Norwegian Communications Authority

Archive:	2109259
Date:	15. november 2021
Case handlers:	Lars Edvard Storjord, Frode Sørensen

Discussion paper – DNS-based security measures

General assessment of the security exception in the Open Internet Regulation Article 3(3)(b), and specific assessment of the application on DNS-based security measures, in particular regarding the passage "as necessary, and only for as long as necessary" (Article 3(3)) based on "strict interpretation" (recital 11).

Background information

Would it be allowed for an ISP (Internet Service Provider) to offer "security filters" to their internet access service which prevents subscribers from accessing servers that constitutes security threats, for example sites containing malware, sites that are used for hacking, identity theft or similar?

The essence of the case is that the ISP establishes a list of sites which subscribers are blocked from accessing, which in principle is contradictory to the core of the Open Internet Regulation, that end-users themselves should decide how to use their internet access service. With such a filter, the ISP is exerting control over the subscribers' internet access service.

To that end, usage of security software on the end-user computer would be a less interfering method, since installing and running such software is fully under the control of the end-user. Furthermore, the end-user equipment is out of scope of the Open Internet Regulation.

Another approach could be that the ISP offers an opt-in DNS-based security filter, i.e. that the filter is deactivated by default, and which the end-user could choose to activate (ref. BEREC Guidelines para 32b). Such a filter would run on an additional DNS resolver which would be out of scope of the Open Internet Regulation (ref. BEREC Guidelines para 78c).

The tricky question is whether a DNS-based security filter would be in line with the Regulation in case it is offered as an opt-out solution, i.e. that the filter is activated by default, but the end-user could choose to deactivate the filter at any time. Such a filtering would (to some extent) be under the control of the ISP, and it would be in scope of the Regulation since it is activated by default, running on the default DNS resolver (ref. BEREC Guidelines para 78a).

The Open Internet Regulation describes an exception for blocking etc. for security reasons. Essential in the assessment of which security measures that are justified as exceptions, is the requirement that the exceptions are not applied "except as necessary, and only for as long as necessary" (Art. 3(3)). Furthermore, exceptions should be subject to "strict interpretation" (recital 11).

General considerations regarding the security exception

Article 3(3)(b) describers that the security exception applies in order to "preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users". The provision applies inter alia to security of *services* provided to the end-user, as well as of the *terminal equipment* of the end-user.

Furthermore, recital 14 describes examples of relevant security threats as "preventing cyber-attacks that occur through the spread of malicious software or identity theft of end-users that occurs as a result of spyware." In other words, the recital describes threats against both user equipment (malicious software) and the end-user (identity theft).

Examples of attacks on end-user equipment and measures against malicious software are also described in the BERECs Open Internet Guidelines. Furthermore, the guidelines describe "blocking lists from recognised security organisations" as a source of information about relevant security threats.

Finally, the guidelines underline that since security exceptions may be used as a basis for circumvention of the Regulation, regulators should carefully consider whether the requirements of this exception are met. When assessing this, the regulator should request justification from the ISP. Regarding such assessment, the guidelines refer to the ENISA guidelines about security measures.

Specific considerations regarding the ENISA guidelines

Given that blocking of some security threats may fall under the security exception, it is relevant to consider whether the provision of ***opt-out DNS-based security filter*** as a method would be in line with the necessity requirement, based on a strict interpretation.

The ENISA guidelines mention explicitly DNS-based filtering as an example of security measure by listing "DNS blackholing" which don't return an IP address, and "DNS redirection" which returns an alternative IP address, when requesting domain name resolution.

The ENISA guidelines recommend these four evaluation factors when assessing the necessity of security measures: ***Security risk, effectiveness, proportionality, appropriateness.***

Regarding the evaluation of the security risk, this depends in the specific security threat, and this is further discussed in the next section. The analysis in this section presupposes that the security measure is targeted against specific security threats with high risk. Typical examples of such threats may be hacking attacks and malicious software.

Effectiveness

The ENISA guidelines describe that it could be taken into account to what extent the measure reduces the security risk. DNS-blocking could provide a relatively good protection for ordinary internet users, since most of the internet communication is based on DNS resolution prior to the initiation of the communication. The security filter could be avoided by switching to another DNS resolver, or by communicating directly towards IP addresses that are provided without DNS resolution. However, such technical measures are not frequently met among ordinary internet users.

When comparing opt-out DNS-filters with opt-in DNS-filters, as well as comparing with security software installed on end-user computers, the opt-out DNS-filter will have considerable better effectiveness, since not all end-users will in practice activate an opt-in filter DNS-filter or install security software on their computers.

The fewer users that use security measures, the more negatively this will impact the level of security of those who actually use security measures, since unprotected user equipment will constitute an access point to security attacks and the spreading of malicious software.

The effectiveness of using opt-out DNS-filters as a security measure is therefore considered to be reasonably good for ordinary internet users, as long as the security threats are identified correctly.

Proportionality

Furthermore, the ENISA guidelines explain that the scope of the security measure should be considered, as well as limitation of any side-effects. Then the guidelines describe that it is important to consider whether the measure may also lead to blocking of content that is not intended to be blocked. Regarding DNS-filtering, there is a risk of false positives, since the list of blocked sites to some extent may also block sites where the threat is removed, and some of the blocked sites may contain both content that constitutes a security threat and content that does not.

