Ato nº 77, de 05 de janeiro de 2021

Publicado: Terça, 05 Janeiro 2021 10:16 | Última atualização: Quinta, 21 Janeiro 2021 10:48 | Acessos: 1427

Observação: Este texto não substitui o publicado no Boletim de Serviço Eletrônico em 5/1/2021.

O SUPERINTENDENTE DE OUTORGA E RECURSOS À PRESTAÇÃO - ANATEL, no uso das atribuições que lhe foram conferidas pela Resolução n.º 715, de 23 de outubro de 2019, e

CONSIDERANDO a competência dada pelos Incisos XIII e XIV do Art. 19 da Lei n.º 9.472/97 – Lei Geral de Telecomunicações;

CONSIDERANDO o Art. 22 do Regulamento para Avaliação da Conformidade e Homologação de Produtos para Telecomunicações, aprovado pela Resolução n.º 715, de 23 de outubro de 2019;

CONSIDERANDO a Estratégia Nacional de Segurança Cibernética, aprovada por meio do Decreto nº 10.222, de 5 de fevereiro de 2020;

CONSIDERANDO a Lei Geral de Proteção de Dados Pessoais, aprovada pela Lei nº 13.709, de 14 de agosto de 2018;

CONSIDERANDO os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G, aprovados pela Instrução Normativa nº 4, de 26 de março de 2020 do Gabinete de Segurança Institucional da Presidência da República;

CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

CONSIDERANDO que a Resolução nº 740, de 21 de dezembro de 2020, que aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, estabelece que o tema da avaliação da conformidade de equipamentos para telecomunicações, quanto à segurança cibernética, deve ser objeto dos procedimentos de avaliação da conformidade e homologação dos produtos para telecomunicações; e

CONSIDERANDO o constante dos autos do processo nº 53500.026122/2019-70,

R E S O L V E :

Art. 1º Aprovar os Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações, nos moldes do Anexo a este Ato.

Art. 2º Este Ato entra em vigor 180 (cento e oitenta) dias após a data de sua publicação no Boletim de Serviços Eletrônico da Anatel.

VINICIUS OLIVEIRA CARAM GUIMARÃES

Superintendente de Outorga e Recursos à Prestação

ANEXO AO ATO Nº 77, DE 05 DE JANEIRO DE 2021

REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES

1. OBJETIVO E ABRANGÊNCIA

1.1. Estabelecer um conjunto de requisitos de segurança cibernética para equipamentos para telecomunicações visando minimizar ou corrigir vulnerabilidades por meio de atualizações de *software/firmware* ou por meio de recomendações em configurações.

1.1.1. Este documento abrange os produtos relacionados na Lista de Referência de Produtos para Telecomunicações publicada pela Agência Nacional de Telecomunicações que possuem função de equipamento terminal com conexão à Internet ou de equipamento de infraestrutura de redes de telecomunicações.

1.2. No caso de certificação e homologação iniciais dos equipamentos, o requerimento de homologação deverá conter uma declaração do interessado informando a quais requisitos listados neste documento o produto e seu fornecedor atendem.

1.2.1. A qualquer tempo, por meio do programa de Supervisão de Mercado, a Anatel poderá avaliar se o produto homologado e seu fornecedor estão em conformidade com a declaração inserida no requerimento de homologação.

1.3. Quaisquer falhas de segurança cibernética identificada 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.

2. REFERÊNCIAS

2.1. Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações, aprovado pela Resolução n.º 715, de 23 de outubro de 2019.

2.2. OECD - Enhancing the Digital Security of Products - Draft Scoping Paper (November 2019).

2.3. IEEE Internet Technology Policy Community White Paper - Internet of Things (IoT) Security Best Practices (February 2017).

2.4. IETF - Internet of Things (IoT) Security: State of the Art and Challenges - RFC 8576.

2.5. LAC-BCOP-1 (May/2019) – Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition.

2.6. Documento conjunto LACNOG-M3AAWG: Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1 - Maio 2019.

2.7. ENISA - Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures (November 2017).

2.8. GSMA IoT Security Guidelines – Complete Document Set.

2.9. ETSI GS NFV-SEC 001 V1.1.1 (2014-10) - Network Functions Virtualisation (NFV); NFV Security; Problem Statement.

2.10. GSMA - FS.16 - Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements.

2.11. Council to Secure the Digital Economy - The C2 Consensus on IoT Device Security Baseline Capabilities.

2.12. ISO/IEC 27402 — Cybersecurity — IoT security and privacy — Device baseline requirements [DRAFT].

2.13. Lei Geral de Proteção de Dados Pessoais, aprovada pela Lei nº 13.709, de 14 de agosto de 2018.

2.14. FIRST *Vulnerability Coordination SIG / Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure,* acessível *em:* https://www.first.org/global/sigs/vulnerability-coordination.

