APRITEL

SEGURANÇA E INTEGRIDADE DAS COMUNICAÇÕES ELECTRÓNICAS

Resposta da Associação dos Operadores de Telecomunicações à Consulta Pública sobre Comunicação de Violações de Segurança e Perdas de Integridade de Redes e Serviços de Comunicações Electrónicas e Existência de Interesse Público na sua Divulgação

27 de Janeiro de 2012

I. COMENTÁRIOS INTRODUTÓRIOS

Na sequência da consulta pública lançada pelo ICP-ANACOM, no passado dia 30.12.2011, referente aos Projetos de Decisão relativos às circunstâncias, formato e procedimentos aplicáveis à comunicação das violações de segurança ou das perdas de integridade com impacte significativo no funcionamento das redes ou serviços de comunicações electrónicas acessíveis ao público e, bem assim, às condições em que o ICP-ANACOM considera existir um interesse público na divulgação dessa informação ao público, vem a APRITEL apresentar os seus comentários.

Antes de mais, a APRITEL congratula-se com o reconhecimento pelo Regulador de que a matéria relativa à segurança e integridade das redes e serviços de comunicações electrónicas é **inteiramente nova** no quadro regulatório nacional e europeu e que o disposto na Lei n.º 5/2004, de 10 de Fevereiro, alterada pela Lei n.º 51/2011, de 13 de Setembro ("LCE"), quanto à adopção por parte das empresas de medidas para a gestão de riscos de segurança ou garantia de integridade das redes, **é suficientemente preciso para que as empresas possam continuar a desenvolver o seu trabalho**.

Refira-se, quanto a isto, que **os associados da APRITEL já atribuem uma importância primordial à questão da segurança e integridade** das suas redes e serviços de comunicações electrónicas, tendo implementado diversos procedimentos internos de garantia e prevenção de incidentes de segurança e promovido e participado em mecanismos de cooperação setorial, tais como o CSRIT, que têm por objecto o estabelecimento de formas de cooperação entre os signatários nas áreas da segurança informática e da utilização segura da Internet.

Exemplo da prioridade desta matéria para os operadores é o **avultado esforço de investimento que o setor**, como um todo, realizou na implementação de medidas de garantia de segurança.

É pois ajustado afirmar-se que **os associados da APRITEL são os primeiros interessados em garantir o adequado funcionamento e continuidade das suas redes e serviços de comunicações electrónicas,** por forma a que estes funcionem da melhor e mais segura maneira possível, indo ao encontro das necessidades dos clientes.

Isto dito, a APRITEL compreende o racional que subjaz a uma obrigação de notificação à autoridade reguladora nacional de violações de segurança e de perdas de integridade que tenham um impacte efetivamente significativo nas redes e serviços de comunicações electrónicas. É fundamental contribuir para o reforço do nível de segurança das comunicações electrónicas, e dotar os Reguladores dos meios e informações necessários para avaliar o nível de segurança das redes ou serviços e ter em conta o estado da técnica.

Considera, porém, que **qualquer decisão** a tomar neste âmbito, quanto ao tipo de situações que devam ser objecto de notificação, **deve pautar-se pela proporcionalidade e flexibilidade** de abordagem, tendo em especial conta os encargos que são impostos às empresas que oferecem redes e serviços de comunicações electrónicas e o fim último que se visa assegurar.

No caso concreto, a APRITEL entende que o ICP-ANACOM acabou por adoptar, nos seus Projetos de Decisão, uma posição demasiado exigente para o setor, colocando um ónus desproporcional aos operadores, face aos encargos daí advenientes e aos fins visados – e tendo em especial conta o período particularmente difícil que a economia atravessa –, e sem qualquer paralelo nas posições adoptadas pela agência ENISA ou por outras entidades reguladoras nacionais, como seja a autoridade Britânica OFCOM.

Com efeito, e no que respeita ao **Projeto de Decisão relativo às comunicações de violações de incidentes de segurança**, não se vislumbra por que razão é que o ICP-ANACOM entendeu ser adequado, para o caso Português, estabelecer condições (*triggering thresholds*) mais exigentes que os estabelecidos, por exemplo, pela OFCOM.

Isto no que toca quer à duração do incidente (sendo a duração mínima de um incidente que despoleta a obrigatoriedade de notificação em Portugal significativamente menor no seu global, que no Reino Unido), quer aos prazos de notificação (que, face à matéria em causa e relativa imprevisibilidade do impacto, não devem nem podem ser peremptórios e muito menos insuficientes), quer ao número de notificações exigidas e respectivo conteúdo (duas notificações obrigatórias e uma terceira eventualmente exigível de acordo com um critério subjetivo [face ao número máximo de dois *reports* no Reino Unido] e todas elas com conteúdo exigível muito extensivo), entre outros aspectos.

