Segurança em Cenários de Internet das Coisas em Redes 5G: Desafios e Recomendações

Dalton C. G. Valadares, Newton C. Will, Álvaro A. C. C. Sobrinho, Anna C. D. de Lima, Igor S. de Morais, Pedro Graciliano, Danilo F. S. Santos

***Resumo*— Enquanto os trabalhos de especificação, pesquisa e desenvolvimento para as redes 6G já se iniciam, a implantação das redes 5G já é realidade em alguns países. Uma das novidades do 5G é o MMTC (Massive Machine-Type Communication), que permitirá até 1 milhão de dispositivos conectados transmitindo pequenas quantidades de dados a baixas taxas de transmissão. A limitação de recursos dos dispositivos IoT torna-os vulneráveis, pois mecanismos robustos de segurança frequentemente não podem ser implementados. Como um dispositivo vulnerável pode ser elo de acesso à infraestrutura 5G, em caso de ataque, este trabalho aborda desafios e recomendações de segurança neste contexto.**

***Palavras-Chave*— Segurança, IoT, Redes 5G.**

***Abstract*— While the specification, research, and development work for 6G networks have already begun, the deployment of 5G networks is already a reality in some countries. One of the novelties of 5G is the MMTC (Massive Machine-Type Communication), which will allow up to 1 million connected devices to transmit small amounts of data at low transmission rates. The resource constraints of IoT devices make them vulnerable, as robust security mechanisms often cannot be implemented. Once a vulnerable device can be a link to access the 5G infrastructure, in the event of an attack, this work addresses security challenges and recommendations in this context.**

***Keywords*— Security, IoT, 5G Networks.**

I. Introdução

As redes de comunicação de 5ª geração, 5G, já estão sendo implantadas em vários países. Melhoria na qualidade de serviço, latências baixas e alta confiabilidade são algumas das características do 5G [1], [2]. Os serviços serão disponibilizados nas redes 5G com base em três pilares tecnológicos: *enhanced mobile broadband* (eMBB), *ultra-reliable low latency communication* (URLLC) e *massive machine-type communication* (mMTC). O eMBB fornece elevada largura de banda com picos de 10 a 20 Gbps e um mínimo de 100 Mbps. O URLLC provê conexões altamente confiáveis e com baixíssima latência, alcançando 5 ms entre equipamento de usuário (*user equipment* - UE) e a estação base (eNB), transmitindo a médias taxas que variam entre 50 kbps e 10 Mbps. O mMTC suporta uma alta densidade de dispositivos conectados, podendo atingir um milhão de dispositivos por quilômetro quadrado se comunicando a baixas taxas que variam entre 1 e 100 kbps.

O mMTC do 5G possibitará a conexão massiva de dispositivos de Internet das Coisas (IdC) diretamente na infraestrutura. Segundo a *International Telecommunication Union* (ITU)[1], IdC é uma infraestrutura global que habilita serviços avançados pela conexão de coisas (físicas e virtuais) e é baseada em tecnologias de comunicação existentes e em evolução [3]. As coisas são objetos do mundo físico ou virtual que podem ser identificados e conectados a redes de comunicação. Dispositivo é qualquer equipamento com capacidade de comunicação que pode possuir capacidades de sensoriamento, atuação, coleta de dados, armazenamento e processamento. O decreto 9.854 [4], que institui o Plano Nacional de Internet das Coisas, no Brasil, apresenta definições semelhantes para IdC, coisas e dispositivos. A Anatel[2] é responsável por regulamentar e fiscalizar o que está disposto no decreto.

Uma característica da IdC é a heterogeneidade de dispositivos em relação a plataformas de hardware e padrões de comunicação [3]. Além disso, os diferentes cenários de IdC são dinâmicos, dado que podem variar com frequência o número de dispositivos implantados bem como o estado de cada dispositivo. Essas características, juntamente com os recursos bem limitados em termos de memória e processamento, podem ser exploradas para realizar diferentes ataques que podem culminar na indisponibilização de serviços ou no acesso não autorizado a dados sensíveis. Desse modo, um cenário típico com diversos dispositivos conectados diretamente a uma infraestrutura 5G, por meio do mMTC, pode ser alvo de ataques.

