DIÁRIO OFICIAL DA UNIÃO

Publicado em: 27/03/2020 | Edição: 60 | Seção: 1 | Página: 2

Órgão: Presidência da República/Gabinete de Segurança Institucional

INSTRUÇÃO NORMATIVA Nº 4, DE 26 DE MARÇO DE 2020

Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso das atribuições dos incisos I e II do parágrafo único do art. 87 da Constituição e tendo em vista o disposto no inciso V do art. 10 da Lei nº 13.844, de 18 de junho de 2019; no art. 12 do Decreto nº 9.637, de 26 de dezembro de 2018; no Decreto nº 10.139, de 28 de novembro de 2019; e conforme o disposto no Decreto nº 10.222, de 5 de fevereiro de 2020, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º A presente Instrução Normativa trata dos requisitos mínimos de segurança cibernética que deverão ser adotados no estabelecimento das redes de 5ª geração (5G) de telefonia móvel, de cumprimento obrigatório pelos órgãos e entidades da administração pública federal encarregados da implementação das redes 5G.

Art. 2º Para os fins desta instrução normativa, considera-se:

I - cessionária: fabricante de equipamentos de telecomunicações que compõem a infraestrutura das redes de quinta geração;

II - prestadora, provedora ou operadora de serviços de telecomunicações: pessoa jurídica que fornece o serviço de telecomunicações, mediante concessão, permissão ou autorização por parte do Governo;

III - redes de núcleo: redes pertencentes às prestadoras de serviços de telecomunicações;

IV - **roaming**: capacidade de enviar e receber dados na telefonia móvel por intermédio de redes móveis fora do local em que a própria companhia fornece os serviços, numa zona onde o serviço é provido por outra operadora;

V - solução **end-to-end**: solução que busca controlar um processo do seu início até o seu término; e

VI - IPV6: evolução do padrão de endereçamento atual (IPV4) onde, ao invés de endereços de 32 bits, são usados endereços de 128 bits.

Parágrafo único. Os demais conceitos relacionados à temática dessa Instrução Normativa poderão ser consultados no Glossário de Segurança da Informação, aprovado pela Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República.

Art. 3º Os requisitos estabelecidos neste ato buscam elevar a proteção da sociedade e das instituições nacionais, em face da possibilidade de existência de vulnerabilidades e **backdoors** em sistemas de tecnologia 5G.

Parágrafo Único. As vulnerabilidades e **backdoors** existentes nos equipamentos 5G, implementadas de forma intencional ou involuntária pelos fornecedores da tecnologia, poderão ocasionar o comprometimento da segurança do sistema.

Art. 4º Os requisitos mínimos de segurança cibernética constantes da presente norma atendem aos seguintes princípios de:

I - interoperabilidade;

II - disponibilidade;

III - integridade;

IV - autenticidade;

V - diversidade;

VI - confidencialidade;

VII - prioridade; e

VIII - responsabilidade.

CAPÍTULO II

REQUISITOS MÍNIMOS DE SEGURANÇA CIBERNÉTICA

Art. 5º Cabe aos órgãos e entidades da administração pública federal encarregados da implementação das redes e dos sistemas 5G, em todos os atos administrativos relativos a essa tecnologia, a observância do cumprimento dos seguintes requisitos mínimos de segurança cibernética:

I - a empresa prestadora de serviços de telecomunicações deverá exigir que os serviços prestados e os equipamentos utilizados cumpram os protocolos de comunicação e as especificações técnicas de infraestrutura reconhecidos pela Agência Nacional de Telecomunicações ou, na sua ausência, aqueles estabelecidos pela Associação Brasileira de Normas Técnicas (ABNT) ou reconhecidos internacionalmente;

II - a empresa prestadora de serviços de telecomunicações, nos termos da legislação vigente, deverá dispor de mecanismos de interoperabilidade com as demais prestadoras, por meio de mecanismos seguros;

III - a fim de evitar que redes **roaming** acessem os sistemas de núcleo, as empresas prestadoras de serviço deverão implementar o SEPP (**Security Edge Protection Proxy**) no 5G para fornecer as seguintes funções de proteção nas fronteiras daquelas redes:

a) esconder a topologia;

b) filtrar mensagens;

c) estabelecer canais TLS (**Transport Layer Security**); e

d) implementar proteção de segurança na camada de aplicação para mensagens do tipo **roaming** através de redes IPX (**Internetwork Packet Exchange**);

IV - a empresa prestadora de serviços deverá cumprir a regulamentação da Agência Nacional de Telecomunicações, especialmente a que se refere à qualidade e à disponibilidade do serviço prestado, destacando-se a previsão e o teste de rotas alternativas para o tráfego de dados, no caso de a infraestrutura de determinada cessionária estar comprometida. Quando a temática estiver relacionada às rotas alternativas, deve-se prever uso de infraestrutura de outras prestadoras em casos emergenciais;

