VULNERABILIDADES NA REDE WI-FI

Lennon da Cruz Cortes[1]
Bruna da Silva Pinto[2]
Anderson santos da silva [3]
Marcelo Pereira das Neves[4]

RESUMO

Com a demanda por mobilidade e disponibilidade de acesso a informação por dispositivos como *Smatphones*, *Tables* e *Notebooks* massificou o uso de redes Wi-Fi em ambientes diversos como em Instituições de Ensino. Com as redes Wi-Fi, surgiram novos riscos aos usuários e às instituições que proveem esse tipo de rede. Esta pesquisa teve como objetivo analisar e exemplificar algumas vulnerabilidades e ameaças presentes nas redes Wi-Fi. Inicialmente, levantou-se, por meio de uma pesquisa bibliográfica, seus mecanismos de segurança e as principais vulnerabilidades existentes nessa arquitetura. A análise dos resultados revelou que mudanças pontuais e de baixo custo podem aprimorar a segurança dessas redes.

Palavras-chave: Internet, rede, wi-fi.

ABSTRACT

With the demand for mobility and availability of access to information by devices such as Smatphones, Tables and Notebooks, the use of Wi-Fi networks has become widespread in diverse environments such as in Educational Institutions. With Wi-Fi networks, new risks have arisen for users and institutions that provide this type of network. This research aimed to analyze and exemplify some vulnerabilities and threats present in Wi-Fi networks. Initially, through its bibliographic research, its security mechanisms and the main vulnerabilities existing in this architecture were raised. The analysis of the results revealed that occasional and low-cost changes can improve the security of these networks.

Keywords: Internet, network, wi-fi.

[1]Acadêmico do Curso Superior em Tecnologia em Programação para Internet – Faculdade Alcides Maya. lennoncortes.sb@gmail.com
[2]Acadêmica do Curso Superior em Tecnologia em Programação para Internet – Faculdade Alcides Maya. simone.dutra@alcidesmaya.edu.br
[3]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. anderson_silva@alcidesmaya.edu.br
[4]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. Marcelo_neves@alcidesmaya.edu.br

1. Utilizar um SSID ou senha padrão

SSID é o “nome” da rede Wi-Fi, ou seja, aquele que aparece quando se visualiza as redes sem fio disponíveis em uma área. Embora pareça simples, o SSID pode virar uma arma interessante para garantir maior segurança à sua rede assim como esse também pode ser um problema, caso não tenha cuidado na hora de configurar o roteador e escolher o nome do Wi-Fi.

O termo SSID significa "service set identifier" ("identificador do conjunto de serviços", em tradução livre).

Nomes de rede Wi-Fi podem ter até 32 caracteres onde pode haver distinção entre minúsculas e maiúsculas, por exemplo: “minharede” é diferente de “MinhaRede”. Alguns caracteres especiais podem ser usados na criação de um SSID para a sua rede, embora o ideal seja evitar o uso desses símbolos por conta de problemas de compatibilidade com dispositivos mais antigos.

Pode-se usar como estratégia desligar esse recurso: dessa forma, quem quiser se conectar à rede terá de saber o SSID e a senha, já que o Wi-Fi não vai aparecer automaticamente como disponível ao seu redor. Isso é possível por meio da interface de configuração do seu roteador. Nas configurações wireless haverá uma opção para ocultar o SSID, impedindo que o dispositivo transmita o nome.

2. Não proteger os APs e hardware de rede

Apesar de implementar os melhores protocolos de segurança Wi-Fi do mundo, e eles ainda poderiam ser facilmente ignorados se alguém obtiver acesso físico a seus pontos de acesso sem fio ou outros componentes de rede . Por exemplo, se você tem um AP em uma mesa em uma sala destravada, alguém pode entrar como visitante e, com o toque de um botão (reset) rapidamente redefinir o AP para as configurações padrão de fábrica, abrindo acesso não seguro à rede. Ou se houver uma porta de rede aberta no lobby ou na área de espera, alguém pode rapidamente conectar um AP rogue, dando a ele acesso sem fio seguro ou mesmo seguro à rede.