Considerando essa preocupação, iniciou-se uma investigação sobre recomendações de segurança para cenários de IdC com infraestrutura 5G entre instituições técnicas e órgãos governamentais. Foram reunidas algumas recomendações da ITU, além de recomendações de um projeto de lei dos EUA[3]. Além disso, também foram pesquisadas algumas ameaças e vulnerabilidades comuns a dispositivos e aplicações de IdC que podem ser exploradas para ataques à infraestrutura 5G.

As principais contribuições deste trabalho, no contexto de IdC com comunicação 5G, são:

- a definição de um modelo de ameaças que considera 5 superfícies de ataque;
- a recomendação de aplicação de métodos existentes para classificar e atribuir pontuação de criticidade a ameaças

Dalton C. G. Valadares, Instituto Federal de Pernambuco, Caruaru-PE, e-mail: dalton.valadares@embedded.ufcg.edu.br; Newton C. Will, Depto. de Ciência da Computação, Universidade Tecnológica Federal do Paraná, Dois Vizinhos-PR, e-mail: will@utfpr.edu.br; Álvaro A. C. C. Sobrinho, Depto. de Ciência da Computação, Universidade Federal do Agreste de Pernambuco, Garanhuns-PE, e-mail: alvaro.alvares@ufape.edu.br; Anna C. D. de Lima, UFCG, anna.lima@embedded.ufcg.edu.br; Igor S. de Morais, UFCG, e-mail: igor.morais@embedded.ufcg.edu.br; Pedro Graciliano, UFCG, e-mail: pedro.santos@embedded.ufcg.edu.br; Danilo F. S. Santos, Centro de Engenharia Elétrica e Informática, Universidade Federal de Campina Grande, Campina Grande-PB, e-mail: danilo.santos@virtus.ufcg.edu.br.

[1] https://www.itu.int/

[2] https://www.gov.br/anatel/pt-br

[3] https://www.congress.gov/bill/115th-congress/senate-bill/1691/text

e vulnerabilidades;
- uma lista de desafios com ameaças e vulnerabilidades conhecidas;
- uma lista de recomendações para mitigação de possíveis problemas com segurança.

O restante desse documento está organizado como segue: alguns fundamentos para este trabalho, como propriedades de segurança e modelo STRIDE, são apresentados na Seção II; o modelo de ameaças definido para cenários de aplicações e serviços de IdC com comunicação 5G é apresentado e explicado na Seção III; na Seção IV são apresentados alguns desafios, como ameaças e vulnerabilidades, nos cenários de IdC que podem causar problemas em uma infraestrutura 5G; algumas recomendações de segurança são apresentadas na Seção V; por fim, a conclusão é apresentada na Seção VI.

II. Fundamentos

A. Propriedades de Segurança

O padrão NIST FIPS 199 [5] apresenta confidencialidade, integridade e disponibilidade como os três objetivos de segurança para informações e para sistemas de informação. Esses três objetivos são conhecidos como *tríade CID*, e são elencados a seguir.

1) Confidencialidade: Restringe a visualização dos dados apenas a quem detém os requisitos para visualizá-los, dificultando o acesso a esses dados a quem não tem essa permissão. A técnica mais comum para garantir a confidencialidade dos dados é a criptografia, onde os dados são cifrados utilizando uma chave e somente o detentor da mesma chave, para criptografia simétrica, ou de uma chave complementar, para criptografia assimétrica, poderá decifrar os dados [6].

2) Integridade: É o fornecimento de proteção contra a corrupção ou modificação não autorizada dos dados, garantindo que os dados que estão sendo lidos são exatamente os mesmos que foram previamente gravados ou enviados. A forma mais comum de garantir a integridade dos dados é a utilização do MAC (*Message Authentication Code*). A utilização do MAC permite que qualquer alteração na mensagem seja detectada, visto que diferentes conjuntos de dados irão gerar diferentes *hashes* [7].

3) Disponibilidade: Implica que o serviço esteja disponível para usuários legítimos, o tempo todo e sem interrupções, assegurando o acesso e o uso das informações de forma confiável e em tempo adequado. O nível de disponibilidade exigido para um determinado serviço aumenta de acordo com a criticidade de tal serviço. Diversos ataques podem ocasionar na perda ou redução da disponibilidade de um determinado serviço, e estes podem ser amenizados com o uso de sistemas de autenticação ou com a utilização de sistemas de detecção de intrusão e *firewalls*.

