BEUC The European Consumer Organisation

The Consumer Voice in Europe

THE REVIEW OF THE NETWORK AND INFORMATION SECURITY DIRECTIVE

BEUC's response to the public consultation

Contact: Frederico Oliveira da Silva – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2020-117 - 08/12/2020

Why it matters to consumers

The number of services migrating to the digital environment is skyrocketing and reaching all sectors of society, including transport, health, banking and energy. While digitalisation provides many benefits for consumers, the cybersecurity risks and challenges this transition entails are significant. A cyberattack on companies that ensure the functioning of key sectors of our society, such as energy power plants, road systems or cloud services, can have a particularly negative impact on consumers and societies. EU rules need to ensure that these companies have implemented strong cybersecurity features that will increase their resilience to malicious attacks.

Summary

BEUC welcomes the Commission's public consultation on the revision of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information security across the Union (NIS Directive).

While the NIS Directive was expected to strengthen cybersecurity across the EU, several challenges remain. In this sense, BEUC would like to highlight the following elements for a successful review of the Directive:

- The telecoms sector should be included in the definition of 'Operators of Essential Services' (OES).
- Social media platforms should be included in the category 'Digital Service Providers' (DSPs).
- The selection procedure of OES must be consistent all across the EU.
- The same rules should apply to DSPs and OES. The current light-touch approach applicable to OES should be abandoned.
- The provisions on security requirements should be more prescriptive.
- Affected users should be notified immediately about the reason behind the unavailability of their services. This notification should include information that would allow them to mitigate the adverse effects of the cyberattack.
- The implementation of the NIS rules must be accompanied by strong oversight mechanisms. Affected users should have the right for remedies whenever there is evidence of negligence or non-compliance with the rules from OES/DSPs.

1. Introduction

BEUC welcomes the Commission's public consultation on the revision of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information security across the Union (NIS Directive).

The list of cyberattacks on critical infrastructure is long and growing and reconfirm the need for strong IT security. In December 2015, a cyberattack targeting a power grid left 230,000 Ukrainians in the dark.[1] In June 2019, a cyberattack hit four hospitals in Romania.[2] This attack led to a slowing down of admissions, discharges and prescriptions. The ransomware used to hack the hospitals system would have been detected by antivirus software but none of the affected hospitals had that in place. In September 2020, a patient passed away in Germany after a cyberattack caused the failure of a hospital's IT system.[3]

The NIS Directive obliges Member States to establish a national strategy for the security of network and information systems. This strategy should set out strategic objectives and appropriate policy and regulatory measures. It also obliges Member States to improve the cybersecurity of critical sector operators, including health, energy and financial services, and certain digital service providers such as search engines, cloud services or online marketplaces.

However, while the NIS Directive was expected to strengthen cybersecurity across the EU, several challenges remain.

2. Scope of the NIS Directive

BEUC supports an expansion of the scope of the Directive's two main categories of services – Operators of Essential Services (OES) and Digital Service Providers (DSPs).

The **telecoms sector** should be included in the definition of 'Operators of Essential Services'. While the recent review of the European Electronic Communications Code (EECC) has introduced robust cybersecurity provisions, it is important to ensure consistency between organisations that provide essential services, including undertakings providing public communications networks or publicly available electronic communications. For this reason, we support the introduction of the telecoms sector in the scope of the NIS law provided it is in line with the *lex specialis derogat legi generali* principle. In other words, the EECC rules shall prevail over the new NIS rules, who will only apply as a 'safety net' when and if the EECC rules fail to regulate a specific situation.

Moreover, **social media platforms** should be included in the category 'Digital Service Providers'. These services are among those whose exposure to cybersecurity attacks is among the highest. However, despite their popularity among users and continuous cybersecurity breaches/vulnerabilities, they are currently excluded from the scope of the Directive. While social media platforms already fall under the scope of the General Data Protection Regulation (Arts. 32 – 34 in particular, related to the security of personal data processing), the rules of the NIS Directive go beyond personal data and have a specific focus on security (e.g. a service can become unavailable whilst not having issues related to personal data protection).

[1] Ref.: https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report
[2] Ref.: https://www.romania-insider.com/cyberattack-victor-babes-hospital-june-2019
[3] Ref: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94

3. Selection procedure of 'operators of essential services'

The European Commission's proposal must ensure that the selection of operators of essential services is consistent across the EU (Article 5).

