Roteadores Mal Configurados: Porta de Entrada para Ameaças Cibernéticas nas Redes Domésticas e Empresariais

Emanoel Guilherme Barros
e.guilherme.barros@outlook.com
Universidade de Pernambuco
Recife / PE

Dr. Sidney Marlon de Lima
smll@ecomp.poli.br
Univercidade Federal de Pernambuco
Recife / PE

RESUMO

Em um mundo cada vez mais conectado, os roteadores Wi-Fi tornaram-se parte essencial do cotidiano, tanto em residências quanto em empresas. No entanto, o que muitos usuários não percebem é que esses dispositivos, quando mal configurados, podem representar sérias ameaças à segurança digital. Este artigo investiga os principais riscos associados à má configuração de roteadores, revelando como falhas simples – como senhas padrão, firmware desatualizado e serviços desnecessários ativados – podem abrir caminho para ataques cibernéticos, comprometendo dados pessoais, financeiros e corporativos. Por meio de uma revisão bibliográfica aprofundada e análise de casos reais, o estudo destaca os impactos dessas vulnerabilidades e apresenta um conjunto de boas práticas acessíveis e eficazes para fortalecer a segurança das redes. Mais do que uma questão técnica, proteger o roteador é uma atitude de responsabilidade digital que deve fazer parte da rotina de qualquer usuário conectado. O objetivo deste trabalho é justamente ampliar essa consciência, oferecendo orientações claras que ajudam a transformar o roteador – muitas vezes negligenciado – no primeiro e mais importante guardião da rede.

Palavras chaves: segurança de redes; roteadores mal configurados; ameaças cibernéticas; Wi-Fi; IoT; exploits; mitigação de riscos.

ABSTRACT

In an increasingly connected world, Wi-Fi routers have become an essential part of everyday life, both at home and in the workplace. However, many users fail to realize that these devices, when poorly configured, can pose serious threats to digital security. This article investigates the main risks associated with misconfigured routers, revealing how simple oversights - such as default passwords, outdated firmware, and unnecessary services left enabled - can open the door to cyberattacks, compromising personal, financial, and corporate data. Through an in-depth literature review and analysis of real-world cases, the study highlights the impacts of these vulnerabilities and presents a set of practical and effective best practices to strengthen network security. More than just a technical matter, securing the router is an act of digital responsibility that should be part of every connected user's routine. The goal of this work is to raise awareness on this issue by offering clear guidance that helps transform the route - often overlooked - into the first and most important line of defense in a network.

Keywords: network security; misconfigured routers; cyber threats; Wi-Fi; IoT; exploits; risk mitigation.

1. INTRODUÇÃO

Em um mundo onde estar conectado é quase tão essencial quanto ter acesso à eletricidade, os roteadores Wi-Fi tornaram-se peças fundamentais na infraestrutura digital de residências e empresas. Esses dispositivos, muitas vezes instalados de forma rápida e sem a devida atenção, são os verdadeiros portões de entrada para a internet — e, por consequência, para tudo que acessamos e armazenamos online. No entanto, a praticidade que oferecem vem acompanhada de riscos significativos quando suas configurações são negligenciadas.

Senhas fracas, firmware desatualizado, portas abertas e serviços desnecessários ativados são apenas alguns exemplos de falhas comuns que tornam os roteadores alvos fáceis para cibercriminosos. A consequência? Desde o roubo de dados pessoais até o comprometimento de dispositivos e redes corporativas inteiras.

Este artigo tem como objetivo analisar essas vulnerabilidades e os perigos reais que elas representam em dois contextos distintos, mas igualmente vulneráveis: o ambiente doméstico e o corporativo. A proposta é não apenas mapear os riscos, mas também oferecer orientações práticas e acessíveis para mitigá-los — afinal, proteger o roteador é proteger toda a rede que ele sustenta.

Mais do que um desafio técnico, a segurança de roteadores exige conscientização e responsabilidade digital. Cada usuário, seja em casa ou na empresa, tem

um papel fundamental para garantir que esses dispositivos não se transformem em portas escancaradas para ataques cibernéticos. A prevenção começa na configuração — e é aí que este estudo busca fazer a diferença.

Diante desse cenário, este artigo não apenas mapeia os principais riscos relacionados à má configuração de roteadores, como também propõe um conjunto inédito de recomendações práticas estruturadas, voltadas à mitigação eficaz desses riscos tanto em ambientes residenciais quanto corporativos. A proposta visa contribuir com a literatura ao oferecer um modelo de referência acessível, capaz de orientar usuários e profissionais de segurança sobre os principais cuidados técnicos e preventivos.

