Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

SEGURANÇA EM DISPOSITIVOS CPE: AVALIAÇÃO DE CONFORMIDADE COM O ATO 2436 DA ANATEL E FRAMEWORK NIST

SECURITY IN CPE DEVICES: COMPLIANCE ASSESSMENT WITH ANATEL'S ACT 2436 AND THE NIST FRAMEWORK

Micael Reino dos Santos
Fatec de Americana
Micael.santos7@fatec.sp.gov.br

Resumo

Este trabalho tem quanto objetivo medir a responsabilidade de dispositivos CPE certificados pela Anatel, com foco nos requisitos do Ato 2436 e na aplicação do Framework NIST. Em um cenário em que a conectividade de dispositivos é cada vez maior, a proteção de equipamentos críticos torna-se indispensável para a responsabilidade das redes de telecomunicações. A pesquisa combina uma decomposição detalhada das exigências regulatórias com testes práticos. Além disso, sanado propostas melhorias com alicerce em boas práticas de responsabilidade para voltar esses dispositivos mais confiáveis. A prática visa tributar-se para a ativação das medidas de proteção em dispositivos largamente utilizados por consumidores e empresas.

Palavras-chave: CPE, Segurança da Informação, Ato 2436, Framework NIST.

Abstract

This study aims to assess the security of CPE devices certified by Anatel, focusing on Ato 2436 and the application of the NIST Framework. In a context of increasing device connectivity, protecting critical equipment is essential for the security of telecommunications networks. The research combines a detailed analysis of regulatory requirements with practical tests. Additionally, improvements are proposed based on security best practices to make these devices more reliable. This study aims to strengthen protection measures for devices widely used by consumers and businesses.

***Keywords**: CPE, Cybersecurity, Anatel, Ato 2436, NIST Framework.*

Fatec Americana Ministro Ralph Biasi

Centro Paula Souza

SÃO PAULO GOVERNO DO ESTADO

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Micael Reino dos Santos

SEGURANÇA EM DISPOSITIVOS CPE: AVALIAÇÃO DE CONFORMIDADE COM O ATO 2436 DA ANATEL E FRAMEWORK NIST

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 02 de dezembro de 2024

Banca Examinadora:

Marcus Vinicius Lahr Giraldi (Presidente)
Especialista
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Marco Antonio da Silveira Campos (Membro)
Especialista
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Lucas Serafim Parizotto (Membro)
Especialista
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

1. Introdução

A constante expansão da conexão dos através da Internet das Coisas (IoT) transformou a maneira como os aparelhos se conectam com as redes de comunicação e os usuários. Contudo, conforme o número de dispositivos ligados cresce exponencialmente, surgem novos obstáculos à segurança cibernética, principalmente obstáculos relacionados aos dispositivos instalados nas instalações do cliente (CPE), como modems e roteadores, que funcionam como uma cerca, responsável por separar redes externas de aparelhos conectadas a redes internas.

A aplicação imprópria ou a não aplicação de mecanismos de segurança nesses aparelhos pode resultar em falhas graves, como a falta de autenticação segura, a utilização de protocolos ultrapassados e configurações padrão vulneráveis. A partir destas falhas, atacantes podem realizar ataques direcionados a dispositivos CPE, como interceptação de tráfego e acesso remoto não permitido, e estes ataques estão se tornando cada vez mais frequentes.

Sabendo da importância da proteção em dispositivos conectados, a Agência Nacional de Telecomunicações (Anatel) estabeleceu normas rigorosas para a certificação de CPEs no Brasil. O Ato 2436, em particular, destaca-se ao definir requisitos técnicos relacionados à implementação de autenticação, criptografia, credenciais seguras e controle de acesso. Alinhada a essas diretrizes, a pesquisa adota também o Framework de Cibersegurança do National Institute of Standards and Technology (NIST), conhecido como uma base sólida para a implementação de controles e para a análise de vulnerabilidades (NIST, 2018).

