Revista Multidisciplinar do Nordeste Mineiro, v.01, 2024
ISSN 2178-6925

SEGURANÇA CIBERNÉTICA PARA DISPOSITIVOS MÓVEIS

CYBER SECURITY FOR MOBILE DEVICES

Iago Amaral
Acadêmico do 8° período do curso de Sistemas de Informação
Faculdade Presidente Antônio Carlos-UNIPAC
E-mail: iagoamaral36@gmail.com

Jeferson Alves Silva
Acadêmico do 8° período do curso de Sistemas de Informação
Faculdade Presidente Antônio Carlos-UNIPAC
E-mail: jeferson3531@gmail.com

Filipe Nogueira Mota
Acadêmico do 8° período do curso de Sistemas de Informação
Faculdade Presidente Antônio Carlos-UNIPAC
E-mail: filipenogueira_13@outlook.com

Cosmo Pereira Da Silva
Bacharel em ciência da computação
Pós Graduado em Projetos de Aplicativos Móveis
E-mail: cosmosilva.dev@gmail.com

RESUMO

A rede Wi-Fi é uma conexão sem fio que oferece vantagens, como a eliminação do cabeamento e a facilidade de conexão com outros dispositivos compatíveis com essa tecnologia. Além disso, o uso de hotspots proporciona um controle aprimorado do acesso e reforça a segurança. No entanto, foi identificado um problema em que os usuários enfrentam dificuldades para acessar a rede sem fio devido à utilização do método de autenticação WPA com senha padrão, resultando em um nível de segurança inadequado e na falta de controle de acesso por parte dos administradores. Uma análise da estrutura da rede revelou a ausência de um controle de acesso eficaz, levando à decisão de implementar um projeto de implantação de hotspots. Os resultados dessa análise confirmaram que, apesar dos avanços tecnológicos, a segurança da informação em dispositivos móveis nesse contexto ainda depende muito do usuário.

Palavras-chave: Wi-fi, hotspots, WpaEnterprise.

ISSN 2178-6925

ABSTRACT

Wi-Fi is a wireless connection that offers advantages such as eliminating cabling and making it easier to connect to other devices compatible with this technology. In addition, the use of hotspots provides improved access control and strengthens security. However, a problem was identified in which users face difficulties accessing the wireless network due to the use of the WPA authentication method with a default password, resulting in an inadequate level of security and a lack of access control by administrators. An analysis of the network structure revealed the absence of effective access control, leading to the decision to implement a hotspot deployment project. The results of this analysis confirmed that, despite technological advances, information security on mobile devices in this context still depends a lot on the user.

Keywords: Wi-fi, hotspots, WpaEnterprise.

1 INTRODUÇÃO

A segurança cibernética para dispositivos móveis é uma preocupação crescente na era digital. Com o rápido avanço da tecnologia móvel e a proliferação de *smartphones* e *tablets*, os dispositivos móveis tornaram-se alvos atrativos para *hackers* e criminosos cibernéticos. A falta de conscientização e medidas de segurança adequadas pode levar a sérios riscos, como roubo de dados pessoais, invasão de privacidade, infecção por *malware* e acesso não autorizado a informações sensíveis (CABRAL; PONTES, 2021).

A segurança cibernética para dispositivos móveis envolve um conjunto de práticas e medidas projetadas para proteger tanto o dispositivo em si quanto os dados armazenados e transmitidos por ele. Existem várias áreas-chave que devem ser consideradas, ao abordar a segurança cibernética para dispositivos móveis. Em primeiro lugar, é essencial garantir que o dispositivo esteja protegido por meio de senhas fortes ou mecanismos de autenticação biométrica, como impressões digitais ou reconhecimento facial. Isso impede o acesso não autorizado ao dispositivo, caso seja perdido ou roubado (MESQUITA, 2018).

Além disso, é importante manter o *software* do dispositivo atualizado. As atualizações de segurança, são frequentemente lançadas pelos fabricantes para corrigir vulnerabilidades conhecidas e proteger contra novas ameaças. Ignorar essas atualizações pode deixar o dispositivo exposto a ataques. O uso de aplicativos confiáveis provenientes de fontes oficiais, como a loja de aplicativos do sistema operacional, é outra prática importante. Esses aplicativos passam por verificações de

ISSN 2178-6925

segurança antes de serem disponibilizados para download, reduzindo o risco de instalar *software* malicioso (SILVA *et al*., 2021).