2. METODOLOGIA

Para compreender os riscos envolvidos na má configuração de roteadores Wi-Fi e suas consequências em ambientes residenciais e corporativos, este estudo adotou uma abordagem baseada em **revisão bibliográfica sistemática** e análise qualitativa de dados. A pesquisa foi conduzida em bases de dados acadêmicas reconhecidas, como IEEE Xplore, Scopus, SpringerLink e Google Scholar, bem como em fontes técnicas confiáveis da internet, como CERT.br e publicações de fabricantes de equipamentos de rede.

Os termos utilizados na busca incluíram: *"router security"*, *"Wi-Fi vulnerabilities"*, *"misconfigured routers"*, *"enterprise network security"* e *"home network threats"*. A seleção dos materiais considerou artigos publicados entre **2017 e 2024**, priorizando estudos com evidências práticas, experimentos reais ou diretrizes adotadas por especialistas em segurança da informação. Exemplos incluem os trabalhos de Singh et al. (2019), que discutem a persistência de falhas em firmwares populares, e o estudo de Almeida e Costa (2022), que analisa os impactos da má configuração de roteadores domésticos no Brasil.

Após a coleta, os materiais foram analisados criticamente com foco em três frentes principais: (1) identificação de padrões de vulnerabilidades técnicas; (2) mapeamento dos impactos dessas falhas nos diferentes ambientes; e (3) levantamento de medidas eficazes para mitigação. Também foram incorporados **casos reais** de comprometimento de redes devido a configurações incorretas, como os ataques vinculados à botnet Mirai (Antonakakis et al., 2017) e ao malware VPNFilter (Symantec, 2018).

A partir dessa análise, o conteúdo foi sistematizado em seções temáticas — introdução, vulnerabilidades e perigos, medidas de prevenção e conclusão — de forma a garantir **clareza, coesão lógica e rigor técnico**. Todo o processo de redação seguiu as normas acadêmicas da ABNT, incluindo a correta citação das fontes utilizadas, assegurando a rastreabilidade das informações e a credibilidade do conteúdo apresentado.

3. DISCUSSÕES

3.1 Vulnerabilidades Comuns em Roteadores

Apesar de sua função crítica, muitos roteadores são instalados e mantidos com configurações padrão que os tornam alvos fáceis para cibercriminosos. As vulnerabilidades mais comuns incluem:

3.1.1 Senhas Padrão e Credenciais Fracas

Uma das falhas de segurança mais básicas e, paradoxalmente, mais difundidas, é a manutenção de senhas padrão de fábrica para acesso ao painel administrativo do roteador. Muitos fabricantes utilizam credenciais genéricas como "admin/admin" ou "admin/password". Essas informações são amplamente conhecidas e facilmente encontradas em bancos de dados públicos ou através de buscas simples na internet [1]. Um atacante pode, com pouco esforço, acessar o roteador, alterar configurações, redirecionar tráfego ou até mesmo instalar firmware malicioso.

3.1.2 Firmware Desatualizado

O firmware é o software que controla o hardware do roteador. Assim como qualquer outro software, ele pode conter falhas de segurança (bugs) que são descobertas e corrigidas pelos fabricantes ao longo do tempo. A não atualização do firmware deixa o roteador vulnerável a exploits conhecidos que podem permitir que atacantes assumam o controle do dispositivo. Muitos usuários não têm o hábito de verificar e instalar atualizações de firmware, tornando seus roteadores alvos fáceis para ataques automatizados que exploram essas vulnerabilidades [2].

3.1.3 Portas Abertas e Serviços Desnecessários

Roteadores frequentemente vêm com portas de rede abertas por padrão ou com serviços como Telnet, FTP ou UPnP (Universal Plug and Play) ativados. Embora esses serviços possam ter funcionalidades legítimas, quando não são configurados corretamente ou são deixados abertos sem necessidade, eles se tornam pontos de entrada para ataques. O UPnP, por exemplo, pode permitir que dispositivos na rede abram portas automaticamente no roteador sem a intervenção do usuário, criando brechas de segurança [3].