B. Modelo STRIDE

STRIDE é um modelo de classificação de ameaças para avaliação de segurança que deriva de um acrônimo das seguintes categorias de ameaças [8]:

- ***S**poofing*: tentativa de obter acesso a um sistema usando uma identidade falsa, com o objetivo de obter uma vantagem ilegítima;
- ***T**ampering*: modificação não autorizada de dados, seja no seu armazenamento ou transmissão;
- ***R**epudiation*: capacidade dos usuários (legítimos ou não) de negar que realizaram ações ou transações específicas;
- ***I**nformation Disclosure*: exposição indesejada de dados privados a indivíduos que não devem ter acesso a eles;
- ***D**enial of Service*: processo de tornar um sistema ou aplicação indisponível, ou com a disponibilidade prejudicada, a usuários legítimos;
- ***E**levation of Privilege*: ocorre quando um usuário com privilégios limitados assume a identidade de um usuário com maiores privilégios para obter acesso a um ativo.

O modelo STRIDE é usado por desenvolvedores e empresas para categorizar as ameaças aos sistemas, levando em consideração seus efeitos no quesito de segurança. A definição de um modelo de ameaças auxilia na avaliação e documentação dos riscos de segurança associados a um sistema, permitindo a definição de requisitos de segurança eficientes, realistas e significativos. Além disso, a identificação adequada de ameaças e a seleção apropriada de contramedidas ajudam a reduzir a capacidade dos invasores executarem operações ilegítimas.

C. Pontuação CVSS

O *Common Vulnerability Scoring System* (CVSS) é um método utilizado para classificar vulnerabilidades e seus riscos que, através de um sistema de pontuações, define um grau de qualificação para a vulnerabilidade. Tal método é amplamente utilizado em sistemas computacionais e ambientes de TI, para categorizar as vulnerabilidades [9].

O CVSS é composto por três grupos de métricas: Base (BM), Temporária (TM) e Ambiental (EM). A métrica base (BM) reflete a gravidade de uma vulnerabilidade de acordo com suas características intrínsecas e imutáveis, ou seja, características que não se alteram ao longo do tempo ou em diferentes ambientes. Tal grupo é subdividido em métricas de explorabilidade (EM) e métricas de impacto (IM), com o primeiro medindo os meios técnicos e a facilidade com que a vulnerabilidade pode ser explorada e o segundo envolvendo as três propriedades de segurança descritas na Seção II-A. A métrica temporária (TM) ajusta a métrica base de acordo com fatores que mudam ao longo do tempo, e a métrica ambiental (EM) ajusta a BM e TM a um ambiente específico. Tipicamente, apenas a métrica base é publicada, visto que ela não sofre alterações ao longo do tempo e é comum a todos os ambientes.

O CVSS 3.0 define cinco níveis de severidade para uma vulnerabilidade, sendo esses: Nenhum (*score* 0.0); Baixo (*score* entre 0.1 e 3.9); Médio (*score* entre 4.0 e 6.9); Alto (*score* entre 7.0 e 8.9); e Crítico (*score* entre 9.0 e 10.0).

III. Modelo de Ameaças

Considerando possíveis superfícies de ataques em aplicações de Internet das Coisas com infraestrutura 5G, definimos o modelo de ameças exibido na Fig. 1. O símbolo de caveira representa possíveis atacantes, seja em dispositivos ou canais de comunicação.

O modelo de ameaças definido considera 5 superfícies de ataque:

- Dispositivos - Cada dispositivo pode ser alvo de atacantes e, ao serem invadidos, permitem comunicação com a infraestrutura 5G ou com *gateways*, ampliando a superfície de ataque para outros alvos;

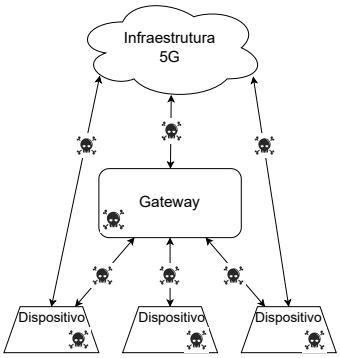

Fig. 1. Modelo de ameaças considerado

- *Gateway* - De forma similar, os *gateways* podem ser invadidos, possibilitando comunicação com os dispositivos e com a infraestrutura 5G;
- Canal de comunicação dispositivo/*gateway* - atacantes podem explorar a comunicação entre dispositivos e *gateways*;
- Canal de comunicação *gateway*/infraestrutura - atacantes podem explorar o canal entre *gateways* e a infraestrutura 5G;
- Canal de comunicação dispositivo/infraestrutura - atacantes podem explorar o canal entre os dispositivos e a infraestrutura 5G, no caso de conexão direta dos dispositivos.

