Resposta do Grupo ONI ao Sentido Provável de Decisão (SPD) do ICP-ANACOM sobre Notificação de violações de segurança e perdas de integridade nas redes e serviços de comunicações electrónicas e respectiva divulgação pública

27-01-2012

1 Enquadramento

Este documento apresenta a resposta do Grupo ONI ao Sentido Provável de Decisão (SPD) do ICP-ANACOM sobre Notificação de violações de segurança e perdas de integridade nas redes e serviços de comunicações electrónicas e respectiva divulgação pública. As empresas do Grupo Oni representadas nesta resposta são a ONITELECOM, a KNEWON e a F300.

O Grupo ONI atribui, desde o início da sua actividade, uma importância fundamental à segurança das redes e serviços que opera e disponibiliza aos seus clientes. Nesse sentido, desenvolveu, ao longo da sua história, competências e especialização reconhecidas pelo mercado, tendo como uma das suas importantes áreas de negócio a consultoria e fornecimento, aos seus clientes, de soluções de segurança de redes e de informação. Tem também participado activamente no CSIRT nacional.

Por outro lado, assinalando a especial preocupação do Grupo ONI com estas matérias, o nosso Data Centre da Matinha foi recentemente certificado de acordo com a norma ISO 27001.

Assim, é com especial atenção que o Grupo ONI acolhe e tem participado em todas as iniciativas dessa Autoridade em matéria de segurança de redes e serviços de comunicações electrónicas, nomeadamente no que diz respeito à transposição para a Lei Nacional e respectiva implementação operacional do artigo 13.ºA da Directiva Quadro.

O SPD agora em consulta pública representa, pois, um passo importante para a implementação operacional das disposições já transpostas para a Lei Nacional, pelo que se saúda esta iniciativa do ICP-ANACOM. No entanto, as disposições constantes do SPD carecem de ajustes importantes para estarem alinhadas com a realidade do mercado, terem em conta a real utilidade da informação a prestar, não contribuir para um aumento do nível de risco e não causar alarmismos injustificados no público, nem contribuir, indevidamente, para a má imagem do sector. Nas secções seguintes apresentamos comentários detalhados às várias disposições do SPD.

2 Comunicações de incidentes de segurança

2.1 Circunstâncias

O SPD define os parâmetros e respectivos valores para determinação dos incidentes de segurança considerados significativos e que devem ser objecto de notificação ao ICP-ANACOM por parte dos OPS.

No entender do Grupo ONI, os critérios que determinam os incidentes a notificar devem estar alinhados com as práticas de mercado, nomeadamente com as exigências que os próprios clientes fazem aos OPS a este nível. Acresce que os procedimentos operacionais implementados pelos OPS estão focados na resolução rápida dos incidentes e suas consequências, já que afectam o negócio e os clientes finais. Uma vez que do SPD não se depreende qualquer intenção do ICP-ANACOM de intervir operacionalmente na resolução dos incidentes, as notificações parecem destinar-se apenas a fins estatísticos. Assim, entende o Grupo ONI que quaisquer exigências de notificação devem ser ponderadas no sentido de não constituírem um entrave ao desenvolvimento dos procedimentos operacionais de resolução de incidentes, devendo integrar-se nestes o mais naturalmente possível.

Assinala-se, logo aqui, que essa Autoridade optou por definir níveis de exigência muito superiores aos que a ENISA definiu no seu *Technical Guideline on Reporting Incidents*. Com efeito, enquanto que a ENISA define como limiar mínimo de impacto incidentes com duração superior a 1 hora que afectem mais de 15% dos utilizadores, o SPD tem por limiar mínimo incidentes de pelo menos 15 minutos que afectem pelo menos 500.000 assinantes/acessos (menos de 5% da população). Por outro lado, no SPD estes parâmetros são combinados com a área geográfica afectada, o que a ENISA não exige. A ENISA só exige, no que diz respeito ao parâmetro geografia, que se notifiquem incidentes que afectem áreas rurais (com impacto em mais de 10% dos utilizadores dessas áreas ou com duração superior a 4 horas). Alerta-se que os sistemas operacionais utilizados para tratamento de incidentes não permitem a determinação imediata de áreas afectadas.

