SEGURANÇA EM DISPOSITIVOS IOT: ANÁLISE EM CÂMERAS IP

Danilo José Gonçalves de Matos
Faculdade de Tecnologia de Assis
danilo_djgm@hotmail.com

André Felipe Marques Canton
Faculdade de Tecnologia de Assis
andrecantones@gmail.com

Fabio Eder Cardoso
Faculdade de Tecnologia de Assis
fabio.cardoso@fatec.sp.gov.br

RESUMO

"A popularidade das câmeras IP, facilitada pela instalação e monitoramento remoto, aumentou a preocupação com sua segurança. A vulnerabilidade desses dispositivos, devido a limitações de *hardware*, falta de atualizações e suporte descontinuado, expõe os usuários a riscos de invasão e vazamento de dados. Este trabalho utiliza abordagem quali-quantitativa, analisa as principais vulnerabilidades em câmeras IP. A pesquisa combina revisão bibliográfica e análise de dados empíricos sobre a exposição de câmeras IP na Internet. A análise inicial destaca a alta vulnerabilidade dessas câmeras, revelando falhas de segurança e exposição a ameaças."

Palavras-chave: Segurança, vulnerabilidades, privacidade, práticas de segurança.

ABSTRACT

The popularity of IP cameras, facilitated by remote installation and monitoring, has increased concerns about their security. The vulnerability of these devices, due to hardware limitations, lack of updates and discontinued support, exposes users to risks of intrusion and data leakage. This work, using a qualitative-quantitative approach, analyzes the main vulnerabilities in IP cameras. The research combines a literature review and analysis of empirical data on the exposure of IP cameras on the Internet. The initial analysis highlights the high vulnerability of these cameras, revealing security flaws and exposure to threats.

Keywords: *Security, vulnerabilities, privacy, security practices.*

1 INTRODUÇÃO

A era digital trouxe uma série de inovações que transformaram profundamente a maneira como se vive, trabalha e interage com o mundo ao redor. Entre essas inovações, as câmeras IP se destacam como ferramentas essenciais para ambientes que vão desde residências até grandes corporações e espaços públicos. Sua praticidade, aliada à capacidade de monitoramento remoto, fez com que esses dispositivos se tornassem onipresentes na sociedade moderna, respondendo a uma demanda crescente por segurança e vigilância (Bonilla, 2025).

Essa mesma conectividade, que permite o acesso remoto e a integração com outros dispositivos da Internet das Coisas (IoT), também expõe as câmeras IP a uma série de riscos cibernéticos. A facilidade de instalação, muitas vezes sem configurações de segurança robustas, contribui para a vulnerabilidade desses dispositivos, tornando-os alvos atraentes para ciber criminosos (*Magrani*, 2018). Ataques como o da Botnet Mirai, que teve impacto global, ilustram a extensão dos danos que podem resultar de falhas de segurança em dispositivos IoT (Security Leaders). No Brasil, um dos países mais afetados por essa Botnet, câmeras de segurança IP, gravadores digitais de vídeo (DVRs) e outros dispositivos conectados foram amplamente comprometidos, resultando em invasões e vazamentos de dados sensíveis (Da Silva, 2023).

Além disso, a aparente segurança oferecida por câmeras IP pode mascarar uma realidade inquietante: a vulnerabilidade intrínseca desses dispositivos pode levar a sérios problemas de privacidade e segurança. A falta de atualizações regulares de *firmware*, configurações de segurança inadequadas e a utilização de credenciais fracas são fatores que ampliam a exposição dessas câmeras a ameaças cibernéticas. Isso se torna especialmente preocupante em um cenário onde segurança física e digital está cada vez mais interligada, e a proteção de dados sensíveis é crucial para a integridade de indivíduos e organizações (Da Silva, 2023).

Diante desse contexto, este estudo tem como objetivo geral analisar a percepção dos proprietários/usuários quanto às vulnerabilidades das câmeras IP e propor medidas de segurança eficazes para mitigar esses riscos. Dedica-se a analisar práticas recomendadas de segurança para dispositivos IoT, com ênfase na proteção de câmeras IP, além de oferecer recomendações práticas para a mitigação de riscos em dispositivos de vigilância conectados.