Na prática, **estas exigências correspondem a obrigações que recaem sobre as empresas, implicando custos administrativos significativos**, e que **são claramente desproporcionais** face ao esforço que exigem dos operadores, ao *benchmark* existente, à *ratio* da obrigação de notificação – de garantir que apenas os incidentes *realmente* significativos sejam notificados – à utilidade que o ICP-ANACOM retirará do elevado volume de notificações que expectavelmente receberá caso mantenha os critérios assim definidos e, acima de tudo – sublinhe-se –, às **potenciais coimas previstas na LCE para o desrespeito da obrigação de notificação à ARN, que podem ir até €1M**.

Refira-se, neste contexto, os comentários particularmente pertinentes da OFCOM que demonstram bem as preocupações deste Regulador em garantir a proporcionalidade das obrigações a impor aos operadores, face ao propósito que se visa assegurar: "*OFCOM aims to take a proportionate and flexible approach*", "*the reporting process is intended to minimise the burden on providers as far as possible, while still ensuring no significant incidents go unreported*", "*the threshold for reporting in the first stage is set at a level intended to minimise the risk of significant incidents going unreported*", "*the risk of imposing undue burden due to the volume of reports is mitigated by making these first stage reports as lightweight as possible. For incidents which require additional information, which we expect to be few in number, a second stage of follow up reports will be used*", "*the initial report should be submitted within a few days of the incident, but where the incident may be life affecting (…) we expect to be notified within 24 hours*"…

Já no que respeita ao **Projeto de Decisão relativo às condições em que o ICP-ANACOM considera existir um interesse público na divulgação da informação ao público**, a APRITEL considera desajustada a opção do Regulador em face, por exemplo, da total ausência de orientações da ENISA ou da OFCOM nesta matéria – que aparentemente deixam a determinação do que deve ser divulgado por ser do interesse público para uma apreciação casuística com base nos méritos de cada situação.

A APRITEL não pode, pois, concordar com o presente Projeto de Decisão, entendendo que o ICP-ANACOM deve seguir a posição tomada pela ENISA ou pela OFCOM, determinando, caso a caso, que incidentes merecem divulgação ao público, dadas as respectivas características concretas do caso que determinarão, ou não, a existência de um interesse público na divulgação generalizada ao público.

E isto assim é não apenas porque a adopção de um Projeto de Decisão nesta matéria exigiria investimentos por parte dos operadores, potenciaria danos de imagem e comportaria riscos acrescidos de segurança para as redes, mas sobretudo porque os associados da APRITEL já prevêem, neste momento, mecanismos reativos de informação aos assinantes afectados sobre os incidentes de segurança de maior impacto.

Aliás, isto dito, sublinhe-se que as disposições legais que regem esta matéria indicam que a divulgação ao público de incidentes de segurança que revistam um especial interesse público é, originariamente, uma obrigação da autoridade reguladora nacional (epígrafe do artigo 54.º-E da Lei n.º 5/2004, de 10 de Fevereiro, na sua última redação). Só quando o Regulador, perante um caso concreto, considere ser do interesse público informar o público da ocorrência em questão, ou eventualmente determinar às empresas que o façam, é que é justificado haver lugar a uma divulgação.

Isto mesmo é confirmado pelo novo n.º 3 do artigo 13.º-A da Diretiva 2002/21/CE, que foi transposto para o Direito Nacional para a LCE, dispondo "*a autoridade reguladora nacional em questão pode informar o público ou exigir que as empresas o façam, sempre que determine que* ***a revelação da violação*** *é do interesse público*." [1]

Portanto, face a cada violação (de segurança, subentenda-se – e não já de uma qualquer ocorrência) concreta, é que poderá haver lugar a uma avaliação do interesse público na sua divulgação, tendo em conta as características, duração e especial gravidade da situação.

A APRITEL não concorda, por isso, com a abordagem seguida pelo ICP-ANACOM, entendendo que não é minimamente adequado ou proporcional prever que é do interesse público a divulgação de todos os incidentes de segurança que são notificáveis ao abrigo do primeiro Projeto de Decisão (Anexo A da consulta).

Impor às empresas uma verdadeira *obrigação* de divulgação geral ao público de um escopo tão alargado de incidentes previamente definidos, além de despiciendo e de não ter uma concreta base legal, poderá provocar alarmismo por parte dos consumidores.