A proteção dos dados pessoais é fundamental na segurança cibernética para dispositivos móveis. É recomendável usar criptografia para proteger as informações armazenadas no dispositivo e evitar o compartilhamento de dados sensíveis, como informações bancárias ou números de documentos, por meio de redes *Wi-Fi* públicas ou não confiáveis (ZEQUIM; RIBEIRO, 2022).

Outra medida de segurança importante, é ter um *software* antivírus confiável instalado no dispositivo móvel. Isso pode ajudar a detectar e remover *malware*, além de oferecer proteção em tempo real contra ameaças cibernéticas. A conscientização do usuário também desempenha um papel fundamental na segurança cibernética para dispositivos móveis. É essencial que os usuários sejam educados sobre os riscos envolvidos e as práticas recomendadas de segurança, como evitar clicar em *links* suspeitos, não abrir anexos de *e-mails* desconhecidos e ter cuidado ao fornecer informações pessoais *online* (BRAGA *et al.,* 2012).

Diante disso, foi abordado uma problemática onde o usuário tem dificuldade no acesso à rede sem fio porque o método de autenticação utilizado é o WPA, com senha padrão ocasionado um nível de segurança muito baixo e falta de controle de acesso por parte dos administradores. O objetivo deste trabalho é validar a importância da segurança cibernética para os dispositivos móveis, buscando demonstrar seu histórico de utilização, seu procedimento e execução nas redes de segurança. Foi realizada uma análise de estrutura de redes, e constatado a ausência de um controle de acesso eficiente e, partir disso, foi decidido a realização de um projeto de implantação de hotspots.

Em resumo, a segurança cibernética para dispositivos móveis é um aspecto crucial na era digital atual. Ao adotar práticas de segurança adequadas, como proteger o dispositivo com senhas fortes, manter o *software* atualizado, usar aplicativos confiáveis, proteger os dados pessoais e ter um *software* antivírus confiável, os usuários podem minimizar os riscos e desfrutar de uma experiência móvel segura. A conscientização e a educação contínuas são essenciais para se manter atualizado sobre as ameaças emergentes e as melhores práticas de segurança cibernética (BERTOGLIO *et al.,* 2022).

ISSN 2178-6925

2 REVISÃO TEÓRICA

2.1 EVOLUÇÃO DOS DISPOSITIVOS MÓVEIS E AMEAÇAS CIBERNÉTICAS

A evolução dos dispositivos móveis tem sido impressionante ao longo dos últimos anos. Desde os primeiros telefones celulares simples até os *smartphones* modernos, houve avanços significativos em termos de capacidade de processamento, armazenamento, conectividade e funcionalidades. Os dispositivos móveis agora possuem poder de processamento comparável a computadores pessoais, permitindo executar aplicativos complexos e realizar multitarefas. Eles também têm uma capacidade de armazenamento considerável, com muitos modelos oferecendo dezenas ou até mesmo centenas de *gigabytes* de espaço (AVERSARI; KULESZA; MOREIRA, 2017).

A conectividade também melhorou consideravelmente. Além das redes móveis de alta velocidade, como 4G e 5G, os *smartphones* também são capazes de se conectar a redes *Wi-Fi* e *Bluetooth*. Isso possibilita a transferência rápida de dados, o uso de serviços baseados em nuvem e a integração com outros dispositivos. Quanto às funcionalidades, os *smartphones* modernos oferecem uma variedade de recursos, além das chamadas e mensagens. Eles são utilizados para tirar fotos e gravar vídeos de alta qualidade, reproduzir músicas e vídeos, navegar na internet, realizar transações financeiras, executar aplicativos de produtividade e muito mais. Além disso, os dispositivos móveis são cada vez mais utilizados para acessar redes sociais e aplicativos de mensagens instantâneas, tornando-se uma parte essencial da comunicação e interação social (CABRAL; DELOSKI; STADLER, 2018).

No entanto, com a evolução dos dispositivos móveis, também surgiram ameaças cibernéticas cada vez mais sofisticadas. Os *hackers* e criminosos cibernéticos aproveitam as vulnerabilidades dos dispositivos móveis para realizar ataques e roubar informações pessoais e financeiras dos usuários. Uma das principais ameaças cibernéticas em dispositivos móveis é o *malware* móvel. Esses são aplicativos maliciosos que podem ser baixados de fontes não confiáveis ou serem disfarçados como aplicativos legítimos. O *malware* móvel pode roubar informações confidenciais, como senhas e dados bancários, além de controlar remotamente o dispositivo do usuário (SILVA *et al.,* 2021).