3.1.4 Wi-Fi Inseguro (Criptografia Fraca ou Ausente)

A segurança da rede Wi-Fi é diretamente

ligada à configuração do roteador. O uso de protocolos de segurança antigos e fracos, como WEP (Wired Equivalent Privacy), ou a ausência de qualquer criptografia, permite que qualquer pessoa nas proximidades intercepte o tráfego de dados. Mesmo o WPA (Wi-Fi Protected Access) pode ser vulnerável se a senha for fraca. O padrão atual e mais seguro é o WPA2 ou WPA3, que oferecem criptografia robusta para proteger a comunicação sem fio [4].

3.1.5 Vulnerabilidades de Injeção e Cross-Site Scripting (XSS)

Assim como aplicações web, as interfaces de administração de roteadores podem ser suscetíveis a vulnerabilidades como injeção de comandos ou Cross-Site Scripting (XSS). Um atacante pode explorar essas falhas para executar comandos arbitrários no dispositivo ou injetar scripts maliciosos no navegador do usuário que acessa o painel de controle do roteador, comprometendo a segurança [5].

3.1.6 Pontos de Acesso Rogue (Rogue Access Points)

Em ambientes corporativos, a presença de "pontos de acesso rogue" é uma preocupação. Estes são roteadores ou pontos de acesso Wi-Fi não autorizados conectados à rede da empresa por funcionários desavisados ou por atacantes. Eles podem contornar as políticas de segurança da rede, criando uma porta dos fundos para acesso não autorizado e facilitando ataques de man-in-the-middle [6].

3.2.1 Perigos em Ambientes Residenciais

Em um ambiente residencial, um roteador mal configurado pode transformar a conveniência da conectividade em uma porta aberta para invasores. Os perigos são variados e podem ter consequências significativas para a privacidade e segurança dos moradores:

Acesso Não Autorizado à Rede Doméstica.

Quando um roteador possui senhas padrão, firmware desatualizado ou configurações de segurança fracas, ele se torna um alvo fácil para qualquer pessoa com intenções maliciosas que esteja dentro do alcance do sinal Wi-Fi. Um invasor pode se conectar à rede doméstica sem permissão, utilizando-a para atividades ilegais que podem ser rastreadas até o proprietário da rede. Além disso, o acesso à rede permite que o atacante explore outros dispositivos conectados.

3.2.2 Roubo de Dados Pessoais e Financeiros

Uma vez dentro da rede, o cibercriminoso pode tentar acessar dispositivos conectados, como computadores, smartphones, tablets e dispositivos de armazenamento em rede (NAS). Isso pode levar ao roubo de informações pessoais, como fotos, documentos, senhas salvas em navegadores e, o mais crítico, dados financeiros. Transações bancárias, compras online e outras atividades sensíveis realizadas em uma rede comprometida podem ser interceptadas, resultando em fraudes e perdas financeiras.

3.2.3 Ataques de Phishing e Redirecionamento de Tráfego

Roteadores vulneráveis podem ser explorados para redirecionar o usuário a sites falsos, mesmo quando ele tenta acessar páginas legítimas, como de bancos. Um exemplo disso foi o ataque do malware *VPNFilter*, que infectou mais de 600 mil roteadores no mundo. Segundo o IDEC (2018), o vírus permitia interceptar dados e direcionar o tráfego para sites maliciosos, expondo usuários a fraudes financeiras. A recomendação foi reiniciar os aparelhos, atualizar o firmware e alterar as credenciais de acesso do roteador.

3.2.4 Controle de Dispositivos IoT (Internet das Coisas)

Com a crescente popularidade de dispositivos IoT em residências (câmeras de segurança, assistentes de voz, lâmpadas inteligentes, termostatos, etc.), um roteador comprometido pode dar ao atacante o controle sobre esses dispositivos. Isso pode variar desde a visualização de imagens de câmeras de segurança até a manipulação de sistemas de automação residencial, comprometendo a privacidade e a segurança física da casa. Muitos dispositivos IoT possuem vulnerabilidades conhecidas que podem ser exploradas se o roteador não estiver protegendo a rede adequadamente.

3.2.5 Inclusão em Botnets

Roteadores mal configurados ou vulneráveis podem ser sequestrados e incluídos em redes de bots (botnets). Uma botnet é uma rede de dispositivos comprometidos que são controlados remotamente por um atacante para realizar atividades maliciosas, como ataques de negação de serviço distribuída (DDoS), envio de spam ou mineração de criptomoedas. O proprietário do roteador pode nem perceber que seu dispositivo está sendo usado para fins ilícitos, o que pode resultar em lentidão na internet e, em casos extremos, em problemas legais.

