The Consumer Voice in Europe

REVIEW OF THE NETWORK AND INFORMATION SYSTEMS DIRECTIVE (NIS 2)

Position paper

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-2021-042 - 06/05/2021

Why it matters to consumers

Most consumer services – whether transport, health, banking or energy – are moving to a digital environment. While digitalisation provides many benefits for consumers, the cybersecurity risks and challenges it brings are significant. A cyberattack on companies that ensure the normal functioning of our daily lives, 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 measures that will increase their resilience to malicious attacks.

Summary

BEUC welcomes the Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union[1] ('NIS 2'), which will replace the current Network Information Systems (NIS) Directive.

While the NIS Directive aimed to strengthen cybersecurity across the EU, several challenges remain. That is because it does not cover all digital service providers (such as social media). Even where the NIS Directive does cover a sector, such as health, it gave Member States too much autonomy to determine which specific entities from that sector are covered.

Thus, BEUC would like to highlight the following elements for a successful review of the Directive and a strong NIS 2:

- Expand the scope:
  - The scope of the new NIS Directive should be expanded to cover all web-based services (e.g. apps and websites) available to consumers.
  - The new law must ensure that the implementation of the NIS Directive, in particular the selection of additional entities that play a "key role for the economies and societies of Member States" mentioned in Art. 2 (2) of the proposal, is consistent across the EU.

- Strengthen the obligation to notify about cybersecurity incidents and threats:
  - Whenever there is an incident having a significant impact on the provision of a service (Art. 20 (1)) or a significant cybersecurity threat to a service (Art. 20 (2)), the default rule should be that affected users or potentially affected users of those services should be notified *immediately* about the unavailability or possible unavailability of the service.
  - In both situations (incident and threat), users should be provided with information that would enable them to mitigate the adverse effects of the cyberattacks.
  - Whenever there is a breach of the obligation to notify, essential and important entities shall be held liable for the damaged caused to consumers by such inaction.

[1] https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

- Better enforcement of the rules:
  - As it is the case for 'essential entities', competent authorities should be able to monitor the compliance of 'important entities' with the Directive's rules *ex-ante* (Article 18).
  - Affected users should have the right for remedies (e.g. financial compensation in case of damage) whenever there is evidence of non-compliance from essential or important entities with the rules of NIS 2.
  - The NIS 2 should be added to Annex I of the Representative Actions Directive[2] to allow for better access to remedies in case consumers have been harmed due to non-compliance with the directive.

- The Report on the state of cybersecurity in the Union (Art. 15) should not be limited to cybersecurity problems exclusive to the NIS Directive. It must include regular assessment of the general level of cybersecurity awareness amongst consumers as well as on the general level of security of consumer connected devices.

[2] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

1. Introduction

BEUC welcomes the Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union ('**NIS 2**'), which will replace the current NIS Directive[3].

Recent cyberattacks reconfirmed the need for strong IT security of critical infrastructure and digital services. In December 2015, a cyberattack targeting a power grid left 230,000 Ukrainians in the dark.[4] In June 2019, a cyberattack hit four hospitals in Romania.[5] 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.[6]

The current rules of the NIS Directive oblige 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 NIS Directive was expected to strengthen cybersecurity across the EU, several challenges remain at this stage.

First, the scope of the NIS Directive is too limited, especially when it comes to digital service providers. For example, as recent events have shown us[7], social media platforms are among the digital service providers whose exposure to cybersecurity attacks is among the highest. They have nevertheless been excluded from the scope of the Directive and therefore have no obligation to comply with its cybersecurity rules.

Secondly, according to the current NIS Directive, it is under the responsibility of each Member State to identify their 'operators of essential services' (OES) that would be subject to the rules of the Directive. Even if the Directive provides a mandatory list of seven key sectors form which these entities must be selected, Member States have the autonomy to establish the criteria for the selection of operators of essential services which makes everything more complex and insecure. This led to Member States following very different approaches when it comes to the selection of OES. This means that consumers in some countries will be more vulnerable to cyberattacks on important infrastructure.

Another important question is the need to cover key providers who do not fall under the scope of the NIS Directive. In the health sector for example, not all hospitals or healthcare professionals may be identified as part of critical infrastructure, and therefore do not fall under the scope of the NIS Directive.

[3] Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union;
[4] https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report
[5] https://www.romania-insider.com/cyberattack-victor-babes-hospital-june-2019
[6] https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94
[7] https://www.washingtonpost.com/politics/2021/04/06/cybersecurity-202-massive-facebook-breach-underscores-limits-current-data-breach-notification-laws/

2. Scope of the NIS Directive (Article 2)

2.1. Extension of the scope

BEUC welcomes the introduction of the telecoms sector (Article 2 (2) a) i) of the proposal) to the scope of the Directive. First, while the review of the European Electronic Communications Code (EECC)[8] introduces cybersecurity rules (Art. 40 and 41 EECC), some of the critical measures it puts in place (such as encryption) are not mandatory. Under the current NIS 2.0 proposal, however, cybersecurity requirements, including encryption are mandatory (Article 18 (2) g)). Secondly, the inclusion of this sector under the NIS will ensure legal consistency in terms of cybersecurity requirements as well as enforcement procedures in all sectors of society (energy, healthcare, etc.).