Seria correto que os principais componentes da rede, incluindo o modem, o roteador e o switch, estejam protegidos em uma sala ou armário fechado e que o resto da rede e os componentes estejam fisicamente seguros e fora do alcance, especialmente em áreas públicas do prédio.

3. Compartilhar a senha Wi-Fi com todos os colaboradores

Compartilhando sua rede Wi-Fi particular com outras pessoas, principalmente visitantes que não são frequentes na sua casa, está aumentando os riscos para todos os dispositivos conectados. Na rede principal, é possível com alguns passos ter acesso a qualquer outro aparelho que faça uso da mesma, o que é muito perigoso caso a senha caia nas mãos de gente má intencionada.

Já uma rede Wi-Fi para visitantes pode ser configurada com restrições. Você pode fazer com que o usuário não possa acessar nenhum outro aparelho, seja um servidor ou uma impressora, e fique restrito única e simplesmente a seu próprio gadget. Ao mesmo tempo, redes para visitantes blindam os dados trafegados, impedindo a propagação de vírus, malwares e outras pragas para os conectados na rede principal.

Tal recurso é muito útil até para testar o tráfego de um dispositivo suspeito, fazendo-o se conectar à rede Wi-Fi secundária e monitorando suas atividades, sem que ele afete outros aparelhos.

4. Utilizar autenticação de PIN do WPS

O WPS (Wi-Fi Protected Setup) é um recurso existente na maioria dos roteadores sem fio e alguns APs de negócios. Ele torna as redes de segurança mais fáceis, no entanto pode se tornar um problema. Uma vulnerabilidade no método de autenticação de PIN do WPS pode facilitar o crack do PIN de 8 dígitos, recuperando a senha quando o modo pessoal de segurança está sendo usado, permitindo que alguém entre na rede. Devido a isso, é importante que as empresas utilizam o modo corporativo de segurança WPA2, pois os recursos WPS não

funcionam nesse modo, impedindo que hackers invadam a rede ou entrando no próprio dispositivo e desativando o mesmo.

5. Permitir acesso não autorizado por meio de VLANs mal configuradas

Muitas empresas permitem o acesso a seu Wi-Fi para funcionários, fornecedores e outros visitantes e, para manter a segurança, utilizam recursos capazes de projetar apenas a internet e algumas porções da rede, sem acesso a rede privada da organização. Em roteadores empresariais, switches e APs é possível emular essa funcionalidade configurando LANs virtuais e vários SSIDs. Entretanto, muitas vezes, as empresas se esquecem de verificar se sua rede privada é realmente segura enquanto está no acesso de convidado. É necessário que o processo seja realizado por profissionais capacitados. Assim, depois de instalar a rede, a TI deve garantir que tudo esteja funcionando como o planejado. Muitas são as vulnerabilidades que podem atrapalhar o funcionamento da rede sem fio de uma corporação. Por isso, é importante proteger seus dados e informações, principalmente em um cenário no qual os ataques têm se tornado cada vez mais comuns.

REFERÊNCIAS

CAÇADOR, D. M. Segurança e Mobilidade em Redes IEEE 802.11 Modelo de suporte à decisão na escolha de arquitecturas e tecnologias de redes sem fios. [s.l.] Universidade Católica Portuguesa, 2014, Acessado em: 23 out 2020.

LASHKARI, A. H. et al. A Survey on Wireless Security protocols (WEP , WPA and WPA2 / 802 . 11i). Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, n. 1 v 3, p. 48–52, 2009, Acessado em: 23 out 2020.

MORENO, Daniel. Pentest em Redes Sem Fio. São Paulo: Novatec, 2016, Acessado em: 23 out 2020.

VASCONCELLOS, RONALDO Segurança em Redes sem fio. Disponível em: . Acessado em: 23 out 2020.

WALIULLAH, M.; GAN, D. Wireless LAN Security Threats & Vulnerabilities : International Journal of Advanced Computer Science and Applications, v. 5, n. 1, p. 176–183, 2014, Acessado em: 23 out 2020.