A relevância deste estudo se justifica pelo uso cada vez mais frequente das câmeras IP em diversos setores e pelo aumento das ameaças de segurança nestes dispositivos. A vulnerabilidade das câmeras IP não é apenas uma questão de privacidade, mas também de segurança pública e corporativa. Com a expansão acelerada dos dispositivos IoT e a crescente dependência de tecnologias conectadas para segurança e vigilância, há uma necessidade urgente de implementar práticas de segurança mais robustas. Este trabalho visa contribuir tanto para a comunidade acadêmica quanto para o setor de segurança, oferecendo uma análise detalhada e recomendações práticas que promovam o uso mais seguro e consciente desses dispositivos em um mundo cada vez mais digital e interconectado.

2 REVISÃO DE LITERATURA

A crescente utilização de sistemas de vídeo monitoramento, compostos por câmeras IP, analógicas e térmicas, integrados à Internet das Coisas (IoT), tem se mostrado uma ferramenta cada vez mais eficaz na prevenção e investigação de crimes. Esses sistemas estão presentes em uma ampla gama de ambientes, como empresas, escolas, residências e espaços públicos, desempenhando um papel crucial na segurança e na dissuasão de atividades ilícitas. Estudos

demonstram que a presença dessas tecnologias pode levar a uma redução significativa nos índices de criminalidade, ao mesmo tempo em que facilita a identificação de suspeitos e a resolução de casos (*Grinberg et al*., 2024).

No entanto, a proliferação de dispositivos IoT, incluindo câmeras de segurança, também levanta questões importantes relacionadas à privacidade e à segurança. A integração de câmeras IP em redes domésticas e corporativas aumenta significativamente a superfície de ataque disponível para cibercriminosos. Esses dispositivos, muitas vezes configurados de maneira inadequada ou com senhas padrão, tornam-se vulneráveis a invasões, permitindo que *hackers* acessem imagens em tempo real e até mesmo controlem os dispositivos remotamente (Menezes, 2017).

Felman (2023) apresenta uma visão abrangente sobre o crescimento exponencial da Internet das Coisas e destaca como a expansão desses dispositivos amplifica os desafios de segurança. Com a previsão de que bilhões de dispositivos estarão conectados nos próximos anos, a segurança da IoT torna-se uma preocupação central, especialmente em relação às câmeras IP. Segundo o mesmo autor, a diversidade de dispositivos e a falta de padrões de segurança unificados aumentam o risco de ataques cibernéticos.

Além disso, a vulnerabilidade das câmeras IP é frequentemente exacerbada por limitações de *hardware*, descontinuidade de suporte e a falta de atualizações de *software*. Esses fatores são explorados por atacantes para comprometer a integridade e a confidencialidade dos dados. A falta de conscientização entre os usuários sobre a importância de configurar corretamente esses dispositivos agrava ainda mais a situação, deixando uma vasta quantidade de câmeras expostas na internet (Brochado, 2023).

De acordo com dados do mecanismo de pesquisa de IoT, mais de 124 mil câmeras de segurança conectadas à internet estão atualmente acessíveis a terceiros em todo o mundo. Isso inclui câmeras de segurança industrial, que expõem imagens de usinas de energia, instalações industriais e outros ambientes sensíveis, bem como dispositivos domésticos inteligentes, comprometendo a privacidade individual e coletiva (Brochado, 2023).

Nick Viney, vice-presidente sênior da Avast Partner, alerta que a grande maioria dos dispositivos domésticos inteligentes vulneráveis está em risco devido a credenciais de segurança fracas. Viney sublinha que essa falha é evitável e que tanto empresas quanto usuários devem adotar práticas de segurança mais rigorosas, como a implementação de autenticação multifatorial e a utilização de senhas robustas, para proteger dados sensíveis e prevenir invasões (Viney, 2023).

A Tabela 1 apresenta a quantidade de câmeras conectadas à Internet por país que estão abertas e acessíveis a terceiros, conforme levantamento de dados originais da Shodan.io, apresentado em uma postagem no site CISO *Advisor*.

