S.  R.

MINISTÉRIO DAS OBRAS PÚBLICAS TRANSPORTES E COMUNICAÇÕES

COMISSÃO DE PLANEAMENTO DE EMERGÊNCIA DAS COMUNICAÇÕES

C. P. E. C.

Contributo da CPEC para a Consulta pública sobre a abordagem regulatória às novas redes de acesso (NRA)

Questão 3:
Identifica a nível das NRA algum aspecto relacionado com as questões de **segurança e emergência** que justifiquem particular atenção?

1 – Aspectos Gerais

É reconhecido por todas as entidades envolvidas no sector das comunicações electrónicas que às Redes de Nova Geração (RNG), baseadas no protocolo IP, se apresentam um conjunto de potenciais desafios cuja resolução se tem revelado bastante complexa:

- Roubo de identidade do utilizador
- Garantir a privacidade do utilizador
- Roubo de identidade das aplicações
- Exposição da rede a aplicações de terceiros
- Recusa de Serviço (DoS)
- Captura e distribuição de conteúdos não autorizados
- Dificuldades acrescidas na manutenção da integridade dos dados
- Normas de segurança inadequadas

Estes desafios colocam dificuldades acrescidas, em termos de segurança, às RNG, sendo necessário assegurar um conjunto de funções essenciais para o seu correcto funcionamento:

- Autenticação e controle do acesso
- Não-repudiação
- Confidencialidade
- Segurança das comunicações

- Integridade dos dados
- Disponibilidade
- Privacidade

Sendo as RNG baseadas na transferência de “pacotes”, será previsível que a realização de grande parte das funções de segurança atrás referenciadas recaia nos equipamentos associados às redes de acesso, nomeadamente nos equipamentos terminais e nos equipamentos (DSLAM’s, p. ex.) instalados nos armários intermédios (necessários em qualquer das configurações possíveis – FTTH, FTTCab, FTTCurb, FTTNode, FTTBuilding, etc.).

Neste contexto e apesar de, como é referido no texto de apoio, o CPE não se enquadrar no âmbito desta consulta, parece-nos que as suas capacidades em termos de controlo de segurança - nomeadamente a autenticação e o controle de acesso, a encriptação/desencriptação de dados, o reconhecimento de chamadas de emergência, etc. - terão de ser objecto de particular atenção.

O mesmo se aplica aos equipamentos de rede a que o CPE está ligado: deverão ter rotinas de segurança capazes de validar as comunicações efectuadas e de neutralizar (ou pelo menos minimizar) quaisquer ataques “lógicos” a que sejam sujeitos, tanto do equipamento terminal como os oriundos da própria rede.

Ainda em relação a estes equipamentos, existem outros factores que, na nossa perspectiva, deverão ser avaliados no contexto da NRA’s:

- Se, por um lado, a sua dispersão os torna mais vulneráveis a ataques físicos e falhas locais de energia, por outro, a sua concentração (eventual co-locação) resultará num acréscimo de vulnerabilidade face a incidentes não programados (fogos, ataques terroristas, etc.).

- Situação semelhante poderá ocorrer no que respeita à partilha de condutas decorrente da necessidade da instalação dos meios de transmissão associados, uma vez que a rede local de condutas não está, normalmente, projectada para suportar meios de transmissão de várias origens, obrigando à sua concentração e consequente aumento da sua vulnerabilidade; acresce que essa rede já se encontra parcialmente ocupada pelas infra-estruturas necessárias à operação das redes já existentes.

2 – Infra-estruturas Críticas

Outra questão que se coloca tem a ver com a criticidade das infra-estruturas de comunicações: parece-nos indiscutível que a futura infra-estrutura de comunicações electrónicas e, em particular, a sua componente de acesso, será, à semelhança do que se passa com a existente, considerada como infra-estrutura crítica, em relação à qual a dependência de outras infra-estruturas se acentuará cada vez mais.