Regarding proportionality, the ENISA guidelines suggest considering whether the scope of the security measure is limiting specific traffic, specific networks or specific users. Compared to an opt-in DNS-filter, and compared to security software installed in the end-user computer, an opt-out DNS-filter will have a broader scope since it applies to all subscribers unless they deactivate the filter.

The proportionality of providing a DNS-filter as a security measure is therefore considered to have a more limited scope when it is provided as an opt-in solution than when it is provided as an opt-out solution. There is also a risk of false positives. However, the number of subscribers what are impacted in practice could be reduced by providing user-friendly ways to deactivate the filter, as well as informing properly about the availability of the possibility to deactivate the filter. Furthermore, the tendency of false positives could be mitigated by the provider by establishing and performing effective procedures for checking the blocking lists, as well as informing properly about how to report about false positives. The accuracy of the filter is crucial for this criterion.

Appropriateness

Regarding the appropriateness, the ENISA guidelines describe that it could be considered whether the security measure is recommended as an industry good practice or standard, and whether alternatives exist which are more effective or proportionate.

DNS-filtering is already often used to block subscribers from accessing sites that court orders mandate ISPs to block under to Article 3(3)(a). DNS-filtering as a method to prevent people from accessing selected sites could therefore be considered to be an industry standard.

Regarding alternative security measures, an opt-in DNS-filter and security software installed on the end-user computer would be less effective than opt-out DNS-filter, but the alternatives would provide more proportionate measures, as discussed in the two subsections above.

Overall consideration

In summary, an opt-out DNS-filter would have reasonably good effectiveness as a security measure for ordinary internet users. At the same time, the proportionality would be limited since the measure would apply to all subscribers unless they deactivate the filter, and since there is a risk for false positives. Regarding appropriateness, DNS-filtering could be considered an industry standard, but alternatives to opt-out DNS-filtering exist. The alternatives would be less effective, even though they would be more proportionate. (Regarding assessment of security risk, refer to next section.)

In conclusion, when comparing opt-out DNS-filter, opt-in DNS-filter and security software installed on end-user computers, the latter two methods could unconditionally be applied in line with the Open Internet Regulation. However, opt-out DNS-filter could also be applied in specific cases, under the conditions that the ISP exercises comprehensive procedures ensuring high degree of accuracy of the filter, as well as high level of transparency. These two conditions are discussed in the next section.

Nasjonal kommunikasjons-myndighet

Guidance regarding DNS-based security measures

The conclusion of this discussion paper corresponds to BEREC guidelines (para 32b) which clarifies that when assessing restrictions implemented by the ISP as endpoint-based services (such as opt-in DNS-filter and security software installed on end-user computers), the regulator may take into account whether end-users remain in full control of the internet access service, and the end-user may activate and deactivate the security measure, and whether the default configuration that the ISP activates fully complies with the Open Internet Regulation.

Furthermore, the discussion paper has considered an opt-out DNS-filter implemented by the ISP on the internet access service offered, assessed under the security exception (ref. Article 3(3)(b)), in particular with regard to the passage "as necessary, and only for as long as necessary", based on a strict interpretation (ref. recital 11).

The conclusion is that the security exception ***may be applicable under certain conditions***.

Considerations regarding security risk of different security threats

Average users of the internet access service are in general not technically skilled and have limited knowledge about how to protect their internet communication against security threats. On the other hand, internet users are today exposed to many security threats, which constitute a threat against the individual user, but also a significant threat against the society. Since our society is becoming increasingly dependent on internet communication, the need to ensure a good level of security of the internet access service is high.

Regarding which ***types of security threats*** that could be considered to constitute sufficiently high risk (ref. ENISA guidelines), the following generic threats could be relevant examples of concrete attacks and threats which could be further assessed for inclusion in an opt-out DNS-filter:

- computer viruses, worms, and other types of malicious software
- hacking, botnets and denial of service attacks
- identity theft and other internet-based fraud
- websites hosting phishing activity

Regarding the necessity requirements "as necessary, and only for as long as necessary", it is a prerequisite that the ISP ensures that ***each specific, concrete security blocking*** included in the blocking constitutes a severe security threat, and that it is removed from the list as soon as possible when the threat decreases. The ISP is referred to the ENISA guidelines for a more detailed description of the evaluation factors to assess for each specific security blocking. Nkom will closely monitor compliance, and the ISP will be requested to report, and/or substantiate, how the necessity requirements are enforced in practice.

Detailed guidance regarding opt-out DNS-based security filters

If an ISP offers opt-out DNS-based security filters, it is a prerequisite that the ISP:

- Ensures that each specific security blocking included in the blocking list constitutes a severe security threat in line with the requirements of the Open Internet Regulation, and ensures that the list is continuously up to date. The regulators may according to Article 5(2) of the Open Internet Regulation at any time request information about the assessments conducted by the ISP for the specific security measures.
- Provides clear and comprehensible explanation about the security measures and what kind of security threats that are blocked, and informs about how the ISP ensures that the security measure is in lined with the Open Internet Regulation.

- Provides transparent, user-friendly and efficient procedures to address complaints regarding any blocking which is suspected to be caused by false positives.
- Provides transparent, user-friendly and effective methods for the subscribers to deactivate (and activate) the security measure at any time.
- In each concrete occurrence of blocking, provides clear and comprehensible explanation to the end-user about why the blocking took place, and informs about the methods for the subscribers to deactivate the security filter.
- Preferably uses a dedicated web page to inform about the security measure together with other information related to open internet. This would contribute to increased visibility and accessibility to information about the security measure, which is a prerequisite for the internet users to actually be informed.