O objetivo deste trabalho consiste em avaliar a conformidade de dispositivos CPE com alguns dos requisitos do Ato 2436 e propor melhorias na segurança desses equipamentos com base no Framework NIST. Para isso, serão conduzidos testes práticos em dispositivos certificados, focando a análise em algoritmos de criptografia e os serviços habilitados por padrão.

2. Referencial Teórico

A segurança da informação desempenha um papel crucial no contexto da Internet das Coisas (IoT), especialmente em dispositivos de borda como os CPEs (Customer Premises Equipment). Estes equipamentos, incluindo modems e roteadores, são componentes críticos em redes de telecomunicações, uma vez que conectam redes domésticas à internet. No entanto, sua posição estratégica os torna alvos potenciais de ataques cibernéticos.

A literatura especializada em IoT destaca a crescente vulnerabilidade dos dispositivos conectados devido a falhas como autenticação fraca, criptografia obsoleta e utilização de serviços considerados obsoletos. Essas falhas de segurança podem ser exploradas por agentes maliciosos para comprometer a privacidade, a integridade e a disponibilidade dos dados em redes locais e externas. Conforme Anderson e Longa (2006), a introdução de controles robustos, como métodos de autenticação seguros e a aplicação de criptografia atualizada, é fundamental para proteger esses dispositivos contra ameaças modernas.

No Brasil, a Agência Nacional de Telecomunicações (Anatel) desempenha um papel central ao regular a conformidade técnica e de segurança de dispositivos CPE. O Ato 2436, de 2022, estabelece requisitos de segurança que incluem a implementação de autenticação segura, uso de protocolos criptográficos confiáveis e que apenas serviços essenciais estejam habilitados por padrão.

Adicionalmente, o Framework de Cibersegurança do National Institute of Standards and Technology (NIST) fornece uma base teórica e prática que pode ser utillizada para abordar as vulnerabilidades em dispositivos CPE. Este framework é estruturado em cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar, que formam um ciclo contínuo de segurança. Por exemplo, a função "Identificar" inclui o mapeamento de ativos e a análise de vulnerabilidades, enquanto a função Proteger orienta a aplicação de medidas de controle, como firewalls,

autenticação forte e criptografia. Já as funções Detectar e Responder garantem a monitoração contínua e a resposta rápida a incidentes de segurança, enquanto a função "Recuperar" foca na restauração de sistemas afetados, reduzindo o impacto de eventuais ataques (NIST, 2018).

A combinação entre os requisitos estabelecidos pela Anatel e as boas práticas estabelecidas pelo NIST permite que seja realizada uma análise e melhoria da segurança em dispositivos CPE. Este referencial teórico serve como base para os testes realizados no presente estudo, alinhando as diretrizes regulatórias locais a um framework amplamente reconhecido globalmente.

3. Materiais e Métodos (ou Metodologia)

Este trabalho possui uma natureza de pesquisa aplicada, com abordagem experimental, direcionada à análise e implementação de controles de segurança em dispositivos CPEs (Customer Premises Equipment), em conformidade com as diretrizes estabelecidas pelo Ato 2436 da Anatel e pelo NIST Cybersecurity Framework (CSF). A investigação consiste em realizar uma abordagem teórica e prática, envolvendo tanto uma análise bibliográfica quanto a execução de testes empíricos em dispositivos reais.

Seleção dos Dispositivos e Cenário de Teste

O dispositivo escolhido para análise se trata de um CPE, dada sua relevância em redes de telecomunicações domésticas e corporativas. A seleção foi orientada pela representatividade de equipamentos amplamente utilizados e pela presença de certificação Anatel, garantindo que os resultados sejam aplicáveis a cenários reais de conectividade.

Os testes foram conduzidos em um ambiente controlado, simulando condições típicas de uso. As interfaces de gerenciamento local (LAN), remoto (WAN) e sem fio (WLAN) foram analisadas, avaliando a conformidade de controles de segurança

essenciais, como autenticação, gerenciamento de firmware e proteção contra vulnerabilidades.

