Avaliação de Conformidade de Equipamentos de Telecomunicações com Requisitos de Segurança Cibernética

Guilherme Rocha[†], Diego Pereira[†], Victor Pimentel[†], Ramon Fontes[*], Augusto Neto[*] and Roger Immich[*]
[*]Universidade Federal do Rio Grande do Norte, Natal, RN
[†]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Parnamirim, RN

***Abstract*—O Ato 77 da Anatel define um conjunto de requisitos de segurança cibernética para dispositivos de telecomunicações. O objetivo é reduzir ou corrigir vulnerabilidades, seja através de atualizações de *software* ou *firmware*, ou por meio de recomendações de configuração. Este artigo descreve a realização de um trabalho de avaliação da conformidade de diversos produtos classificados como equipamentos terminais com conexão à Internet e equipamentos de infraestrutura de redes de telecomunicações com os requisitos estabelecidos pelo Ato 77. A pesquisa envolve uma análise dos critérios relacionados a área capacidade de mitigação de ataques. Os resultados revelam níveis variados de conformidade, destacando áreas críticas para melhorias e propondo recomendações para assegurar o pleno atendimento às exigências regulatórias. Este estudo visa contribuir para a melhoria da segurança cibernética dos equipamentos de telecomunicações no Brasil, a partir de análises de equipamentos disponíveis no mercado nacional.**

***Index Terms*—Segurança Cibernética, Equipamentos de telecomunicações, Avaliação da conformidade, Análise de lacunas, Ato 77**

I. Introdução

A segurança cibernética tem se tornado uma preocupação central à medida que o número de dispositivos conectados à Internet continua a crescer exponencialmente. Em resposta a essa crescente demanda por segurança, regulamentações específicas têm sido desenvolvidas por órgãos reguladores em todo o mundo para assegurar que os equipamentos de telecomunicações atendam a critérios rigorosos de proteção. No Brasil, o Ato 77 da Agência Nacional de Telecomunicações (Anatel) [1] é um exemplo significativo dessas iniciativas, estabelecendo um conjunto de requisitos de segurança cibernética para equipamentos de telecomunicações.

Publicado em janeiro de 2021, o Ato 77 foi elaborado com o objetivo de minimizar ou corrigir vulnerabilidades em equipamentos de telecomunicações por meio mecanismos automatizados para atualização segura de *software/firmware*, a implementação de métodos robustos de autenticação e criptografia, e a capacidade de mitigar ataques cibernéticos. A importância dessas medidas é reforçada pela Estratégia Nacional de Segurança Cibernética [2], que destaca a necessidade de proteger a infraestrutura crítica do país contra vulnerabilidades e ataques.

Nesse contexto, a conformidade com o Ato 77 é fundamental para garantir que os dispositivos não apenas atendam aos padrões de segurança atuais, mas também sejam capazes de se adaptar a novas ameaças à medida que estas surgem. Ele deve ser aplicado a dispositivos presentes na Lista de Referência de Produtos para Telecomunicações[1], abrangendo tanto equipamentos terminais com conexão à Internet quanto equipamentos de infraestrutura de redes de telecomunicação. As suas diretrizes alinham-se com padrões internacionais, refletindo uma preocupação global com a integridade e a segurança das redes de telecomunicações.

Este estudo visa avaliar a conformidade de diversos produtos classificados como equipamentos terminais com conexão à Internet e de infraestrutura de redes de telecomunicações com os requisitos do Ato 77. A metodologia envolve uma análise detalhada dos dispositivos para verificar sua adesão aos critérios de segurança estabelecidos com a área de capacidade de mitigar ataques. Os resultados dessa avaliação são parte de um estudo inicial para identificar lacunas na conformidade e propor melhorias, contribuindo para o desenvolvimento da segurança cibernética na infraestrutura de telecomunicação de produtos comercializados no Brasil.

