Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation

VERSION 1.0 - DECEMBER 2018

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use resilience@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Authors

Eleni Vytogiannni, Marnix Dekker

Acknowledgements

This guideline is the result of a close collaboration between ENISA and the members of the Article 13a Expert Group. The ENISA Article 13a Expert group is a group of experts from national authorities and electronic communication regulators in the EU and EFTA countries, focusing on telecom security. BEREC's Net Neutrality Expert Working Group reviewed this guideline. In preparing this paper we conducted a survey to assess the state of play. We received survey responses from 38 providers across Europe. Their input was vital in the development of this paper and we would like to thank them for their contribution.

ISBN: 978-92-9204-271-4, DOI: 10.2824/94531

Table of Contents

Executive Summary

In the EU, net neutrality is guaranteed by the so-called Open Internet Regulation[1] (Regulation (EU) 2015/2120), which came into force in 2016 and establishes rules for providers of internet access services in the EU to ensure equal and non- discriminatory treatment of internet traffic. Article 3 of the regulation states that providers can implement *reasonable traffic management measures*, which must be transparent, non-discriminatory, proportionate, and based on objective technical quality of service requirements. Beyond these reasonable traffic management measures, providers can *not* implement traffic management measures that block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, *except* when it is necessary

a) to comply with EU or national legislation or court orders,
b) to preserve the integrity or security of the networks, the services using the networks, or the end-user equipment, or
c) to prevent an impending network congestion, which is temporary and exceptional.

Article 5 of the Open Internet Regulation requires National Telecom Regulatory Authorities (NRAs) to supervise and enforce net neutrality, requiring them to, among other things, closely monitor and ensure compliance with Article 3. In doing so, NRAs may assess whether a traffic management measure applied by a provider, in a specific case, is permissible under Article 3. In its recent Opinion[2] BEREC indicates it will work on further clarifications on how NRAs may assess security measures under Article 3.

This document is a technical guideline for NRAs to support them in assessing when security measures are justified under point (b) above. This guideline contains:

- A list of evaluation factors that may be taken into account by NRAs to understand whether a security measure is justified or not (see Section 3.1).
- An evaluation checklist that NRAs may use when assessing if a measure is justified (see Section 3.2).
- A justification form that may be used by NRAs to collect information about a security measure from providers (see Section 3.3). The justification form may be used also by providers as part of their internal processes to document which security measures they consider to fall under this exception.

It is important to note that whether or not a security measure is *justified* under exception b (see above) depends on the circumstances, the type of networks, services, etc. Security is a fast moving field and cyber-attacks are changing constantly. What may have been an effective measure at one point in time, in the middle of a large-scale attack for instance, may be considered as unnecessary and disproportionate later on.

In the annex of this paper we give two *hypothetical* examples showing how the justification form and the evaluation checklist could be filled in.

[1] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC and Regulation (EU) No 531/2012 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=EN

[2] BEREC Opinion for the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines"

1. Introduction

The EU's Open Internet Regulation (Regulation (EU) 2015/2120), which came into force in 2016, establishes rules for providers of internet access services in the EU to ensure equal and non- discriminatory treatment of internet traffic. The Regulation allows providers to make two types of traffic management:

- Traffic management measures that are *reasonable,* where reasonable means that they have to be proportionate, transparent, non-discriminatory, not be based on commercial considerations, based on objective technical quality of service requirements.
- Exceptional traffic management measures going beyond reasonable traffic management measures (which block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof) that are *necessary,*
    a. to comply with EU or national legislation or court orders,
    b. to preserve the integrity or security of
        i. networks
        ii. services using the networks
        iii. end-user equipment
    c. to prevent an impending network congestion, which is temporary and exceptional.

This document is a technical guideline for NRAs to provide guidance on point b above.

1.1 Scope

The scope of this guideline is the security exception (point b above) to the net neutrality rule. The goal is to help NRAs in evaluating whether or not a particular security measure is *necessary* to preserve the integrity or security of networks, services using the networks. This guideline does *not* prescribe or exhaustively list justifiable security measures, or cyber threats that must be mitigated by providers, because what is justifiable under the exception depends on the circumstances.