Tabela 1 - Levantamento de câmeras de vigilância invadidas

1	Vietnã	VN	14.967
2	Taiwan	TW	12.169
3	Coreia do Sul	KR	10.519
4	Estados Unidos	US	9.366
5	Rússia	RU	6.374

6	Japão	JP	5.077
7	China	CN	5.055
8	Brasil	BR	4.963
9	Alemanha	DE	4.075
10	Tailândia	TH	4.063

Fonte: INVASÃO a 150 mil câmeras de vigilância acende alerta para dispositivos IoT. CISO Advisor, 25 mar. 2021. Disponível em: https://www.cisoadvisor.com.br/invasao-a-150-mil-cameras-de-vigilancia-acende-alerta-para-dispositivos-iot/. Acesso em: 26 ago. 2024. Dados originais coletados pela Shodan.io.

Portanto, a literatura revisada aponta para uma necessidade urgente de medidas regulatórias e técnicas que garantam a segurança dos sistemas de vídeo-monitoramento e demais dispositivos IoT. A regulamentação do uso dessas tecnologias, juntamente com a implementação de melhores práticas de segurança, é fundamental para mitigar os riscos associados à crescente conectividade desses dispositivos.

4 METODOLOGIA

Este estudo adotou uma abordagem de pesquisa mista, combinando métodos qualitativos e quantitativos para explorar as vulnerabilidades de segurança em dispositivos IoT, com ênfase em câmeras IP, e identificar as melhores práticas para mitigar esses riscos. A integração dessas abordagens permite uma análise mais abrangente e detalhada, proporcionando uma compreensão mais profunda dos fenômenos estudados.

4.1 Abordagem Qualitativa

A etapa qualitativa da pesquisa foi conduzida por meio de uma revisão bibliográfica aprofundada. Realizou-se a busca por termos como "segurança em dispositivos IoT", "câmeras IP", "vulnerabilidades em sistemas de vigilância" e "ataques cibernéticos" em bases de dados acadêmicas renomadas, como Google Scholar e Scielo, com o intuito de coletar artigos científicos, relatórios técnicos e teses que oferecessem informações detalhadas sobre o estado da segurança em câmeras IP.

Os critérios de seleção das fontes incluíram a atualidade das publicações, priorizando materiais dos últimos cinco anos, a relevância dos autores no campo da segurança cibernética e a aplicabilidade dos estudos ao contexto específico das câmeras IP. Além das fontes acadêmicas, analisaram-se relatórios de segurança e notícias de sites confiáveis, como *Krebs on Security*, *Security Leaders* e o mecanismo de busca de dispositivos *IoT*, para complementar a pesquisa com casos reais e dados práticos sobre ameaças e vulnerabilidades.

4.2 Abordagem Quantitativa

Na abordagem quantitativa, realizou-se a análise de dados empíricos coletados de bases como Shodan.io, que fornece informações detalhadas sobre a exposição de dispositivos IoT, incluindo câmeras IP, na internet. Coletaram-se e analisaram-se dados relativos ao número de câmeras IP conectadas à internet e vulneráveis a acessos não autorizados, segmentados por países. Este levantamento permitiu uma análise estatística das tendências de exposição e vulnerabilidade, facilitando a identificação de padrões globais e regionais.

Organizaram-se os dados quantitativos em tabelas e gráficos, proporcionando uma visualização clara das informações coletadas. A análise estatística desses dados incluiu

cálculos de frequências, médias e distribuições, visando identificar correlações e tendências significativas no que diz respeito à segurança de câmeras IP.

4.3 Integração dos Métodos

A combinação dos métodos qualitativos e quantitativos permite a triangulação dos dados, onde os resultados qualitativos oferecem contexto e profundidade para a interpretação dos dados quantitativos. Essa integração metodológica fortalece as conclusões do estudo, proporcionando uma compreensão das vulnerabilidades e das melhores práticas de segurança em dispositivos IoT.

5 RESULTADOS E DISCUSSÃO

A pesquisa realizada por meio do formulário aplicado a usuários de câmeras IP teve como objetivo compreender o nível de conhecimento sobre segurança cibernética, práticas adotadas e vulnerabilidades percebidas nesses dispositivos. A seguir, são apresentados os principais achados do estudo.

5.1 Perfis dos Usuários

A amostra da pesquisa contou com 50 respostas, abrangendo diversas faixas etárias, incluindo 18 anos ou menos, 18-24 anos, 25-34 anos, 35-44 anos e 44 ou mais. A maioria dos respondentes afirmou utilizar câmeras IP para segurança residencial ou monitoramento, como de parentes necessitados ou animais, enquanto alguns mencionaram não utilizá-las ou não possuí-las. Todos os 49 respondentes consideram a segurança das informações coletadas pelas câmeras um aspecto importante, embora nem todos adotem medidas adequadas de proteção.