ISSN 2178-6925

Ao longo dos anos, os dispositivos móveis passaram por uma incrível evolução tecnológica, oferecendo recursos avançados e tornando-se uma parte indispensável da vida moderna. Desde os primeiros telefones celulares até os atuais *smartphones*, testemunhamos um aumento significativo na capacidade de processamento, armazenamento e conectividade desses dispositivos (VIANNA; DE SOUSA, 2017).

Os smartphones modernos são verdadeiros computadores de bolso, equipados com poderosos processadores que rivalizam com muitos PCs e *laptops*. Eles oferecem uma experiência multitarefa eficiente e a capacidade de executar aplicativos complexos e exigentes, desde jogos avançados até ferramentas de produtividade sofisticadas. Além disso, o armazenamento interno dos dispositivos móveis aumentou consideravelmente. Agora, é comum encontrar *smartphones* com capacidade de armazenamento de dezenas a centenas de *gigabytes*, permitindo que os usuários armazenem grandes quantidades de dados, incluindo fotos, vídeos, músicas e documentos (CABRAL; PONTES, 2021).

A conectividade também se tornou mais rápida e amplamente disponível. As redes móveis evoluíram de 2G para 3G, 4G e, mais recentemente, 5G, proporcionando velocidades de internet cada vez mais rápidas e maior estabilidade de conexão. Além disso, os dispositivos móveis podem se conectar a redes *Wi-F*i em casa, no trabalho ou em locais públicos, permitindo um acesso contínuo à internet e uma variedade de serviços *online* (MESQUITA, 2018).

O *phishing* móvel também é uma ameaça séria. Os criminosos enviam mensagens de texto falsas, e-mails ou criam *sites* fraudulentos que se assemelham a serviços legítimos para enganar os usuários a fornecerem informações confidenciais, como senhas e números de cartão de crédito. As redes *Wi-Fi* públicas e não seguras também representam um risco. Os *hackers* podem interceptar o tráfego de dados nessas redes e obter acesso a informações pessoais transmitidas pelo dispositivo móvel (ZEQUIM; RIBEIRO, 2022).

O roubo de dados é outra ameaça importante. Quando um dispositivo móvel é perdido ou roubado, todas as informações armazenadas nele, como contatos, mensagens, fotos e documentos, podem cair nas mãos erradas. Além disso, os ataques de engenharia social são uma ameaça crescente. Os criminosos exploram a confiança dos usuários, por meio de ligações, mensagens de texto ou e-mails falsos, para obter acesso a informações pessoais ou induzi-los a realizar ações prejudiciais,

como clicar em links maliciosos ou fornecer informações confidenciais (BRAGA et al., 2012).

2.2 TECNOLOGIAS DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS

As tecnologias de segurança para dispositivos móveis, têm se tornado cada vez mais importantes na proteção contra ameaças cibernéticas. Aqui estão algumas das principais tecnologias utilizadas para fortalecer a segurança em dispositivos móveis:

- Criptografia de dados: A criptografia é uma técnica que protege os dados armazenados no dispositivo e durante a transmissão. Ela converte as informações em um formato ilegível para qualquer pessoa sem a chave de criptografia correta. Isso garante que, mesmo se os dados forem interceptados, eles permaneçam inacessíveis para terceiros.
- Autenticação multifator: A autenticação multifator acrescenta uma camada extra de segurança para o acesso ao dispositivo. Além de uma senha, é necessário fornecer um segundo fator de autenticação, como uma impressão digital, reconhecimento facial ou um código enviado por mensagem de texto. Isso dificulta o acesso não autorizado ao dispositivo mesmo que a senha seja comprometida.
- VPN (Rede Virtual Privada): Uma VPN permite que os dispositivos móveis estabeleçam uma conexão segura com a internet, criptografando todo o tráfego de dados. Isso protege contra-ataques em redes Wi-Fi não seguras, garantindo que as informações transmitidas estejam protegidas contra espionagem e interceptação.
- Gerenciamento de dispositivos móveis (MDM): As soluções de MDM permitem que as empresas gerenciem a segurança dos dispositivos móveis usados por seus funcionários. Isso inclui a implementação de políticas de segurança, como senhas fortes, restrições de aplicativos, criptografia e a capacidade de rastrear e apagar remotamente os dados em caso de perda ou roubo do dispositivo.
- Antivírus e segurança móvel: Assim como nos computadores, existem aplicativos antivírus e de segurança, disponíveis para dispositivos móveis. Esses aplicativos protegem contra *malware*, detectando e removendo

aplicativos maliciosos, verificando a segurança de *sites* e fornecendo recursos adicionais, como localização remota e bloqueio do dispositivo em caso de perda.

