Raising standards for consumers

The Consumer Voice in Europe

CYBERSECURITY FOR CONNECTED PRODUCTS

Position Paper

Contact: Chiara Giovanni (ANEC) and Frederico Silva (BEUC) – anec@anec.eu - digital@beuc.eu

Ref: ANEC-DIGITAL-2018-G-001final - BEUC-X-2018-017
07/03/2018

ANEC, THE EUROPEAN ASSOCIATION FOR THE CO-ORDINATION OF CONSUMER REPRESENTATION IN STANDARDISATION
Av. de Tervueren 32, box 27 – 1040 Brussels - +32 (0)2 743 24 70 - www.anec.eu
EC register for interest representatives: identification number 507800799-30

BUREAU EUROPEEN 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 • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Funded by the European Union

Table of content

Why it matters to consumers

Consumers are increasingly using connected devices in their daily lives. Already today, Europeans can remotely switch on the lights in their house, turn on their washing machine or open their door lock with their smartphone. This ongoing digitalisation requires that consumers' devices are protected against cyberattacks. While the number of connected products is rising, many of these products are manufactured without basic security features embedded in their system. This lack of security eventually increases the risk that consumers become victims of a malicious cyberattack and will distrust the Internet of Things. Thus, a EU policy response to reduce cybersecurity risks is urgently needed.

Summary

Today, most of the connected devices available in the EU's Single Market are designed and manufactured without the most basic security features embedded in their software.

In order to trust the Internet of Things, consumers must be assured that the connected products they purchase or services they use are secure and protected from software and hardware vulnerabilities. For this to happen security by design and by default must become a priority.

To this end, ANEC and BEUC would like to suggest some elements to improve the current regulatory framework as well as the European Commission's proposal for a Cybersecurity Act:

- A minimum set of security measures should be obligatory for all connected products as a condition for putting them on the market. These requirements should include at least encryption, software updates and strong authentication methods.

- The General Product Safety Directive as well as product specific safety legislation (Toy Safety Directive, Low Voltage Directive, Radio Equipment Directive, etc.) must be updated to ensure that they are in line with the new 'security for safety' concept of the general legal framework[1].

- ANEC and BEUC call on the European Commission to swiftly adopt a delegated act clarifying which products would fall under the 'privacy requirement' foreseen in Article 3 (3) of the Radio Equipment Directive. Connected products for consumers should be included within this category.

- For high-risk-affected connected products (e.g. self-driving cars, products for children, smart home and security products, smart cities systems, medical devices), the application of minimum security requirements should be complemented with mandatory cybersecurity certification.

- National authorities should be able to withdraw products from the market that do not comply with legal security requirements and/or certification schemes.

[1] It is interesting to note that in many languages the term 'safety' and 'security' are the same (*surete*, *seguridad*, *sicurezza*, *Sicherheit*).

1. Context and background

In recent years, consumers' daily lives have become increasingly connected and digitalised. With the Internet of Things (IoT), the number of connected devices and services skyrocketed and interconnectivity between products reached all sectors of society (transport, health, banking, energy, etc.). According to recent estimations from the European Commission, there will be up to six billion connected products by 2020.[2]

The Internet of Things and the proliferation of connected devices brings many benefits to consumers. Connected devices are convenient and simplify numerous aspects of consumers' daily routines. For example, consumers are now able to track their physical activity, to use their energy more efficiently and even open their doors remotely through a smart lock in case they forgot their keys inside. According to a recent study, 67% of Europeans believe that digital technologies have a positive impact on their quality of life.[3]

However, from a consumer perspective, an increase in the number of connected products is also a cause for concern. More connected products translate in more vulnerabilities for hackers to exploit. As the IoT ecosystem grows, the exposure of connected products to an eventual cybersecurity breach also increases. As pointed out by the European Commission, in 2016 more than 4,000 ransomware[4] attacks happened per day. This represents an increase of 300% compared to 2015. In some Member States, half of all the crimes are cybercrimes.[5]

Consumers are concerned about the security of their products. According to the latest European Commission Eurobarometer survey, 86% of consumers believe that the risk of becoming a victim of a cybercrime is increasing. Also, 87% of consumers avoid disclosing personal information online because of cybersecurity-related issues.[6]

One of the key reasons behind the increase of cyberattacks is the lack of security functionalities incorporated in the design of the connected products and/or services. Today, most of the connected devices available in the EU's Single Market are designed and manufactured without the most basic security features embedded in their software.