We also welcome the inclusion of additional services such as social media services to the scope of the new law. These services are very popular with consumers and among those whose exposure to cybersecurity attacks is the highest.

We believe however that the scope of this law should also be generally extended to web-based digital services (such as mobile applications, online websites) available to consumers. These services are currently not subject to any specific IT security EU law and are thus not obliged to comply with any cybersecurity requirements. While web-based services 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 and those of the new proposal go beyond personal data and focus on security. That is, a web-based digital service can become unavailable whilst not having issues related to personal data protection.[9]

2.2. Important and essential entities

One of the main shortcomings of the current NIS Directive is the selection procedure of 'operators of essential services' (Article 5 of the NIS Directive). As explained above, the high level of discretion left to Member States has led to an inconsistent application of the current rules. As noted by the Commission[10], in certain Member States, major hospitals do not fall within the scope of the current NIS Directive and are thus not required to implement security measures. On the other hand, in other Member States, almost every single healthcare provider is covered by the rules of the NIS.

For that reason, we strongly support the abolition of the obligation to identify 'operators of essential services' and the introduction instead of two different categories: 'essential entities' listed in Annex I and 'important entities' listed in Annex II.

2.3. Exception regarding small and medium enterprises (Art. 2 (2)).

When it comes to entities that are not included in Annex I (essential entities) or Annex II (important entities), including small and medium enterprises, they will fall under the scope of the new law if they play a "*key role for the economies and societies of Member States*" (Recital 9). This is the case when:

- An entity is a public administration entity (Art. 2 (2) b))
- An entity that is the sole provider of a service in a Member State (Art. 2 (2) c));

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG;
[9] In a recent position paper, our German member VZBV also highlighted the need to improve the current rules of the NIS Directive and to expand its scope to digital services.
[10] Page 1 of the Explanatory Memorandum accompanying the Proposal.

- An entity in which a potential disruption of the service it provides could have an impact on public safety, public security or public health (Art. 2 (2) d));
- An entity in which a potential disruption of the service it provides could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact (Art. 2 (2) c)).

Member States shall establish a list of entities identified according to these subpoints and submit it to the Commission 6 months after the transposition deadline of the new law. This list shall be reviewed on a "regular basis and at least every two years" (Art. 2 (2)).

As was the case for the current NIS Directive regarding the selection of 'operators of essential services', we fear that the discretion given to Member States in the selection procedure of these additional entities under the scope of NIS 2 will lead to legal fragmentation. To avoid this, the new law must ensure that the implementation of the NIS Directive, in particular the selection of additional entities mentioned in Art. 2 (2) of the proposal, is consistent across the EU.

BEUC demands:

- BEUC supports the expansion of the scope to the telecoms sector and to social media.
- The new NIS Directive should be expanded to all web-based services available to consumers.
- The new law must ensure that the implementation of the NIS Directive, in particular the selection of additional entities that play a "key role for the economies and societies of Member States" mentioned in Art. 2 (2) of the proposal, is consistent across the EU.

3. Report on the State of the Union (Article 15)

According to Article 15 of the proposal, the European Union Agency for Cybersecurity (ENISA) will issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union.

BEUC welcomes this new initiative and the increasing active role of ENISA in cybersecurity topics in the EU. ENISA is in a privileged position to support the development of a coherent EU approach towards cybersecurity and to help ensure the protection of consumers' privacy and security. We believe however that the report should not be exclusive to cybersecurity problems related to the NIS Directive.

For example, the report should also include an assessment on the general level of cybersecurity awareness amongst consumers as well as on the general level of security of consumer connected devices. [11]

Raising consumers' awareness about cyber hygiene best practices, such as whether to open an email from an unknown sender (to avoid the so-called `phishing´ practice), install a software update or use two factor authentications system, can make the difference between an attempt and a successful cyberattack. It is important to keep monitoring the level of knowledge of EU consumers regarding these challenges.

[11] For context, see BEUC's position paper on cybersecurity here.

BEUC demand:

- The Report on the state of cybersecurity in the Union should not be limited to cybersecurity problems exclusive to the NIS Directive. It must include regular assessment of the general level of cybersecurity awareness amongst consumers as well as on the general level of security of consumer connected devices.

4. Notification of a cybersecurity incident to consumers (Article 20)

The establishment of a culture of information sharing and cooperation is key to increase cybersecurity resilience and consumer protection. Crucially, consumers whose data has been accessed following a cybersecurity attack must be notified in a timely manner. Unfortunately, the proposal does not establish a sufficiently strong obligation on service providers to notify users affected by a cyberattack or cyberthreat.

According to Article 20 (1), *where appropriate,* essential and important entities shall notify without undue delay the users of their services of any *incident having a significant impact* in the provision of that service.