1.2 Target audience

This guideline is intended for NRAs in the EU and EFTA countries. This guideline may also be useful for providers of internet access services operating in the EU and EFTA countries.

1.3 Terminology

The term "security measure" is broad and in general security measures can range from the installation of an antivirus software on a computer, to background checks on personnel, incident response procedures, backup power diesel generators, failover submarine cables, etc. In this guideline the term "security measures" refers to the security measures relevant under this exception (i.e. item b of Article 3.3 of the Open Internet Regulation).

In practice, the security measures most commonly implemented by providers under this exception, include measures like port blocking, permanently or temporarily, for certain traffic, for instance outbound traffic, or for certain customers, DNS blackholing, to address malware of DDoS attacks by using DNS redirection, or blocking of IP addresses. In most cases these security measures are directly related to ongoing or recent DDoS attacks or malware campaigns or critical vulnerabilities in common software or protocols.

2. Legal context

The EU's Open Internet Regulation establishes the rules for equal and non- discriminatory treatment of internet traffic provision across Europe. The Regulation enshrines the principle of Net Neutrality into EU law and protects rights of end-users of electronic communication networks and services by providing a legal framework for an open internet. Providers of internet access services are not allowed to block, throttle or discriminate certain end-users or certain traffic, services or applications, except in certain cases. These are when the exceptions of Article 3(3) of the Regulation are met.

We quote Article 3(3) verbatim for the sake of reference:

Article 3 Safeguarding of open internet access

3. Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used.

The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary.

Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:

(a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers;

(b) preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users;

(c) prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

Examples of traffic management measures going beyond the reasonable ones and which might be permissible under the exception b) are mentioned in the preamble 14 of the Open Internet Regulation:

" (14) Second, traffic management measures going beyond such reasonable traffic management measures might be necessary to protect the integrity and security of the network, for example by preventing cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware.".

BEREC in its "Guidelines on the Implementation by National Regulators of European Net Neutrality Rules"[3] provides recommendations to the NRAs on the implementation of their obligations. We quote BEREC's guideline in relation to the security exception (article 3(3) b), for the sake of completeness:

"Article 3(3) (b)

83. Typical attacks and threats that will trigger integrity and security measures include:

• flooding network components or terminal equipment with traffic to destabilise them (e.g. Denial of Service attack);

• spoofing IP addresses in order to mimic network devices or allow for unauthorised communication;

• hacking attacks against network components or terminal equipment;

• distribution of malicious software, viruses etc.

84. Conducting traffic management measures in order to preserve integrity and security of the network could basically consist of restricting connectivity or blocking of traffic to and from specific endpoints. Typical examples of such traffic management measures include:

• blocking of IP addresses, or ranges of them, because they are well-known sources of attacks;

• blocking of IP addresses from which an actual attack is originating;

• blocking of IP addresses/IAS showing suspicious behaviour (e.g. unauthorised communication with network components, address spoofing);

blocking of IP addresses where there are clear indications that they are part of a bot network;

• blocking of specific port numbers which constitute a threat to security and integrity.

85. NRAs should consider that, in order to identify attacks and activate security measures, the use of security monitoring systems by ISPs is often justified. In such cases, the monitoring of traffic to detect security threats (such as those listed in paragraph 84) may be implemented in the background on a continuous basis, while the actual traffic management measure preserving integrity and security is triggered only when concrete security threats are detected. Therefore, the precondition "only for as long as necessary" does not preclude implementation of such monitoring of the integrity and security of the network.

86. Besides monitoring the integrity and security of the network, possible security threats may also be identified on the basis of reports/complaints from end-users or blocking lists from recognised security organisations.

87. This exception could be used as a basis for circumvention of the Regulation because security is a broad concept. NRAs should therefore carefully assess whether the requirements of this exception are met and to request that ISPs provide adequate justifications when necessary."

[3] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules
https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

3. Evaluating the necessity of security measures

This section provides guidance for NRAs in evaluating the necessity of security measures and contains

- A list of evaluation factors that could be taken into account by NRAs,
- A checklist for evaluating the factors and weighing the pros and cons of a measure,
- A justification form, which could be used by NRAs to collect information from providers

3.1 Evaluation factors

Providers of internet access services need to have appropriate security measures in place. To keep their networks and services secure they continuously make risk assessments about security threats, risks and measures. Following a risk assessment, a provider may decide that a certain security measure is necessary to protect the networks, the services using the network, or end-user equipment. This risk assessment takes into account many factors, including the severity of the threat, the cost and complexity of a measure, side-effects etc.