- *Firewall* de rede: Alguns dispositivos móveis possuem recursos de *firewall* embutidos ou aplicativos de *firewall* podem ser instalados. Esses *firewalls* monitoram o tráfego de rede e bloqueiam conexões suspeitas ou não autorizadas, aumentando a segurança contra-ataques externos.
- Atualizações de segurança regulares: É fundamental manter o sistema operacional do dispositivo e os aplicativos atualizados com as versões mais recentes. As atualizações geralmente incluem correções de segurança que abordam vulnerabilidades conhecidas, garantindo que o dispositivo esteja protegido contra as ameaças mais recentes (BERTOGLIO et al., 2022).

Ao implementar essas tecnologias de segurança e adotar boas práticas de uso, como baixar aplicativos apenas de fontes confiáveis e ter cuidado ao clicar em links desconhecidos, é possível fortalecer significativamente a segurança dos dispositivos móveis e reduzir o risco de ataques cibernéticos.

A implementação de um projeto de hotspots se torna crucial devido a várias razões. Em primeiro lugar, proporciona uma camada adicional de segurança, permitindo a implementação de autenticação segura e criptografia, o que ajuda a proteger informações sensíveis e dados pessoais dos usuários (LEVY; ANTÔNIO; ZAMPIER, [s.d.]). Além disso, os hotspots possibilitam um controle mais eficaz sobre o acesso à rede, o que é útil para restringir o uso não autorizado. Também simplifica o monitoramento e o gerenciamento do tráfego de rede, facilitando a identificação e solução de problemas (NAKAMURA e GEUS, 2007). A experiência do usuário é aprimorada, eliminando a necessidade de inserir senhas repetidamente. A implementação adequada de hotspots ajuda as organizações a cumprir regulamentos de segurança e estabelecer políticas de acesso personalizadas. Além disso, reduz os riscos de ataques cibernéticos, como acesso não autorizado à rede. Por fim, ao configurar hotspots para fornecer uma conexão de alta qualidade, melhora-se a experiência do usuário em termos de velocidade e confiabilidade, tornando essa implementação essencial em cenários onde a segurança e a gestão eficiente da rede são prioridades.

ISSN 2178-6925

2.3 VULNERABILIDADES E ATAQUES COMUNS

Os dispositivos móveis estão cada vez mais presentes em nosso dia a dia, e, infelizmente, também estão expostos a várias vulnerabilidades e ataques cibernéticos. Aqui estão algumas das vulnerabilidades e ataques comuns em segurança cibernética para dispositivos móveis:

- *Malware* móvel: Os dispositivos móveis são frequentemente alvos de ataques de *malware*, incluindo vírus, cavalos de Troia e *ransomware*. Esses *malwares* podem ser baixados por meio de aplicativos infectados, *links* maliciosos ou até mesmo através de redes *Wi-Fi* não seguras. Eles podem comprometer a segurança do dispositivo, roubar informações pessoais, como senhas e dados bancários, ou bloquear o acesso aos arquivos do usuário, exigindo um resgate.
- *Phishing* móvel: O *phishing* é uma técnica comum em que os *hackers* tentam enganar os usuários para obter informações confidenciais, como senhas, informações bancárias e números de cartão de crédito. Isso geralmente ocorre por meio de mensagens de texto, *e-mails* ou *sites* falsos que se fazem passar por empresas legítimas, levando os usuários a divulgar suas informações sem saber.
- Redes Wi-Fi não seguras: Conectar-se a redes Wi-Fi públicas ou não seguras, pode expor os dispositivos móveis a ataques de interceptação de dados. Os *hackers* podem criar redes *Wi-Fi* falsas ou usar técnicas de "*sniffing*" para capturar informações transmitidas pelo dispositivo, como credenciais de login, dados pessoais ou até mesmo informações financeiras.
- Ataques de engenharia social: Os ataques de engenharia social visam explorar a confiança e a ingenuidade dos usuários para obter acesso a informações confidenciais. Isso pode incluir chamadas telefônicas fraudulentas, mensagens de texto ou *e-mails* enganosos que solicitam informações pessoais ou levam o usuário a clicar em *links* maliciosos.
- Vulnerabilidades de sistema operacional: Os dispositivos móveis podem estar sujeitos a vulnerabilidades de segurança em seus sistemas operacionais. Se o sistema operacional não estiver atualizado com as últimas correções de segurança, os hackers podem explorar essas vulnerabilidades para ganhar acesso não autorizado ao dispositivo ou aos dados do usuário.