2.15. Common Vulnerability Scoring System (CVSS), acessível em: https://www.first.org/cvss.

2.16. ETSI EN 303 645 v2.1.1 (2020-06) - *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*.

2.17. ETSI TS 133 117 V16.5.0 (2020-08) - *Universal Mobile Telecommunications System (UMTS); LTE; Catalogue of general security assurance requirements*.

2.18. Conjunto de especificações Técnicas do 3GPP: SCAS - *Security Assurance Specifications*, acessível em: https://www.3gpp.org/DynaReport/WiSpec--790015.htm.

2.19. EU 5G Security Toolbox, acessível em: https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security.

3. DEFINIÇÕES

3.1. Algoritmos de criptografia: algoritmos baseados na ciência da criptografia, abrangendo algoritmos de encriptação/decriptação, algoritmos de *hash* criptográficos, algoritmos de assinatura digital e algoritmos de trocas de chaves.

3.2. Backdoor: mecanismo não documentado contido no *software/firmware* do produto que possibilita acesso não autorizado ao equipamento. A presença de *backdoors* no produto final pode ser intencional ou acidental.

3.3. Customer Premise Equipment (CPE): equipamento utilizado para conectar assinantes à rede do provedor de serviços de telecomunicações. Para fins de aplicação deste conjunto de requisitos, CPE deve ser considerado o equipamento associado aos serviços fixos de telecomunicações.

3.4. Dados pessoais: adota-se a definição contida na Lei Geral de Proteção de Dados Pessoais.

3.5. Dados pessoais sensíveis: adota-se a definição contida na Lei Geral de Proteção de Dados Pessoais.

3.6. Firmware: *software* acessível somente para leitura, programado em um hardware de propósito específico e armazenados de forma funcionalmente independente do armazenamento principal do equipamento.

3.7. Fornecedor: é o solicitante da homologação do equipamento para telecomunicações, podendo ser o próprio fabricante nacional do equipamento ou o representante nacional de um fabricante estrangeiro.

3.8. Hashing: algoritmo matemático baseados em padronização internacionalmente reconhecida que mapeia dados de comprimento variável na entrada de uma função para um conjunto de dados de comprimento fixo na saída da função.

3.9. Métodos adequados de criptografia: protocolos ou algoritmos criptográficos, baseados em padronização internacionalmente reconhecida, em suas versões atualizadas. A implementação deve permitir a seleção de conjuntos de cifras e tamanhos de chave atualizados, e implementar as exclusões especificadas no padrão no que se refere a elementos considerados obsoletos.

3.10. Métodos adequados de autenticação: protocolos ou algoritmos de autenticação baseados em padronização internacionalmente reconhecida, em suas versões atualizadas. Diferentes tecnologias e fatores de autenticação podem ser empregados (por exemplo, *chip* criptográfico, *tokens*, biometria, etc.). A implementação não deve utilizar credenciais de autenticação (exemplo: senhas, chaves criptográficas) com valores comuns fixados no código-fonte (*hard-coded*).

3.11. Supervisão de mercado: procedimento de fiscalização especificado no Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações.

3.12. Usuário: aquele manipula, configura, se aproveita das utilidades e está sujeito aos impactos resultantes de vulnerabilidades e falhas apresentadas por equipamentos para telecomunicações.

3.13. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

4. ORIENTAÇÕES GERAIS

4.1. Ao requerer a homologação do produto para telecomunicações junto à Anatel, o requerente deve apresentar uma declaração:

a) indicando que o produto foi desenvolvido em observância ao princípio de *security by design;*

b) relacionando a quais requisitos deste documento o equipamento e seu fornecedor atendem naquele momento; e

c) reconhecendo ter ciência de que os requisitos de segurança cibernética estão sujeitos a atualizações, inclusive normativas e administrativas, em compasso com o desenvolvimento tecnológico, com o surgimento de novas ameaças ou vulnerabilidades.

4.1.1. O escopo da declaração deve considerar as diferentes características técnicas dos equipamentos (quantidade de memória, capacidade de processamento de dados, interfaces do usuário, interfaces de comunicação, características e versões do sofware/firmware - não se limitando a estas) e os fins a que se destinam, apontando quais são os requisitos atendidos.

4.1.2. Para produtos enquadrados na definição de CPE, a declaração deve orientar-se, adicionalmente, pelo conjunto de requisitos contidos na referência 2.5.

4.2. Nas atividades de Supervisão de Mercado, a Agência poderá avaliar se o produto e seu fornecedor mantêm conformidade aos requisitos deste documento.