As notificações ao público devem ser limitadas a incidentes realmente graves: a título de exemplo, seria mais relevante reportar ao público incidentes que afectem o acesso ao número único de emergência 112 do que incidentes que afectem números limitados de utilizadores.

Sugere-se, pois, que o ICP-ANACOM pondere a necessidade de adopção do Projeto de Decisão, no sentido de acomodar a sua abordagem à posição tomada pela ENISA ou pela OFCOM ou, no limite, prever apenas os incidentes referidos no parágrafo anterior.

[1] Novo n.º 3 do artigo 13.º-A da Directiva 2002/21/CE relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (Directiva Quadro), alterada pela Directiva 2009/140/CE.

Em face de tudo o exposto, a APRITEL entende que **é essencial que o ICP-ANACOM tome em devida conta os comentários recebidos em sede de consulta pública e proceda à revisão dos Projetos de Decisão à luz das preocupações do setor** no sentido de flexibilizar a sua abordagem e adaptá-la à realidade das empresas, que se descreve nos capítulos seguintes.

Como nota final, a APRITEL vem ainda expressar a **profunda preocupação dos seus associados quanto ao prazo de implementação** definido pelo ICP-ANACOM nos seus Projetos de Decisão. Com efeito, a implementação de procedimentos complexos e onerosos de adaptação, face aos atualmente implementados pelos operadores para detecção e reporte de incidentes de segurança no prazo de 30 dias proposto pelo ICP-ANACOM **é manifestamente inexequível**.

Considerando que o próprio ICP-ANACOM reconhece a novidade do tema para o setor, entende a APRITEL que os operadores devem dispor de mais tempo para efetuarem as devidas alterações necessárias para a sua implementação, alterações essas que poderão exigir investimentos em SI´s, modificações organizacionais, modificação de contratos de trabalho e outras medidas que os operadores possam ainda vir a identificar.

Nesse sentido, a APRITEL entende que os seus associados deverão dispor de um **prazo nunca inferior a 6 meses para implementação dos procedimentos após a divulgação da decisão final**.

II. PROJECTO DE DECISÃO RELATIVO ÀS CIRCUNSTÂNCIAS, FORMATO E PROCEDIMENTO DAS NOTIFICAÇÕES DE 'INCIDENTES DE SEGURANÇA' PELAS EMPRESAS

Introdução

Conforme acima referido, a APRITEL considera que o ICP-ANACOM adoptou uma posição demasiado exigente que coloca um ónus desproporcional aos operadores, quando ponderados os encargos envolvidos na respetiva implementação e os fins visados pela obrigação de notificação.

No entender da APRITEL, é essencial que o ICP-ANACOM procure flexibilizar o Projeto de Decisão em causa por forma a prever que apenas devam ser notificados incidentes que causem uma efetiva interrupção de serviços significativos e relevantes do ponto de vista da sua utilização.

Para tal, e em primeiro lugar, é necessário que o ICP-ANACOM **delimite de forma clara o âmbito da obrigação de notificação**, estabelecendo que estão em causa incidentes e violações de segurança que impliquem a interrupção da prestação de serviços de comunicações electrónicas, isto é, incidentes que afectem a continuidade/disponibilidade do serviço.

Este entendimento está em linha com o conceito de incidentes e violações de Segurança vertido nas Linhas de Orientação da ENISA (ponto 4.1), de acordo com as quais, o âmbito da obrigação de notificação abrange *"Network and Information security incidents having a significant impact **on the continuity of supply** of electronic communications networks or services"*.

De facto, apenas os incidentes que causam interrupção do serviço é que poderão ser relevantes para o efeito pretendido. Por exemplo, um incidente que afecte, temporariamente, a qualidade de serviço não deverá ser considerado neste âmbito. Existem outros mecanismos, designadamente ao nível da publicação de índices de QoS, que permitem aferir este tipo de situações.

Propõe-se, assim, que o ICP-ANACOM, na decisão final que venha a adoptar, expressamente estabeleça que os "incidentes de segurança" que caem no âmbito de uma obrigação de notificação, para efeitos do artigo 54º-B da LCE, são aqueles que "provocam perturbação grave no funcionamento das redes e serviços, com impacto na sua continuidade, impedindo a sua utilização".

Em segundo lugar, além do exposto, é também necessário que o **ICP-ANACOM flexibilize os critérios que, no seu entender, qualificam** a existência de um **"impacte significativo no funcionamento das redes e serviços"**.

Com efeito, os critérios propostos no Projeto de Decisão são globalmente mais exigentes que os previstos pela OFCOM e pela ENISA sem que tenha sido indicada qualquer fundamentação para isso.