ISSN 2178-6925

- Falta de autenticação robusta: Senhas fracas ou a ausência de autenticação multifator podem tornar os dispositivos móveis mais vulneráveis a ataques de força bruta, onde hackers tentam adivinhar ou quebrar as senhas para obter acesso indevido ao dispositivo.
- Perda ou roubo de dispositivo: A perda ou roubo de um dispositivo móvel pode expor informações pessoais e dados confidenciais. Se o dispositivo não estiver devidamente protegido com senha, criptografia ou recursos antirroubo, um atacante pode acessar facilmente os dados armazenados no dispositivo.
- Aplicativos não confiáveis: Baixar aplicativos de fontes não confiáveis ou de lojas de aplicativos não oficiais pode expor o dispositivo a aplicativos maliciosos. Esses aplicativos podem ter acesso não autorizado aos dados do usuário, coletar informações pessoais ou até mesmo controlar remotamente o dispositivo.
- Vulnerabilidades de rede: Além das vulnerabilidades específicas do dispositivo, as vulnerabilidades de rede também representam uma ameaça à segurança dos dispositivos móveis. Isso inclui ataques como o Man-in-the-Middle (MitM), onde um atacante intercepta a comunicação entre o dispositivo móvel e a rede, podendo acessar ou modificar os dados transmitidos.
- Falta de conscientização do usuário: Uma vulnerabilidade comum é a falta de conscientização e educação dos usuários sobre as práticas de segurança cibernética. Os usuários podem inadvertidamente clicar em links suspeitos, baixar aplicativos não confiáveis ou compartilhar informações confidenciais sem perceber os riscos envolvidos (AVERSARI; KULESZA; MOREIRA, 2017).

Diante dessas vulnerabilidades e ameaças, é essencial adotar medidas de segurança adequadas para proteger os dispositivos móveis. Isso inclui manter o sistema operacional e os aplicativos atualizados, usar senhas fortes e autenticação multifator, evitar redes Wi-Fi não seguras, baixar aplicativos apenas de fontes confiáveis, estar atento a sinais de *phishing*, proteger o dispositivo com recursos antirroubo e ter uma consciência constante sobre as práticas de segurança cibernética. Além disso, é importante investir em soluções de segurança móvel, como antivírus e *firewalls*, para fornecer uma camada adicional de proteção contra ameaças conhecidas e emergentes. Com a devida precaução e medidas de segurança, é

ISSN 2178-6925

possível mitigar os riscos e manter os dispositivos móveis protegidos contra vulnerabilidades e ataques cibernéticos.

2.4 POLÍTICAS E REGULAMENTAÇÕES DE SEGURANÇA CIBERNÉTICA

A segurança cibernética é um assunto cada vez mais importante nos dias de hoje, e as políticas e regulamentações de segurança cibernética são essenciais para proteger as empresas e os indivíduos de ataques. As políticas de segurança cibernética, estabelecem as regras e diretrizes que as empresas devem seguir para proteger seus sistemas e dados. As regulamentações de segurança cibernética são leis que exigem que as empresas sigam certas práticas de segurança cibernética. As políticas de segurança cibernética geralmente incluem diretrizes para a criação de senhas fortes, a instalação de *software* antivírus e a atualização regular de sistemas e aplicativos. Essas políticas também podem incluir diretrizes para o acesso a dados confidenciais e informações de clientes (CABRAL; DELOSKI; STADLER, 2018).

As políticas de segurança cibernética devem ser atualizadas regularmente para se adaptar às ameaças emergentes. As regulamentações de segurança são estabelecidas por agências governamentais e exigem que as empresas sigam determinadas práticas de segurança cibernética. As regulamentações de segurança podem variar de país para país, mas geralmente exigem que as empresas protejam os dados dos clientes e notifiquem os clientes em caso de violação de dados. As políticas e regulamentações de segurança cibernética são essenciais para proteger as empresas e os indivíduos de ataques cibernéticos (VIANNA; DE SOUSA, 2017).

As empresas que não seguem essas políticas e regulamentações estão em risco de violações de dados e outras formas de ataques cibernéticos. Além disso, essas empresas podem enfrentar multas e outras penalidades. As políticas e regulamentações de segurança cibernética também ajudam a proteger a privacidade dos indivíduos. As empresas que coletam informações pessoais devem seguir as políticas e regulamentações de segurança cibernética para proteger essas informações. Isso inclui informações como nome, endereço, número de telefone e informações financeiras (CABRAL; PONTES, 2021).

