INTERFACE TECNOLÓGICA

ANÁLISE DE SEGURANÇA EM DISPOSITIVOS INTERNET DAS COISAS

SECURITY ANALYSIS OF INTERNET OF THINGS DEVICES

Thiago Martiusi Moura – thiagomartiusi@yahoo.com.br
Faculdade de Tecnologia de Americana – Americana – São Paulo – Brasil

João Emmanuel D' Alkmin Neves – professoralkmin@gmail.com
Faculdade de Tecnologia de Americana – Americana – São Paulo – Brasil

DOI: 10.31510/infa.v18i2.1174
Data de submissão: 14/07/2021
Data do aceite: 03/11/2021
Data da publicação: 30/12/2021

RESUMO

Dispositivos baseados em internet das coisas atualmente encontram-se disseminados nos diferentes ambientes, sejam domésticos, corporativos ou mesmo ao ar livre. Tais equipamentos realizam conexões com suas respectivas redes e com a internet, permitindo o compartilhamento de informações com usuários, com servidores online e com outros dispositivos inteligentes. Embora hoje existam diversos protocolos e serviços de segurança disponíveis para dispositivos computacionais de propósito geral como computadores pessoais, outros dispositivos de propósito mais específico ainda carecem de melhores soluções de segurança. Nesse contexto, o presente trabalho objetiva identificar as principais vulnerabilidades de segurança em dispositivos inteligentes, pesquisar o comportamento dos usuários desses dispositivos a partir de formulário de coleta anônima sem fins lucrativos para pesquisa descritiva e analisar os recursos de segurança disponíveis em diferentes equipamentos inteligentes, promovendo uma verificação de vulnerabilidades físicas nos aparelhos analisados. Ao final faz-se ponderações entre os padrões de segurança adotados em aparelhos inteligentes em comparação com os padrões empregados em indústrias tradicionais, cujos produtos encontram-se há mais tempo no mercado e com protocolos de segurança bem estabelecidos.

Palavras-chave: Internet das Coisas. Segurança. Vulnerabilidades.

ABSTRACT

Internet of Things devices are now disseminated in different places, whether domestic, corporate, or even outdoors. Those devices can connect with their respective networks and with the internet and sharing information with users, online servers and others smart devices in this process. Although there are now several security protocols and services for general purpose computing devices such as personal computers, others more specific purpose devices still need better security solutions. In this scenario, this work aims to identify the main security vulnerabilities in smart devices, research the behavior of user of these devices through an anonymous non-profit collection form for descriptive research and analyze the security features available in different smart devices, promoting a verification of physical vulnerabilities in the

analyzed devices. At the end, considerations are made between the safety standards adopted in smart appliances in comparison with the standards used in traditional industries, whose products have been on the market longer and with well-established safety protocols.

Keywords: Internet of Things. Security. Vulnerabilities.

1 INTRODUÇÃO

As facilidades trazidas por dispositivos baseados no conceito de Internet das Coisas, também conhecida por seu nome e sigla em inglês, *Internet of Things* (IoT) vão desde dispositivos vestíveis como *smartbands* e *smartwatches*, capazes de monitorar sinais vitais do usuário em tempo real ao mesmo tempo em que desempenham funções antes relegadas aos relógios e celulares, até *smartTVs* que transformaram um dispositivo que antes era exclusivamente receptivo de sinais analógicos, operando passivamente, em um aparelho dinâmico, capaz de oferecer uma variedade de conteúdos ilimitada, bastando uma conexão à internet, muitas vezes explorando conteúdos alocados em nuvem, sem exigir grande consumo de recursos de hardware.