5.2 Níveis de Conhecimento sobre Segurança

Ao analisar o nível de conhecimento dos usuários, constatou-se que 16,7% não estão cientes das vulnerabilidades comuns em câmeras, como acesso não autorizado ou exposição de dados. Enquanto isso, 47,9% possuem algum conhecimento sobre o assunto e 35,4% se consideram bem informados. Quanto às práticas básicas de segurança digital, 60% dos participantes afirmaram estar familiarizados, 28% não se consideram familiarizados e 12% têm conhecimento limitado.

5.3 Práticas de Segurança Adotadas

Em relação às práticas de segurança adotadas, apenas 45,8% alteraram a senha padrão da câmera após a instalação, enquanto 25% não o fizeram e 29,2% não sabem ou não se lembram. Sobre atualizações, 22,9% realizam-nas regularmente a cada poucos meses, 29,2% ocasionalmente uma vez por ano, 18,8% raramente menos de uma vez por ano e 29,2% nunca atualizam. Quanto a medidas adicionais de segurança, apenas 18,8% utilizam recursos como firewall, enquanto 75% não as adotam e 6,2% não sabem.

5.4 Vulnerabilidades Percebidas

No que diz respeito às vulnerabilidades percebidas, 16,7% dos usuários relataram já ter tido algum incidente de segurança, como acesso não autorizado ou vazamento de imagens, enquanto 81,3% não tiveram e 2% não sabem. Sobre a percepção de risco, 29,2% consideram o risco alto, 18,8% médio, 16,7% baixo e 35,4% não sabem avaliar. Quando questionados

sobre sua preparação para incidentes, 57,1% sabem exatamente o que fazer se a segurança da câmera for comprometida, 8,2% têm uma ideia geral e 34,7% não sabem como agir.

5.5 Impactos das Vulnerabilidades nas Câmeras IP

Os dados coletados evidenciam que a falta de segurança nas câmeras IP pode resultar em diversos impactos negativos para os usuários. Entre as principais consequências estão a invasão de privacidade, o roubo de informações sensíveis e até mesmo o uso desses dispositivos como pontos de entrada para ataques mais complexos.

A preocupação dos usuários com acessos não autorizados foi um dos pontos mais mencionados na pesquisa, indicando que a percepção de risco existe, mas nem sempre é acompanhada da adoção de medidas preventivas. Além disso, ataques a dispositivos IoT, como as câmeras IP, podem permitir que hackers utilizem esses equipamentos para realizar ataques em larga escala, como os ataques de negação de serviço distribuído (DDoS).

Portanto, reforçar práticas de segurança e conscientizar os usuários sobre a importância de configurações adequadas é fundamental para minimizar esses riscos e garantir uma utilização mais segura das câmeras IP.

6 CONCLUSÃO

O estudo evidenciou que, apesar da popularização das câmeras IP, ainda há um grande desconhecimento sobre os riscos de segurança associados a esses dispositivos. Muitos usuários mantêm configurações padrão e não adotam medidas essenciais, como atualização de firmware e autenticação multifator, o que os torna alvos fáceis para ataques cibernéticos.

A pesquisa também revelou que a percepção de segurança dos usuários contrasta com a realidade técnica, pois, embora considerem suas câmeras confiáveis, a falta de boas práticas aumenta significativamente a vulnerabilidade desses dispositivos. Dessa forma, campanhas de conscientização e a implementação de regulamentações mais rígidas são fundamentais para mitigar esses riscos.

Assegurar a privacidade e a segurança dos usuários de câmeras IP demanda uma abordagem integrada entre fabricantes, usuários e órgãos reguladores. Os fabricantes devem investir em soluções mais seguras, como a implementação obrigatória de senhas robustas e atualizações automáticas. Os usuários, por sua vez, precisam adotar práticas mais seguras, como a troca regular de senhas, atualização do firmware e segmentação de redes. Além disso, iniciativas educacionais e normativas que padronizem diretrizes de segurança podem contribuir significativamente para a redução das vulnerabilidades.