Isto é particularmente de estranhar tendo em atenção que a ENISA refere claramente que, apesar de não se debruçar sobre os esquemas nacionais de *reporting* de incidentes de segurança, "ao *fornecer uma **definição única dos parâmetros dos incidentes e dos thresholds**, está providenciar uma orientação de base para os esquemas nacionais*" (tradução nossa).

Assim sendo, a APRITEL propõe que os critérios que qualificam um incidente de segurança como tendo um impacto significativo sejam adaptados à realidade prática com que as empresas se deparam, e às orientações dadas pela ENISA.

Por último, a APRITEL considera também que **os procedimentos de notificação exigidos, em termos de formato, conteúdo e prazos, são demasiado exigentes.**

Desde logo, importa a este propósito clarificar qual o papel que o ICP – ANACOM pretende assumir durante o período do incidente. Caso o regulador não tenha uma intervenção ativa na resolução do incidente não se justifica a imposição de prazos tão exigentes para a notificação. Bastará obter a informação *a posteriori,* inclusive após a resolução do incidente. Apenas nas situações em que o regulador assuma um papel cativo na resolução do incidente, por exemplo na promoção de contactos entre diversas entidades relevantes para a resolução do incidente, poderá haver justificação para prazos de notificação mais exigentes.

O ICP-ANACOM deve fundamentar concretamente a necessidade de receber duas a três notificações por incidente (com a quantidade de informação exigida) e efetuar uma análise de ponderação do custo que isso implica para as empresas, face aos fins para que o ICP-

27 de Janeiro de 2012

ANACOM se propõe utilizar as ditas notificações. No limite, deve considerar-se que um volume excessivo de notificações pode inclusive implicar um congestionamento do sistema do Regulador (com d*enial of service*), não trazendo qualquer utilidade acrescida.

Nos subcapítulos seguintes apresentam-se alguns comentários e sugestões de índole mais específica relativos aos critérios de objecto de notificação, e ao formato, prazos e procedimentos previstos.

Circunstâncias

Em primeiro lugar, a APRITEL considera que seria relevante, à semelhança do que efetuou a ENISA nas suas Linhas de Orientação, que o ICP-ANACOM efetuasse a **distinção do tipo de serviço afectado por incidente**.

Do Projeto de Decisão sob consulta não consta qualquer especificação dos serviços elegíveis para o processo de notificação, pelo que os associados da APRITEL se veriam na obrigação de reportar ao ICP-ANACOM incidentes de segurança que afectem quaisquer dos serviços prestados aos seus clientes – serviços de dados, televisão, telefonia, *vídeo on demand*, email, etc.

A matriz constante do ponto I.a) deve ser devidamente alterada para distinguir níveis de criticidade por serviço (por exemplo, um incidente no serviço de email não deverá estar sujeito ao mesmo nível de impacto para efeitos de *reporting,* de um incidente no serviço de telefonia).

Os serviços não devem ter o mesmo tratamento nem, refira-se, devem ter o mesmo tratamento todos os acessos, independentemente da sua capacidade. Não faz sentido que um acesso Ethernet a 1 Gbps e uma linha de rede tenham o mesmo tratamento/importância.

Em segundo lugar, a APRITEL entende que o ICP-ANACOM deve esclarecer qual o entendimento relativo a operações de manutenção preventivas e/ou corretivas ou melhorias de rede programadas. Uma vez que não fará qualquer sentido que estes eventos sejam elegíveis para efeitos de notificação, deve o ICP-ANACOM indicar claramente este ponto na sua decisão final.

Em terceiro lugar, e já quanto aos critérios constantes da matriz prevista do ponto I.a), deve ser clarificado se os indicadores apresentados são exclusivos ou cumulativos. Não é claro se os critérios são cumulativos e/ou como deverão ser conjugados. Considerando um exemplo concreto: um incidente que tenha duração de 20 minutos e afecte 400.000 assinantes/acessos deve ser considerado para efeitos de notificação?

A respeito dos **patamares de duração** definidos, considera-se que são excessivamente curtos, sendo injustificada a notificação de incidentes cujo impacto tenha, por exemplo, uma duração de apenas 15 minutos. Interrupções com durações tão reduzidas como as propostas não se consideram significativas nem do ponto de vista europeu (*vide* considerações da ENISA), nem do ponto de vista de outros reguladores (OFCOM), pelo que não se vislumbra qual o critério que presidiu à inclusão de patamares com tão reduzida duração.