Políticas e regulamentações de segurança cibernética são fundamentais para proteger as informações pessoais e confidenciais dos usuários na internet. Essas medidas incluem a implementação de senhas fortes, a criptografia de dados e a

utilização de softwares antivírus. Além disso, é importante estar atento a possíveis ameaças de hackers e ataques cibernéticos, e sempre manter o sistema operacional e os aplicativos atualizados (MESQUITA, 2018).

Outra medida importante é a conscientização dos usuários sobre as melhores práticas de segurança cibernética, como não compartilhar senhas, não clicar em *links* suspeitos e não baixar *softwares* de fontes não confiáveis. As empresas também devem investir em treinamentos e capacitações para seus funcionários, a fim de garantir que todos estejam cientes dos riscos e saibam como agir em caso de incidentes de segurança. Além disso, as políticas e regulamentações de segurança cibernética devem ser constantemente revisadas e atualizadas para se adaptar às novas ameaças e tecnologias (SILVA *et al.,* 2021).

A segurança cibernética é uma área crucial na era digital, e para garantir a proteção dos sistemas de informação, várias políticas e regulamentações têm sido desenvolvidas em todo o mundo. Essas políticas têm como objetivo principal mitigar os riscos de ataques cibernéticos, proteger a privacidade dos usuários e promover a confiança e a segurança nas comunicações digitais. Aqui estão algumas das principais políticas e regulamentações de segurança cibernética:

- Legislação de Proteção de Dados: Muitos países têm leis que regem a proteção de dados pessoais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Essas leis estabelecem diretrizes para a coleta, armazenamento e processamento de informações pessoais e exigem medidas de segurança adequadas para proteger esses dados contra violações e vazamentos.
- Leis de Notificação de Violação de Dados: Essas leis exigem que as organizações notifiquem as autoridades competentes e os indivíduos afetados em caso de violação de dados pessoais. Isso visa garantir que as pessoas sejam informadas sobre quaisquer incidentes de segurança que possam afetar sua privacidade e permitir que tomem medidas para proteger suas informações.
- Normas e padrões de segurança cibernética: Existem várias normas e padrões estabelecidos por organizações e consórcios, como a ISO (International Organization for Standardization) e o NIST (National Institute of Standards and Technology). Essas normas fornecem diretrizes e melhores práticas para a implementação de medidas de segurança cibernética, abrangendo aspectos

como gerenciamento de riscos, controle de acesso, criptografia e resposta a incidentes.

- Estratégias e políticas nacionais de segurança cibernética: Muitos países desenvolveram estratégias nacionais de segurança cibernética para enfrentar os desafios emergentes na esfera digital. Essas estratégias abordam questões como proteção de infraestrutura crítica, defesa cibernética, cooperação internacional e conscientização pública. Elas também estabelecem os papéis e responsabilidades das várias entidades envolvidas na segurança cibernética ao nível nacional.
- Regulamentações setoriais: Além das políticas gerais de segurança cibernética, alguns setores específicos podem ter regulamentações adicionais. Por exemplo, no setor financeiro, existem normas específicas para proteger as transações e informações financeiras dos clientes. Da mesma forma, setores como saúde, energia e transporte também podem ter regulamentações específicas para proteger suas infraestruturas críticas e dados sensíveis (ZEQUIM; RIBEIRO, 2022).

Essas são apenas algumas das políticas e regulamentações de segurança cibernética que têm sido implementadas em todo o mundo. À medida que a tecnologia evolui e novas ameaças surgem, é fundamental que essas políticas sejam atualizadas e reforçadas para garantir a segurança contínua dos sistemas de informação e a proteção dos usuários.

2.5 DESAFIOS E TENDÊNCIAS FUTURAS

A segurança cibernética para dispositivos móveis enfrenta constantemente desafios e evolui para acompanhar as tendências tecnológicas em constante mudança. Cabral e Pontes (2021) apresentam alguns desafios e tendências futuras relevantes para a segurança cibernética em dispositivos móveis:

- Aumento das ameaças de *malware* móvel: Com a crescente popularidade dos dispositivos móveis, os criminosos cibernéticos estão cada vez mais direcionando seus ataques para essas plataformas. O *malware* móvel, como aplicativos maliciosos e *ransomware*, representará uma ameaça crescente para a segurança dos dispositivos móveis.