Os objetos inteligentes, contudo, também necessitam zelar para que o armazenamento, processamento e a transmissão de informações extraídas dos dados coletados ocorram de modo seguro, sem colocar em risco outros dispositivos conectados. Nesse contexto, a inovação alcançada na esteira das facilidades oportunizadas pelos equipamentos inteligentes nem sempre vem acompanhada das cautelas e garantias exigíveis para aparelhos que estão inseridos em redes com diversos outros dispositivos conectados, compartilhando recursos e informações. As hipóteses para a problemática apresentada compreendem o comportamento do usuário quanto à segurança da informação, a possibilidade de utilização de solução antivírus e a possibilidade de alteração de configurações pré-definidas com vistas a mitigar vulnerabilidades passíveis de exploração. Este trabalho objetiva abordar os aspectos relacionados à segurança nas operações de dispositivos IoT, tendo em vista que, diferente dos computadores tradicionais com boas práticas de segurança já consolidadas, a introdução de novos equipamentos levanta novos desafios a serem considerados para a boa interoperacionalidade entre todos os diferentes dispositivos integrados.

As abordagens apresentadas partem da identificação dos principais riscos inerentes aos dispositivos IoT para apresentar soluções que possibilitem aos usuários elevar os padrões de

segurança, bem como permitam aos consumidores estabelecer critérios a serem considerados ao se adquirir novos equipamentos, oportunizando distinguir as melhores soluções quanto à segurança da informação em meio a grande variedade de objetos inteligentes disponíveis no mercado.

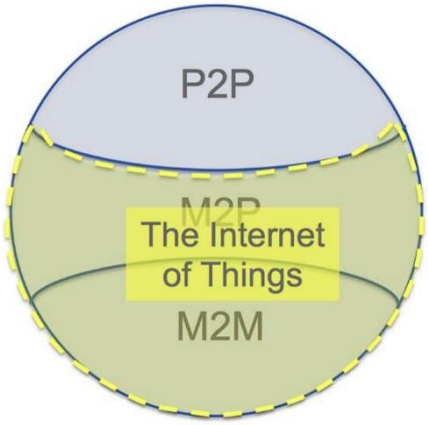
2 FUNDAMENTAÇÃO TEÓRICA

2.1 A Internet das Coisas

Embora os dispositivos IoT tenham se tornado uma realidade somente nos últimos anos, seu conceito vem de mais tempo. Em 1991 Bill Joy, cofundador da Sun Microsystems, pensou sobre a conexão de Dispositivo para Dispositivo - *Device to Device* (D2D), Magrani (2018). Em 1999, Kevin Ashton do *Massachussetts Institute of Technology* (MIT) propôs o termo "Internet das Coisas" e dez anos depois escreveu o artigo "A Coisa da Internet das Coisas" para o RFID Journal (ASHTON, 2009).

O conceito de IoT prevê a capacidade de conexão entre dispositivos sem necessariamente usar um roteador como intermediário. Dentre as tecnologias empregadas para essa comunicação D2D estão *Bluetooth* e *Wi-fi Direct*. Grande parte dos dispositivos IoT, contudo, utilizam de redes convencionais centralizadas por roteadores e, muitas vezes, utilizada para conectar diversos dispositivos distintos numa mesma rede local.

Imagem 1 – Área de operação de dispositivos IoT



Fonte: International Telecommunication Union (2017)

A imagem 1 exibe o campo de atuação de dispositivos IOT. Na imagem os dispositivos estão inseridos dentro das conexões *Machine-to-Person* (M2P) e *Machine-to-Machine* (M2M).

2.2 A segurança em dispositivos IoT

A segurança da informação surgiu a partir das primeiras vulnerabilidades exploradas em computadores. Nesse âmbito diversos recursos, protocolos e procedimentos foram implementados como a navegação pela internet segura por HTTPS, a utilização de *firewall* e soluções antivírus e a implementação de criptografia para transmissão de informações sensíveis. Os computadores pessoais atualmente apresentam diversas soluções de segurança disponíveis, algumas dessas inclusive são instaladas juntamente com o sistema operacional como firewall e solução antivírus. Outros dispositivos inteligentes como *smartphones*, *smartTVs* e *smartwatches* são conectados em redes domésticas nem sempre com os mesmos cuidados de segurança que ceram os computadores integrantes da mesma rede. Observa-se que os recursos e soluções de segurança da informação em geral são desenvolvidos de modo reativo.