4.3. Identificada, no produto homologado, qualquer falha ou vulnerabilidade que afete a segurança de seus usuários ou das redes de telecomunicações do país , a Agência notificará o responsável pela homologação a sana-la, indicando prazo adequado para esse fim, considerando-se o grau de severidade da vulnerabilidade, avaliado conforme o *Common Vulnerability Scoring System* (CVSS) (referência 2.15).

4.3.1. O prazo estipulado para a correção das vulnerabilidades poderá ser prorrogado, a critério da Agência, com base em ponderações apresentadas pelo solicitante da homologação e na complexidade do problema.

4.3.2. Decorrido o prazo sem que se verifique as correções necessárias ou sem apresentação de justificativa aceita pela Anatel para não implementação das correções, a Agência poderá suspender a homologação do produto e indicar o recolhimento ou substituição do mesmo no mercado, garantidas as demais previsões regulamentares referentes ao direito do consumidor.

4.3.3. A suspensão da homologação do equipamento será mantida até que as vulnerabilidades apontadas sejam sanadas ou até que o potencial risco à segurança dos usuários ou dos serviços para telecomunicações seja mitigado, considerando-se o prazo máximo estabelecido na regulamentação vigente.

4.3.4. Após o prazo máximo determinado para sua suspensão, a homologação será cancelada, caso a vulnerabilidade não seja solucionada.

5. REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES

5.1. Requisitos para equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações, em suas versões finais destinadas à comercialização:

5.1.1. Quanto à atualização de *software/firmware*:

a) Possuir mecanismos automatizados e seguros para atualização de *software/firmware* que empregam métodos adequados de criptografia, autenticação e verificação de integridade.

b) Permitir que os usuários verifiquem, de forma manual, a disponibilidade de atualizações de *software/firmware* e as implementem facilmente.

c) Possuir mecanismos para informar ao usuário as alterações de *software/firmware* implementadas devido às atualizações, especialmente aquelas relacionadas à segurança.

d) Preservar as configurações existentes no equipamento após finalizado o procedimento de atualização. Alterações na configuração dos equipamentos podem ser implementadas no processo de atualização somente se resultarem em melhorarias na segurança do dispositivo.

5.1.2. Quanto ao gerenciamento remoto:

a) Possuir mecanismo para gerenciamento e administração remotos que empreguem métodos adequados de autenticação e criptografia.

b) Implementar mecanismos de controle de acesso às interfaces de gerenciamento e administração remotos, de tal forma a limitar o acesso quanto à origem (por exemplo, segmento de rede específico, URL selecionada, etc.).

5.1.3. Quanto à instalação e à operação:

a) Implementar rotinas simplificadas adequadas para sua instalação e configuração, evitando potenciais falhas de segurança não intencionais.

b) Por padrão de fábrica, o dispositivo deve ser configurado de forma restritiva ao invés de forma permissiva. A seleção de parâmetros para as configurações iniciais de fábrica deve primar por opções nativamente seguras, alinhadas aos princípios de segurança e privacidade.

c) Realizar verificação da integridade do *software/firmware* durante a inicialização do sistema, sendo capaz de alertar ao usuário nos casos de comprometimento de sua integridade.

d) Possuir mecanismo de monitoramento de comportamentos não usuais do *software/firmware*, alertando o usuário ou reiniciando-se automaticamente caso um comportamento suspeito seja detectado. Após reinicialização deverá ser ofertada ao usuário a opção de restauração do equipamento aos padrões de fábrica.

e) Implementar ferramenta de registro de atividades (*logs*) relacionadas à, no mínimo, autenticação de usuários, alteração de configurações do sistema e funcionamento do sistema.

f) Fornecer documentação que descreva, no mínimo, o nome, a versão e as funcionalidades do *software/firmware* e/ou sistema operacional, bem como nome completo e versão de cada *software* de código aberto incorporado ao sistema. A documentação pode ser em formato eletrônico.

5.1.4. Quanto ao acesso para configuração do equipamento:

a) Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.

b) Não utilizar senhas iniciais que sejam derivadas de informações de fácil obtenção por métodos de escaneamento de tráfego de dados em rede, tal com endereços MAC - *Media Access Control*.

c) Forçar, na primeira utilização, a alteração da senha inicial de acesso à configuração do equipamento.

d) Não permitir o uso de senhas em branco ou senhas fracas.

e) Possuir mecanismos de defesa contra tentativas exaustivas de acesso não autorizado (ataques de autenticação por força bruta).

f) Garantir que os mecanismos de recuperação de senha sejam robustos contra tentativas de roubo de credenciais.

g) Não utilizar credenciais, senhas e chaves criptográficas definidas no próprio código fonte do *software/firmware* e que não podem ser alteradas (*hard-coded*).

h) Proteger senhas, chaves de acesso e credenciais armazenadas ou transmitidas utilizando métodos adequados de criptografia ou *hashing*.

i) Implementar rotinas de encerramento de sessões inativas (*timeout*).