V - a empresa prestadora de serviços deverá implementar as funções de detecção e de mitigação de "tempestades" de pacotes maliciosos, de forma a prevenir e minimizar os efeitos de ataques cibernéticos do tipo negação de serviço DDoS (**Distributed Denial of Service**), sem prejuízo de que pelo

menos uma das funções possua a responsabilidade de prever o monitoramento de metadados de tráfego de rede, para identificação de padrões anormais;

VI - a empresa prestadora de serviços deverá habilitar mecanismos para verificação da integridade dos dados trafegados nas redes 5G, no caso de estes mecanismos estarem disponíveis pela tecnologia, em consonância com as normas expedidas pela Agência Nacional de Telecomunicações;

VII - a empresa provedora de serviços deverá implementar o isolamento de segurança NFV (**Network Function Virtualization**) como uma solução **end-to-end** que estará, obrigatoriamente, disponível nos equipamentos a serem utilizados, os quais adotarão ao menos os padrões nos moldes do SEC009 (**Multi-tenant hosting management security**) e do SEC002x (**Security feature management of open source software**), definidos pela ETSI (**European Telecommunications Standards Institute**);

VIII - a empresa provedora de serviços deverá habilitar os mecanismos de autenticação para os dados trafegados utilizando o protocolo IPV6, a fim de se evitar o tráfego de dados forjados, sem prejuízo da proteção da origem dos dados trafegados;

IX - deve-se promover a diversidade de provedoras de serviço por região e por faixas de frequências com intuito de promover a concorrência e a consequente qualidade dos serviços prestados, bem como a sua continuidade no caso de falha de prestação de serviços por determinada prestadora de serviços ou cessionária;

X - as prestadoras de serviço deverão subcontratar fornecedores distintos, de forma que uma mesma área geográfica possua, pelo menos, duas prestadoras utilizando equipamentos de fornecedores distintos;

XI - as empresas prestadoras de serviços deverão habilitar camada de proteção criptográfica dos dados a serem trafegados na rede 5G, em conformidade com as normas expedidas pela Agência Nacional de Telecomunicações;

XII - as redes 5G deverão permitir a adoção de protocolos adicionais de criptografia por parte dos usuários, principalmente as relacionadas às infraestruturas críticas;

XIII - os **softwares** utilizados nos equipamentos de infraestrutura de redes 5G deverão ser, preferencialmente, abertos e serão passíveis de auditoria em termos de segurança;

XIV - diante da eventual exploração de uma vulnerabilidade e da consequente necessidade de "derrubar" um nó de rede a fim de isolá-lo, a prestadora de serviços deverá, sempre que possível, selecionar o nó com menor prioridade, ou seja, aquele que não afete as infraestruturas críticas;

XV - é obrigatória a utilização de processos de auditoria que assegurem a segurança cibernética dos sistemas utilizados na rede 5G, podendo ser fornecidos de forma conjunta com as prestadoras de serviços e empresas interessadas em fornecer tecnologia 5G;

XVI - a atividade de auditoria deve, preferencialmente, englobar empresas, consumidores, parceiros, governo e instituições de pesquisa, além de incentivar o trabalho conjunto de tais atores, para garantir a qualidade necessária em termos de segurança, tendo como resultado deste trabalho as informações essenciais para a tomada de decisão sobre a possibilidade de uso dos equipamentos ofertados;

XVII - deverá ser designado órgão central do sistema de auditoria para coordenação de tal atividade, com intuito de verificar a conformidade com os requisitos mínimos estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República e com outros requisitos que vierem a ser estabelecidos ou adotados pelo órgão;

XVIII - cabe à empresa prestadora de serviços manter os aspectos de segurança da informação, quais sejam: disponibilidade, integridade, e confidencialidade na atividade de tráfego na rede 5G, em cumprimento às recomendações deste ato normativo, sem prejuízo, em caso de comprometimento da segurança, da esfera penal, cível e administrativa;

XIX - na hipótese de se apurar grave falha de segurança, intencional ou não, que comprometa as informações e a proteção de dados pessoais, a empresa prestadora de serviço e as cessionárias subcontratadas responderão na medida de suas responsabilidades, nos termos da legislação correspondente;

XX - as prestadoras de serviço deverão fornecer mecanismos que possibilitem inspeção, inclusive a sua auditoria, em equipamentos em produção, até mesmo com a retirada de **hardware** para avaliação em laboratório;

XXI - mensalmente, as prestadoras de serviço deverão registrar o estado de configuração dos equipamentos de sua rede (resultado do gerenciamento de configuração), contendo informações como topologia de rede, versões de **hardware** e de **software** dos equipamentos, a fim de auxiliar a atividade de auditoria; e

XXII - os incidentes de segurança cibernética ocorridos deverão ser informados, imediatamente, ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO III

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 6º Esta Instrução Normativa entra em vigor na data de sua publicação.

AUGUSTO HELENO RIBEIRO PEREIRA