Unfortunately, this has not been the case so far with Member States following very different approaches when it comes to the selection of OES. According to a recent report from the European Commission, the number of identified OES per Member State ranges from 12 to 87. While we can expect that larger Member States would identify slightly more OES than smaller Member States, the report adds that there is not a strong correlation between the size of a Member States and the number of services selected.

First, Member States have been establishing very different thresholds to identify OES: some have been using single quantitative factors (e.g. number of users relying on a service); others have been using a larger number of quantitative factors (e.g. number of users plus market share).

One of the consequences of (high) quantitative thresholds is that smaller but critically important essential services (e.g. clinics and other healthcare organisations whose unavailability can endanger the safety of consumers) are left out of the scope of the Directive. It is absolutely crucial that a reform of the NIS Directive ensures that smaller operators of essential services also fall under its scope.

Secondly, in certain Member States, entire sectors of essential services mentioned in Annex II (e.g. healthcare) were excluded from the scope of the Directive. A review of the NIS Directive should clarify this issue by ensuring that all the sectors/subsectors are covered by the Member States. Furthermore, it is particularly important to ensure that all hospitals are covered by the mandatory cybersecurity requirements. Often the same databases and patient records storage systems are used in healthcare settings at national level, therefore by allowing exemptions for smaller hospitals it might create 'weak' spots for unauthorised access to data.

This inconsistency in the selection procedure increases the lack of legal clarity for companies, consumers and Member States authorities. As a consequence, the risk of successful cybersecurity attacks increases.

4. Rules applicable to 'digital service providers' and 'operators of essential services'

BEUC does not agree with the differentiated and light-touch approach applicable to DSPs. These services are very popular with consumers and – as the current pandemic has shown – increasingly important to our economy and society. The consequences of a successful cyberattack would have an important impact. (Many companies have migrated their work to cloud services during the pandemic. An attack in their service would probably paralyse them.)

As it is the case with OES, national competent authorities should have the obligation to supervise pro-actively and generally monitor whether DSPs comply with the security measures foreseen in the NIS Directive.

Also, Art. 15 (4) states that in the event of security breaches that also affect personal data, Computer Security Incident Response Teams (CSIRTs) shall contact data protection authorities. But this seems to hold only for OES-related incidents. In the corresponding Article for DSPs (Art. 17), no such provision is given.

5. Cybersecurity requirements

The provisions on security requirements (Article 14 (1) and (2); Article 16 (1) and (2)) should be more prescriptive. In addition to the generic reference to 'security measures', these provisions should underline, in detail, a minimum set of measures that every Member State needs to implement. Only a certain level of detail in terms of the basic mandatory requirements will allow convergence of national approaches in the implementation of these rules. In this regard, it is important to note that the revised rules should continue to follow a minimum harmonisation approach which enable Member States to implement stricter rules.

When it comes to which specific security measures should be made mandatory for both OES and DSPs, those established in the Implementing Regulation and guidance document applicable from the Cooperation Group should be carefully considered.

Finally, operators of essential services should be obliged to ensure compliance with the obligations of the new NIS law by means of mandatory certification.

6. Notification of cybersecurity incident

The establishment of a culture of information sharing and cooperation is key to increase cybersecurity resilience and consumer protection.

First, the new law needs to improve the rules on notification of incidents to affected users (Articles 14 (6) and 16 (7)). While it is understandable that information about an incident may not be disclosed to the general public (e.g. public disclosure could trigger further cyberattacks), affected users should be notified immediately about the reason behind the unavailability of their services. This notification should include information that would allow them to mitigate the adverse effects of the cyberattack.

Second, when it comes to the 'incident notification' provisions, several terms lack legal clarity. E.g. 'incidents having significant impact' must include (i) successful cybersecurity attacks but also (ii) failed cybersecurity attempts (i.e. incidents that could have had a significant impact on the continuity of the service if it wasn't for the efficient prevention).

7. Enforcement of the NIS Directive

The new law the rules must be accompanied by strong oversight mechanisms. For example, national competent authorities in charge of monitoring the application of the new law (Art. 8) should be able to perform regular checks to ensure the respect of the rules and the good functioning of a mandatory certification scheme. They should be provided with the adequate resources to do so. Also, dissuasive penalties should be put in place against OES/DSPs who have not complied with the obligations of the Directive. In this regard, the new law must clarify that affected users should have the right for remedies whenever there is evidence of negligence or non-compliance with the rules from OES/DSPs.

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).