[redacted]

From: [redacted]@oni.pt>
Sent: 14 de março de 2017 17:32
To: regulamento.seguranca@anacom.pt
Cc: [redacted]
Subject: Resposta da NOWO e ONI à consulta sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas
Attachments: Resposta NOWO_ONI ao Projecto Regulamento Segurança (PÚBLICA).pdf; Resposta NOWO_ONI ao Projecto Regulamento Segurança (CONFIDENCIAL).pdf

Exmos. Srs.,

Enviamos em anexo as versões confidencial e pública da resposta da NOWO e ONI à consulta sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas.

Sem outro assunto, apresentamos os nossos melhores cumprimentos

[redacted]

ONI TELECOM INFOCOMUNICAÇÕES S.A.
ALAMEDA DOS OCEANOS LT 2.11.01 E
EDIFÍCIO LISBOA, PARQUE DAS NAÇÕES
1998-035 LISBOA | PORTUGAL
WWW.ONI.PT

RESPOSTA DA NOWO E ONI À CONSULTA PÚBLICA SOBRE O PROJETO DE REGULAMENTO RELATIVO À SEGURANÇA E À INTEGRIDADE DAS REDES E SERVIÇOS DE COMUNICAÇÕES ELETRÓNICAS

1. Introdução

A NOWO Communications, S.A. ("NOWO") e a ONITELECOM – Infocomunicações, S.A. ("ONI") vêm por este meio apresentar os seus comentários no âmbito da consulta pública sobre o Projeto de Regulamento Relativo à Segurança e à Integridade das Redes e Serviços de Comunicações Eletrónicas ("Projeto de Regulamento").

Nesta secção apresentamos comentários gerais ao Projeto de Regulamento. Na secção seguinte, apresentamos uma estimativa de impacto financeiro resultante da implementação das medidas preconizadas.

2. Comentários gerais

Para a NOWO e a ONI, a segurança e a integridade das suas redes e serviços são fatores fundamentais para a sua reputação e posicionamento no mercado, pois contribuem decisivamente para a satisfação dos seus clientes finais com os serviços prestados. Assim, estas empresas têm feito investimentos e desenvolvido processos que permitem adequar as suas redes, sistemas e serviços aos níveis de ameaças a que se encontram expostas. Recordamos que em 2012 tivemos oportunidade, em resposta ao levantamento que essa Autoridade fez junto dos operadores do estado de implementação de um conjunto de medidas de segurança e integridade alinhadas com a recomendação da ENISA *"Technical Guidance for Minimum Security Measures: Guidance for Minimum Security Measures in Article 13-A (version 1.0, December 2011)"*, de mostrar que nos encontrávamos num estado avançado de implementação de muitas dessas medidas.

Nowo Communications S.A.
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €5.000.040,00
Pessoa Colectiva e Matrícula nº 503062081 CRC Palmela

Oni Telecom Infocomunicações, S.A
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €4.630.000,00
Pessoa Colectiva e Matrícula nº 504073206 CRC Lisboa

Assim, foi com surpresa que constatámos que o Projeto de Regulamento adota uma aproximação complexa e intrusiva, ao prescrever uma série de medidas técnicas de execução muito específicas, fazendo tábua rasa das medidas que as empresas de comunicações eletrónicas ("operadores") já tenham implementado para os mesmos fins. Isto é feito, sublinhe-se, em contradição com as recomendações da ENISA apresentadas no documento acima mencionado, onde se advoga (pág. iii) que *"One size does not fit all"*, devendo as medidas específicas ser adequadas à dimensão e particularidades de mercado de cada operador, sendo estes quem está melhor posicionado para escolher as medidas a adotar. Note-se que o impacto financeiro da substituição das medidas existentes pelas definidas no Projeto de Regulamento é elevado, como se demonstra na segunda secção desta nossa resposta.

Em consequência, defendemos a revisão do Projeto de Regulamento no sentido de serem definidos objetivos de segurança e integridade, alinhados com as recomendações da ENISA, ficando os operadores livres de adotar as medidas concretas de execução que melhor se adequarem às suas especificidades e que permitam cumprir esses objetivos.

Não se compreende, também, a razão da opção do Regulador por um nível de exigência tão elevado nas medidas preconizadas, já que o nível de risco em Portugal é comparativamente baixo. Note-se que a ENISA prevê três níveis de sofisticação para as medidas de execução, sendo que essa Autoridade, no Projeto de Regulamento, optou, em algumas medidas, pelo nível mais sofisticado, sem que para tal tenha apresentado uma justificação fundamentada.