Procedimentos e Ferramentas

A avaliação prática envolveu o uso de ferramentas reconhecidas em cibersegurança, como o Nmap para análise de portas e serviços, e o Wireshark para captura de tráfego e análise de protocolos. Os testes seguiram os critérios técnicos estabelecidos pela Anatel, com atenção especial às exigências relacionadas ao uso de funções criptográficas seguras e o uso de serviços essenciais e seguros.

Metodologia de Análise

Os resultados foram analisados à luz dos requisitos do Ato 2436, com o objetivo de identificar lacunas de segurança e propor melhorias alinhadas às melhores práticas recomendadas pelo NIST. A abordagem comparativa foi utilizada para avaliar o nível de conformidade dos dispositivos, destacando boas práticas implementadas e vulnerabilidades detectadas. Além disso, foram analisados os impactos potenciais dessas vulnerabilidades, considerando cenários de exploração realistas e o contexto operacional dos dispositivos. Essa análise detalhada buscou fornecer uma visão abrangente do panorama atual de segurança.

Com esta metodologia, o trabalho visa não apenas avaliar o estado atual de segurança dos dispositivos CPE, mas também oferecer diretrizes práticas para mitigar os riscos, fortalecendo a proteção contra ameaças cibernéticas e promovendo a conformidade com os regulamentos vigentes. Essas diretrizes incluem recomendações técnicas e operacionais, como a implementação de criptografia robusta, políticas de atualização frequentes e a adoção de medidas proativas para identificação precoce de ameaças. Tais ações visam não só atender às exigências legais, mas também melhorar a resiliência dos dispositivos frente a ataques sofisticados.

Por fim, o estudo evidencia a importância de um compromisso contínuo com a segurança, destacando a necessidade de colaboração entre fabricantes, reguladores e usuários finais. Essa colaboração é essencial para a criação de um ecossistema confiável e alinhado com os desafios cibernéticos contemporâneos. Os resultados apresentados têm como objetivo servir de referência tanto para profissionais da área quanto para formuladores de políticas, impulsionando melhorias significativas na proteção dos dispositivos CPE e, consequentemente, das redes que os utilizam.

4. Resultados e Discussões

Os testes realizados neste trabalho buscaram avaliar a conformidade de dispositivos CPE em relação aos requisitos de segurança definidos pelo Ato 2436 da Anatel. Esse regulamento estabelece critérios técnicos para proteger dispositivos de telecomunicações contra vulnerabilidades cibernéticas, garantindo a integridade, confidencialidade e disponibilidade das redes.

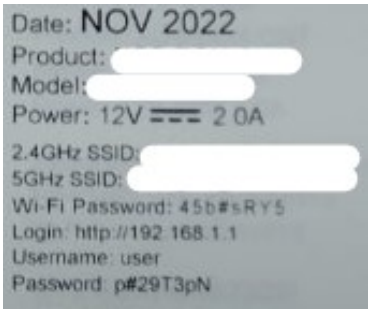
Para estruturar a análise, foram aplicados os princípios do NIST Cybersecurity Framework (CSF), que organiza práticas de segurança em cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar. Essas funções oferecem uma abordagem sistemática para identificar falhas de segurança, implementar controles e melhorar a resiliência dos dispositivos. A seguir, são apresentados os resultados de cada requisito testado, com observações específicas sobre conformidade e vulnerabilidades identificadas.

Senhas providas de fábrica

É necessário que as senhas e credenciais providas de fábrica não sejam fracas, utilizando como base o item 3.1.3 do Ato 2436 da Anatel, uma senha é considerada fraca quando não atende a critérios mínimos, sendo eles possuir 8 caracteres e incluir uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais (Anatel, 2022).