This has recently become evident with the exposure of two critical security flaws - named 'Meltdown' and 'Spectre' – in computer processors produced by Intel, AMD and ARM over the last two decades.[7]

Tests by our member organisations have demonstrated similar risks. Two recent campaigns from our Norwegian member Forbrukerrådet have echoed the inadequate security mechanisms of popular consumer connected products intended for children – and sold across the EU. The first campaign (#ToyFail[8]), which was launched in December 2016, looked at the technical features of popular connected toys sold in the EU market. They

[2] Ref.: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
[3] European Commission, Special Eurobarometer 460, Attitudes towards the impact of digitalisation and automation on daily life, May 2017
[4] Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. (Definition from Wikipedia)
[5] European Commission Staff Working Document, Impact Assessment accompanying the proposal for a Regulation on a Cybersecurity Act, Part 1, p. 12
[6] European Commission, Special Eurobarometer 464a, Europeans' attitudes towards cyber security, September 2017
[7] Ref.: https://www.cnet.com/news/spectre-meltdown-intel-arm-amd-processor-cpu-chip-flaw-vulnerability-faq/
[8] Ref.: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

discovered that with a few simple steps anyone could access the microphone of the doll Cayla, one of the connected toys tested, and speak with the children through it without the knowledge of their parents. The second campaign (#WatchOut[9]), which was launched in October 2017, tested the security features of smart watches whose main function is to enable parents to keep in touch with their children and track their real-time location. Again, Forbrukerrådet discovered serious security flaws in these devices, including the possibility for an attacker to easily change the geo-location of the watch ('location spoofing'[10]) as well as track and contact the child directly.

Recent investigation from Which?, our UK member group, revealed that four out of seven tested connected toys could easily be hacked and enable anybody to use the toy to communicate with a child.[11] In a recent campaign, Test-Achats/Test-Aankoop[12], Stiftung Warentest[13] and OCU[14], consumer organisations from Belgium, Germany and Spain, found similar security flaws and revealed that anyone could connect to the Bluetooth network of the toys without being required to insert a password or any other type of authentication setting.

While these campaigns reveal the impact that the vulnerability of connected devices can have on the consumers themselves, it is important to keep in mind that the general lack of security of connected products can also have an adverse impact on society. In January 2014, security researchers uncovered that the first massive IoT botnet attack[15] was performed by more than 100,000 poorly secured consumer connected products, such as smart TVs or smart fridges, that had been affected without their consumers' knowledge.[16] More recently, in October 2016, a massive attack used hundreds of thousands of insecure consumer devices who had been infected with a specific malware called Mirai to disrupt the internet and bring down websites such as Twitter, Amazon, Spotify and Netflix.[17]

The current EU regulatory framework is not fit to address the current security threats of products connected to the IoT environment. In key consumer product legislation such as the General Product Safety Directive[18], Radio Equipment Directive[19], Toys Safety Directive[20] and Low Voltage Directive[21], the safety concept is completely outdated and does not cover security risks that are generated through the connected products and the risk to be hacked.

