Comentários da ZON à Consulta sobre a notificação de violações de segurança e perdas de integridade nas redes e serviços de comunicações eletrónicas e respetiva divulgação pública

Versão Não Confidencial

27 de Janeiro de 2012

A presente resposta visa apresentar a posição comum das empresas do Grupo ZON MULTIMÉDIA, compreendendo a ZON TV CABO, a ZON TV CABO MADEIRENSE e a ZON TV CABO AÇOREANA, doravante designadas no seu todo como “ZON”, relativamente à consulta pública sobre a notificação de violações de segurança e perdas de integridade nas redes e serviços de comunicações eletrónicas e respetiva divulgação pública, aprovada pelo Conselho de Administração do ICP-ANACOM em deliberação de 22 de Dezembro de 2011.

Nos referidos Projetos de Decisão o ICP-ANACOM aborda uma matéria, relativa à segurança e integridade das redes e serviços de comunicações eletrónicas, que é totalmente nova no quadro regulatório nacional e europeu.

A ZON, seguindo as melhores práticas do setor, tem investido profundamente em processos de controlo interno visando a garantia e prevenção de incidentes de segurança, bem como participado, aos mais diversos níveis, nos fóruns especializados de acompanhamento e investigação de práticas de políticas de segurança.

Desde logo, a ZON, na sua atividade de operador de comunicações eletrónicas, está particularmente empenhada na prevenção e combate a violações de segurança e de perdas de integridade que possam impactar as redes e serviços de comunicações eletrónicas.

Assim, qualquer notificação que possa revelar um incidente deve ser tratada com um nível de confidencialidade que impeça, por um lado, a repetição do mesmo, e por outro, a indicação de falhas que possam ser exploradas em qualquer outra tentativa de intrusão. E aqui, a forma como as notificações devem ser conduzidas assume uma importância primordial, devendo ser restringidas a um número muito restrito de intervenientes.

Qualquer decisão de notificação deve, deste modo, estar assente em três pilares: **utilidade, proporcionalidade** e **flexibilidade**.

A ZON entende que a adoção das medidas preconizadas no Projeto de Decisão reveste uma excessiva quebra da reserva da informação, nomeadamente, no que respeita a notificações com relevância para divulgação pública.

Este Projeto de Decisão apresenta um modelo que significa um conjunto de obrigações que excede largamente o preconizado na Diretiva 2002/21/CE (Diretiva Quadro), alterada pela Diretiva 2009/140/CE, bem como o que a ENISA define na sua *Technical Guideline on Incident Reporting*.

Este excesso está patente em diversos tipos distintos de obrigações:

1. Os *triggering thresholds* preconizados impõem a obrigação de notificação de Portugal em incidentes com uma duração mínima muito inferior às *Guidelines* anteriormente referidas, e mesmo quando comparado com o caso em que outra NRA (OFCOM) já definiu as regras de atuação no referido contexto. Tal escolha revestirá uma carga desproporcional e excessiva de comunicações de incidentes para os operadores, sem que se vislumbre a necessidade de tal

2. Os prazos de notificação, não contemplam a reserva e importância da matéria em causa, bem como a sua relativa imprevisibilidade do impacto, sendo imperativos e insuficientes face às características do incidente;

3. O número de notificações exigidas e respetivo conteúdo (duas notificações obrigatórias e uma terceira eventualmente exigível de acordo com um critério subjetivo) não contemplam o enfoque em que o operador deve concentrar os seus esforços.

Estas exigências, que representarão um aumento significativo dos custos administrativos no cumprimento das mesmas, sem que se identifique uma vantagem associada face á diferença relativamente à *Technical Guideline on Incident Reporting*, reforçam, pelo contrário, um conjunto de preocupações com o desvio dos esforços de contenção com um potencial incidente para a preparação de comunicações administrativas, que podem naturalmente ser preparadas e enviadas em janelas temporais mais alargadas.

Outra preocupação, esta com maior impacto na reserva necessária nos incidentes ora em análise, surge da publicidade dos mesmos definida de forma genérica e abstrata no Projeto de Decisão, quando, a contrário, deveria ser definida caso a caso, de acordo com a relevância dos incidentes e mediante critérios apertados quanto à sua divulgação.

Isto é o que resulta do novo n.º 3 do artigo 13.º-A da Diretiva 2002/21/CE, que foi transposto para o Direito Nacional através da LCE, dispondo o seguinte - "*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*."

Não é demais frisar que o objetivo primário da revelação pública não deve colidir com a segurança futura das redes e serviços de comunicações eletrónicas, uma vez que esta revelação pode, inadvertidamente, apontar falhas e caminhos para outras intrusões, pervertendo o objetivo das medidas citadas.

Finalmente, o presente Projeto de decisão será inovador, não existindo ainda qualquer informação que possa ser obtida de outras NRA sobre as vicissitudes da implementação do referido normativo. Não obstante a novidade, o ICP-ANACOM preconiza um prazo de 30 dias para a implementação do sistema de comunicações, após a aprovação final.

Ora, a ZON e certamente os demais operadores, terão que adequar os seus sistemas de reporte e comunicações internos, o que será impossível concretizar no prazo anunciado (30 dias). Face à complexidade associada a ZON entende que deve ser concedido um prazo mínimo de 6 meses após a deliberação final, podendo ser estendido caso se verifique algum constrangimento não identificado *ab initio* pelo presente Projeto de Decisão.

Em conclusão, a ZON entende que a Diretiva 2002/21/CE (Diretiva Quadro), alterada pela Diretiva 2009/140/CE, bem como o que a ENISA define na sua *Technical Guideline on Incident Reporting* visam primordialmente incidentes de segurança, não estando cobertos quaisquer temas de Qualidade de Serviço.

Estes incidentes de segurança, que devem ser exaustivamente definidos, deverão servir para uma articulação dos operadores na resposta a tentativas de intrusão que possam comprometer a integridade das suas redes e serviços de comunicações eletrónicas, quer no plano nacional quer europeu, consoante a dimensão e abrangência.

Ao invés, as comunicações, ora em análise, não devem impor um novo conjunto de obrigações sem que a respetiva análise de impacto regulatório seja efetuada e partilhada com os *stakeholders*, servindo a mesma para avaliar os impactos daí resultantes.