Programas maliciosos, comumente referenciados como malwares, são descritos por Melo et al. (2011) como programas inseridos em um sistema, normalmente de forma encoberta, com objetivo de comprometer a integridade, confidencialidade ou disponibilidade de informações, de aplicativos ou do sistema operacional.

Para analisar a segurança nas operações de dispositivos IOT é necessário identificar os riscos associados a esses equipamentos. Nessa senda, pode-se segmentar esses riscos em duas tipologias distintas, conforme apresentado nos quadros a seguir.

Quadro 1 – Principais vulnerabilidades físicas

Vulnerabilidade Física	Principais riscos associados
Conexões físicas	Reprodução automática de conteúdo (exemplo: entrada USB)
Informações impressas	Presença de dados de conexão e informações de permissões de acesso (exemplo: nome de usuário e senha escritos próximos ao dispositivo)

Fonte: os autores (2021)

As vulnerabilidades físicas, conforme demonstrado no quadro 1, podem decorrer das configurações do dispositivo, caso das conexões físicas, nas quais softwares mal-intencionados podem se aproveitar da característica de reproduzir automaticamente conteúdos ao ser conectado um novo dispositivo por uma conexão física, como ocorre, por exemplo, com a conexão de um dispositivo de armazenamento em uma porta do padrão *Universal Serial Bus* (USB). Também podem ocorrer a partir de um comportamento inseguro do usuário como, por

exemplo, manter uma anotação próxima ao equipamento com o nome de usuário e senha de acesso para autenticação.

Quadro 2 – Principais vulnerabilidades lógicas

Vulnerabilidade Lógica	Principais riscos associados
Usuário e senha padrão	Acesso indevido ao dispositivo
Ausência de *Firewall*	Ausência de filtro sobre as transmissões de dados, controle de portas e conexões e de bloqueio de potenciais ataques pela rede
Ausência de Antivírus	Não monitoramento e identificação de arquivos, páginas de rede e executáveis maliciosos ou suspeitos
Firmware desatualizado	Exploração de falhas de segurança existentes por ataques direcionados
Ausência de criptografia	Acesso a informações e dados sensíveis
Criptografia fraca	Ataques de força bruta para quebra da criptografia, ataques *man-in-the-middle*
Portas e serviços habilitados	Ataques *Ransomware,* acesso privilegiado a recursos restritos

Fonte: os autores (2021)

No caso de vulnerabilidades lógicas, quadro 2, existem diferentes abordagens para cada falha de segurança. Um atacante pode obter acesso de administrador de um equipamento ao realizar a autenticação com o nome de usuário e senha padrões que não foram alterados pelo usuário. O *Firewall* constitui de uma camada de segurança adicional, seja a nível de hardware ou de software, encarregada de controlar e restringir o acesso às portas de conexão de rede abertas, possibilita a restrição e a filtragem do tráfego de rede e o bloqueio de ataques de rede em potencial. No caso de *Firmware* desatualizado, uma boa prática consiste em manter uma rotina de verificação periódica de atualizações disponibilizadas pelos fabricantes, evitando-se manter um equipamento desatualizado em serviço. A criptografia possibilita manter a segurança das informações armazenas, bem como daquelas transmitidas pela rede. Caso o protocolo de criptografia adotado esteja obsoleto, um ataque de força bruta pode ser empregado para quebrar a segurança, valendo-se de equipamentos com elevado poder computacional para testar todas as chaves possíveis e obter o acesso não autorizado.

Dentre os protocolos de criptografia disponíveis, é comum aos dispositivos com comunicação via redes sem fio o *Wired Equivalent Protocol* (WEP). Trata-se de protocolo que se encontra defasado, apresentando vulnerabilidades que comprometem sua utilização.

