hacking and Penetration Testing Guide**. Boca Raton: CRC Press, 2014.

BARTZ, Robert J. ***CWTS® Certified Wireless Technology Specialist****, 2nd Edition.* Indianapolis: John Wiley & Sons, Inc., 2012.

GAST, Matthew. *802.11* ***Wireless Networks: The Definitive Guide.***Sebastopol: O'Reilly, 2005.***https://www.cvedetails.com/***.* 12 01, 2016. https://www.cvedetails.com/.

LEÃO, Lúcia, Org. ***Derivas: cartografias do ciberespaço.*** São Paulo, São Paulo: Annablume, 2004.

MARTINHÃO, Maximiliano Salvadori. ***TIC Domicílios 2015 - Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros.*** São Paulo: Câmara Brasileira do Livro, SP, Brasil, 2016.

NAKAMURA, Emilio Tissato, andDE GEUS,Paulo Lício. ***Segurança de Redes em Ambientes Cooperativos****.* São Paulo: Novatec Editora, 2007.

RUFINO, Nelson Murilo de **O.** ***Segurança em Redes sem Fio.*** *Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth.* São Paulo: Novatec, 2011.
Sobre o CERT. Br. 11 12, 2016. http://www.cert.br/sobre/.