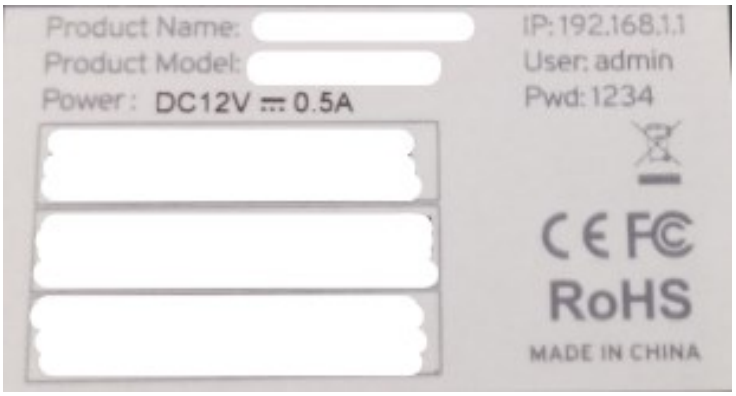
- **Situação analisada:** Analisando as credenciais providas de fábrica presentes nas etiquetas dos dispositivos, foi possível observar que as credenciais se separam em dois grupos:
    - Credenciais que atendem aos requisitos estabelecidos no item 3.1.3 do Ato 2436 da Anatel
    - Credenciais que não atendem aos requisitos estabelecidos no item 3.1.3 do Ato 2436 da Anatel
- **Análise NIST:** Se as senhas iniciais não forem fortes a capacidade de prevenir e detectar acessos não autorizados se torna limitada, o que resulta em um impacto nas funções Proteger e Detectar.

Figura 1 – Credenciais iniciais que atendem aos requisitos contidos no item 3.1.3



Fonte: Autoria própria

Figura 2 – Credenciais iniciais que não atendem aos requisitos contidos no item 3.1.3



Fonte: Autoria própria

Algoritmos de Criptografia

Seguindo o requisito 6.C do Ato 2436, o dispositivo deve proteger as credenciais e informações transmitidas utilizando métodos adequados de criptografia ou hashing.

- **Situação analisada**: Através da captura de pacotes de rede, foram noticiados três possíveis comportamentos que os dispositivos podem realizar enquanto há o tráfego de informações credenciais pela rede:
    - Trafegar informações utilizando funções a fim de esconder as credenciais transmitidas, assim "fortalecendo" o protocolo HTTP
    - Utilizar o protocolo HTTPS e majoritariamente o TLS v1.2
    - Não utilizar HTTPS ou funções que protejam as informções trafegadas através de criptografia ou hashing através
- **Análise NIST**: Caso as credenciais sejam transmitidas de forma criptografada ou através de hashing a função Proteger é atendida, caso contrário, ela não será atendida, tendo em vista que as credenciais estão sendo transmitidas de modo suscetível a captura.

Figura 3 – Pacote contendo valores utilizados para hashing e resultado

```
HTTP/1.1 200 OK
Content-Type: application/javascript; charset=utf-8
Content-Length: 241
Set-Cookie: JSESSIONID=deleted; Expires=Thu, 01 Jan 1970 00:00:01 GMT; Path=/; HttpOnly
Connection: keep-alive

var logoUrl="";
var adminSetting=0;
var userSetting=1;
var ee="010001";
var nn="EBDF71CB0C6957463F8A3792FB2995AAAC1599EFED58F7719D528F7B0AB0CB7558392BA28AC2ED4AE8CDE4AF93F59189E1A8E4D01ABAAE10170EF324D1CC3FF9";
var seq="203318970";
$.ret=0;
POST /cgi_gdpr?9 HTTP/1.1
Host: 192.168.0.1
Connection: keep-alive
Content-Length: 462
Accept: text/plain, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Content-Type: text/plain
Origin: http://192.168.0.1
Referer: http://192.168.0.1/
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

sign=c4217bc635188c530d4ffe36ee3030cf469036f00dc2f394a05cea755c4407c3ee0267cfb81a214943f415e4bf294de44b22ec03d85f2b266670ba383a4ea13f09b3cfb05c573665056d
3e1901ce28adc39c6e611713ba94a6165eb3826989f775887c76d2e352e979e2d7f0fb9ffc49ea204785c9c5fcbcaa58527eb6700800
data=JJRH/K8zlQF1PFPqwoOpjy1YgJ8XWRe02v3PR8Cvce8gmLFreFOZY/ls43e50+zq0ynP4uG2mqspB8iYjEXSK4aoD5tqK0jXsil9LKBq/k0xqZ40Pivlj/TNjxPCKiodtkzeVL/
tCU+DRwnANb8jia+d/CRXsFafXAmwBCl3Y+HxswpnwA4eUhJIicCk2pba
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Set-Cookie: JSESSIONID=4eb4da353a1b555638c15a417fbfed; Path=/; HttpOnly
Connection: keep-alive

HYZDGHHdk/AEhiLk1WZruQ==POST /cgi_gdpr?9 HTTP/1.1
```