Qualquer que seja o patamar mínimo de duração a estabelecer, o mesmo deverá, em todo o caso, ser estabelecido tendo em linha de conta as orientações da ENISA, e considerando a percentagem do total de clientes afectados num serviço concreto.

Acresce que a notificação de incidentes que se prevê que tenham uma duração muito curta não é sequer exequível devido a questões concretas e operacionais. Por exemplo, alguns incidentes tão curtos, de 15 minutos, poderão não ser sequer detectáveis.

Quanto ao **critério "Assinantes/acessos ou Área Geográfica",** entende-se que a conjugação de duas variáveis para avaliação da dimensão do impacto torna o processo demasiado exaustivo e complexo, sem que se antecipe valor acrescentado nesse processo. Sugere-se, assim, que seja apenas considerada a variável "assinantes/acessos". Esta sugestão ganha maior acuidade se for tido em conta que presentemente não estão implementadas (ou disponíveis) ferramentas que permitam calcular a área geográfica (em km2) afectada por este tipo de incidentes, nem se prevê que estejam disponíveis a curto/médio prazo.

Releva-se ainda que, em determinadas circunstâncias, por exemplo se o incidente ocorrer ao nível das plataformas *core* da rede, a avaliação do número de utilizadores afectados requer uma análise morosa e exaustiva, que não é compatível com a notificação ao regulador no prazo de duas horas. Na realidade, em situações anteriores verificou-se que em alguns casos foi preciso cerca de um dia útil para apuramento dos clientes afectados.

Existem ainda outras situações em que as plataformas de rede poderão não permitir identificar o número de clientes afectados. Por exemplo, no caso de um incidente tornar o acesso móvel indisponível, não é possível determinar quantos clientes foram realmente afectados durante o período de interrupção do serviço.

Em quarto lugar, relativamente ao ponto I.b), quanto às situações com i**mpacto no acesso ao número único de emergência**, a APRITEL entende que a definição proposta pelo ICP-ANACOM é demasiado ampla, na medida em que a mesma implicaria que todas as falhas de rede com o mínimo de 15 minutos numa área fossem notificadas, pois sempre que existir uma falha de acesso ao serviço de voz fixa as potenciais chamadas para o 112, tal como as restantes, deixarão de ser concretizadas.

No caso dos serviços fixos, o ICP-ANACOM deve aplicar o conceito defendido pela ENISA, quanto à combinação dos limiares de percentagem de assinantes/acessos afectados e duração do incidente.

No caso dos serviços móveis, entende-se que os mesmos deverão ser excluídos do âmbito destas notificações porque se a rede de um operador móvel estiver indisponível, as chamadas para o 112 serão encaminhadas pela rede de outro operador móvel. Esta funcionalidade é disponibilizada automaticamente nas redes e terminais móveis.

Em quinto lugar, no que respeita ao ponto I.c) (i), a notificação de incidentes com **impacto acumulado**, nos termos propostos pelo regulador, revela-se inexequível, uma vez que não existem processos nem sistemas capazes de registar e verificar os incidentes de forma a analisar as suas causas/efeitos e determinar se contribuíram para o mesmo tipo de incidente, nem efetuar a consolidação desses resultados para obter o efeito acumulado.

De igual modo, quanto ao ponto I.c) (ii), é impraticável o registo e reporte dos incidentes com **impacto acumulado em várias empresas**. O reporte destas situações exigiria que os operadores trocassem constantemente informação sobre os incidentes registados individualmente para averiguar se a causa afecta mais do que uma empresa e apurar se o impacto acumulado preenche os requisitos de notificação. Esta situação implicaria a existência de um processo e sistema/aplicação central com capacidade para, constantemente, receber informação dos operadores e efetuar essa análise, pelo que não é realista considerar a sua existência. Adicionalmente, levantaria questões de partilha de informação sensível e confidencial entre operadores.

Em sexto lugar, a execução dos requisitos **associados às datas especiais** previstas no ponto I.c) (iii), implica um conhecimento prévio dos operadores de um calendário oficial com as datas, eventos, duração, locais e clientes críticos a monitorizar. A ser implementado este critério deve caber ao Regulador o ónus de enviar a todos operadores, com a devida antecedência face à ocorrência, todos os elementos indicados. Para além disso, a aplicação deste critério exige alterações pontuais aos processos que o torna de difícil execução.

Em sétimo lugar, no que se refere ao ponto ponto I.d), a APRITEL nota, antes de mais, que enquanto que os clientes empresariais são tratados com o mesmo grau de importância dos clientes residenciais – tal como é prática da ENISA – o ICP-ANACOM abre uma exceção ao considerar que devem ter tratamento especial as entidades com relevância pública e social. Isto vai além do que é recomendado pela ENISA e os termos genéricos em que é colocado permite que, por exemplo, instituições privadas de solidariedade social possam ser incluídas.