De acordo com Vilela (2014, p. 40), dentre as vulnerabilidades presentes no protocolo WEP está: “tamanho da chave – o WEP é passível a ataques de força bruta utilizando o método de dicionário, devido ao tamanho reduzido da chave compartilhada”

Outra abordagem possível a partir da ausência de criptografia ou do uso de uma criptografia obsoleta é o ataque *man-in-the-middle* (MITM) no qual o invasor monitora a comunicação pela rede em busca de informações relevantes.

Caso o dispositivo mantenha portas de conexões abertas sem utilizá-las ou habilite serviços e conexões que permitam acessar recursos sensíveis do equipamento, como por exemplo manter o modo de depuração de um dispositivo ativado, diversas ameaças podem aproveitar as opções que se apresentam a partir dessas configurações para a realização de ataques. A identificação de portas abertas a partir de scanners de redes possibilitam a invasão de dispositivos para ataques de *ransomwares,* bloqueando o acesso ao equipamento e aos dados armazenados ao passo em que se exige um pagamento pela promessa de liberação dos aparelhos infectados.

A fundação *Open Web Application Security Project* (OWASP *Foundation*) elencou as dez principais vulnerabilidades em dispositivos IoT em 2018, conforme se apresenta no quadro 3 a seguir:

Quadro 3 – Principais vulnerabilidades em dispositivos IoT

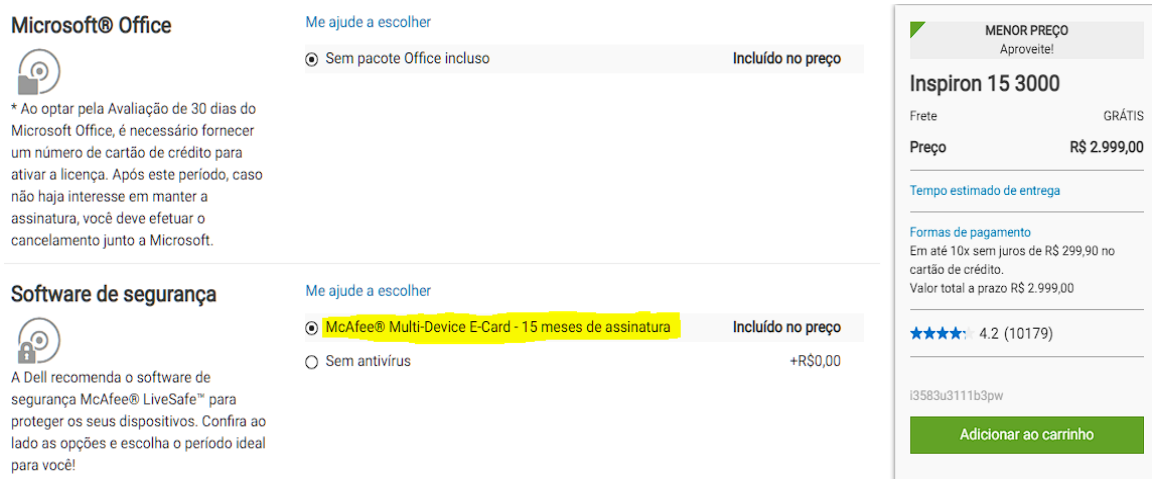
1	Senhas fracas
2	Serviços de redes inseguros
3	Interfaces inseguras
4	Ausência de mecanismos de atualizações seguros
5	Uso de componentes desatualizados
6	Proteção de privacidade insuficientes
7	Transferência e armazenamento de dados inseguros
8	Falta de gerenciamento de dispositivos
9	Configurações padrão inseguras
10	Falta de fortalecimento físico

Fonte: Elaborado pelos autores, baseado em OWASP (2018)

Embora vários fatores afetem a segurança dos dispositivos conectados a uma rede como o perfil de uso do(s) usuário(s) dos equipamentos, os computadores de propósito geral apresentam recursos e soluções de segurança embarcados que nem sempre acompanham dispositivos IoT. Para um consumidor que adquire um computador montado, pronto para uso, é comum o equipamento vir da loja com sistema operacional com soluções de segurança pré-

instalados como software firewall e antivírus. Tal política de segurança, contudo, ainda não é comum nos equipamentos IoT.