---

[9] Ref.: https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf
[10] A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage (Definition from Wikipedia)
[11] Ref.: http://press.which.co.uk/whichpressreleases/which-issues-child-safety-warning-on-connected-toys/
[12] Ref.: https://www.test-achats.be/action/espace-presse/communiques-de-presse/2017/interconnected-toys
[13] Ref.: https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/
[14] Ref.: https://www.ocu.org/organizacion/prensa/notas-de-prensa/2017/juguetes-conectados-201217 and https://www.ocu.org/consumo-familia/bebes/noticias/juguetes-conectados-wifi
[15] A botnet attack can be typically described as a network of infected devices (botnet) that once activated by the master can be used for illicit purposes (Definition from ENISA)
[16] Ref.: https://arstechnica.com/information-technology/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet/
[17] Ref.: https://www.test.de/Schadsoftware-Das-Internet-der-Dinge-infiziert-5249226-0/
[18] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety
[19] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
[20] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys
[21] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits

Furthermore, while there are different pieces of legislation that contain cybersecurity provisions[22], the security essential requirements of connected products remain unregulated. For example, while the Radio Equipment Directive could potentially contribute to ensure the security of the data of connected products when placed on the EU market, its scope of application remains however unclear.

In November 2017, four global and European consumer organisations[23], including BEUC and ANEC, published general recommendations to make consumer rights, privacy and security core features of the Internet of Things.[24]

2. Security by design and by default

In order to trust the Internet of Things, consumers must be assured that the connected products they purchase or services they use are secure and protected from software and hardware vulnerabilities. For this to happen, security by design and by default must become a priority.

Security by design means that all connected products and services should better incorporate state of the art cybersecurity functionalities at an early stage of their design process and before the products are put on the market. Security by default means that the settings of a connected device and service are secure as a basic setting (e.g. only high-security measures for authentication such as complex and long passwords should be allowed for ID authentication).

It is important to ensure that the design of the products is constantly being improved and developed. While non-connected products could stay in the market for twenty years without having to develop their design, this is no longer the case with connected products. In many consumer-oriented connected devices, common practices often include cheap components in order to cut costs. This could negatively impact on security implementation, as the security features in low-cost and low-energy components are often limited.

To ensure a high-level of security by design and by default, a minimum set of requirements for security should be binding for all connected products as a condition for putting them on the market. Such a horizontal and binding framework should be established as a complement of existing and pending legislation that requires cybersecurity measures such as the General Data Protection Regulation[25] and the proposal for a European Electronic Communication Code.[26]

While identifying in detail the specific security measures needed to ensure security by design and by default for all products would go beyond the scope of this paper, we enumerate below some principles that should underpin the security features of every consumer connected device. On this note, it is key that the legislative framework

[22] Directive on security of network and information systems (NIS Directive), Telecoms Framework and proposal for a directive establishing the European Electronic Communications Code, General Data Protection Regulation (GDPR), proposal for a e-Privacy Regulation
[23] ANEC, BEUC, Consumers International and International Consumer Research & Testing (ICRT)
[24] http://www.beuc.eu/publications/beuc-x-2017-137_securing_consumer_trust_in_the_internet_of_things.pdf
[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[26] Proposal for a Directive establishing the European Electronic Communications Code

establishing a minimum set of security requirements is regularly reviewed to ensure that the list of requirements keeps track of the technological evolution.

2.1. Encryption

Currently, many connected devices and services don't have the most basic encryption[27] protection. Encryption is an essential tool to enhance safety and security in digital products and services. It helps protecting information and is often the last place of defence within a specific product. For instance even if passwords are breached, encryption systems can prevent hackers from accessing the content of the data.

All manufacturers and service providers should ensure that the data stored in their services as well as the data stored by their connected products is properly encrypted. They should also ensure that third parties that access the data are keeping it properly encrypted. In this regard, the use of techniques such as 'hashing', 'obfuscation' and 'asymmetric methods' should be encouraged. Finally, any communications coming in and out of the connected product should be encrypted end-to-end.

2.2. Up-to-date software

When consumers buy a connected product such as mobile phone, a smart TV or a connected toy, they have the right to a product that is as complete and secure as possible considering the state of technology at the time. Manufacturers shall make sure that when they first put a product on the market, the software that runs on the product is as secure and up-to-date as it can be.

In addition, manufacturers should also be required to ensure that the software is updated during the entire lifecycle of the product whenever this is needed to guarantee that it remains secure.