Sem prejuízo do acima exposto, e quanto aos critérios definidos no ponto I.d), sempre seria necessário que o Regulador definisse uma lista oficial de **entidades governamentais e regionais** que devem ser consideradas para este efeito. Adicionalmente, o conceito de "outras entidades relevantes em termos de serviços à sociedade e aos cidadãos" não está explicitado de forma objectiva, sendo necessário definir e manter também uma listagem com a identificação destas entidades.

Questiona-se ainda a relevância do exemplo apresentado - SIRESP (Sistema Integrado de Redes de Emergência e Segurança de Portugal). O SIRESP é por definição um sistema que deve ser independente dos operadores comerciais de comunicações, de modo a assegurar o funcionamento de uma rede de emergência autónoma de suporte a forças de segurança, serviços de emergência e outras entidades. Deste modo, a falha dos serviços dos operadores não deve impactar o SIRESP, cuja missão, conforme indicado, é precisamente suportar as comunicações críticas dessas entidades relevantes para a sociedade (http://www.siresp.com/utilizadores.html).

Por último, importa ainda acautelar questões legais quanto ao tratamento diferenciado dos vários utilizadores dado que, tal como é do conhecimento do Regulador, impende atualmente sobre os operadores uma obrigação de não discriminação.

Formato

Relativamente aos **prazos e formatos** definidos pelo ICP-ANACOM para as notificações associadas aos incidentes, a APRITEL considera, desde logo, que a necessidade de notificar o ICP-ANACOM, no mínimo, duas vezes por incidente, é excessiva, onera os operadores de

forma desproporcional e não tem paralelo nas posições assumidas pela ENISA ou por outros reguladores, como a OFCOM.

Questiona-se desde logo qual a necessidade ou utilidade de recepção de tal número de notificações pelo ICP-ANACOM que, em última análise, poderá não ter capacidade para analisar (ou sequer receber) tanta informação.

Em segundo lugar, quanto ao formato previsto para a **submissão das notificações**, por correio electrónico, a APRITEL nota que apenas foi indicado um único endereço para o efeito. Cumpre saber como é que os associados da APRITEL podem certificar-se que o e-mail foi devidamente recebido pelo Regulador, qual a forma como o Regulador acusa a recepção do mesmo e em que prazo, e ainda como os operadores devem proceder em caso de incidente no serviço de e-mail deste ou mesmo do próprio operador.

Importa ponderar que se o serviço afectado for o serviço de Internet ou de correio electrónico, poderá não ser possível efetuar a notificação até que o serviço esteja restabelecido. Este formato de notificação deverá recorrer a mecanismos de autenticação, integridade e não repúdio como, por exemplo, a certificação digital. O regulador deverá também garantir que o conteúdo das notificações é salvaguardado.

Em terceiro, a APRITEL reitera que é **inexequível que as empresas**, cujas redes ou serviços sejam impactados no seu funcionamento por um mesmo incidente de segurança, **cooperem entre si para a notificação** desse incidente de segurança.

Em quarto lugar, a respeito da identificação das **causas associadas**, deve ser tido em consideração que quando a interrupção do serviço tem como causa a falha no fornecimento de serviços por uma entidade externa (por exemplo o fornecedor de energia eléctrica ou outro operador), nem sempre é possível obter a curto/médio prazo a informação das causas e do tempo estimado de resolução. Podem ainda existir alguns tipos de incidentes cujas causas nem sempre são determináveis, devido à arquitetura tecnológica de rede implementada, incapacidade de algumas plataformas manterem registos, etc.

Em quinto lugar, quanto às **notificações,** no que respeita **à notificação inicial**:

- O prazo de 2 horas para notificação é manifestamente insuficiente, por razões de impraticabilidade operacional, atrás referidas.

- A notificação deve ser feita num prazo de 2 dias úteis (em consonância, por exemplo, com a orientação da OFCOM), por ser mais realista face aos condicionalismos de uma situação de incidentes, devendo este prazo ser contabilizado a partir do momento da detecção do incidente e não do seu início.

No que respeita **à notificação final:**

- Sugere-se que a "notificação final" seja designada e assuma os contornos de um "Relatório de Incidente".