Fonte: Autoria própria

Figura 4 – Captura de pacotes evidenciando uso de protocolo HTTPS

17	4.460043013	192.168.1.6	192.168.1.1	TCP	74 53706 → 443 [SYN]
18	4.463171416	192.168.1.1	192.168.1.6	TCP	74 443 → 53706 [SYN,
19	4.463254429	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
20	4.464254256	192.168.1.6	192.168.1.1	TLSv1.2	583 Client Hello
21	4.468361284	192.168.1.1	192.168.1.6	TCP	66 443 → 53706 [ACK]
22	4.543985086	192.168.1.1	192.168.1.6	TLSv1.2	1454 Server Hello, Cer
23	4.544046345	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
24	4.548930293	192.168.1.6	192.168.1.1	TLSv1.2	192 Client Key Exchan
25	4.552320029	192.168.1.1	192.168.1.6	TCP	66 443 → 53706 [ACK]
26	4.562933990	192.168.1.1	192.168.1.6	TLSv1.2	117 Change Cipher Spe
27	4.563231949	192.168.1.6	192.168.1.1	TLSv1.2	1120 Application Data
28	4.581755290	192.168.1.1	192.168.1.6	TLSv1.2	112 Application Data
29	4.591056881	192.168.1.1	192.168.1.6	TLSv1.2	2962 Application Data,
30	4.591117038	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
31	4.595751116	192.168.1.1	192.168.1.6	TLSv1.2	462 Application Data,
32	4.600582502	192.168.1.1	192.168.1.6	TLSv1.2	1514 Application Data,
33	4.600614410	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
34	4.606119343	192.168.1.1	192.168.1.6	TLSv1.2	1490 Application Data,
35	4.627076696	192.168.1.1	192.168.1.6	TLSv1.2	1514 Application Data,
36	4.627128983	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
37	4.631061375	192.168.1.1	192.168.1.6	TLSv1.2	500 Application Data,
38	4.665652266	192.168.1.1	192.168.1.6	TLSv1.2	2962 Application Data,
39	4.665708916	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
40	4.669920991	192.168.1.1	192.168.1.6	TLSv1.2	624 Application Data,
41	4.684578145	192.168.1.1	192.168.1.6	TLSv1.2	1514 Application Data,
42	4.684634661	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
43	4.688941548	192.168.1.1	192.168.1.6	TLSv1.2	321 Application Data,
44	4.702311666	192.168.1.1	192.168.1.6	TLSv1.2	1514 Application Data,
45	4.702368211	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
46	4.706822285	192.168.1.1	192.168.1.6	TLSv1.2	515 Application Data,
62	4.724403663	192.168.1.1	192.168.1.6	TLSv1.2	1514 Application Data,
63	4.724515544	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
64	4.728717573	192.168.1.1	192.168.1.6	TLSv1.2	836 Application Data,
65	4.756034301	192.168.1.1	192.168.1.6	TLSv1.2	1514 Application Data,
66	4.756100630	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
67	4.760063941	192.168.1.1	192.168.1.6	TLSv1.2	378 Application Data,
68	4.763172981	192.168.1.1	192.168.1.6	TLSv1.2	214 Application Data,
69	4.763749117	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [ACK]
70	4.764132590	192.168.1.6	192.168.1.1	TLSv1.2	97 Encrypted Alert
71	4.764262145	192.168.1.6	192.168.1.1	TCP	66 53706 → 443 [FIN,
72	4.767315982	192.168.1.1	192.168.1.6	TCP	60 443 → 53706 [RST]
73	4.767316119	192.168.1.1	192.168.1.6	TCP	60 443 → 53706 [RST]