NRAs may need to assess whether or not a certain security measure is justified, for example following a complaint by an end-user. In general, this assessment requires a case-by-case evaluation, because it depends on circumstances, which are specific for that provider. It is impossible to make an exhaustive or prescriptive list of security measures that are justified.

NRAs could take into account the following factors when evaluating if a security measure is necessary:

1) Security risk – the security risk for the network, services, and/or end-user equipment
2) Effectiveness - the effectiveness of the security measure in reducing the risk
3) Proportionality - the proportionality of the measure, i.e. limited in time and scope, few side-effects
4) Appropriateness – the appropriateness of the measure, i.e. in line with industry good practices

The evaluation factors are explained in more detail below.

3.1.1 Security risk

A security risk, associated with a threat, is high if the potential impact of the threat is high and the likelihood that the threat materializes is high. In this context, what matters is the risk for the network, services, and/or the end-user equipment. If the security risk is not high, then the security measure may not be justifiable. Questions to ask:

- How severe and urgent is the security threat?
- What is the potential impact of the security threat?
- What is the likelihood that the security threat materializes and has an impact?

To assess security risk one must look at both the likelihood and the impact. Threats with a low potential impact and a low probability, for instance, are minor risks. Threats with high probability and high impact are major risks. Annex B includes a standard table to rate risks based on likelihood and impact.

3.1.2 Effectiveness

A security measure is effective if it reduces the security risk (see above) significantly. If the measure does not reduce the risk by much, then the security measure may not be justifiable. Questions to ask:

- To what extent is the risk mitigated when the security measure is implemented?
- What would the impact be on the network, services and customers if the measure is not applied?

- What is the residual risk?

3.1.3 Proportionality

A security measure is proportional when it mitigates the threat effectively, without too many side-effects. In the context of the net neutrality rules it is important to assess the impact of the measure on competing services, on 'good' network traffic, 'normal' use of end-user equipment, etc. If the security measure blocks a lot of 'good' network traffic or if the blocking disables an entire network protocol or software application, then the security measure may not be justifiable. Questions to ask:

- Is the scope of the measure limited to specific traffic, networks, or end-user?
- What is the duration, is the measure time-limited?
- Is there impact on 'good' network traffic and legitimate services (false positives)?
- Is there impact for the end-users?

3.1.4 Appropriateness

A security measure is appropriate when it is the right measure for this risk, considering the threat landscape, the technology, industry standards and good practices, alternatives solutions, etc. Questions to ask:

- Is the measure considered the appropriate measure to mitigate this threat/risk?
- Is the measure recommended in industry good practices or standards?
- Are there alternatives that are more effective or more proportionate?

As mentioned already, whether or not a security measure is justifiable as being necessary depends on the circumstances. Providers will need to do a risk assessment and evaluate this on a case-by–case basis. Also, the NRAs may need to evaluate if a security measure is justifiable, by looking at all the factors, weighing the pros and the cons. The table below gives some examples of how these factors could weigh in an evaluation.

FACTORS	MORE JUSTIFIED (+)	LESS JUSTIFIED (-)
Security risk	The risk is major	The risk is minor
Effectiveness	Residual risk is significantly reduced.	Residual risk hardly changed. Risks before and after are similar.
Proportionality	Targeted scope and duration, few side-effects.	Blunt and wide-ranging, many side-effects, lots of good traffic and services are blocked.
Appropriateness	It is a common approach, an industry good practice. No alternatives.	It is an unusual measure for mitigating this threat. Usually done differently.

3.2 Evaluation checklist

An NRA may receive a complaint or be otherwise triggered to investigate if a security measure is justifiable under the net neutrality rules. NRAs can use the evaluation factors in an evaluation procedure, for example as part of an evaluation checklist. We give an example checklist below.