The effort to maintain connected products continuously secured is important because many cyberattacks are only possible precisely because the security protections of connected products are inadequate, outdated, or the necessary security updates have not been rapidly provided.

In the proposal for a Directive on Digital Content[28], the European Parliament and the Council of the European Union are considering specific obligations concerning updates applicable to software included in goods will probably be stipulated. Such updates should be provided during the lifetime of the product. The adoption of this legislative proposal is expected in late 2018.

Not all updates are related to increasing the security of the connected product. The current flood of updates, for example for mobile phones, can be burdensome for consumers who are not informed whether the update is for security reasons or for the functionality of the device. In general, overloading consumers, especially consumers in vulnerable circumstances, with complex technical information is not an effective way to inform them.

[27] Encryption is the process of encoding a message or information in such a way that only authorized parties can access it (definition from Wikipedia)
[28] Proposal for a Directive on certain aspects concerning contracts for the supply of digital content

It is therefore important to improve the transparency of software updates for consumers. At present, it is not always clear whether the proposed updates are necessary to improve security, to resolve a software bug, or to install new functionalities or whether they serve other purposes. Suppliers must explain the reason of the update and its impact on the product, and importantly, must never misuse the update for example to unilaterally change the conditions of the service. Consumers should be informed about the consequences of not accepting a software upgrade.

Additional measures are necessary in critical situations where vulnerabilities are discovered and can be imminently exploited, putting millions of consumers and their connected products at risk of cyberattacks. For example, in the recent 'Wannacry' ransomware attack[29], Microsoft issued a patch to correct a vulnerability in their Windows operating system. However, some months later, several companies had not yet implemented the patch therefore remaining vulnerable to a cyberattack. In May 2017, a massive cyberattack exploited this vulnerability and affected more than 200,000 computers worldwide running on Windows by encrypting the users' data and demanding ransom payments.

To avoid these critical situations, where thousands of connected products remain vulnerable during a substantial period of time even if a security update has already been provided, manufacturers must take measures to ensure that consumers and companies are aware that a critical security update has been issued and that the security of their products and services depends on its implementation.

In exceptional circumstances where there is an increased risk to the safety of consumers (e.g. when using a self-driving car), security updates can be installed automatically. However, in this case, the update should only be processed automatically on the condition that

(i) consumers are notified about it immediately,
(ii) the update does not negatively affect the performance of the connected device and
(iii) manufacturers are not circumventing the rules on consent established by the data protection legislation, including the ePrivacy Regulation[30], under the disguise of critical security updates.

2.3. Strong authentication settings installed by default

Lack of or weak ID authentication is often the favoured entrance door for hackers. For example, a recent campaign from our UK member Which? discovered that the Bluetooth connection of I-Que Intelligent Robot, a popular connected toy which had already been investigated by our Norwegian member in 2016, is unsecure. Because no authentication settings (i.e. password) were installed by default anyone would have been able to download the app that connects with the toy, find an i-Que within Bluetooth range and start chatting with the child using the robot's voice by typing into a text field.[31]

[29] Ref.: https://www.europol.europa.eu/wannacry-ransomware
[30] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Proposal for a Regulation on Privacy and Electronic Communications
[31] Ref.: https://www.youtube.com/watch?v=Ogy7xjEWEp

Connected products and services intended for consumers should by default only accept state of the art security authentication methods. This is for example the case of passwords that contain a certain level of complexity (e.g. usage of uppercase, lowercase letters and numbers needed; encourage the use of symbols, enable the use of ASCII characters, UNICODE characters and emojis; not accept passwords with less than 8 characters, etc.).

Another example of authentication method with a high level of security is two-factor authentication. Manufacturers and service providers should be encouraged to add two-factor authentication systems to their default settings. Typically, two-factor authentication systems confirm the users' identity through two different elements: something they know (e.g. password) and something they possess (e.g. code sent to personal email or personal phone).