Imagem 2 - Site de compra com oferta de notebook com antivírus pré-instalado



Fonte: Loja Dell (2021)

A despeito da menor variedade de opções de softwares de segurança disponíveis para dispositivos IoT, já comum aos computadores pessoais como demonstrado na imagem 2, um fator preponderante para o surgimento de vulnerabilidades advém da dificuldade de compreensão do usuário ao adquirir e manter esses equipamentos. Nem sempre o usuário percebe que ao utilizar um aparelho sem os devidos cuidados com a segurança ele acaba por colocar em risco toda a rede da qual o dispositivo está inserido.

2.3 Pesquisa sobre adoção de solução antivírus

Uma pesquisa sobre a adoção de solução antivírus em diferentes dispositivos foi realizada entre os discentes do curso de Análise e Desenvolvimento de Sistemas da FATEC – Americana. A coleta ocorreu por meio de questionário online na plataforma Google Forms com preenchimento anônimo e sem fins lucrativos e foi realizada entre os dias 13 e 14 de abril de 2021 com um total de 43 participantes, apresentando os seguintes resultados:

Tabela 1 – Utilização de antivírus em dispositivos inteligentes.

Resposta	Você usa antivírus em seu computador pessoal (*notebook*/PC)?	Você usa antivírus em seu *smartphone*?	Você usa antivírus em sua *smartTV*?
Sim	21	6	0

Não	19	36	39
Ambos	3	1	1
Não possui	0	0	3
TOTAL	**43**	**43**	**43**

Fonte: os autores (2021)

A tabela 1 apresenta os resultados obtidos nos três questionários que compõem a pesquisa. Para o primeiro questionário o participante informa se adota *software* antivírus em seu computador pessoal, *personal computer* (PC) ou notebook. No segundo questionário os participantes respondem sobre a adoção da referida solução em seu *smartphone*. No último questionário é perguntado sobre a utilização do antivírus em sua *smartTV*. As respostas disponíveis para serem selecionadas contemplam, além da confirmação (sim) e da negativa (não), a opção de possuir dispositivos com e sem antivírus (ambos) e uma opção caso o participante não possua um dispositivo daquela categoria (Não possui), promovendo-se os devidos esclarecimentos no formulário para eventuais dúvidas quanto ao preenchimento.

2.4 Estudo de vulnerabilidades físicas

Um estudo prático sobre vulnerabilidade física em *smartTVs* foi realizado com três modelos distintos, SONY KD-49X755F, SEMP L32S3900S e SAMSUNG UN40JU6700, com vistas a observar o comportamento e as opções disponíveis para reprodução automática de conteúdo conectado via porta USB. Nessa apuração primeiramente foi observado o comportamento dos dispositivos em suas configurações padrão sem a presença de antivírus ao conectar um *pendrive* com mídias. A próxima verificação objetiva observar o comportamento do equipamento após a instalação de software antivírus, refazendo-se a conexão física. Por fim buscou-se identificar opções de reprodução de conteúdo automático nas configurações dos dispositivos.

Na primeira conexão todos os aparelhos apresentaram a reprodução automática de conteúdo. Para a segunda verificação apenas o dispositivo SONY possui opção de uso de antivírus, neste caso utilizou-se solução gratuita da ESET. Neste teste houve uma verificação rápida pelo antivírus no dispositivo conectado antes de exibir a reprodução automática. Por fim ao se verificar opções de reprodução, apenas no modelo SONY foi encontrada opção de desativação de reprodução automática de conteúdo via USB.