EVALUATION CHECKLIST	
Security measure summary	Provider(s) involved, network/services in scope, summary of security measure

EVALUATION CHECKLIST		
Evaluation factors		
Security risk	++, +, -, or --	Details
Effectiveness	++, +, -, or --	Details
Proportionality	++, +, -, or --	Details
Appropriateness	++, +, -, or --	Details
Overall conclusion	The security measure can/cannot be justified under the security exception in the net neutrality rules, because…	
Recommendation for provider(s)		

3.3 Justification form

As part of an evaluation, NRAs may need to collect information from providers about security measures in place. This section proposes a justification form for collecting and structuring the relevant information about a security measure. Providers could also use this justification form as part of internal processes, to document the reasoning and justification behind security measures.

JUSTIFICATION FORM FOR SECURITY MEASURES – SECURITY EXCEPTION OF THE NET NEUTRALITY REGULATION			
1. General information	**Provider name**	Hint: company name	
	Contact point	Hint: contact name, email	
	Summary	Hint: short name of measure	
2. Legal justification	**Exception to net-neutrality rules, for security measures that are necessary to preserve:**	Hint: Indicate with an X which applies and explain	
	Networks	X	Hint: explain which networks
	services using the networks	X	Hint: explain which services
	end-user equipment	X	Hint: explain which equipment
3. Trigger and duration	**Trigger**	Hint: Describe what triggered the implementation of the measure (external request, request from a CSIRT, internal assessment, user complain, specific event, monitoring etc.)	
	Start time **End time**	Hint: Explain when was the measure first implemented and when it will be removed	

4. Security threat	**Description of the threat**	Hint: Describe the threat (DDoS attack, malware, phishing, spam, vulnerability, etc)
	Reference for the threat	Hint: Reference for this threat of the vulnerability, advisory bulletin and source of information (CVE_ID and other external references describing this vulnerability)
5. Security risk	**Explanation of the risk**	Hint: Explain the risk for the security of the network, service or end-user equipment
	Likelihood	Hint: Assess likelihood, e.g. very low, very high, etc.
	Impact	Hint: Assess impact, e.g. very low, very high, etc.
	Risk	Hint: Rate the risk, e.g. – minor, significant, major
6. Measure details	**Technical description of measure**	Hint: Port blocking, IP blocking, DNS blackholing etc. Specify protocol, port, IPs, inbound/outbound traffic.
	Industry good practice or standard	Hint: Refer to an international standard or industry good practice or recommendation.
	Alternatives	Hint: Alternative measures, possibilities, as possible options for the future
	Networks or services in scope	Hint: All n/w, core, fixed, mobile.
	End-users in scope	Hint: All, some, groups
	Mechanism	Hint: How does the measure protect from the threat
	Effectiveness	Hint: How effective is the measure in reducing the risk
7. Side-effects, communication, opt-out	**Side-effects**	Hint: Are there side-effects for customers (services affected, access to websites), which customers experience side-effects (all, some).
	Communication	Hint: How is the measure communicated to the users (link to policy, or email etc.)
	Opt-out	Hint: Is there an opt-out available for the users, under which circumstances and which is the procedure

In the annex of this guideline we give two examples, using the justification form and the factors for hypothetical cases, using fictitious names of providers:

- Blocking of port TCP/7547 and TCP/5555 (to counter Mirai malware) by the provider FastBits
- Blocking of port UDP/161 (to protect from a Microsoft PC vulnerability) by the provider HomeNet.

Annex A: Examples

In this annex we give two examples by filling in the justification form for some hypothethical cases.

- Blocking of ports TCP/7547 and TCP/5555 to counter Mirai malware by the provider FastBits
- Blocking of ports UDP/161 to protect from a Microsoft PC vulnerability by the provider HomeNet.

For each of these cases, we also show how the factors could weigh in the evaluation by listing, hypothetically, the pros and cons of the implemented security measures.