Além do modelo de ameaças, sugerimos utilizar o modelo STRIDE, para classificar ameaças e vulnerabilidades, e o sistema de pontuação CVSS, para atribuir uma pontuação de criticidade às ameaças e vulnerabilidades conhecidas. Embora esforços tenham sido realizados por Ur-Rehman *et al.* [10] para propor um sistema de pontuação mais adequado para aplicações de IdC ($CVSS_{IoT}$), optamos por utilizar o CVSS 3.0, por ser a versão padrão mais recente. O $CVSS_{IoT}$ adiciona três outras métricas a serem avaliadas, com uma delas sendo relacionada aos danos físicos que uma vulnerabilidade explorada pode causar. A classificação e a pontuação de criticidade auxiliam no processo de gerenciamento e priorização dos riscos decorrentes de ameaças e vulnerabilidades, ajudando a mitigá-las.

IV. Desafios

Dentre os principais desafios relacionados a serviços e aplicações de IdC, que podem ser meios de acesso às redes 5G, podem ser considerados: o desenvolvimento seguro de dispositivos e aplicações/serviços, por exemplo, considerando o conceito de *Security by Design* [11]; o gerenciamento de identidades para os componentes de software das aplicações e serviços, que frequentemente serão dispositivos; a atualização segura dos componentes de software; e o gerenciamento das configurações de funcionamento e comunicação. Além disso, de acordo com a Lei Pública de cibersegurança de IdC nos EUA, também é necessário conhecer as vulnerabilidades existentes e disponibilizar informações acerca destas. A seguir, estão listadas algumas ameaças de segurança que surgem a partir da exploração de vulnerabilidades existentes. Devido à limitação de páginas, são definidas apenas algumas ameaças. Sugere-se classificá-las com o modelo STRIDE e pontuá-las com o sistema CVSS, determinando, assim, o nível de criticidade.

A. Ameaças

1) Eavesdropping: Esse ataque impacta diretamente na confidencialidade do serviço, visto que o foco do *eavesdropping* é bisbilhotar informações e roubar dados. Nesse ataque, o invasor pode monitorar redes, explorar "brechas" de segurança e conexões fracas entre dispositivos IdC e o servidor. De forma geral, o *eavesdropping* é realizado por meio da interceptação de comunicações que não possuem proteção adequada. A defesa contra esse tipo de ataque se dá basicamente com processos de criptografia, como autenticação criptografada (para evitar serviços não autorizados que possam gravar senhas), transmissão de dados criptografados (para que o invasor não consiga ter acesso aos dados que estão sendo enviados) e até mesmo segmentação de rede, com uma parte para comunicação entre usuários e outra para comunicação de informações confidenciais.

2) Distributed Denial of Service - DDOS: Ataques de negação de serviço distribuído, DDoS, visam a afetar a disponibilidade de sistemas, já que sobrecarregam seus alvos com tráfego de Internet indesejado. Durante um ataque, os invasores usam muitas máquinas exploradas e dispositivos conectados pela Internet, incluindo dispositivos de IdC. Este tipo de ataque pode se intensificar em uma rede 5G e fazer com que um pacote infectado contamine vários dispositivos durante as comunicações (podendo formar uma botnet[4]). No contexto de IdC, esse ataque se intensifica ainda mais, visto que podem existir vários ramos e dispositivos comprometidos.

3) Spoofing: A falsificação (*spoofing*) acontece quando um atacante se faz passar por um dispositivo ou usuário autorizado para roubar informações, espalhar *malware*[5] ou ignorar sistemas de controle de acesso. Existem diversos tipos de falsificação, sendo três mais tradicionais: falsificação de endereço IP, em que o atacante transfere pacotes pela rede a partir de um endereço IP falso; falsificação de ARP[6], em que o atacante vincula seu endereço MAC[7] a um endereço IP já autorizado na rede; e falsificação de DNS[8], em que o invasor inicia uma ameaça, com "envenenamento" de *cache*, para redirecionar o tráfego destinado a um tráfego de nome de domínio específico para um endereço IP diferente.