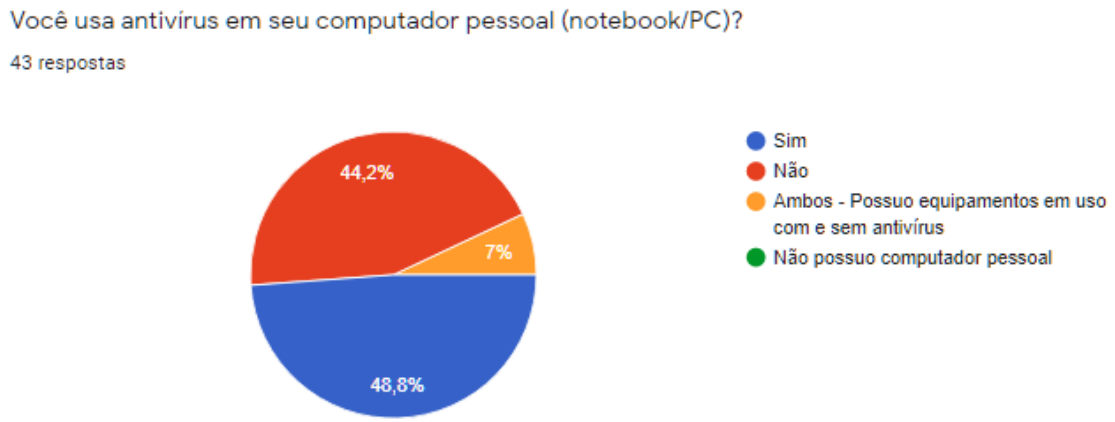
3 PROCEDIMENTOS METODOLÓGICOS

A pesquisa realizada possui uma abordagem quali-quantitativa, partindo de uma coleta realizada a partir de uma amostra entre os discentes do curso de Análise e Desenvolvimento de Sistemas da FATEC – Americana, com a elaboração de métricas dos dados coletados sob gráficos comparativos e a realização de análise a partir das características dos diferentes objetos em estudo. A coleta ocorre por meio de questionário online de preenchimento anônimo sem fins lucrativos para a pesquisa descritiva, possibilitando analisar as relações existentes entre as variáveis dos objetos em estudo. A pesquisa parte da revisão bibliográfica para a realização de levantamento com método comparativo, objetivando compreender as características observadas entre os objetos de estudo.

4 RESULTADOS E DISCUSSÃO

A pesquisa realizada visou obter dados acerca da adoção de sistema antivírus em diferentes dispositivos com acesso à internet. A coleta utilizou a plataforma Google Forms. Os resultados apresentados a seguir estão formatados em gráfico de pizza elaborado dentro da plataforma utilizada.

Gráfico 1 – Utilização de antivírus em computador pessoal.

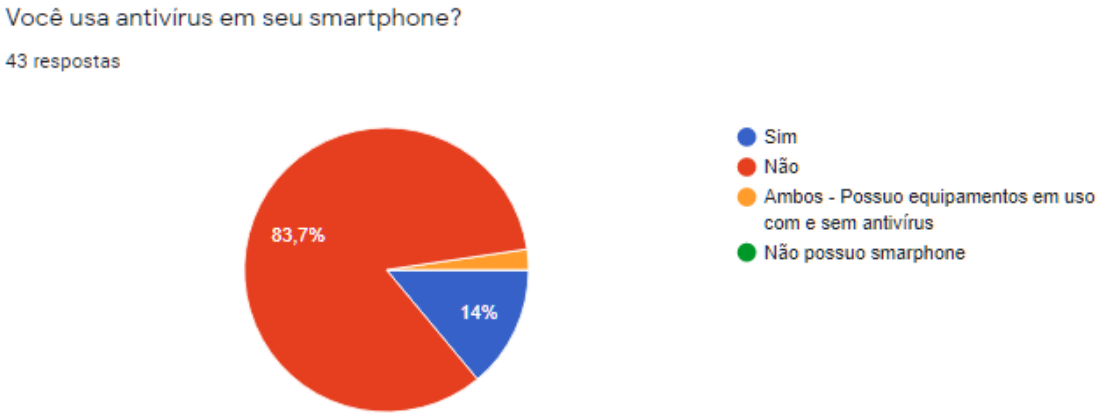


Fonte: os autores (2021)

No questionário sobre a utilização de *software* antivírus em computador 55,8% dos participantes informaram adotar alguma solução ainda que parcialmente, sendo que 48,8% preencheram que adotam e 7% informaram que possuem equipamentos em uso com e sem

solução antivírus. Para este equipamento 44,2% dos participantes informaram que não usam antivírus.