- Ataques de *phishing* em dispositivos móveis: Os ataques de *phishing*, que visam enganar os usuários para obter suas informações pessoais ou financeiras, também estão se tornando mais sofisticados em dispositivos móveis. Os usuários devem estar atentos a e-mails, mensagens de texto e links suspeitos recebidos em seus dispositivos móveis.
- Vazamento de dados em aplicativos: Com a proliferação de aplicativos móveis que coletam e armazenam dados dos usuários, há um aumento no risco de vazamentos de dados. Os usuários precisam ter cuidado ao conceder permissões de acesso a aplicativos e verificar as políticas de privacidade antes de fornecer informações pessoais.
- Internet das Coisas (IoT): Com o crescimento da IoT, dispositivos conectados, como *smartwatches*, dispositivos domésticos inteligentes e veículos autônomos, estão se tornando alvos potenciais para ataques cibernéticos. A segurança desses dispositivos móveis integrados à IoT é crucial para proteger a privacidade e a segurança dos usuários.
- Uso de biometria para autenticação: A autenticação biométrica, como impressões digitais e reconhecimento facial, está se tornando uma forma comum de desbloqueio de dispositivos móveis. No entanto, os desafios futuros incluem garantir a precisão e a segurança dessas tecnologias biométricas contra falsificação ou uso indevido.
- Inteligência Artificial (IA) e segurança cibernética: A IA está sendo cada vez mais usada em dispositivos móveis para melhorar a experiência do usuário. No entanto, também pode ser explorada por atacantes para realizar ataques cibernéticos mais avançados. O desenvolvimento de técnicas de IA para detectar e prevenir ameaças cibernéticas será um desafio crucial no futuro.
- Privacidade e regulamentações de proteção de dados: Com o aumento das preocupações com a privacidade, é provável que ocorram mais regulamentações relacionadas à proteção de dados em dispositivos móveis. Os usuários devem estar cientes das políticas de privacidade dos aplicativos e das regulamentações aplicáveis para garantir a proteção de suas informações pessoais.
- Ameaças de rede móvel: As redes móveis também podem ser alvos de ataques cibernéticos, como interceptação de comunicações ou ataques de negação de

ISSN 2178-6925

serviço. As operadoras e os usuários precisam estar cientes dessas ameaças e implementar medidas de segurança adequadas.

- Criptomoedas e carteiras digitais: Com o crescente uso de criptomoedas e carteiras digitais em dispositivos móveis, a segurança cibernética relacionada a essas tecnologias se torna crucial. Os usuários devem estar cientes dos riscos associados ao armazenamento e à transação de criptomoedas em dispositivos móveis, como ataques de *malware* direcionados a carteiras digitais e *phishing* voltado para obter informações de acesso.
- Proteção contra-ataques avançados: Os atacantes estão constantemente desenvolvendo técnicas mais sofisticadas para comprometer a segurança cibernética em dispositivos móveis. Isso inclui ataques avançados de engenharia social, exploração de vulnerabilidades desconhecidas e uso de técnicas de evasão de detecção. A defesa contra esses ataques requer soluções de segurança igualmente avançadas.
- Integração de segurança no *design* de dispositivos: À medida que a segurança cibernética se torna cada vez mais importante, espera-se que os fabricantes de dispositivos móveis incorporem recursos de segurança desde o *design* inicial dos dispositivos. Isso inclui a implementação de *chips* de segurança, *firmware* seguro e atualizações regulares para mitigar vulnerabilidades conhecidas.
- Aumento da conscientização e educação: A conscientização dos usuários, sobre os riscos e melhores práticas de segurança cibernética para dispositivos móveis é fundamental. Espera-se um maior foco na educação dos usuários, fornecendo informações sobre os tipos de ameaças, como identificá-las e como se proteger adequadamente.

É importante acompanhar essas tendências e desafios em evolução e adotar uma abordagem proativa para fortalecer a segurança cibernética em dispositivos móveis. Isso envolve a implementação de soluções de segurança confiáveis, atualizações regulares de software, conscientização constante e a adoção de boas práticas de segurança por parte dos usuários.

ISSN 2178-6925

3 CONCLUSÃO

As ameaças em constante evolução nesse campo, as melhores práticas de segurança e as medidas preventivas que podem ser adotadas para proteger dispositivos móveis e dados sensíveis. Essa experiência fortaleceu nossa compreensão sobre a importância da segurança cibernética em dispositivos móveis e despertou nosso interesse em continuar nos aprimorando nessa área.