Needless to say, strong security features should not decrease the accessibility level needed by consumers with disabilities to access digital products and services.

ANEC and BEUC recommendations :

- A minimum set of security measures should be obligatory for all connected products as a condition for putting them on the market.
- These requirements should at least include encryption, software updates and strong authentication mechanisms:
    - All manufacturers and service providers should ensure that the data stored in their services and the data stored by their connected products is encrypted. Manufacturers and service providers shall also ensure that third parties accessing the data keep it properly encrypted. Finally, communications coming in and out of the connected product should be encrypted end-to-end.
    - Manufacturers shall make sure that when they first put a product on the market, the software that runs on the product is as secure and up-to-date as it can be. In addition, manufacturers should also be required to ensure that the software is updated during the entire lifecycle of the product whenever this is needed to guarantee that it remains secure.
    - Connected products and services intended for consumers should by default only accept state of the art security authentication methods. This is for example the case of passwords that contain a certain level of complexity (e.g. numbers, capital letters, etc.) and two-factor authentication systems.
- The regulatory framework establishing a minimum set of security requirements shall be regularly reviewed to ensure that the list of security requirements follows the technological evolution.
- The personal data collected through connected devices shall be adequately protected according to the General Data Protection Regulation.

3. Cybersecurity and EU regulatory framework

The current EU legislative framework does not ensure that only safe and secure connected products are placed on the market.

In addition, the current legislation cannot cope with the fact that connected devices come along with a whole new range of players whose actions have an impact on the safety of a product. In particular those who manufacture the product and the software and those who store or may make use of collected data and which offer additional services are often not the same. This may raise a whole new range of questions about who is responsible for safety in case something goes wrong. It also complicates enforcement enormously. As products can receive updates remotely, not all changes in a product may even be under the control of the manufacturer of the device.

3.1. Product Safety

3.1.1 'Security for safety'

Thanks to the General Product Safety Directive and sector-specific legislation such as the above-mentioned Radio Equipment Directive or the Toys Safety Directive**,** manufacturers are obliged to only make safe products available on the market. However, the concept of 'safety' is too narrow and fails to protect consumers from the security flaws which come along with connected devices thereby jeopardising the safety of the users.

This is because product safety is understood in the traditional sense only with regard to their potential harm to consumers' health and physical integrity such as through exposure to harmful chemicals and physical injuries. This concept of product safety is outdated knowing that devices which can connect to the internet can be hacked and thereby create new risks from distance.

Such a restrictive approach also prevents market surveillance authorities from using their enforcement powers and to withdraw unsecure connected products from the EU market. One year after the #ToyFail campaign (see chapter 2) exposed connected toys with serious security flaws they are still being sold on the EU market. All the retailers who removed these products from the market did so on a voluntary basis. Only the German market surveillance authority requested the destruction of these products. It is important to highlight however that this request was not based on product safety legislation but rather on a national anti-espionage act.

If the current safety regulatory framework was broadened to also include security, national market surveillance authorities would be able take specific corrective measures to bring the product back to conformity whenever a product does not comply with the safety requirement. Among these corrective measures is the possibility to withdraw the product from the market.[32]

Furthermore, the extension of product safety legislation would also enable public authorities to notify unsecure products putting at risk the safety of their users on the Rapid Alert System (RAPEX).

[32] Article 40

When the Internet of Things was still a distant reality, the compliance of non-connected devices with safety requirements was sufficient to ensure the safety of their users. This is no longer the case with the proliferation of connected devices. In the Internet of Things era, both the safety and security of the product are key to ensure the safety of their users. The connected toys which our members tested could be considered safe according to product safety legislation but still have serious security flaws that might endanger the safety of their users.[33]

ANEC and BEUC recommendations:

- Product safety legislation needs to be amended to ensure that the security of all connected devices placed in the EU markets do not pose a safety risk for its users.
- The General Product Safety Directive as well as product specific safety legislation (Toy safety directive, Low Voltage Directive, Radio Equipment Directive, etc) must be updated to ensure that they are in line with the new 'security for safety' concept of the general legal framework.