Admitindo, sem conceder, que o Regulador venha a adotar um nível de sofisticação superior ao básico, defendemos que seja estabelecida uma calendarização razoável para se atingir o nível pretendido, a qual permita minimizar o impacto financeiro, para os operadores, das medidas de execução necessárias, devendo iniciar-se o processo pelo nível básico. Em qualquer caso, como acima defendido, deverão ser os operadores a definir as medidas

concretas a adotar para atingir os objetivos de segurança e integridade do nível de sofisticação associado a cada fase da calendarização.

Por outro lado, a classificação de ativos, prevista no Projeto de Regulamento, é complexa e com exigências de análise e reavaliação de riscos que são problemáticas em termos dos recursos necessários para o seu cumprimento (ex.: reanálises de risco após incidentes significativos). Sugere-se que a classificação preveja apenas dois tipos de ativos (críticos e não-críticos), sendo a classificação feita em termos relativos, em função da dimensão da rede de cada operador, em vez de em termos absolutos, como previsto no Projeto de Regulamento.

A análise de risco global é demasiado exigente e complexa, não sendo justificada no contexto nacional. A mesma não deverá abranger a totalidade dos ativos mas apenas os classificados como críticos, usando o operador os seus processos internos para efetuar a sua análise de impacto e mitigação de risco. A periodicidade da análise deve ser suficientemente alargada para permitir a implementação faseada das medidas que se revelem necessárias, para minimizar o esforço financeiro associado. Assim, consideramos que a periodicidade mínima deverá ser de dois anos.

O Projeto de Regulamento prevê, também, a realização de exercícios e testes de segurança que podem, em alguns casos, ter periodicidade semestral. Cumpre alertar que todos os exercícios de segurança podem por em risco a própria segurança e integridade das redes e serviços testados, pelo que devem ser minimizados em frequência e abrangência.

Relativamente às auditorias, defendemos que sejam seguidas as metodologias das normas ISO, pelo que se deverá adotar um ciclo de melhoria contínua, com avaliação, por amostragem, dos ativos e processos dos operadores, de forma a cobrir completamente toda a operação ao fim de um determinado número de auditorias, devendo ser tida em conta a razoabilidade dos investimentos necessários para a resolução das não-conformidades encontradas. No sentido de minimizar o impacto financeiro para os operadores, sugere-se, ainda, que durante a fase de

implementação do Regulamento, estes possam recorrer a auditores internos devidamente certificados nos normativos aplicáveis.

Por fim, informa-se que a NOWO e a ONI subscrevem, na totalidade, a posição apresentada pela APRITEL nesta consulta pública.

3. Impacto financeiro do Projeto de Regulamento sobre a NOWO e a ONI

A NOWO e ONI procederam a uma análise de impacto das medidas de execução preconizadas no Projeto de Regulamento, avaliando os custos de investimento (CAPEX) e operacionais (OPEX) necessários para substituir ou adaptar as medidas de execução que já têm implementadas. No quadro seguinte apresentam-se estimativas para esses custos. São usadas as seguintes abreviaturas:

IT: Information Technology

SW: software

RH: recurso humano

NOC: Networks Operations Center

CIP: Coordenação de Intervenções Programadas

SOC: Services Operations Center

SA: Service Assurance

OPER: Operações

[Início de informação confidencial]

Nowo Communications S.A.
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €5.000.040,00
Pessoa Colectiva e Matrícula nº 503062081 CRC Palmela

Oni Telecom Infocomunicações, S.A
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €4.630.000,00
Pessoa Colectiva e Matrícula nº 504073206 CRC Lisboa

Nowo Communications S.A.
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €5.000.040,00
Pessoa Colectiva e Matrícula nº 503062081 CRC Palmela

Oni Telecom Infocomunicações, S.A
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €4.630.000,00
Pessoa Colectiva e Matrícula nº 504073206 CRC
Lisboa

[Fim de informação confidencial]

4. Conclusão

A NOWO e a ONI subscrevem na totalidade a posição apresentada pela APRITEL nesta consulta pública.

O Projeto de Regulamento é complexo e intrusivo, não tendo em conta as medidas de execução já implementadas pelos operadores, nem o nível efetivo de risco do país. Daqui resultam impactos financeiros significativos para que a NOWO e a ONI substituam ou adaptem essas medidas às exigências do Regulamento.

Defende-se que o Regulamento defina objetivos de segurança e integridade adaptados ao nível de risco do país, deixando aos operadores a liberdade de adotar as medidas de execução mais adequadas, tendo em conta as dimensões das suas redes e particularidades dos mercados em que atuam.

Lisboa, 14 de março de 2017

Nowo Communications S.A.
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €5.000.040,00
Pessoa Colectiva e Matrícula nº 503062081 CRC Palmela

Oni Telecom Infocomunicações, S.A
Alameda dos Oceanos, Lote 2.11.01.E
Edifício Lisboa – Parque das Nações
1998-035 Lisboa
Capital Social €4.630.000,00
Pessoa Colectiva e Matrícula nº 504073206 CRC Lisboa