TABELA I
STRIDE + CVSS

	Eavesdropping	DDoS	*Spoofing*
Spoofing			
Tamper			
Repudiation			
Information Disclosure			
Denial of Service			
Escalation of Privilege			

[4]https://www.avast.com/pt-br/c-botnet
[5]https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml
[6]https://blog.pantuza.com/artigos/o-protocolo-arp-address-resolution-protocol
[7]https://www.controle.net/faq/o-que-e-mac-address
[8]https://tecnoblog.net/responde/o-que-e-dns/

B. Classificação e criticidade de ameaças

Como sugerido, foi realizada a classificação STRIDE e a pontuação das ameaças de acordo com o CVSS, seguindo um exemplo de Marisetty [12], como pode ser visto na Tabela I. As cores representam os níveis de criticidade de acordo com a pontuação CVSS, da seguinte maneira: azul é crítico (CVSS 9-10), laranja é alto (CVSS 7-8,9), amarelo é médio (CVSS 4-6,9) e cinza representa "não se aplica" (N/A).

V. Recomendações

A. Recomendações da ITU para IdC do consumidor

1) Não usar senhas padrão: Deve-se usar senhas únicas, mecanismos que reduzem o risco de ataques automáticos (força bruta) e mecanismos de autenticação apropriados. O dispositivo deve prover uma maneira de alterar o valor de autenticação utilizado e deve ser impraticável realizar um ataque força bruta em dispositivo que não seja tão limitado em termos de recursos.

2) Implementar meios de gerenciar relatórios de vulnerabilidades: Os fabricantes devem possuir política de divulgação de vulnerabilidades e devem tratá-las em tempo hábil. Além disso, devem monitorar continuamente por novas vulnerabilidades e mitigá-las.

3) Manter software atualizado: Todos os componentes de software devem ser atualizados de forma segura, havendo mecanismos para tais procedimentos em dispositivos com recursos suficientes. A atualização deve ser realizada de forma simples e mecanismos automáticos podem ser utilizados para tal. A verificação por atualizações pode acontecer na inicialização do dispositivo e, após, periodicamente. As atualizações automáticas devem ser configuráveis e habilitadas na inicialização. O dispositivo deve usar mecanismos de criptografia apropriados para as atualizações. Estas devem ser oportunas, podendo ser agendadas, e o dispositivo deve verificar autenticidade e integridade das mesmas.

Os fabricantes devem informar aos usuários sobre atualizações necessárias e quais riscos são mitigados por estas, devendo também publicar o período definido para suporte de atualizações ou as justificativas para não tê-las. No caso de dispositivos com recursos bastante limitados, cada dispositivo deve possuir seu modelo claramente identificado, seja por rótulo ou interface física.

4) Armazenar parâmetros de segurança de forma segura (protegidos): Os parâmetros de segurança em armazenamento persistente devem estar protegidos pelo dispositivo. Caso a identidade exclusiva seja codificada no dispositivo, deve ser implementada de forma a evitar adulterações, sejam por meio físico, elétrico ou por software. Parâmetros de segurança críticos não devem ser codificados no código fonte e qualquer parâmetro de segurança usado para verificação de integridade e autenticidade de atualização de software deve ser único por dispositivo e gerado de forma a reduzir o risco de ataques.

5) Realizar comunicação segura: O dispositivo deve usar criptografia apropriada para comunicação segura e implementações avaliadas para prover funcionalidades de segurança e rede, principalmente quando relacionadas à criptografia. Os algoritmos criptográficos devem ser atualizáveis e o acesso ao dispositivo em estado inicial por interface de rede deve ser possível apenas após autenticação na interface. Mudanças nas configurações de segurança dos dispositivos devem ser possíveis apenas após autenticação e os parâmetros de segurança críticos devem ser criptografados durante trânsito. O dispositivo deve proteger a confidencialidade dos parâmetros de segurança críticos que são acessíveis remotamente por interfaces de rede e o fabricante deve seguir padrões e recomendações para gerenciamento seguro destes parâmetros.