3.1.2 Example of the Radio Equipment Directive

In addition to the extension of the concept of safety, the Radio Equipment Directive (RED) also contains a provision addressing the protection of personal data and privacy of the users. This provision also requires that radio equipment is constructed with a certain level of data security. However, this provision is not operational and its full range and potential are still unclear.

Although the RED has been applicable since 13 June 2016, the European Commission has not made use of its prerogative to determine the products to which the 'privacy requirement' should apply. Given the increase of cyberattacks and the threat they represents to the consumers' privacy, it is of the outmost importance to fill the current legal gap and to speed-up the process.

ANEC and BEUC recommendations:

- ANEC and BEUC call on the European Commission to swiftly adopt a delegated act clarifying which products would fall under the 'privacy requirement' foreseen on Article 3 (3) of the RED. Connected products for consumers should be included within this category.

3.2. Product liability

Another severe shortcoming in the legislative framework is the fact that the Product Liability Directive[34] which dates from 1985 is outdated.

[33] It is interesting to note that in many languages the term 'safety' and 'security' are the same (*surete*, *seguridad*, *sicurezza*, *Sicherheit*).
[34] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

These rules should be updated to ensure that rules on product liability apply to any professional in the product supply chain, including creators of digital content or software, when their activities have affected the safety of a product which was then placed on the market. Then, there is a problem about how to identify the liable person when the same product is made by several producers and contributors. There should be joint liability of professionals in the product supply chain. Since the consumer has the burden of proof, the victim will have otherwise no possibility of recourse under the current Directive.

BEUC has already made policy recommendations recently and we hope that the EU Commission will take them up in their ongoing review process of this Directive.

4. EU proposal for a Regulation: 'Cybersecurity Act'

Following the announcement by President Juncker in his State of the Union speech, the European Commission unveiled a board cybersecurity package in September 2017.

This section of the paper outlines BEUC's position only as regards the proposal for a Regulation on ENISA, the 'EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on information and Communication Technology Cybersecurity ("Cybersecurity Act").

In line with the structure adopted in the proposal, we will assess its two main elements – review of ENISA's mandate and the establishment of a Cybersecurity Certification Scheme – separately.

4.1. European Network and Information Security Agency (ENISA)

In the first part of its proposal[35], the European Commission proposed to review and strengthen the current role of the European Union Agency for Network and Information Security (ENISA).

BEUC is in favour of strengthening the role of this agency. The last revision of ENISA's mandate dates from 2013 under Regulation 562/2013[36] and as already explained above, the cybersecurity ecosystem has changed considerably since. In light of the new challenges, a more coordinated EU approach towards cybersecurity is key to ensure the protection of consumers' privacy and security.

In particular, we would like to highlight the following points of the European Commission's proposal:

- **Review of the current mandate**: ENISA is the only EU agency with a fixed term mandate.[37] The European Commission proposal will now convert it into a permanent mandate. BEUC welcomes this proposal as it will enable ENISA to plan consistent long-term strategies but also to comply with its obligations under the Directive on security

[35] Articles 3 to 42
[36] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
[37] ENISA's current mandate expires in 2020

of network and information systems (NIS Directive), which go beyond its current mandate.

- **Consumer protection**: BEUC regrets that the new proposal does not make consumer protection a priority of the new ENISA's mandate. As explained above, consumer connected products lack the most basic security functionalities and 86% of consumers fear that the risk of becoming a victim of a cybercrime is increasing. It is therefore crucial that the proposal includes a clear reference to the protection of consumers.