3.3 Perigos em Ambientes Corporativos

Em um ambiente corporativo, os riscos associados a roteadores mal configurados são amplificados devido à quantidade e sensibilidade dos dados envolvidos, bem como ao impacto potencial na continuidade dos negócios. As consequências podem

ser devastadoras.

3.3.1 Acesso à Rede Interna da Empresa

Um roteador corporativo mal configurado pode servir como um ponto de entrada para a rede interna da empresa. Isso permite que atacantes acessem servidores, estações de trabalho, sistemas de armazenamento e outros recursos críticos. O acesso não autorizado pode levar à exfiltração de dados confidenciais, como informações de clientes, segredos comerciais, propriedade intelectual e dados financeiros, resultando em grandes perdas e danos à reputação da empresa.

3.3.2 Vazamento de Dados Confidenciais e Propriedade Intelectual

Empresas lidam com uma vasta quantidade de dados sensíveis. Um roteador comprometido pode facilitar o acesso a esses dados, permitindo que cibercriminosos os copiem ou os vendam. Isso inclui informações de clientes (dados pessoais, financeiros), dados de funcionários, estratégias de negócios, planos de produtos e propriedade intelectual. O vazamento desses dados pode resultar em multas regulatórias pesadas (como as da LGPD no Brasil), perda de confiança dos clientes e vantagem competitiva para concorrentes.

3.3.3 Interrupção de Serviços e Operações (Ransomware e DDoS)

Atacantes que obtêm acesso a um roteador corporativo podem usá-lo para lançar ataques que interrompem as operações da empresa. Ataques de negação de serviço distribuída (DDoS) podem sobrecarregar a rede, tornando os serviços inacessíveis para funcionários e clientes. Além disso, o acesso à rede pode ser o primeiro passo para a implantação de ransomware, que criptografa os dados da empresa e exige um resgate para sua liberação, paralisando completamente as operações e causando perdas financeiras significativas.

3.3.4 Comprometimento de Sistemas Críticos e Servidores

Roteadores são frequentemente a primeira linha de defesa de uma rede. Se comprometidos, eles podem permitir que atacantes alcancem sistemas internos críticos, como servidores de banco de dados, servidores de e-mail, sistemas ERP (Enterprise Resource Planning) e CRM (Customer Relationship Management). O comprometimento desses sistemas pode levar à manipulação de dados, roubo de informações, interrupção de serviços essenciais e danos irreparáveis à infraestrutura de TI da empresa.

3.3.5 Espionagem Industrial e Fraudes

Em um cenário corporativo, um roteador vulnerável pode ser usado para espionagem industrial. Atacantes podem monitorar o tráfego de rede para coletar informações sobre projetos, estratégias, comunicações internas e negociações. Além disso, o acesso à rede pode facilitar a execução de fraudes financeiras, como a manipulação de transações ou o desvio de fundos, aproveitando-se de vulnerabilidades nos sistemas internos ou na comunicação.

3.3.6 Criação de Backdoors e Persistência

Um atacante que consegue comprometer um roteador corporativo pode instalar backdoors ou outras formas de persistência. Isso permite que eles mantenham o acesso à rede mesmo após a detecção inicial ou a reinicialização do dispositivo. Essa persistência pode ser usada para futuras invasões, exfiltração contínua de dados ou para lançar novos ataques a qualquer momento, tornando a remediação muito mais complexa e demorada.

3.3.7 Evolução das Vulnerabilidades em Roteadores Wi-Fi

A análise comparativa entre os anos de 2016 e 2024 revela uma escalada significativa nas vulnerabilidades associadas a roteadores Wi-Fi. Em 2016, as principais preocupações estavam relacionadas ao uso de senhas padrão e à ausência de atualizações de firmware. Um estudo da ESET, que avaliou mais de 12.000 roteadores domésticos, identificou que 15% dos dispositivos utilizavam senhas fracas ou padrões de fábrica, como "admin" ou "123456", tornando-os suscetíveis a ataques simples de força bruta.

No cenário mais recente, destaca-se a descoberta de mais de 500 vulnerabilidades em roteadores desde 2020, sendo 87 classificadas como críticas. Essas falhas incluem execução remota de código (RCE) e acesso root sem autenticação, evidenciando a necessidade urgente de práticas de segurança mais robustas por parte dos fabricantes e usuários.