A.1 Blocking ports 7547 and 5555 by FastBito to mitigate Mirai botnet

JUSTIFICATION FORM FOR SECURITY MEASURES – SECURITY EXCEPTION OF THE NET NEUTRALITY REGULATION			
1. General information	Provider name	*FastBito*	
	Contact point	*G.Puccini - GP@FastBito*	
	Summary	*Blocking of ports 7547 and 5555 to mitigate Mirai*	
2. Legal justification	Exception to net-neutrality rules, for security measures that are necessary to preserve:		
	Networks	*X*	*DDoS attacks flood out networks*
	services using the networks		
	end-user equipment	*X*	*Routers and other Mirai targets (IoT)*
3. Trigger and start time	Trigger	*Internal assessment, media reports about Mirai impact. Mirai botnet is causing large outages due to ever-growing DDoS attacks. Mirai infections also caused outages by disabling home routers.*	
	Start time	*May 2018*	
	End time	*May 2019*	
4. Security threat	Description of the threat	*Mirai malware exploits vulnerabilities in internet connected devices, including routers and IoT devices. The devices are then used for large-scale DDoS attacks.*	
	Reference for the threat	*ENISA Cyber Security info note : "Mirai" malware, attacks Home Routers*	

		https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html
5. Security risk	**Explanation of the risk**	*The Mirai botnet is used for large-scale DDoS attacks with serious impact for targeted websites.*
	Likelihood	*Very high*
	Impact	*Medium*
	Risk	*Major*
6. Security measure details	**Technical description of measure**	*Port blocking, TCP 7547 and 5555, inbound traffic.*
	Industry good practice or standard	*https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers*
	Alternatives	*N/A*
	Networks or services in scope	*Core network, all inbound traffic*
	End-users in scope	*All customers*
	Mechanism	*Protects from infection by Mirai. Prevents Mirai botnet from growing bigger.*
	Effectiveness	*Reasonably effective, for now, but the Mirai botnet will change its attack vector and there are plenty of internet-connected devices with other vulnerabilities.*
7. Side-effects, communication and opt-out	**Side-effects**	*Limited side-effects because port TCP 7547 is only used for device configuration. Routers are usually not configured via the internet but via the local network of the customers or from dedicated hosts in the ISP network.*
	Communication	*Measure explained and listed at: www.fastbito.com/security*
	Opt-out	*Opt-out not available*

Below we show an example of how to use the evaluation factors in an assessment.

FACTORS	PROS	CONS
Security risk	There is a major risk for the terminal equipment of end-users. There is a major risk for ISP networks because DDoS attacks cause large outages.	

FACTORS	PROS	CONS
Effectiveness	Reasonably effective. Measure prevents Mirai botnet from becoming bigger	There are still plenty of vulnerable devices. This measure will be bypassed by the attackers.
Proportionality	Limited side effects (TCP 7547) used only for device configuration	Permanent is too long, should be time-limited, until when the Mirai threat is resolved.
Appropriateness	Measure is widely implemented by ISPs. Measure is mentioned in good practice guideline on mitigating Mirai	A better way to prevent botnets like Mirai from spreading is to patch devices regularly and not use standard passwords on devices like routers!

A.2 Blocking ports 161 and 162 by HomeNet to protect vulnerable computers

JUSTIFICATION FORM FOR SECURITY MEASURES – SECURITY EXCEPTION OF THE NET NEUTRALITY REGULATION			
1. General information	**Provider name**		*HomeNet - Internet for the home*
	Contact point		*M.Zimmermann - MZ@HomeNet.com*
	Summary		*Blocking SNMP 161 and 162 towards customers*
2. Legal justification	**Exception to net-neutrality rules, for security measures that are necessary to preserve:**		
	networks		
	services using the networks		
	end-user equipment	X	*End user equipment, PCs, computers*
3. Trigger and start time	**Trigger**		*Large scale SNMP reflected amplification DDoS attacks observed. Many cyber-attacks use SNMP.*
	Start time **End time**		*May 2017* *May 2018*
4. Security threat	**Description of the threat**		*SNMP Reflected Amplification DDoS attack targeting user devices that are SNMP enabled on the WAN interface.*
	Reference for the threat		*https://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf*
5. Security risk	**Explanation of the risk**		*Difficult to identify the source of the attackers' host or the bot n/w. Large number of end-users infected by malware, high risk for amplification DDoS attack.*