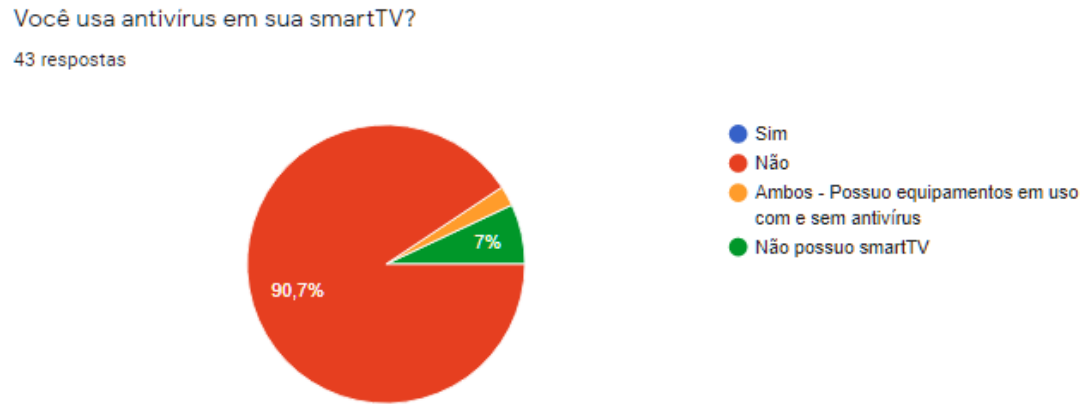
Gráfico 2 - Utilização de antivírus em smartphones.



Fonte: os autores (2021)

Quanto à utilização de antivírus em *smartphones* apenas 16,3% informaram que utilizam, sendo que 14% preencheram que usam antivírus e 2,3% informaram que possuem equipamentos com e sem antivírus. O quantitativo de pessoas que informaram não utilizar antivírus aumentou para 83,7%.

Gráfico 3 - Utilização de antivírus em *smartTV*



Fonte: os autores (2021)

A pesquisa também levantou informações sobre a utilização de antivírus em *smartTVs.* Neste dispositivo somente 2,3% informaram possuir equipamentos com e sem a solução de segurança e nenhum participante indicou possuir a solução em todos os dispositivos. A quantidade de pessoas que informaram não utilizar referido software foi de 90,7% e 7% responderam que não possuem *smartTV*.

A análise dos resultados obtidos a partir de uma pesquisa realizada com público que possui familiaridade com recursos tecnológicos e conhecimento acima da média acerca de vulnerabilidades em segurança da informação demostra que a adoção de software antivírus é maior em dispositivos computacionais tradicionais como computadores pessoais e se reduz para dispositivos inteligentes de vanguarda. Ao se comparar os resultados apresentados para computadores pessoais e *smartTVs* constata-se que o percentual dos que não adotam mencionada solução é pouco acima do dobro no último dispositivo. Um dos motivos para esse percentual elevado consiste no fato de que muitas *smartTVs* não possuem nenhuma solução antivírus disponível em suas lojas de aplicativos. Uma solução encontrada para esse nicho é o software antivírus da ESET disponível gratuitamente para *smartTVs* com sistema operacional androidTV.