- **Governance of ENISA**: The current proposal should ensure that the interests of consumers are appropriately represented in the governance structure of ENISA. This should translate into the nomination of a consumer expert for the Management Board of ENISA as well as a balanced composition of ENISA's Permanent Stakeholders' Group. In the current Permanent Stakeholders' Group, only one expert out of thirty members of the Group represents consumers' interests.[38]

- **EU Cybersecurity Certification Scheme**: Under the European Commission's proposal, ENISA will be entrusted with the task of preparing, at the request of the Commission, a candidate cybersecurity certification scheme. Among other tasks, ENISA will have to consult stakeholders during the preparation of its schemes. BEUC supports the direct involvement of ENISA in the preparation of a certification scheme. However, ENISA should systematically and regularly consult consumer experts during the preparation of a certification scheme. In order to be able to provide a valuable input, the provision of consumers' expertise should be financially supported by the EU institutions, similar to the functioning of the EU's eco-design policy implementation.[39]

- **Awareness raising**: BEUC welcomes the reinforcement of ENISA's role as regards raising awareness to the public about general cyber security threats. ENISA shall, among others, provide guidance on the best cyber hygiene practices as well as regularly organising, in cooperation with Member States, awareness raising campaigns.

  According to the European Commission's latest Eurobarometer, more than half of respondents (51%) considered themselves not well informed about cybercrimes.[40] An informed consumer will significantly decrease his/her chances of being the victim of a successful cyberattack. Raising consumers' awareness about cyber hygiene best practices, such as whether to open an email from an unknown sender (in order to avoid the so-called `phishing´[41] practice), install a software update or use two factor authentications system, can make the difference between an attempt and a successful cyberattack.

- **Impartiality and transparency**: In light of the growing importance of the work of ENISA, impartiality and transparency will be important requirements for the agency in the years ahead.

[38] Ref.: https://www.enisa.europa.eu/about-enisa/structure-organization/psg
[39] Ref.: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009L0125
[40] European Commission, Special Eurobarometer 464a, Europeans' attitudes towards cyber security, September 2017
[41] Phishing attacks are a means to persuade potential victims into divulging sensitive information such as credentials, or bank and credit card details. (…) The attack usually takes the form of SPAM mail, malicious Web sites, email messages, or instant messages, appearing to be from a legitimate source such as a bank, or a social network. (Definition from ENISA)

ANEC and BEUC recommendations:

- ENISA's mandate and tasks should have a clear and prominent obligation to promote a high-level of consumer protection.
- Consumer experts should be systematically and regularly consulted by ENISA during the preparation of a certification scheme. To be able to provide a valuable input, consumers' expertise should be supported financially by the EU institutions.

4.2. EU Cybersecurity certification scheme

In the second part of its proposal, the European Commission proposed to establish a new European ICT Security Certificate *framework* laying down the rules for the development of individuals EU-wide cybersecurity certification schemes for specific ICT products and services or cybersecurity risks.[42] These provisions should lead to the issuing of certificates valid and recognised in the whole EU.

It is important to clarify that the proposal does not introduce operational certification schemes but the rules of procedure for the establishment of such schemes. It determines who requests the schemes (Commission), who prepares them (ENISA), who grants them to the manufacturers (national conformity assessment bodies), the scope of the scheme (e.g. identification of the products to which it applies) as well as the general purpose of the scheme (e.g. ensure compliance with cybersecurity requirements such as the protection of data against unauthorised access).

BEUC welcomes that the European Commission is stepping up on the critical issue of cybersecurity. Our members' campaigns have exposed the poor (or inexistent) level of security features embedded in connected products and the urgent need to address the cybersecurity risk related to mass consumer connected devices.

While we generally support the European Commission's intention to introduce a framework for a EU cybersecurity scheme, we have doubts about the effectiveness of the instrument as proposed by the European Commission due to its voluntary nature and complicated governance structure. We are worried about its potentially limited capacity to improve the security features of consumer connected products and services, which is urgently and quickly needed.

4.2.1 Certification schemes

According to Article 48 (2), the certification of a connected product remains *voluntary*. In other words, the adoption of a certification scheme by the European Commission will not force manufacturers to evaluate the security features of their connected products and/or services in accordance with that scheme.

First, while consumers' trust is likely to improve if a product is tested under a strict and impartial conformity assessment with strong security criteria, there are no guarantees that

[42] Articles 43 to 54

manufacturers will adhere, on a voluntary basis, to the European Commission's certification schemes.