6) Minimizar superfícies de ataques expostas: Todas as interfaces lógicas e físicas não utilizadas devem ser desabilitadas no estado inicial e as interfaces de rede devem minimizar a divulgação não autenticada de informações relacionadas à segurança. Os dispositivos devem evitar exposição desnecessária de interfaces físicas que possam ser alvo de ataques e interfaces de depuração devem ser desabilitadas quando estiverem fisicamente acessíveis. O fabricante deve permitir apenas serviços de software necessários para o devido funcionamento do dispositivo, com o código limitando-se à funcionalidade necessária para operação do dispositivo. O software deve executar com o mínimo necessário de privilégios e o dispositivo deve incluir um mecanismo de controle de acesso em nível de hardware para a memória. O fabricante deve seguir processos de desenvolvimento seguros para software implantado no dispositivo.

7) Garantir integridade de software: O dispositivo deve verificar seu sistema usando mecanismos de inicialização (*boot*) seguros e, caso o sistema detecte uma alteração não autorizada, o dispositivo deve alertar o usuário se conectando apenas às redes necessárias para o alerta.

8) Garantir que dados pessoais estão protegidos: A confidencialidade de dados pessoais transmitidos entre dispositivos e serviços deve ser preservada por meio de criptografia adequada e qualquer capacidade sensora do dispositivo deve ser documentada de forma clara e acessível para o usuário.

9) Ser resiliente a interrupções: Os dispositivos devem ser resilientes, considerando interrupções de energia e comunicação, e devem continuar operando no caso de perda de conexão com a rede de comunicação, além de se recuperar apropriadamente no caso de perda de energia. Devem também considerar a infraestrutura de rede para realizar conexões operacionais e estáveis, minimizando sobrecarga desnecessária.

10) Examinar dados de telemetria: Dados de telemetria, quando coletados, devem ser examinados para evitar anomalias de segurança.

11) Facilitar remoção de dados do usuário: O dispositivo e os serviços devem possuir uma funcionalidade que permita ao usuário remover seus dados de uma maneira simples, quando necessário, e deve haver instruções claras sobre como remover os dados pessoais. Deve haver informação clara de que os dados pessoais foram removidos dos serviços e dispositivos

12) Facilitar instalação e manutenção dos dispositivos: A instalação e manutenção nos dispositivos deve envolver decisões mínimas do usuário e seguir as melhores práticas de segurança em relação à usabilidade. O fabricante deve fornecer guia sobre como configurar o dispositivo de forma segura e como verificar se o mesmo está configurado de forma segura.

13) Validar dados de entrada: O sistema deve validar os dados de entrada considerando tipo e faixas possíveis de valores, por exemplo.

14) Fornecer informações sobre proteção de dados: Deve existir informação sobre quais dados são usados, para que e por quem. Quando necessário processar tais dados, deve-se

solicitar permissão aos usuários e o processamento deve ser apenas dos dados necessários para a funcionalidade. Deve-se possibilitar que usuários que permitiram o processamento dos dados possam cancelar a permissão

B. Lei de Segurança Cibernética de IdC nos EUA

O Senado dos EUA definiu o projeto de lei "*Internet of Things (IoT) Cybersecurity Improvement Act of 2017*" para prover padrões operacionais mínimos de cibersegurança a dispositivos IdC comprados por agências federais. O projeto prevê que:

- qualquer fornecedor de dispositivo de IdC disponibilize um certificado informando que o dispositivo não possui software, hardware ou *firmware* com vulnerabilidades de segurança ou defeitos conhecidos na base de vulnerabilidades do NIST (*National Vulnerability Database*) ou outra base de segurança com credibilidade;
- o dispositivo deve possuir software ou *firmware* capaz de receber atualizações autenticadas e confiáveis do fabricante, e deve usar tecnologias e protocolos da indústria padronizados para funções de comunicação, criptografia e interconexão com outros dispositivos;
- o dispositivo não deve incluir credenciais fixas usadas para administração remota, atualização de software/*firmware*, ou comunicação;
- exceções devem ser expressas de forma escrita e aprovadas pelo responsável da agência federal, quando o fornecedor informar vulnerabilidade conhecida, ações de mitigação e uma justificativa para uso seguro do dispositivo;
- os fabricantes devem notificar as agências caso descubram posteriormente vulnerabilidades durante o contrato;
- o fabricante deve atualizar ou substituir software ou *firmware* em caso de vulnerabilidade ou defeito, de forma a corrigir ou remover a vulnerabilidade ou defeito, de forma autenticada e segura;
- o fabricante deve reparar ou substituir o dispositivo caso uma vulnerabilidade descoberta por meio das bases aceitas não possa ser mitigada;
- o fabricante deve fornecer informações sobre como o dispositivo recebe atualizações de segurança, prazo válido de suporte de segurança, notificação formal quando o suporte de segurança encerrar e informação adicional recomendada pela *National Telecommunications and Information Administration*.