Os *smartphones,* por outro lado, possuem grande variedade de softwares antivírus disponíveis nas principais lojas de aplicativos, como o Avast Free Antivírus disponível gratuitamente para *smartphones* com sistema operacional android. A despeito dessa disponibilidade, a quantidade de participantes que informaram não adotar nenhuma solução nestes dispositivos foi de 83,7%, patamar muito superior aos 44,2% dos computadores pessoais. Tal comparativo permite concluir que existe uma parcela de usuários que adotam antivírus somente em computadores, embora *smartphones e smartTVs* também são usualmente conectados nas mesmas redes dos primeiros. Ademais está cada vez mais comum a realização de compras e transações financeiras diretamente de *smartphones,* já existindo opções inclusive para *smartTVs* e videogames modernos.

5 CONSIDERAÇÕES FINAIS

Ao analisar a segurança em dispositivos IoT verifica-se que existem várias frentes que podem ser objeto de exploração, abrindo caminho para violação de informações a partir dos pontos frágeis encontrados em uma rede. A adoção de procedimentos de segurança não garante a inviolabilidade do sistema de informação, mas fortalece toda a rede, mitigando riscos. Um raciocínio válido para a adoção de procedimentos seguros consiste em comparar esses recursos com os sistemas de segurança embarcados nos veículos, como sistemas de frenagem com tecnologia *Anti-lock Braking System* (ABS) e *Airbags*, um motorista que adota uma condução segura não espera ter de utilizar tais recursos, porém caso em algum momento necessite,

referidas soluções poderão salvaguardar a vida de todos os ocupantes. Nessa linha de raciocínio a indústria automobilística não deixa de lançar novos dispositivos de segurança a cada ano, ainda que os veículos já sejam seguros, essa mesma política pode ser adotada à segurança da informação, sempre buscando novos procedimentos que permitam a confiabilidade de toda a rede. Além dos cuidados individuais um trabalho coletivo pode ser desempenhado pelos órgãos públicos reguladores do sistema como a Agência Nacional de Telecomunicações (ANATEL) para, na esteira da Lei Geral de Proteção de Dados, lei nº 13.709/2018, estabelecer protocolos obrigatórios de segurança para comercialização de dispositivos IoT em território nacional, mantendo-se as normativas em constante atualização.

REFERÊNCIAS

ASHTON, Kevin. **That "Internet of Things" Thing**. RFiD Journal. 22, 97-114, 22 de junho de 2009.

CERT. 2018. **Cartilha de Segurança para Internet**. Disponível em: https://cartilha.cert.br/. Acessado em 28 de março de 2021.

DE MELO, Laerte Peotta, Amaral, D. M., Sakakibara, F., de Almeida, A. R., de Sousa Junior, R. T., & Nascimento, A. (2011). **Análise de Malware: Investigação de Códigos Maliciosos Através de uma Abordagem Prática**. Minicursos do XI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg).

DELL. Disponível em: https://deals.dell.com/pt-br/productdetail/7hox, acessado em 12/04/2021

FILHO, Fernandes, D. S., Afonso, V. M., Martins, V. F., Grégio, A. R. A., Geus, P. L., Jino, M., dos Santos, R. D. C. (2011). **Técnicas para Análise Dinâmica de Malware**. XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg).

MAGRANI, Eduardo. **A internet das coisas**. 1ª edição. Editora FGV, 2018. 192p.

NAÇÕES UNIDAS. International Telecommunication Union. Disponível em https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2017/Nov_IOT/NBTC–ITU-IoT/Session%201%20IntroIoTMZ-new%20template.pdf , acessado em 04/04/2021

OWASP. 2018. **OWASP top10 Internet of things**. Disponível em: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project. Acessado em 29 de março de 2021.

SHARMEEN, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). **Malware Threats and Detection for Industrial Mobile-IoT Networks**. IEEE access, v. 6, p. 15941-15957.

TORSTEN, George, Security Week, "**The Role of Artificial Intelligence in Cyber Security**," January 11, 2017. www.securityweek.com/role-artificial-intelligence-cyber-security, acessado em 22 de abril de 2021.

VILELA, Douglas W. F. L. **Segurança em Redes sem Fio**: Estudo sobre o desenvolvimento de conjuntos de dados para comparação de IDS. UNESP, 2014.