Ao definir níveis de exigência muito superiores aos da ENISA e aos que os próprios clientes exigem aos OPS, essa Autoridade irá obrigar os OPS a um esforço muito significativo devido a uma elevada quantidade de notificações, com impactos importantes quer no adequado tratamento operacional dos incidentes, com vista à sua resolução, quer nos meios humanos e operacionais que os OPS necessitarão. Por outro lado, ao definir durações de incidentes tão curtas (a partir de 15 minutos), cai-se numa situação de confusão entre incidentes de segurança e avarias, que pertencem ao âmbito da avaliação de qualidade de serviço.

Assim, sugere-se que essa Autoridade reveja os níveis de exigência que estabeleceu no SPD, no sentido de os alinhar com os que constam das orientações emanadas pela ENISA.

Alerta-se que o critério associado à indisponibilidade do serviço 112 implica que qualquer incidente que afecte o serviço de voz, independentemente do número de utilizadores e área

afectados, deverá ser notificado ao ICP-ANACOM. Dada a duração definida (15 minutos) deverá haver um elevado número de notificações.

Adicionalmente, são definidos no SPD critérios de acumulação de duração de eventos, quer afectando um único operador, quer vários. Isto coloca vários problemas operacionais. Em primeiro lugar, os sistemas operacionais utilizados não permitem a correlação de eventos separados no tempo para que seja possível a determinação dos tempos acumulados. Por outro lado, não existem procedimentos estabelecidos entre operadores que permitam este tipo de coordenação e a sua implementação é complexa e levanta problemas de custos, recursos técnicos e humanos, bem como de confidencialidade. O Grupo ONI entende, face aos problemas assinalados, que não é realista manter os critérios de acumulação na decisão final.

A ocorrência de incidentes em datas relevantes é mais um critério de decisão que a ENISA não exige e que levanta problemas, a começar pela necessidade de a lista de datas relevantes ser atempadamente comunicada aos OPS e devidamente actualizada, não estando este aspecto acautelado no SPD. Caso contrário os OPS poderão, inadvertidamente, incorrer em situações de incumprimento. Assim, solicita-se que este critério seja também eliminado da decisão final.

Relativamente aos incidentes que afectem ilhas das Regiões Autónomas, defende o Grupo ONI que os critérios para notificação dos incidentes devem estar alinhado com as exigências da ENISA para as designadas zonas rurais (incidentes com impacto em mais de 10% dos utilizadores dessas áreas ou com duração superior a 4 horas).

Por último, as entidades governamentais, regionais e outras socialmente relevantes devem ser listadas e esta lista deve ser mantida actualizada para que os OPS não incorram em situações de incumprimento. Também a duração mínima do evento devia alinhar-se com o que a ENISA exige, pelo que deveria ser de 4 horas.

2.2 Formato e procedimento

O SPD determina o formato das notificações a enviar a essa Autoridade pelos OPS e os procedimentos a seguir. Estão previstas até três notificações, com níveis detalhe elevados, sendo que a primeira deve ser feita no prazo máximo de duas horas após detecção do incidente.

Como se referiu anteriormente, não se encontra no SPD menção a qualquer intenção de intervenção operacional, por parte dessa Autoridade, na resolução dos incidentes, pelo que as notificações cumprirão fins estatísticos. Assim sendo, não se compreende o estabelecimento de um prazo tão curto para a notificação inicial. Acresce que a imposição deste prazo implicará o desvio de meios do OPS, importantes na resolução do incidente, para uma acção que não terá utilidade imediata nessa resolução. Solicita-se, pois, que este prazo seja revisto e sugere-se a adopção de um prazo máximo de 48 horas úteis após detecção do incidente. Assinale-se que a OFCOM, no seu SPD sobre esta matéria, estabeleceu este prazo para a notificação inicial.