Além disso, surgiram ameaças sofisticadas que exploram falhas nos próprios protocolos de segurança Wi-Fi. As vulnerabilidades conhecidas como FragAttacks, identificadas pelo pesquisador Mathy Vanhoef, afetam todos os protocolos de segurança Wi-Fi desde 1997, permitindo que invasores injetem pacotes maliciosos em redes protegidas . Outra ameaça significativa é a vulnerabilidade Kr00k (CVE-2019-15126), descoberta pela ESET, que afeta chips Wi-Fi da Broadcom e Cypress, permitindo que atacantes descriptografem parte do tráfego de redes protegidas pelo protocolo WPA2.

Essa evolução evidencia a importância de uma abordagem proativa na proteção de redes Wi-Fi, incluindo a implementação de senhas fortes, atualizações regulares de firmware, desativação de serviços desnecessários e maior conscientização sobre novas formas de ataques cibernéticos.

Tabela 1 - Comparativo de Vulnerabilidades em Roteadores Wi-Fi: 2016 vs. 2024

Ano	Vulnerabilidades Identificadas	Tipos de Ataques Predominantes	Destaques Tecnologicos e Ameaças Emergentes
2016	15% dos roteadores domésticos com senhas fracas e vulnerabilidades médias a altas	Uso de senhas padrão, firmware desatualizado, acesso remoto não autorizado	Falhas básicas de configuração e ausência de atualizações
2024	Mais de 500 vulnerabilidades descobertas desde 2020, incluindo 87 críticas	Execução remota de código (RCE), acesso root sem autenticação, falhas em protocolos de segurança	Ameaças avançadas como FragAttacks, Kr00k e falhas em chips Wi-Fi

4. MEDIDAS DE PREVENÇÃO E BOAS PRÁTICAS

A boa notícia é que a maioria dos perigos associados a roteadores mal configurados pode ser mitigada com a implementação de medidas de segurança simples, mas eficazes. A proatividade e a conscientização são chaves para proteger redes residenciais e corporativas:

4.1 Altere as Credenciais Padrão Imediatamente

Esta é a primeira e mais crucial etapa. Ao instalar um novo roteador, a primeira ação deve ser alterar o nome de usuário e a senha padrão de fábrica para credenciais fortes e únicas. Utilize uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Evite informações pessoais óbvias e não reutilize senhas de outros serviços. Para ambientes corporativos, utilize senhas complexas e considere a implementação de autenticação de dois fatores (2FA) para acesso ao painel administrativo do roteador, se disponível.

4.2 Mantenha o Firmware Sempre Atualizado

Verifique regularmente o site do fabricante do roteador para novas versões de firmware. As atualizações frequentemente incluem correções de segurança para vulnerabilidades recém-descobertas. Muitos roteadores modernos oferecem a opção de atualização automática, o que deve ser ativado. Caso contrário, estabeleça um cronograma para verificar e instalar as atualizações manualmente. Em ambientes corporativos, a gestão de patches de firmware deve ser parte de uma política de segurança abrangente.

4.3 Desative Serviços e Portas Desnecessárias

Revise as configurações do roteador e desative quaisquer serviços (como Telnet, FTP, SSH, UPnP) e portas que não sejam estritamente necessários para o funcionamento da rede. Quanto menos serviços expostos, menor a superfície de ataque. Para o UPnP, desative-o e configure o redirecionamento de portas manualmente apenas para as aplicações que realmente precisam. Em redes corporativas, a segmentação de rede e a implementação de firewalls robustos são essenciais para controlar o tráfego e limitar o acesso a serviços internos.

4.4 Utilize Criptografia Forte para o Wi-Fi

Sempre configure sua rede Wi-Fi para usar o protocolo de segurança mais forte disponível, que atualmente é o WPA2 ou, preferencialmente, o WPA3. Evite o uso de WEP ou WPA. Utilize uma senha de rede Wi-Fi longa e complexa. Em ambientes corporativos, considere a implementação de WPA2-Enterprise ou WPA3-Enterprise, que utilizam autenticação baseada em servidor (RADIUS) para cada usuário, proporcionando um nível de segurança muito superior.

4.5 Configure um Firewall Robusto

O firewall do roteador é sua primeira linha de defesa contra ameaças externas. Certifique-se de que ele esteja ativado e configurado para bloquear tráfego indesejado. Em ambientes corporativos, a implementação de firewalls de próxima geração (NGFW) com recursos avançados como inspeção profunda de pacotes, prevenção de intrusões (IPS) e filtragem de conteúdo é fundamental. Para usuários domésticos, o firewall padrão do roteador, combinado com um firewall pessoal nos dispositivos, já oferece uma boa proteção.