II. Revisão da Literatura

A. Segurança Cibernética e Normas Internacionais

A segurança cibernética tem se tornado uma prioridade global, impulsionada pelo aumento significativo no número de dispositivos conectados à Internet. Diversos países têm estabelecido normas e regulamentos para garantir a proteção dos dados e a integridade das redes de telecomunicações. Nos Estados Unidos, por exemplo, o padrão *Federal Information Processing Standard* (FIPS) 140-3 define requisitos rigorosos para módulos criptográficos usados por agências governamentais e empresas que lidam com informações sensíveis. Esta norma especifica requisitos para o projeto e a implementação de algoritmos de criptografia, gestão de chaves criptográficas, mecanismos de autenticação, segurança física, dentre outras áreas.

[1]Instituto Metrópole Digital, Universidade Federal do Rio Grande do Norte, Natal, RN.
[2]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Parnamirim, RN. Email: diego.pereira@ifrn.edu.br

[1]https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2020/1493-ato-7280

De forma semelhante, na União Europeia, o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* - GDPR) [3] e a Diretiva de Segurança das Redes e da Informação (NIS *Directive*) são os principais marcos regulatórios que visam proteger dados pessoais e assegurar a segurança das redes de informação. A GDPR, em particular, impõe obrigações rigorosas sobre o tratamento e a proteção de dados pessoais, exigindo que organizações implementem medidas técnicas e organizacionais adequadas para garantir a segurança dos dados. A NIS *Directive*, por sua vez, foca na segurança das redes e dos sistemas de informação, exigindo que os operadores de serviços essenciais e os prestadores de serviços digitais implementem medidas de segurança robustas para proteger suas infraestruturas.

Outros países, como Japão, Singapura, Austrália e Índia também possuem regulamentações que tratam de forma específica o estabelecimento de requisitos de segurança cibernética para proteger as suas infraestruturas críticas de telecomunicações contra ataques.

B. Regulamentação de Segurança Cibernética no Brasil

No Brasil, a Anatel desempenha um papel fundamental na regulamentação e supervisão da segurança dos equipamentos de telecomunicações. O Ato 77, conforme destacado anteriormente, estabelece requisitos específicos de segurança cibernética para esses dispositivos. Este ato foi desenvolvido em consonância com um conjunto de legislações vigentes, tais como, Lei Geral de Telecomunicações [4], Regulamento para Avaliação da Conformidade e Homologação de Produtos para Telecomunicações [5], a Estratégia Nacional de Segurança Cibernética, a Lei Geral de Proteção de Dados Pessoais (LGPD) [6] e o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

De forma geral, o Ato 77 busca minimizar ou corrigir vulnerabilidades através de atualizações seguras de *software*/*firmware*, fornecer recomendações detalhadas de configurações, a implementação de métodos adequados de autenticação e criptografia, e a capacidade de mitigar ataques cibernéticos. Além disso, o Ato exige que os equipamentos possuam mecanismos para gerenciamento remoto seguro e proteção de dados pessoais, alinhando-se às melhores práticas internacionais de segurança.

Enquadram-se produtos que possuem função de equipamento terminal com conexão à Internet ou de equipamento de infraestrutura de redes de telecomunicações, tais como roteadores, *gateways*, *firewalls*, modems, telefones celulares, computadores e dispositivos IoT. Devido a limitação de espaço, apenas parte dos requisitos definidos para o processo de conformidade e homologação junto à norma serão destacados no presente estudo.

O processo de certificação e homologação dos equipamentos, é realizado a partir do requerimento de homologação que contem uma declaração do requerente informando a quais requisitos listados o produto e o fornecedor atendem. A declaração deve contemplar o uso do princípio de *security by design*, proposto pelo *Open Project Application Security Project* (OWASP), para desenvolvimento do produto, que consiste em aplicar as melhores práticas e padrões de segurança cibernética desde a fase de concepção e projeto dos equipamentos, visando minimizar as vulnerabilidades e maximizar a proteção dos dados e das informações [7].

O modelo *security by design* incorpora princípios como a minimização de dados, a defesa em profundidade, a segregação de funções, o princípio do menor privilégio, a criptografia por padrão, entre outros. O uso desse modelo pode contribuir para aumentar a confiança e a qualidade dos equipamentos de telecomunicações no Brasil, bem como para atender às expectativas dos usuários e às normas regulatórias.