Fonte: Autoria própria

Figura 5 – Captura de pacotes contendo valor limpo das credenciais utilizadas

```
▸ Frame 37: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits) on interface eth1, id 0
▸ Ethernet II, Src: PCSSystemtec_51:7e:a7 (08:00:27:51:7e:a7), Dst:
▸ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1
▸ Transmission Control Protocol, Src Port: 53328, Dst Port: 80, Seq: 1, Ack: 1, Len: 531
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▸ Form item: "frashnum" = ""
    ▸ Form item: "action" = "login"
    ▸ Form item: "Frm_Logintoken" = "2"
    ▸ Form item: "Username" = "admin"
    ▸ Form item: "Password" = "1234"
```

Fonte: Autoria própria

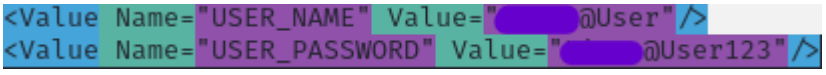
Senhas definidas no código-fonte do software/firmware

Tendo como base o requisito 6.B do Ato 2436, senhas definidas no código fonte (hard-coded) representam um risco significativo para a segurança cibernética, tendo em vista que não podem ser alteradas facilmente e uma vez que são descobertas, vários dispositivos se tornam vulneráveis a ataques.

- **Situação analisada**: Através de uma análise ao código-fonte de software de alguns dispositivos, foram localizadas senhas hard-coded apenas em um.

- **Análise NIST**: Caso o dispositivo possua senhas hard-coded as funções Identificar, Proteger, Detectar e Responder são comprometidas devido às vulnerabilidades que essas credenciais fixas introduzem.

Figura 6 – Credenciais hard-coded para realizar login como usuário comum



Fonte: Autoria própria

Figura 7 – Credenciais hard-coded para realziar login como superusuário

Fonte: Autoria própria

Serviços não essenciais habilitados

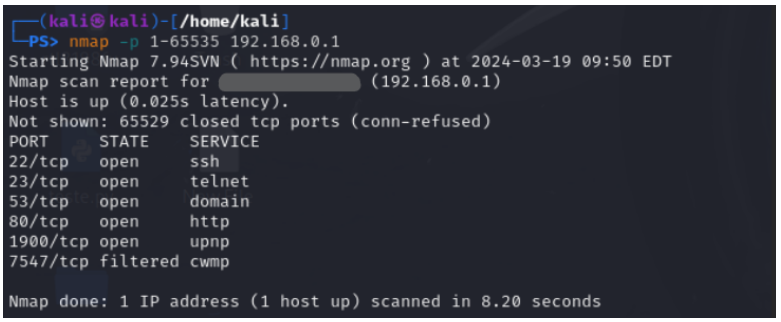
A fim de diminuir a superfície de ataques, os dispositivos devem possuir o máximo de portas e serviços não essenciais desabilitados, conforme mencionado no requisito 6.E do Ato 2436.

- **Situação analisada**: Através de uma varredura realizada nas interfaces LAN, WLAN e WAN utilizando a ferramenta Nmap, foi observado que uma parcela

dos dispositivos não possui portas desnecessárias abertas, contudo, maior parte dos dispositivos possui portas desnecessárias abertas o que resulta em uma vasta superfície de ataque.