Similarly, Article 20 (2) establishes that, *where appropriate*, essential and important entities shall notify to the recipients of their services that are potentially affected by a *significant cybersecurity threat* of any measures or remedies that those recipients can take in response to the threat.

While it is understandable that information about an incident can remain hidden from the general public (e.g., public disclosure could trigger further cyberattacks), the default rule should be that affected users or potentially affected users should be notified immediately about the reason behind the unavailability of their services or about any potential serious threat. Such notification should include information that would allow them to mitigate the adverse effects of the cyberattack.

The obligation to notify affected and potentially affected users can only be delayed in case of overriding reasons such as high risk that a notification could lead to new attacks or worsen the ongoing situation. However, in this scenario, organisations need to communicate to their national competent authorities, once the attack or threat is no longer ongoing, the reasons behind such delay.

Whenever there is a breach of the obligation to notify, essential and important entities should be held liable for the damaged caused to consumers by such inaction. If consumers are not aware of an ongoing cyberattack or threat, they will not be able to avoid any (additional) damage.

BEUC demands:

- Whenever there is an incident having a significant impact on the provision of a service (Art. 20 (1)) or a significant cybersecurity threat to a service (Art. 20 (2)), the default rule should be that affected users or potentially affected users of those services should be notified immediately about the unavailability or possible unavailability of the service.
- In both situations (incident and threat), users should be provided with information that would enable them to mitigate the adverse effects of the cyberattacks.

- The obligation to notify affected users or potentially affected users can only be delayed in case of overriding reasons (such as a high risk that notification worsens the ongoing attack). This decision needs to be communicated to the national competent authorities once the attack or threat have ended.
- Whenever there is a breach of the obligation to notify, essential and important entities shall be held liable for the damaged caused to consumers by such inaction. If consumers are not aware of an ongoing cyberattack or threat, they will not be able to avoid any (additional) damage.

5. Role of certification schemes (Article 21)

Under Article 21 of the proposal, Member States may require essential and important entities to use certification schemes to demonstrate compliance with certain cybersecurity requirements of the new NIS directive.

BEUC supports the use of certification schemes for the purposes of ensuring compliance with the substantive rules of the directive provided that the schemes are mandatory. From a consumer perspective, consumers' trust is likely to improve if a service is tested under a strict and impartial conformity assessment procedure. In this regard, ENISA and the European Commission should start working on possible future schemes related to the compliance of the new NIS Directive rules.

These certification schemes however should be mandatory.

BEUC demand:

- The use of certification schemes by essential and important entities to ensure compliance with the NIS Directive should be mandatory (Art. 21).

6. Enforcement of the NIS Directive (Articles 28 – 34)

6.1. Differentiation between 'Essential entities' and 'important entities'

While the new proposal has the merits to merge the substantial cybersecurity measures applicable to 'essential entities' and 'important entities' under the same provision (Art. 18), significant and concerning disparities between these two categories exist at the enforcement level.

First, competent authorities can act ex-ante when it comes to 'essential entities' (Art. 29 of the proposal). However, when it comes to 'important entities', they can only act ex-post when they are provided with evidence or indication that an important entity is not in compliance (Art. 30 (1) of the proposal).

Also, Article 29 (5) of the proposal establishes that where enforcement actions prove ineffective, Member States' authorities will have the possibility to set a deadline and require the 'essential entity' to take the necessary action to comply with the Directive. If the requested action is not taken within the deadline, national authorities will have the power, inter alia, to suspend part or all the services or activities provided by the essential activity. Unfortunately, similar rules are not applicable to 'important entities'.

BEUC does not agree with this approach. 'Important entities' such as social media and postal services are very popular with consumers and – as the current pandemic has shown – increasingly important to our economy and society.

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

To be able to successfully comply with these tasks, national competent authorities should be given the adequate human, financial and technical resources.

6.2. Remedies for affected users

The new law must guarantee that users affected by a cyberattack on an essential or important entity should have the right to remedies, such as financial compensation in case of damage, whenever there is evidence of non-compliance from the service provider with the cybersecurity measures established in Art. 18 of the proposed NIS Directive that caused the damage.

For example, if a non-compliant internet service provider is hacked and as a consequence an entire neighbourhood has no internet for several hours, affected consumers should receive compensation for the damage they have suffered (e.g., impossibility to work).

In this regard, it is important to ensure that the NIS 2 is added to Annex I of the Representative Actions Directive in a similar way to Article 72 of the Digital Services Act. This would allow a number of consumers to jointly bring a court case to obtain compensation for damage which arises from the same cyberattack.

BEUC demands:

- As it is the case for 'essential entities', competent authorities should be able to monitor the compliance of 'important entities' with the Directive's rules *ex-ante* (Article 18).

- Affected users should have the right for remedies (e.g., financial compensation in case of damage) whenever there is evidence of non-compliance from essential or important entities with the rules of NIS 2.

- The NIS 2 should be added to Annex I of the Representative Actions Directive to allow for better access to remedies in case consumers have been harmed due to non-compliance with the Directive.

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