Também é importante destacar que, a qualquer tempo, por meio do programa de Supervisão de Mercado, a Anatel pode avaliar a conformidade do produto e seu fornecedor com a declaração inserida no requerimento de homologação. Além disso, quaisquer falhas de segurança cibernética identificadas em equipamentos homologados que afetem a segurança de seus usuários, prestadoras ou das redes de telecomunicações do país podem ser objeto de avaliação pela Anatel, ainda que a característica afetada não tenha sido objeto da declaração que compõe o requerimento de homologação.

Assim, identificada uma falha ou vulnerabilidade , a Anatel notificará o responsável para saná-la dentro de um prazo adequado, considerando a severidade conforme o *Common Vulnerability Scoring System* (CVSS). Este prazo pode ser prorrogado pela Anatel. Se não corrigido no prazo estabelecido, a homologação pode ser suspensa e o produto recolhido ou substituído. A suspensão permanece até que a vulnerabilidade seja superada ou o risco mitigado. Após o prazo máximo, a homologação será cancelada caso a falha não for resolvida.

C. Requisitos de segurança cibernética do Ato 77

Os requisitos do Ato 77 são organizados em várias seções que cobrem aspectos essenciais da segurança cibernética para equipamentos de telecomunicações. Primeiramente, é avaliado se o dispositivo foi desenvolvido com base no princípio de *security by design*. Em seguida, são delineadas diretrizes para atualização segura de software e firmware (4 requisitos), gerenciamento remoto (2 requisitos), instalação e operação dos dispositivos (6 requisitos), acesso à configuração dos equipamentos (9 requisitos), serviços de comunicação de dados (4 requisitos), proteção de dados pessoais e sensíveis (4 requisitos), e capacidade de mitigar ataques (3 requisitos). Para cada requisito, deve-se apresentar justificativas específicas caso não seja atendido.

Esta pesquisa ficará restrita a seção de capacidade de mitigar ataques. Para obter conformidade com este seção, o equipamento deve ter conformidade três requisitos, são eles:

a) Possuir mecanismo para limitação da taxa de transmissão de dados de saída (upload), além do usualmente necessário, a fim de minimizar sua utilização como vetor em ataques a outros equipamentos ou sistemas (ataque de negação de serviço).

b) Implementar mecanismos para validação do endereço de origem dos pacotes de dados, filtrando pacotes com endereço de origem falsificados (filtro antispoofing), em especial na transmissão de dados de saída (upload).
c) Ser projetado para mitigar os efeitos de ataques de negação de serviço em andamento, sendo resistentes a um número excessivo de tentativas de autenticação, por meio de, por exemplo: priorização de sua capacidade de processamento às sessões de comunicação já estabelecidas e autenticadas; e limitação do número de sessões de autenticação concorrentes, descartando tentativas de estabelecimento de novas sessões quando superado limite estabelecido.

III. Metodologia

A metodologia empregada neste trabalho visa fornecer uma estrategia para a verificação e recomendação para obter adequação de equipamentos terminais com conexão à Internet e de infraestrutura de redes de telecomunicações com o Ato 77, garantindo que esses dispositivos atendam aos requisitos de segurança estabelecidos pela regulamentação previsto para área de capacidade de mitigar ataques. O processo metodológico é dividido nas seguintes etapas:

1) Levantamento dos Requisitos do Ato 77 da Anatel: foi realizado um levantamento detalhado dos requisitos específicos estabelecidos pelo Ato 77. Esta etapa envolveu uma análise aprofundada do texto da regulamentação, bem como a identificação e compreensão dos padrões de segurança e privacidade exigidos para os equipamentos;
2) Análise dos Equipamentos de Telecomunicações Existentes: consistiu na análise detalhada das funcionalidades e configurações dos equipamentos selecionados a partir de consulta no mercado. A seleção incluiu uma variedade de modelos, principalmente aqueles utilizados por usuários com menor capacidade técnica para implementar estratégias voltadas a segurança da informação;
3) Identificação de Lacunas de Conformidade: com base nos requisitos estabelecidos pelo Ato 77 e na análise dos equipamentos existentes, identificaram-se as lacunas de conformidade entre os dispositivos e os padrões regulatórios. Esta fase permitiu uma compreensão clara das áreas que necessitam de melhorias para atender às exigências de segurança estabelecidas;
4) Desenvolvimento de Recomendações: a partir da identificação das lacunas de conformidade, foram desenvolvidas recomendações específicas para aprimorar os dispositivos de modo a garantir sua conformidade com o Ato 77. Essas recomendações, conforme descrito no início da seção, ficaram restritas a capacidade de mitigar ataques.

IV. Resultados

A partir da avaliação dos dispositivos, os resultados foram sumarizados na Tabela I. É destacada a capacidade de mitigar ataques de cada equipamento, evidenciando os mecanismos de defesa implementados, a limitação de taxa de upload, presença de filtro anti-spoofing e a mitigação de ataques de negação de serviço.

Dentre os oito equipamentos avaliados, apenas três deles tem total conformidade com a capacidade de mitigar ataques, o ASUS ZenWiFi XD6, ASUS ZenWiFi AX (XT8) e TP-Link Archer AX6000. Outros quatro equipamentos, TP-Link Archer C6, TP-Link Archer C21, Intelbras RG 1200 e D-Link DIR-846 AC1200, obtiveram uma avaliação parcial para a mitigação de ataques DoS. O equipamento APsystems ECU-R não provê conformidade com nenhum dos requisitos.

Roteadores como o TP-Link Archer C21 são amplamente adotados e facilmente encontrados no mercado brasileiro devido à sua popularidade e disponibilidade generalizada. Por outro lado, modelos como o ASUS ZenWiFi XD6, TP-Link Archer AX6000 e ASUS ZenWiFi AX (XT8) destacam-se como exemplos de dispositivos focados especificamente na segurança. Eles oferecem recursos avançados, como firewall integrado, proteção contra ataques DDoS e criptografia robusta, atendendo às necessidades daqueles que priorizam a proteção de suas redes.

Já roteadores como o Intelbras RG 1200, D-Link DIR-846 AC1200 e TP-Link Archer C6 representam opções mais intermediárias. Eles demonstram a capacidade de equilibrar a segurança com um preço mais acessível, oferecendo funcionalidades básicas de segurança, como firewall SPI, controle parental e criptografia WPA/WPA2. Esses dispositivos são adequados para usuários que buscam uma proteção sólida sem comprometer significativamente o orçamento.

Os resultados demonstram que os roteadores ASUS ZenWiFi XD6, TP-Link Archer AX6000 e ASUS ZenWiFi AX (XT8) atendem plenamente aos três requisitos de defesa. Isso significa que esses dispositivos possuem recursos robustos para limitar a taxa de upload, implementar filtros anti-spoofing e mitigar ataques de negação de serviço, proporcionando uma camada sólida de proteção para as redes domésticas ou empresariais.

Por outro lado, alguns dispositivos, como TP-Link Archer C21 e APsystems ECU-R, demonstram adequações parciais ou nulas em relação aos mecanismos de defesa avaliados. Embora alguns desses dispositivos possam oferecer alguma forma de mitigação de ataques, eles podem não ser tão eficazes quanto os dispositivos que atendem plenamente aos requisitos.

A presença de mecanismos de defesa eficazes, conforme destacado nesta tabela, desempenha um papel crucial na proteção das redes contra ameaças cibernéticas. Portanto, ao selecionar um dispositivo de rede, é essencial considerar não apenas os recursos de conectividade, mas também sua capacidade de fornecer segurança robusta contra possíveis ataques. Este aspecto é fundamental para garantir a integridade e a confiabilidade das redes domésticas ou empresariais no ambiente digital atual.