Por fim, é imprescindível que novas pesquisas aprofundem a compreensão sobre ameaças emergentes e soluções eficazes para mitigar riscos. A evolução tecnológica dos dispositivos *IoT* deve ser acompanhada por um constante aprimoramento das medidas de segurança, garantindo que os usuários possam usufruir dos benefícios das câmeras IP sem comprometer sua privacidade e proteção digital.

7 REFERÊNCIAS

BONILLA, Maria Helena; PRETTO, Nelson. Movimentos colaborativos, tecnologias digitais e educação. *Em Aberto*, v. 28, n. 94, p. 23-40, 2015. Disponível em: https://www.researchgate.net/profile/Jain-3/publication/327052389_An_Analytical_Study_on_the_Effects_of_WTO_on_India's_Foreign_Trade_performance/links/5b754e6fa6fdcc87df809ca9/An-Analytical-Study-on-the-Effects-of-WTO-on-Indias-Foreign-Trade-performance.pdf#page=5. Acesso em: 27 ago. 2024.

BROCHADO, Luis Armando da Silva et al. Segurança de dispositivos IoT: análise de vulnerabilidades de uma câmera IP. 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/253380. Acesso em: 27 ago. 2024.

CISO ADVISOR. Invasão a 150 mil câmeras de vigilância aciona alerta para dispositivos IoT. 25 mar. 2021. Disponível em: https://www.cisoadvisor.com.br/invasao-a-150-mil-cameras-de-vigilancia-acende-alerta-para-dispositivos-iot/. Acesso em: 21 ago. 2024.

DA SILVA, Michel Bernardo Fernandes. Cibersegurança: visão panorâmica sobre a segurança da informação na internet. Rio de Janeiro: Freitas Bastos, 2023. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=5MCnEAAAQBAJ&oi=fnd&pg=PT148&dq=No+Brasil,+um+dos+pa%C3%ADses+mais+afetados+por+essa+Botnet,+c%C3%A2meras+de+seguran%C3%A7a+IP,+gravadores+digitais+de+v%C3%ADdeo+(DVRs)+e+outros+dispositivos+conectados+foram+amplamente+comprometidos,+resultando+em+invas%C3%B5es+e+vazamentos+de+dados+sens%C3%ADveis+&ots=2gbmpCy-5V&sig=sdcRerXDFUl9bm3zAd4MVv8io28#v=onepage&q&f=false. Acesso em: 28 ago. 2024.

FELMAN, Marcelo. Cyber Signals: oportunidades e riscos relacionados à IoT. 2023. Disponível em: https://securityleaders.com.br/cyber-signals-oportunidades-e-riscos-relacionados-a-iot/. Acesso em: 20 ago. 2024.

GRINBERG, Felipe. Prisões por reconhecimento facial avançam pelo país, mas erros em série desafiam tecnologia de combate ao crime. 2024. Disponível em: https://oglobo.globo.com/brasil/noticia/2024/01/05/prisoes-por-reconhecimento-facial-avancam-pelo-pais-mas-erros-em-serie-desafiam-tecnologia-de-combate-ao-crime.ghtml. Acesso em: 21 ago. 2024.

KREBS, Brian. Hacked cameras, DVRs powered today's massive Internet outage. 2016. Disponível em: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. Acesso em: 21 ago. 2024.

MAGRANI, Eduardo. A internet das coisas. 1. ed. Rio de Janeiro: Editora FGV, 2018. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=qYtlDwAAQBAJ&oi=fnd&pg=PA1&dq=acesso+remoto+e+a+integra%C3%A7%C3%A3o+com+outros+dispositi-vos+da+Internet+das+Coisas+(IoT),+facilidade+de+instala%C3%A7%C3%A3o,+muitas+vezes+sem+configura%C3%A7%C3%B5es+de+seguran%C3%A7a&ots=rhSoAvje44&sig=vY6f67JdNotmBcBMEKvujdHt95g#v=onepage&q&f=false. Acesso em: 27 ago. 2024.

SECURITY LEADERS. Câmeras de segurança são usadas para espalhar ataques virtuais. 2017. Disponível em: https://securityleaders.com.br/cameras-de-seguranca-sao-usadas-para-espalhar-ataques-virtuais/. Acesso em: 20 ago. 2024.