Caso as recomendações anteriores se tornem inviáveis, pode haver exceções desde que devidamente justificadas e que forneçam níveis de segurança equivalentes por meio de adoção de medidas de segurança conhecidas. Nestes casos, requisitos adicionais de gerenciamento e uso podem ser considerados para os dispositivos que não estejam em conformidade. O NIST e as agências federais determinarão padrões industriais aceitos com níveis equivalentes de segurança ou superiores às recomendações definidas. Para dispositivos que sigam estes padrões, deve haver certificado. O NIST e as agências federais também poderão definir processos de avaliação de segurança com nível equivalente ou superior ao nível das recomendações.

Devem ser disponibilizados guias para divulgação de vulnerabilidades de segurança e defeitos, com base no padrão ISO/IEC 29147. Os órgãos e departamentos federais devem manter um inventário atualizado de dispositivos de IdC utilizados, contendo informações sobre os dispositivos e fabricantes.

VI. Conclusão

Considerando as preocupações com segurança em cenários de aplicações e serviços de IdC com comunicação 5G, este trabalho reuniu recomendações da ITU e recomendações sugeridas por um projeto de lei nos EUA. Estas recomendações podem direcionar regulamentações nacionais, por exemplo, relacionadas ao Plano Nacional de Internet das Coisas, principalmente considerando que a infraestrutura 5G está sendo implantada no Brasil. Além disso, podem auxiliar também a regulamentação de serviços ofertados por operadoras de telecomunicações que disponibilizem/necessitem de dispositivos de IdC.

Além das recomendações, foram listadas e definidas algumas ameaças e vulnerabilidades conhecidas no contexto de IdC com comunicação 5G. Foi considerado um modelo de ameaças com 5 superfícies de ataque e, para gerenciamento dos riscos e preocupações com segurança, sugeriu-se utilizar o modelo STRIDE com o sistema de pontuação de criticidade CVSS. Como trabalho futuro, sugere-se dar continuidade ao estudo, reunindo mais recomendações e identificando novas ameaças e vulnerabilidades. Além disso, sugere-se também a elaboração de sugestões de como mitigar tais ameaças e vulnerabilidades. No momento, uma revisão sistemática da literatura está sendo executada neste sentido.

Agradecimentos

Este trabalho foi parcialmente financiado pela ANATEL e apoiado pelo Núcleo VIRTUS da UFCG.

Referências

[1] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, 2019.

[2] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues, "Security in 5G-enabled internet of things communication: Issues, challenges, and future research roadmap," *IEEE Access*, vol. 9, 2021.

[3] I. T. S. S. of ITU, *Overview of the Internet of Things*, ITU-T Std., 2012.

[4] "DECRETO Nº 9.854 - Plano Nacional de Internet das Coisas," http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm, 2019.

[5] FIPS PUB, *Standards for Security Categorization of Federal Information and Information Systems*. Federal Information Processing Standards Publication, 2004.

[6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. CRC Press, 2014.

[7] F. Hou, Z. Wang, Y. Tang, and Z. Liu, "Protecting integrity and confidentiality for data communication," in *Intl Sym on Computers And Communications*. Alexandria, Egito: IEEE, 2004.

[8] F. Swiderski and W. Snyder, *Threat Modeling*. Microsoft Press, 2004.

[9] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS," *ACM Computing Surveys*, vol. 53, no. 2, 2020.

[10] A. Ur-Rehman, I. Gondal, J. Kamruzzuman, and A. Jolfaei, "Vulnerability modelling for hybrid IT systems," in *Intl Conf on Industrial Technology*. Melbourne, VIC, Austrália: IEEE, 2019.

[11] J. McManus, "Security by design: Teaching secure software design and development techniques," *Journal of Computing Sciences in Colleges*, vol. 33, no. 3, 2018.

[12] Suresh Marisetty, "Five Steps to Successful Threat Modelling," https://community.arm.com/arm-community-blogs/b/internet-of-things-blog/posts/five-steps-to-successful-threat-modelling, 2019.