4.6 Segmente a Rede (Redes de Convidados e IoT)

Para aumentar a segurança, especialmente em ambientes com muitos dispositivos, considere segmentar sua rede. Crie uma rede Wi-Fi separada para convidados, isolando- os da sua rede principal e dos seus dispositivos. Para dispositivos IoT, crie uma rede IoT dedicada, com acesso restrito à internet e sem comunicação com sua rede principal. Isso impede que um dispositivo IoT comprometido seja usado como ponte para atacar
outros dispositivos na sua rede.

4.7 Desative o Acesso Remoto (se não for essencial)

Muitos roteadores permitem o acesso remoto ao painel administrativo pela internet. Se você não precisa acessar seu roteador de fora de casa ou do escritório, desative essa funcionalidade. Se for essencial, utilize uma VPN (Virtual Private Network) para acessar a rede de forma segura antes de gerenciar o roteador. Além disso, altere a porta padrão de acesso remoto (geralmente 80 ou 443) para uma porta não padrão, dificultando a varredura por atacantes.

4.8 Monitore a Atividade da Rede

Fique atento a atividades incomuns na sua rede, como lentidão inexplicável, novos dispositivos conectados que você não reconhece ou tentativas de acesso suspeitas nos logs do roteador. Em ambientes corporativos, a implementação de sistemas de SIEM (Security Information and Event Management) e ferramentas de monitoramento de rede são cruciais para detectar e responder rapidamente a incidentes de segurança.

4.9 Proposta de Recomendações Técnicas para Configuração Segura de Roteadores

Com base na análise das vulnerabilidades mais recorrentes e nas boas práticas identificadas na literatura e em guias técnicos, propõe-se um conjunto de diretrizes práticas que podem ser aplicadas por usuários domésticos e equipes de TI em ambientes corporativos. A proposta visa consolidar ações prioritárias de segurança que, se adotadas de forma sistemática, reduzem significativamente o risco de comprometimento de redes. A Tabela 2 apresenta esse conjunto de recomendações.

Tabela 2 - Diretrizes técnicas para configuração segura de roteadores

Recomendações	Aolicações	Nível de Prioridade
Alterar credenciais padrão	Residencial e corporativo	Alta
Atualizar firmware periodicament	Ambos	Alta
Desativar serviços desnecessários	Principalmente corporativo	Médio
Habilitar criptografia WPA2/WPA3	Ambos	Alta
Segmentar redes (IoT, convidaddos etc.	Residencial e corporativo	Médio
Desabilitar acesso remoto (quando possível)	Ambos	Alta
Monitorar dispositivios conectados	Corporativo	Alta

5. CONCLUSÃO

Os roteadores, embora muitas vezes esquecidos no dia a dia, são verdadeiros pilares da nossa vida digital. Por trás da conexão constante que temos com o mundo, eles operam silenciosamente — mas quando mal configurados, podem se transformar em portas escancaradas para cibercriminosos. A evolução das ameaças nos últimos anos, evidenciada por vulnerabilidades como FragAttacks, Kr00k e centenas de falhas críticas registradas desde 2020, mostra que confiar em configurações padrão ou negligenciar atualizações não é mais uma opção segura.

Tanto residências quanto empresas estão expostas. Em casa, o risco vai além da lentidão na internet: envolve privacidade, dados bancários e até o controle de dispositivos IoT. No ambiente corporativo, as consequências são ainda mais amplas, podendo incluir espionagem industrial, roubo de propriedade intelectual e interrupção total de serviços. A comparação com o cenário de 2016 revela que, embora a tecnologia tenha avançado, a superfície de ataque cresceu junto — e a falta de preparo ainda persiste.

Como contribuição prática e inédita, este estudo apresenta uma proposta estruturada de recomendações técnicas para a configuração segura de roteadores, aplicável em contextos domésticos e corporativos. A sistematização dessas medidas busca apoiar tanto o usuário comum quanto profissionais de TI na construção de ambientes digitais mais seguros e resilientes.

A boa notícia é que a segurança não exige conhecimento técnico avançado. Medidas simples, como mudar a senha padrão, atualizar o firmware, segmentar redes e desativar acessos remotos desnecessários, já fazem uma enorme diferença. E mais do que uma prática técnica, isso representa uma atitude de responsabilidade digital.

