ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

Str. Delea Nouă nr.2, Sector 3, 030925 Bucureşti, România
Telefon: 0372 845 400 / 0372 845 454. Fax: 0372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

Autor	ANCOM
Persoană de contact	Simona CONSTANTIN
Adresa e-mail contact	simona.constantin@ancom.org.ro
Cod document	2018/01/04/RO
Data publicării inițiale	12.04.2018
Data ultimei modificări	-
Data încheierii procesului de consultare publică	30.04.2018
Statut	Chestionar
Acțiune așteptată	Răspuns

ENISA Questionnaire: Security exceptions in the net neutrality legislation

1 Background

ENISA, following a request by NRAs, is running an EU-wide questionnaire for telecom providers and ISPs about the security exceptions in the net neutrality legislation.

Regulation (EU) 2015/2120 (also called the Net Neutrality Regulation) establishes the rules for equal and non-discriminatory treatment of internet traffic provision across Europe and sets the framework for an open internet where providers are not allowed to apply blocking, throttling and discrimination of internet traffic unless specific exceptions are met (Article 3(3)).

These specific exceptions are:

a) To comply with EU or national laws
b) To preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users
c) To prevent and mitigate the effects of exceptional or temporary network congestion.

The objective of this questionnaire is to collect information about the security measures you take under the security part (point b) of this exception, measures taken to protect the security of the network, services using the network and/or end-user equipment. For example, a provider might block the port used by the SMTP email protocol, because a third-party notified about large amounts of spam emails.

This questionnaire targets large telecom providers and ISPs, which have 10% or higher market share in their country, nationally.

The information collected through this questionnaire will be used by ENISA for the development of a document that gives a general aggregated overview of how these exceptions are being used, what are good practices in this area, challenges, etc.

In the rest of this questionnaire, the term “security measures” means the security measures taken using this security exception, and should be understood as encompassing all the traffic management practices which block, slow down, shape, transcode, degrade, limit or filter in any form end—to-end connectivity, in order to preserve the integrity and security of the network or services. Such measures include but are not limited to TCP/UDP port blocking, specific application or service blocking (e.g. UPnP, NetBIOS/SAMBA), IP blocking , DNS filtering and redirection, URL filtering, packet filtering, content injection, which may result in blocking, throttling or traversing internet traffic (content/application or services).

2 Questionnaire

Country	
Provider	
Name/Surname	
Email	

QS1	Estimate, how often, how many times in a year, do you take these security measures?
Answer	
QS2	What portion of these measures targets to specific customers, which are broad measures for a large group of customers?
Answer	

QS3	Which is the most common reason for applying these security measures: a. To preserve the integrity and security of network and services b. to preserve the security of the terminal equipment of end-users, or c. to preserve the security of services using the networks (such as OTT applications)
Answer	
QS4	What kind of security issues do you try to prevent, typically. Please explain the most common situations
Answer	
QS5	What kind of security measures do you apply and which are the most commonly used?
Answer	

QS6	Which are the most common triggers for activating these security measures? (i.e. user complaints, detection by the provider, a CSIRT, a LEA, etc)?
Answer	
QS7	Do you disclose your policy about these security measures? If yes, what kind of information and by which means? (pls provide link, if available)
Answer	
QS8	Do you have a mechanism or a communication channel where users can report incidents to you? If yes, pls provide the link
Answer	
QS9	Do you have a mechanism or a communication channel to discuss with the users the impact of these security measures? If yes, pls explain or provide the link
Answer	

QS10	Do you provide to your users opt-out provision or exceptions to the security policies (for example for port blocking policies)? Pls explain
Answer	
QS11	In your experience, which are the top 5 ports which are permanently or more frequently blocked?
Answer	
QS12	Which are the alternatives to port blocking you consider in order to mitigate a security risk and which are the reasons for not choosing them?
Answer	
QS13	In case of blocking a specific port, do you provide alternatives to end users upon their request and if yes which ones?

QS14	How do you assess the effectiveness of the measures you apply?
Answer	
QS15	How do you determine the duration of the applied measures?
Answer	
QS16	Please provide links to relevant good practices, guidelines, or standards you apply.
Answer	
QS17	Which problems do you identify in the application of the article (Article 3(3) b) and what do you propose in order to resolve them?
Answer	
QS18	Would you agree to be contacted by ENISA for a follow-up interview?
Answer	