5.1.5. Quanto aos serviços de comunicação de dados:

a) Estar desprovido de qualquer ferramenta de teste ou *backdoor* utilizados nos processos de desenvolvimento do produto e desnecessários à sua operação usual.

b) Estar desprovido de qualquer forma de comunicação não documentada, incluindo aquelas para envio de informações de perfil de uso do equipamento para fabricantes ou para terceiros.

c) Ser fornecido com serviços de comunicação de dados (serviço associado a uma porta/*port*) não usualmente utilizados desabilitados, reduzindo sua superfície de ataque.

d) Facultar ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais à operação ou ao gerenciamento do equipamento.

5.1.6. Quanto aos dados pessoais e dados pessoais sensíveis, observada a legislação vigente:

a) Possibilitar a utilização de métodos adequados de criptografia para a transmissão de dados sensíveis, incluindo informações pessoais.

b) Possibilitar a utilização de métodos adequados de criptografia para o armazenamento de dados sensíveis, incluindo informações pessoais.

c) Permitir que os usuários deletem facilmente seus dados pessoais e sensíveis armazenados, possibilitando o descarte ou a substituição do equipamento sem riscos de exposição de informações pessoais.

d) Conter em sua documentação informações ao usuário sobre quais dados pessoais, sensíveis ou não, são coletados, utilizados e armazenados.

5.1.7. Quanto à capacidade de mitigar ataques:

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.

6. REQUISITOS PARA FORNECEDORES DE EQUIPAMENTOS PARA TELECOMUNICAÇÕES

6.1. Requisitos para fornecedores de equipamentos terminais que se conectam à Internet e de equipamentos de infraestrutura de redes de telecomunicações:

6.1.1. Possuir uma política clara de suporte ao produto, especialmente em relação à disponibilização de atualizações de *software/firmware* para correção de vulnerabilidades de segurança.

6.1.2. Deixar claro para o consumidor até quando e em quais situações serão providas atualizações de segurança para o equipamento.

6.1.3. Quando o equipamento dispuser de processos de atualização automática de *software/firmware,* garantir que as atualizações sejam realizadas em fases (em partes da totalidade de dispositivos) a fim de evitar que erros não intencionais da nova versão de *software/firmware* sejam distribuídos simultaneamente a todos os equipamentos passíveis de atualização.

6.1.4. Garantir o provimento de atualizações de segurança por, no mínimo, 2 (dois) anos após o lançamento do produto ou enquanto o equipamento estiver sendo distribuído ao mercado consumidor, sendo aplicável a opção que mais se estender.

6.1.5. Disponibilizar um canal de comunicação que possibilite aos seus clientes, usuários finais e terceiros reportarem vulnerabilidades de segurança identificadas nos produtos.

6.1.6. Possuir implementados processos de Divulgação Coordenada de Vulnerabilidades baseados em boas práticas e recomendações reconhecidas internacionalmente.

6.1.7. Disponibilizar um canal público de suporte, por meio de página na internet em língua portuguesa, para:

a) Informar sobre novas vulnerabilidades identificadas em seus produtos, medidas de mitigação e correções de segurança associadas;

b) Manter histórico de: vulnerabilidades identificadas, medidas de mitigação e correções de segurança;

c) Permitir acesso a correções de segurança e/ou novas versões de *software/firmware* para seus produtos; e

d) Fornecer manuais e outros materiais com orientações relativas à configuração, atualização e uso seguro dos equipamentos.

7. DISPOSIÇÕES FINAIS

7.1. Considerando as ininterruptas evoluções tecnológicas do setor de telecomunicações e o incessante surgimento de novas ameaças à segurança cibernética para equipamentos de telecomunicações, este documento está sujeito a atualizações a fim de manter-se alinhado ao estado da arte do setor, à regulamentação expedida pela Anatel e a outras medidas por ela adotadas.

7.2. A declaração do fornecedor, citada no item 4 deste documento, deve ser apresentada em português conforme modelo publicado na página da Anatel na internet.

7.3. A gerência da Anatel competente pela certificação e homologação de produtos poderá aceitar, para fins de comprovação de atendimento aos requisitos listados neste documento, declarações de que o equipamento atende a normas ou recomendações internacionais que possuam escopo alinhado aos Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações.

7.4. A leitura dos documentos referenciados no item 2 (Referências), incluindo suas atualizações, é fortemente recomendada.

7.4.1. Os *links* para páginas da internet contidos nas referências estão sujeitos a alterações, sendo necessária a busca pelos documentos nos casos em que os *links* estiverem inoperantes.