- A notificação deste relatório de incidente deve ter associado um prazo mais alargado, dado que, conforme referido, para certos incidentes o prazo de 10 dias úteis é insuficiente para permitir uma avaliação e identificação de todos os parâmetros de

reporte. Esta situação é sobretudo pertinente quando existem dependências de informações a serem obtidas junto de terceiros (por exemplo fornecedores) ou em situações em que as causas raiz se revelem de difícil precisão.

- Relativamente ao conteúdo, a informação solicitada é demasiado extensiva e, caso os critérios referidos no ponto "I. Circunstâncias" não sejam alterados, de modo a delimitar claramente os serviços elegíveis para notificação, bem como a flexibilizar os critérios de duração e do número de assinantes/acessos ou área afectada, os associados da APRITEL terão de canalizar de forma permanente os seus esforços e recursos para a elaboração de relatórios de incidente, desviando o foco do fundamental que é assegurar a manutenção da rede e dos serviços aos clientes. Sugere-se quanto a isto que, à semelhança do sugerido pela ENISA, seja adoptado um único documento de reporte (*template*) a ser utilizado por todas as entidades,

Entrada em vigor

O prazo estipulado para entrada em vigor destas alterações é inviável e inaceitável.

Dada a novidade do tema, e a adopção necessária de novos procedimentos internos por parte dos associados da APRITEL, que exigirão investimentos adicionais nessa matéria, bem como alterações organizacionais, modificações de procedimentos laborais e outras medidas que, nesta fase, não são ainda identificáveis, o prazo mínimo de implementação deverá ser, no mínimo, de 6 meses.

Isto é particularmente importante uma vez que o incumprimento da obrigação de notificação de incidentes de segurança ao ICP-ANACOM constitui uma contraordenação grave, punível com uma coima até 1M€.

III. PROJECTO DE DECISÃO RELATIVO ÀS CONDIÇÕES EM QUE O ICP-ANACOM CONSIDERA EXISTIR UM INTERESSE PÚBLICO NA DIVULGAÇÃO AO PÚBLICO, POR PARTE DAS EMPRESAS, DAS VIOLAÇÕES DE SEGURANÇA OU PERDA DE INTEGRIDADE DAS REDES

Introdução

Tal como se disse acima, a APRITEL considera demasiado restritiva a abordagem do ICP-ANACOM, sugerindo ao Regulador **pondere a necessidade de adopção do Projeto de Decisão, no sentido de acomodar a sua abordagem à posição tomada pela ENISA ou pela OFCOM ou, no limite, prever apenas que determinados incidentes graves, que afectem o acesso ao 112**, sejam abrangidos pela determinação prévia de "interesse público na divulgação ao público".

Neste contexto, importa relembrar que os associados da APRITEL já preveem processos de comunicação reativos para esclarecer os clientes que contactam os operadores telefonicamente ou por e-mail com questões sobre falha de serviços. Este tipo de processos tem a vantagem de transmitir apenas a informação necessária aos clientes afectados (e não

a todos os clientes ou ao público em geral), além de permitir a adaptação do serviço prestado às necessidades de cada cliente.

Acresce que a divulgação generalizada e sistemática de incidentes poderá criar "alarmismo" desnecessário nos clientes e no público em geral. Por exemplo, poderá haver clientes que são notificados de situações relativas a serviços que nem sequer usam ou que usam muito pontualmente.

Mais, a implementação de processos de divulgação proactivos para o público ou clientes, com os riscos referidos nos pontos acima, pode ainda contribuir para a descredibilização dos serviços de comunicações perante o público, objectivo que é contrário ao intuito do Regulador.

E, para além do exposto, este tipo de divulgação ao público generalizado poderá incitar uma grande quantidade de clientes a tentar verificar constantemente se a rede/serviço está disponível, contribuindo para uma sobrecarga da rede e maior demora na reposição do serviço para os clientes que realmente necessitem de os utilizar naquele momento.

Em face do que se expõe, a APRITEL urge o ICP-ANACOM a ponderar devidamente a necessidade e a utilidade da imposição de procedimentos específicos de notificação proactiva de incidentes, aplicáveis transversalmente a todos os operadores.

Em bom rigor, e como referido nos comentários introdutórios, o novo n.º 3 do artigo 13.º-A da Diretiva 2002/21/CE, que foi transposto para o Direito Nacional para o artigo 54.º-E da Lei n.º 5/2004, de 10 de Fevereiro, na sua última redação, aponta no sentido de que o Regulador pode, perante um caso concreto, quando determine que **a revelação da violação** é do interesse público, informar o público ou exigir que as empresas o façam.