Proteger seu roteador é proteger sua rede, seus dados, sua empresa — e, em escala, contribuir para um ecossistema digital mais resiliente. Em um mundo onde ataques são cada vez mais sofisticados e automatizados, a prevenção começa com o básico. E o básico, neste caso, é não ignorar o guardião silencioso que conecta tudo: o roteador. Não o deixe vulnerável.

REFERÊNCIAS

ALMEIDA, J.; COSTA, R. Falhas em roteadores domésticos: uma ameaça silenciosa. *Revista Brasileira de Segurança Digital*, v. 6, n. 2, p. 44–59, 2022.

ANTONAKAKIS, M. et al. Understanding the Mirai Botnet. In: *26th USENIX Security Symposium*, 2017. Disponível em: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis. Acesso

em: 10 jun. 2025.
CANALTECH. Especialistas descobrem mais de 500 vulnerabilidades em roteadores desde 2020. 2022. Disponível em: https://canaltech.com.br/seguranca/especialistas-descobrem-mais-de-500-vulnerabilidades-em-roteadores-desde-2020-220638/. Acesso em: 6 jun. 2025.
CERT.br. Guia de segurança para redes domésticas. NIC.br, 2021. Disponível em: https://cartilha.cert.br/roteadores/. Acesso em: 20 abril. 2025.
ESET. Beyond KrØØk: Even more Wi-Fi chips vulnerable to eavesdropping. *WeLiveSecurity*, 2020. Disponível em: https://www.welivesecurity.com/2020/08/06/beyond-kr00k-even-more-wifi-chips-vulnerable-eavesdropping/. Acesso em: 6 jun. 2025.
ESET. Pelo menos 15% dos roteadores domésticos não estão protegidos. *WeLiveSecurity*, 2016. Disponível em: https://www.welivesecurity.com/br/2016/10/20/roteadores-nao-estao-protegidos/.
Acesso em: 20 abril. 2025.
FRAGATTACKS. FragAttacks: Security flaws in all Wi-Fi devices. 2021. Disponível em: https://www.fragattacks.com/. Acesso em: 6 jun. 2025.
IDEC. *Vírus em roteadores de internet se espalha pelo mundo*. Instituto Brasileiro de Defesa do Consumidor, 2018. Disponível em: https://idec.org.br/noticia/virus-de-roteadores-de-internet-se-espalha-pelo-mundo.
Acesso em: 20 jun. 2025.
IT BRASIL. Segurança de rede sem fio: proteja sua empresa contra ameaças cibernéticas. [s.d.]. Disponível em: https://www.itbrasil.net/post/seguranca-de-rede-sem-fio-proteja-sua-empresa-contra-ameacas-ciberneticas. Acesso em: 6 jun. 2025.
IT FORUM. CIOs, fiquem atentos: 6 formas como hackers exploram a infraestrutura. [s.d.]. Disponível em: https://itforum.com.br/cio-fiquem-atentos-6-formas-como-hackers-exploram-a-infraestrutura/.
Acesso em: 3 jun. 2025.
NETSPOT. Aprenda tudo sobre segurança WiFi. [s.d.]. Disponível em: https://www.netspotapp.com/pt/blog/wifi-security/.
Acesso em: 1 jun. 2025.
RESEARCHGATE. Caracterização das vulnerabilidades dos roteadores Wi-Fi no mercado brasileiro. 2023. Disponível em: https://www.researchgate.net/publication/371932663.
Acesso em: 1 jun. 2025.
SINGH, H. et al. Router firmware vulnerabilities: a global analysis. *IEEE Transactions on Network and Service Management*, v. 16, n. 4, p. 1450–1462, 2019.
STRONG SECURITY. 7 vulnerabilidades de Wi-Fi além de senhas fracas. 2017. Disponível em: https://www.strongsecurity.com.br/blog/7-vulnerabilidades-de-wi-fi-alem-de-senhas-fracas/.
Acesso em: 3 jun. 2025.
SYMANTEC. VPNFilter malware targets routers. *Symantec Security Response*, 2018. Disponível em: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/vpnfilter-iot-router-malware. Acesso em: 6 abril. 2025.
UNIFIA. Vulnerabilidades em rede wireless. 2018. Disponível em: https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/057_estudo10.pdf. Acesso em: 6 jun. 2025.