Não se percebe, por outro lado, a necessidade de uma notificação intermédia e uma notificação final. Dada a complexidade na análise de incidentes de segurança, entende o Grupo ONI que

deverá existir apenas uma notificação final a enviar ao ICP-ANACOM no prazo de um mês após o final do incidente.

2.3 Entrada em vigor

Dada a complexidade do tema e o impacto operacional, de meios técnicos e humanos, bem como de custos para os OPS, entende o Grupo ONI que um prazo de implementação de 30 dias úteis a contar da data da notificação da decisão final é claramente insuficiente. O Grupo ONI solicita que este prazo seja alargado para 6 meses.

3 Divulgação pública de incidentes de segurança

3.1 Condições

O SPD determina que os OPS informem o público da ocorrência de incidentes de segurança significativos e que cumpram as combinações de critérios de duração e número de clientes/acessos ou área geográfica afectada que também são usados para determinar a obrigação de notificação ao ICP-ANACOM.

Como já referido acima, estes critérios são mais exigentes que os estabelecidos pela ENISA e resultarão num elevado número de notificações, criando até confusão entre incidentes de segurança e avarias normais. Ao utilizar os mesmos critérios para determinar a comunicação ao público, o SPD estará, potencialmente, a contribuir para a criação de situações de alarmismo junto do público e de má imagem, injustificada, para o sector das comunicações electrónicas. Por outro lado, cria-se o risco de aumentar o potencial de ataques maliciosos aos OPS por via da divulgação de vulnerabilidades que de outra forma não seriam públicas.

Note-se que os clientes finais do Grupo ONI já são informados em caso de incidentes de segurança que os afectem.

Assim, o Grupo ONI defende que as comunicações ao público devem ser decididas caso a caso pelo ICP-ANACOM. Neste caso ou em caso de manutenção da obrigação de informação sem avaliação prévia pelo ICP-ANACOM, solicita-se que as comunicação ao público sejam limitadas aos incidentes mais graves (maior duração e maior nº de clientes afectados), devendo a informação a publicar ser criteriosamente seleccionada para minimizar riscos acrescidos.

3.2 Conteúdo, meios e prazos para a divulgação

Em coerência com o que se disse na secção anterior, o Grupo ONI defende que a divulgação pública de incidentes de segurança deve ser determinada casuisticamente pelo ICP-ANACOM e a informação a prestar deve ser limitada para minimizar riscos acrescidos. Assim, o Grupo ONI discorda da manutenção de um histórico de incidentes de segurança nas páginas de *web* dos OPS.

Por outro lado, os prazos para publicação da informação e manutenção desta nas páginas de *web* deverão ser revistos. Assim, sendo a avaliação casuística, sugere-se um prazo de 48 horas

úteis para publicação da informação pelo OPS após comunicação do ICP-ANACOM da obrigação de informar o público. O prazo de manutenção da informação nas páginas *web* deverá ser o mais curto possível, sugerindo-se um prazo máximo de 5 dias úteis, sem manutenção de histórico.

A manter-se a disposição do SPD, entende o Grupo ONI que o prazo para disponibilização da informação deve estar alinhado com o da notificação inicial ao ICP-ANACOM, que se sugeriu ser revisto para 48 horas úteis após detecção do incidente. Entende-se, também, que o prazo máximo de manutenção da informação nas páginas *web* deverá ser de 5 dias úteis e não deverá manter-se histórico dos incidentes.

3.3 Entrada em vigor e disposição transitória

Pelas razões já invocadas na secção 2.3 deste documento, solicita-se que o prazo de entrada em vigor e o prazo da disposição transitória sejam de 6 meses e 5 meses, respectivamente, após a notificação da decisão final