Não é pois justificado – nem face ao que já existe na prática, nem face ao que decorre da letra da lei – determinar de antemão que as empresas são obrigadas a divulgar ao público um tão alargado escopo de incidentes como os que constam do Anexo A que, na realidade, podem nem revestir uma importância ou gravidade que o justifique.

Condições

Sem prejuízo do acima exposto, considera-se desajustada e infundamentada a opção do Regulador de definir critérios/patamares de notificação ao público que sejam equivalentes aos previstos no Anexo A, respeitantes à obrigação de notificação de incidentes ao Regulador.

Os **critérios para notificação ao público devem ser substancialmente mais latos**, sendo que os patamares mínimos associados às notificações deveriam considerar incidentes com maior duração e número de assinantes/acessos. O critério da área geográfica não deveria ser considerado porque não é, em si mesmo, significativo. Adicionalmente, o tipo de serviço deve ser também um factor a considerar para os quais devem ser definidos patamares específicos.

Quanto ao facto da informação a disponibilizar dever ser "esclarecedora para o público e tão precisa quanto possível", a APRITEL entende que em alguns tipos de incidentes poderá estar

a revelar-se ao público informação sobre falhas de rede ou vulnerabilidades provocadas pelo incidente cuja divulgação acarreta mais riscos do que benefícios. A indicação do prazo expectável de resolução poderá também potenciar situações de abuso por clientes.

Além disso, sempre seria de considerar que nem todos os serviços afectados terão o mesmo impacto, pelo que deveria ser sempre efectuada uma distinção do tipo de serviço afectado por incidente. A este propósito, cumpre ainda referir que o próprio interesse público na divulgação destes incidentes varia em função do horário em que ocorre o incidente. Assim, o "interesse público" na divulgação de um incidente de segurança com afectação do serviço entre as 20h00 e as 20h15 será necessariamente maior do que o interesse na divulgação de um incidente que afecte os serviços no período entre as 06h00 e as 06h15.

Conteúdos, meios e prazos

Quanto ao **conteúdo das notificações ao público**, dispõe o ICP-ANACOM que a informação a disponibilizar deve ser "*esclarecedora para o público e tão precisa quanto possível",* mas deve esclarecer que isso assim será face às circunstâncias específicas do incidente.

Isto é, a informação a disponibilizar deve ser esclarecedora, mas deve ter o grau de detalhe adequado em função de uma análise custo/benéfico a realizar em cada situação. A divulgação de informação não pode implicar um aumento dos riscos, sem que existam objectivamente benefícios para os utilizadores.

No que respeita aos meios e **forma de divulgação**, a APRITEL solicita ao ICP-ANACOM que reconsidere a opção proposta. Prever que a informação deva ser disponibilizada, no mínimo, através de contacto telefónico específico[2] e de publicação em local de destaque na página electrónica, sendo imposta a manutenção de um histórico de 6 meses de incidentes, é excessivo e pode ser contraproducente face aos riscos de interpretações danosas ou aproveitamento malicioso por terceiros para exploração de potenciais vulnerabilidades das redes de comunicações electrónicas.

Quanto à divulgação ao público **no prazo** de 1 hora, trata-se de um prazo inexequível e irrealista do ponto de vista do tempo necessário à execução dos processos internos de gestão e comunicação de incidentes/crise e de canalização de esforços para a sua resolução. Também do ponto de vista dos utilizadores, tendo em conta a experiência dos associados da APRITEL, a notificação no prazo de 1 hora revela-se desnecessariamente exigente.

Entrada em vigor e disposição transitória

O prazo estipulado para entrada em vigor destas alterações é inexequível e inaceitável.

Desde logo, a APRITEL não concorda com o presente Projeto de Decisão, entendendo que o ICP-ANACOM deve seguir a posição tomada pela ENISA ou pela OFCOM, determinando, caso a caso, que incidentes merecem divulgação ao público, dado o respectivo interesse público. E isto assim é uma vez que os associados da APRITEL já preveem mecanismos de informação aos clientes afectados dos incidentes de segurança de maior impacto.

[2] Este aspecto é claramente excessivo. No limite, os operadores poderão debater-se com a necessidade de estabelecer um ponto de contacto específico para receber milhares de chamadas telefónicas para acontecimentos pontuais.

27 de Janeiro de 2012

Não obstante, caso o ICP-ANACOM entenda adoptar o Projeto de Decisão em análise, reformulando o seu conteúdo, por forma a limitar a predeterminação do que é do interesse público divulgar apenas para casos de incidentes graves, que afectem o acesso ao 112, deve o Regulador prever um prazo de entrada em vigor de 6 meses, em coerência com o prazo de implementação previsto para o primeiro Projeto de Decisão.