TABLE I
AVALIAÇÃO DE CONFORMIDADE COM OS REQUISITOS DE CAPACIDADE DE MITIGAR ATAQUES.

Requisito	**Capacidade de Mitigar Ataques**			
Equipamento	**Adequação**	**Mecanismos de Defesa**		
		Limitação de taxa de upload	**Filtro anti-spoofing**	**Mitigação de ataques DoS**
APsystems ECU-R	Não	Não	Não	Não
ASUS ZenWiFi XD6	Sim	Sim	Sim	Sim
TP-Link Archer AX6000	Sim	Sim	Sim	Sim
ASUS ZenWiFi AX (XT8)	Sim	Sim	Sim	Sim
TP-Link Archer C6	Sim	Sim	Sim	Parcial
TP-Link Archer C21	Parcial	Não	Sim	Parcial
Intelbras RG 1200	Sim	Sim	Sim	Parcial
D-Link DIR-846 AC1200	Sim	Sim	Sim	Parcial

V. CONSIDERAÇÕES FINAIS

Este artigo avaliou a conformidade de equipamentos terminais com conexão à Internet e infraestrutura de redes de telecomunicações com os requisitos do Ato 77 da Anatel. A análise incluiu critérios relacionados a capacidade de mitigação de ataques. Os resultados mostraram variações nos níveis de conformidade dos dispositivos avaliados, destacando a necessidade de aprimoramentos.

Nesse contexto, as recomendações buscam assegurar que os equipamentos atendam plenamente às exigências regulatórias, contribuindo substancialmente para a robustez da segurança cibernética no Brasil. É fundamental que a conformidade com o Ato 77 seja percebida não apenas como uma obrigação regulatória, mas como um componente essencial na proteção das infraestruturas críticas e na segurança dos usuários. Desse modo, a implementação eficiente destas diretrizes reduz vulnerabilidades e fortalece a resiliência contra ameaças cibernéticas, as quais seguem em constante evolução.

Logo, a colaboração entre reguladores, fabricantes e a comunidade de científica deve ser considerada vital para enfrentar os desafios emergentes na segurança cibernética. Adaptações contínuas às mudanças no cenário global de ameaças são essenciais para manter a integridade e a confiabilidade das redes de telecomunicações.

Os trabalhos futuros almejam realizar testes experimentais para comprovar a análise feita a partir da documentação dos equipamentos, assim como ampliar as áreas avaliadas, buscando contemplar todos os requisitos previstos no Ato 77.

AGRADECIMENTOS

O presente trabalho foi realizado com o suporte da Padtec S.A., por meio de projeto de inovação.

REFERENCES

[1] Agência Nacional de Telecomunicações (Anatel), "Ato Nº 77, de 5 de janeiro de 2021: Estabelece requisitos de segurança cibernética para equipamentos de telecomunicações," 2021, Publicado no Diário Oficial da União em 6 de janeiro de 2021.

[2] Presidência da República, "Decreto Nº 10.222, de 5 de fevereiro de 2020: Aprova a Estratégia Nacional de Segurança Cibernética," 2020, Gabinete de Segurança Institucional da Presidência da República.

[3] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," 2016, Official Journal of the European Union, L 119, 4 May 2016.

[4] Presidência da República, "Lei Nº 9.472, de 16 de julho de 1997: Dispõe sobre a organização dos serviços de telecomunicações, a criação e o funcionamento de um órgão regulador e outros aspectos institucionais," 1997, Publicado no Diário Oficial da União em 17 de julho de 1997.

[5] Agência Nacional de Telecomunicações (Anatel), "Regulamento para Avaliação da Conformidade e Homologação de Produtos para Telecomunicações," 2021, Publicado no Diário Oficial da União em 13 de dezembro de 2019.

[6] Presidência da República, "Lei Nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais," 2018, Publicado no Diário Oficial da União em 15 de agosto de 2018.

[7] OWASP Foundation, "Security by Design Principles," 2016, Disponível em: https://wiki.owasp.org/index.php/Security_by_Design_Principles. Acesso em: 31 jul 24.