	Likelihood	*High*
	Impact	*High*
	Risk	*Major*
6. Security measure details	**Technical description of measure**	*Blocking SNMP protocol UDP/161 for all customers on the n/w – i.e. between WAN and customers.*
	Industry good practice or standard	*https://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf*
	Alternatives	*N/A*
	Networks or services in scope	*Core network, all inbound traffic*
	End-users in scope	*All customers*
	Mechanism	*Blocks SNMP reflection DDoS attacks*
	Effectiveness	*Effective*
7. Side-effects, communication and opt-out	**Side-effects**	*Limited side-effects because network management is usually not done via the WAN. Some business users may be using SNMP.*
	Communication	*Measure explained and listed at: www.homenet.com/security*
	Opt-out	*Yes, opt-out available – upon request.*

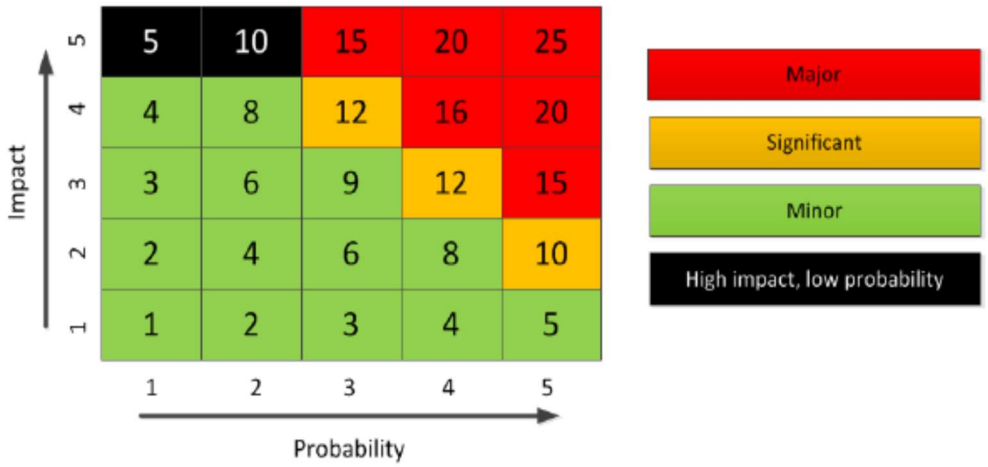
Below we show an example of how to use the evaluation factors in an assessment.

FACTORS	PROS	CONS
Security risk	There is a major risk for the terminal equipment of end-users, of infection of their PCs. There is a major risk for the ISP services, because these infections are used to create DDoS attacks causing outages.	
Effectiveness	Very effective. Measure prevents spreading of infection and reduces DDoS attacks (using SNMP reflection).	
Proportionality	Limited side effects, because SNMP is used for network management which is usually not done over a WAN connection.	

FACTORS	PROS	CONS
	Duration of the measure is time-limited (1 year)	
Appropriateness	Measure is mentioned as an industry good practice	Ideally, remotely exploitable vulnerabilities in devices should be addressed by the device manufacturers and operating system vendors, not the telecom operator.

Annex B: Risk assessment

Risk is usually rated by taking the product of likelihood (probability) and impact. The table below is based on the ISO27005 standard for risk management. In this table, both probability and impact are rated from 1- very low, 2-low, 3-medium, 4-high, to 5-very high.



The resulting scale for risk is minor (green), significant (yellow), major (red) and the risk of threats with a very high impact and a low or very low probability are rated separately, with black. These threats need to be handled with care, because although the chances that these threats materialize are low, the impact may be very high (so-called black swans).

Bibliography

BEREC, "Guideline on the Implementation by National Regulators of European Net Neutrality Rules" [Online]. Available: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

FICORA, Recommendation 312 A/2018 "Filtering traffic in telecommunications operators' networks to certain communications ports for information security reasons", 2018. [Online].
Available: https://www.viestintavirasto.fi/attachments/suositukset/Suositus_312_A_2018_S_EN.pdf

BITAG, "Port Blocking", 2013. [Online].
Available: https://www.bitag.org/documents/Port-Blocking.pdf

BITAG, "Differentiated Treatment of Internet Traffic", 2015. [Online]
Available: https://www.bitag.org/report-differentiated-treatment-of-internet-traffic.php

ENISA, Cyber Security info note ""Mirai" malware, attacks Home Routers", 2016 [Online]
Available: https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

TP-03-18-464-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-271-4
DOI: 10.2824/94531