Alguns desafios enfrentados na segurança cibernética para dispositivos móveis, como o aumento das ameaças de *malware* móvel, a sofisticação dos ataques de *phishing* direcionados a dispositivos móveis, e a necessidade de equilibrar a conveniência dos usuários com a segurança dos dados.

Além disso, ficou claro a importância da conscientização e treinamento dos usuários, pois muitos incidentes de segurança poderiam ser evitados com a adoção de boas práticas e a compreensão dos riscos envolvidos.

Para lidar com os desafios futuros e acompanhar as tendências em segurança cibernética para dispositivos móveis, é fundamental manter-se atualizado sobre as ameaças emergentes, estar ciente das regulamentações e melhores práticas atualizadas e continuar desenvolvendo habilidades técnicas relacionadas à segurança.

Em conclusão, a segurança cibernética para dispositivos móveis foi uma experiência enriquecedora que proporciona uma visão aprofundada dos desafios e práticas de segurança nesse campo em constante evolução. Podemos entender os conhecimentos teóricos e habilidades práticas relacionadas à análise de ameaças, implementação de medidas de segurança, testes de segurança e resposta a incidentes.

A importância de estar atualizado sobre as tendências e as ameaças emergentes em segurança cibernética para dispositivos móveis, bem como a necessidade de uma abordagem proativa para mitigar riscos e proteger os dados sensíveis. Também compreendemos a importância da conscientização e do treinamento dos usuários para garantir uma cultura de segurança sólida e a adoção de boas práticas de segurança cibernética.

ISSN 2178-6925

REFERÊNCIAS

AVERSARI, Lucas OC; KULESZA, Raoni; MOREIRA, Josilene A. Um Estudo Prático sobre o Potencial do Ataque Slowloris a partir de Dispositivos Móveis. In: **Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2017. p. 494-500.

BERTOGLIO, Daniel Dalalana et al. Weasels e a construção de conhecimento em Segurança Ofensiva. In: **Anais do II Simpósio Brasileiro de Educação em Computação**. SBC, 2022. p. 109-117.

BRAGA, Alexandre Melo et al. Introdução à segurança de dispositivos móveis modernos–um estudo de caso em android. **Sociedade Brasileira de Computação**, 2012.

CABRAL, Carlos Gabriel Nunes; DELOSKI, Matheus; STADLER, Júlio Cesar. Uso de técnicas de jogos em seu contexto atual: gamificação e sua importância. **Anais da Jornada Científica dos Campos Gerais**, v. 16, 2018.

CABRAL, Juliana Pereira; PONTES, Herleson Paiva. Segurança em Dispositivos Móveis: Um Estudo Sobre a Adoção de Boas Práticas para Proteção em Celulares. In: **Anais do XLVIII Seminário Integrado de Software e Hardware**. SBC, 2021. p. 58-68.

LEVY, G.; ANTÔNIO, M.; ZAMPIER. **Gerenciamento de uma rede pública utilizando a ferramenta Hotspot do Sistema Operacional RouterOS**. [s.l: s.n.]. Disponível em: <http://repositorioguairaca.com.br/jspui/bitstream/23102004/86/1/TCC%20Tads%20-%20Guilherme%20Levy.pdf>. Acesso em: 20 out. 2023.

MESQUITA, Pablo. Desafios da forense em dispositivos móveis. **Gestão da Segurança da Informação-Unisul Virtual**, 2018.

NAKAMURA, Emilio T. e DE GEUS, Paulo L. **Segurança de redes em ambientes cooperativos.** São Paulo SP: Novatec 2007

SILVA, Alex Aparecido et al. Metodologias ativas ao conceber, desenvolver e controlar fechaduras de forma remota, através do wi-fi com dispositivo móveL. **CIMATech**, v. 1, n. 8, p. 100-110, 2021.

VIANNA, Eduardo Wallier; DE SOUSA, Renato Tarciso Barbosa. Ciber Proteção: a segurança dos sistemas de informação no espaço cibernético. **Revista Ibero-Americana de Ciência da Informação**, v. 10, n. 1, p. 110-131, 2017.

ZEQUIM, Eduarda Pagim; RIBEIRO, Douglas Francisco. O papel da inteligencia artificial na segurança cibernetica: o uso de sistemas inteligentes em benefício da segurança dos dados das empresas. **Revista Interface Tecnológica**, v. 19, n. 1, p. 21-33, 2022.