Nesta perspectiva, consideramos que se deverá, desde o início e em conjunto com todas as entidades relevantes, pôr em prática um conjunto de iniciativas que permitam identificar eventuais constrangimentos decorrentes da utilização destas novas redes, nomeadamente

- Definição, identificação e priorização comuns de serviços críticos em caso de ocorrências de incidentes graves e elaboração dos respectivos planos de restauro;

- Elaboração e implementação de procedimentos para a priorização de capacidades de comunicação com o objectivo de salvaguardar comunicações consideradas vitais, independentemente das soluções específicas já existentes ou em curso (p. ex. RNSI ou SIRESP);

- Avaliação do modo como as NRA's poderão afectar as interdependências existentes entre o sector das comunicações e as restantes infra-estruturas críticas;

- Estabelecimento de acordos para a partilha de informação (nomeadamente registo dos incidentes ocorridos) que permita a protecção e o rápido restauro das infra-estruturas críticas;

- Desenvolvimento de consensos entre os vários operadores para a elaboração de programas de teste entre as várias redes (RNG e existentes) a fim de verificar a ausência de problemas na sua interligação;

- Utilização de um conjunto de normas comuns a fim de evitar problemas de interligação e interoperabilidade entre as diversas redes e equipamentos

3 – Casos particulares: Emergência e Intercepção Legal

É sabido que a migração para as RNG, baseadas no protocolo IP, dificulta a prestação de alguns serviços, em particular *o acesso a serviços de emergência* e *a_possibilidade de intercepção legal de comunicações para aplicação da lei e para defesa da segurança nacional*.

De facto, *o acesso a serviços de emergência* é problemático nestas redes devido a não estarem adstritos a uma localização geográfica fixa: eles podem deslocar-se facilmente (nomadismo).

Esta "nomacidade" coloca grandes desafios à prestação de serviços de emergência, uma vez que as soluções existentes assentam na existência de uma localização geográfica fixa. De facto, os serviços de emergência

necessitam de “conhecer” a localização da chamada, não só para envio de equipas de resposta à emergência para o endereço correcto, mas também, *e à partida*, para contactar com as equipas mais adequadas ao tipo de acidente que estejam mais próximas do local da ocorrência.

Aparentemente, só a médio-longo prazo é que as soluções técnicas para resolver, de forma cabal, esta questão irão aparecer, pelo que, num futuro próximo, é previsível que o acesso aos serviços de emergência, no que respeita aos utilizadores “nómadas” fique sujeito a falhas e a imprecisões. Parece-nos, pois, essencial, *que se ponha em prática a posição acordada no ERG sobre esta matéria*, ou seja:

Que as chamadas de emergência VoIP feitas de locais fixos ou conhecidos devem ser roteadas para o centro de emergência mais próximo na base do endereço físico acordado contratualmente; quando um número de emergência é chamado, a informação da localização do chamador deverá ser fornecida, desde que tecnicamente viável. Nos casos em que a localização do chamador não possa ser determinada pelo fornecedor de serviços VoIP (nomeadamente no caso do uso “nómada” de serviços VoIP), o utilizador final deverá ser informado com clareza e sem quaisquer ambiguidades pelo prestador de serviços VoIP sobre a existência de quaisquer restrições ao roteamento de chamadas de emergência e fornecimento da informação respeitante à localização da chamada, bem como das potenciais consequências de tais limitações.

Finalmente, e no tocante à *intercepção legal de comunicações*, sabe-se que as soluções existentes, baseadas que são nas características próprias das redes de comunicações existentes, não podem ser aplicadas no caso das RNG, comprometendo, assim, a precisão na obtenção dos dados sem afectar a privacidade dos restantes utilizadores. Consideramos, no entanto, ser essencial que as RNG apresentem soluções que permitam garantir a

segurança e a salvaguarda do Estado; assim, eventuais soluções para resolver esta questão (as quais, na nossa perspectiva, se concentrarão no acesso local e deverão ser complexas e dispendiosas) *deverão ser parte integrante da oferta de serviços*.