- **Análise NIST**: Portas não essenciais habilitadas influenciam todas as funções do NIST, especialmente Identificar e Proteger, que devem ser priorizadas para evitar exploração de falhas conhecidas.

Figura 8 – Resultado de varredura de portas realizado nas interfaces LAN e WLAN



Fonte: Autoria própria

5. Considerações Finais

A segurança de dispositivos Customer Premises Equipment (CPE), desempenha um papel fundamental na proteção dos aparelhos e redes domésticas. Esses dispositivos conectam diretamente os usuários finais às redes de internet e, portanto, caso não possuam as devidas configurações de segurança aplicadas, serão pontos entrada para possíveis ameaças cibernéticas. Este trabalho analisou a conformidade de dispositivos CPE com o Ato 2436 da Anatel, utilizando como suporte as diretrizes do NIST Cybersecurity Framework (CSF).

Os resultados deste estudo apresentaram pontos importantes quanto a segurança de dispositivos CPE, especialmente no que se refere à implementação

de controles de segurança básicos. Falhas como o uso de protocolos de gerenciamento inseguros e algoritmos de criptografia ultrapassados demonstram um desalinhamento crítico com as melhores práticas de cibersegurança. Esses problemas indicam que, embora o Ato 2436 estabeleça requisitos claros para proteger os dispositivos contra ameaças, sua implementação prática apresenta desafios significativos.

Conforme identificado, a segurança por design ainda não é uma prioridade na concepção de muitos dispositivos CPE, algo corroborado por estudos como os de Garfinkel (2005), que destacam a resistência de fabricantes em adotar padrões de segurança mais rigorosos devido a restrições econômicas e operacionais.

Embora o Ato 2436 seja um avanço significativo para a segurança dos dispositivos CPE no Brasil, sua implementação ainda enfrenta desafios práticos. A integração de frameworks reconhecidos, como o NIST CSF, e a adoção de padrões internacionais podem reforçar a segurança dos dispositivos, contribuindo para a proteção das redes e dos dados dos usuários. Ao avançar nesse sentido, espera-se que os CPEs se tornem menos vulneráveis a ataques cibernéticos e mais alinhados às exigências de um mundo digital cada vez mais interconectado.

Referências

ALRAWI, O.; RAZZAK, M.; SUZUKI, D.; SANSERINO, E. SoK: Security Evaluation of Home-Based IoT Deployments. IEEE Symposium on Security and Privacy, 2019.

ANATEL. Ato nº 2436, de 4 de maio de 2020. Agência Nacional de Telecomunicações, 2020. Disponível em: https://www.gov.br/anatel.

ANDERSON, R.; FULORIA, S. On the Security Economics of Electricity Metering. In: Workshop on the Economics of Information Security (WEIS), 2010.

ANTONAKAKIS, M.; PERDISCI, R.; DAHL, S.; CHO, Y.; LEE, W. Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, 2017.

GARFINKEL, S. Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable. ACM Computing Surveys, 2005.

IoT Security Foundation (IoTSF). Establishing Principles for IoT Security. IoTSF Framework, 2018.

JONES, M.; BROWN, L. Securing IoT Devices Using NIST CSF: Challenges and Solutions. Journal of Cybersecurity, 2019.

MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A. Handbook of Applied Cryptography. CRC Press, 1997.

NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2018. Disponível em: https://www.nist.gov/cyberframework.

PONEMON INSTITUTE. Cost of a Data Breach Report. IBM Security, 2020. Disponível em: https://www.ibm.com/security/data-breach.

SALONIKAS, H.; SATHYAMURTHY, M. IoT Security Compliance and Testing Standards. International Journal of Network Security, 2020.

STALLINGS, W. Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson, 2018.

Agradecimentos

A toda minha família.