[redacted]

From: [redacted] <[redacted]@fccn.pt>
Sent: 8 de março de 2017 22:29
To: regulamento.seguranca@anacom.pt
Subject: Consulta sobre o projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas
Attachments: Comentarios_FCT-FCCN_20170303.pdf

Exmos Senhores,

Após uma análise cuidada da nossa parte, o projeto de regulamento em epígrafe merece-nos os comentários que podem ser encontrados em anexo.

Melhores Cumprimentos,

[redacted]

[redacted](www.cert.rcts.pt)

Fundação para Ciência e a Tecnologia, I.P. (www.fct.pt)
Unidade FCCN - Computação Científica Nacional (www.fccn.pt)
Av. do Brasil, 101, 1700-066 Lisboa, Portugal
[+351] 218440100

Exmos Sr.

Serve o presente para, no âmbito da consulta pública, realizada pela ANACOM, sobre o Projeto de regulamento relativo à segurança e à integridade das redes e serviços de comunicações eletrónicas, manifestar o seu entendimento de que, considerando o objecto descrito no seu art.º 1.º, este regulamento não se aplica à actividade da FCT-FCCN.

Aproveitamos, no entanto, a ocasião para apresentar um conjunto de comentários/sugestões, que, em nosso entender, podem contribuir para uma melhor segurança das redes e serviços de comuicações electrónicas no nosso país:

a) Recordando o trabalho realizado pela FCT com a comunidade científica, no qual a ANACOM participou, com vista à identificação de uma metodologia nacional de análise de risco, deveria ser encontrada e definida essa mesma metodologia nacional que, implementada, permitiria uma comparação de resultados entre entidades e o benchmark com as melhores práticas internacionais.
b) Considerando a proximidade da transposição da Directiva SRI, que prevê um regime de notificação de incidentes em tudo semelhante ao aqui proposto e considerando que muitas organizações serão objecto de regulação por parte da ANACOM no que às redes e serviços de comunicações eletrónicas diz respeito e de regulação por parte de uma outra entidade no que à Directiva SRI diz respeito, sugerimos uma articulação estreita entre estes dois regimes para simplificação de processos para as organizações.
c) Sugerimos igualmente a utilização de uma taxonomia comum de classificação de incidentes com as comunidades de CSIRT e a Polícia Judiciária. Sugerimos a utilização da recentemente aprovada taxonomia comum aprovada pela Europol e a ENISA, ademais desenvolvida em Portugal.
d) No que se refere à notificação de incidentes prevista no art.º 24.º, a formulação que prevê a notificação de incidentes relativos a "clientes" das "empresas" que prestem "serviços relevantes à sociedade e aos cidadãos ", cf. al. f) do n.º 3 do art.º 24., é bastante subjectivo, e essa relevância dificilmente poderá ser do conhecimento de cada prestador de serviços.
e) O diploma, em vários momentos, alarga o objecto de aplicação para além das "redes de comunicações públicas e serviços de comunicações electrónicas acessíveis ao público", abrindo a porta a possíveis sobreposições com a futura transposição da directiva NIS.
f) A determinação de que "as empresas devem adotar, identificar e caracterizar um Sistema para a Monitorização do Tráfego no acesso à Internet [...] para detecção de ameaças ao funcionamento ou à segurança [...] dos equipamentos terminais dos utilizadores finais." parece-nos excessiva. Parece-nos que constituirá uma intercepção de tráfego dentro da rede, normalmente feita por subscrição de serviço por parte do utilizador.