On the contrary, recent campaigns from our members have proven that, even when confronted with evident security vulnerabilities, manufacturers remain reluctant to act and improve the security functionalities of their products. Almost one year after the #ToyFail campaign, Which? (UK) reassessed the security features of some of the toys tested by Forbrukerrådet (NO) only to find that the security flaws identified in December 2016 had not been corrected yet.[43]

Secondly, a voluntary scheme is likely to lead to market fragmentation, which is precisely what this proposal is trying to prevent. Consumers in Europe would be faced with the situation where some connected products would be certified, while others – used for similar purposes – would not.

Thirdly, it is an established principle in the European Union that products for consumers must be safe. Moreover, manufacturers have to apply the precautionary principle. The adoption of a voluntary certification is likely to lead to the situation where consumers will be faced with the problem that some products are safer or more secure than others with a probable impact on the final price of the product.

For this reason, BEUC believes that it is necessary to establish binding minimum security requirements before connected products and services are placed on the market. In addition, for high risk connected products intended for consumers (e.g. self-driving cars, products for children, door looks, electricity control or heating systems of smart homes and surveillance products like alarms or video cameras), the application of horizontal minimum security requirements should be complemented with mandatory cybersecurity certification. This is necessary to guarantee an appropriate high level of cybersecurity and to improve the trust of consumers in the security features of the products and services they use.

4.2.2 Transparency on the prioritisation of certification schemes on products intended for consumers

According to Article 44 (1) of the European Commission's proposal, it is under the exclusive responsibility of the European Commission, via a request to ENISA to prepare a candidate certification scheme, to start the procedure for the establishment of a certification scheme.

In the Communication accompanying the cybersecurity package, the European Commission identified consumers connected products as one of their key priorities for certification: "*The use of "security by design" methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things: schemes under the framework could be used to signal that the products are built using state of the art secure development methods, that they have undergone adequate security testing, and that the vendors have committed to update their software in the event of newly discovered vulnerabilities or threats*."[44]

While we welcome this reference, the proposal fails to clarify how the European Commission will determine the consumer products and services for which a certification scheme is a priority.

[43] Ref.: http://press.which.co.uk/whichpressreleases/which-issues-child-safety-warning-on-connected-toys/
[44] Joint Communication to the European Parliament and the Council 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', JOIN/2017/0450 final

4.2.3 Security criteria

The proposal further mentions that every certification scheme will provide a detailed specification of the requirements used to evaluate the product.

The security requirements chosen to evaluate a connected product change depending on the product and its main function. Nonetheless, as already highlighted in section 2, there are a few security elements – without the prejudice of adding others – that should always be taken in consideration when assessing the security features of a product.

4.2.4 Different levels of assurance

The European Commission's proposal establishes that a certification scheme *may* specify one or more of the three assurance levels – basic, substantial and high – for connected products and services issued under that scheme.

From a consumer perspective, it is not acceptable to attribute specific levels of assurance to a certification scheme. While we understand that the cybersecurity requirements against which connected products and services are evaluated differ from one product to the other, the hypothetical expectations of consumers should not be taken as a basis. Cybersecurity requirements should always aim for a high level of security for consumers and where appropriate establish additional elements for products in which higher standards of security are needed due to the object of protection e.g. critical infrastructure and health and financial data.

4.2.5 Market surveillance and effective sanctions

The monitoring and surveillance provisions of the national certification supervisory authorities should be strongly reinforced in order to build consumers and other stakeholders' trust in the system. Rigorous and robust market surveillance should be ensured by setting quantifiable and proportionate targets for checks of certified and non-certified products. To this end, Member States should coordinate their inspection activities, and share capacities of their laboratories, to avoid expensive double-testing.

Member States should also be forced to put in place effective sanctions against manufacturers whose products do not comply with this legislation and/or the certification schemes in place. Among these sanctions should be the possibility for national authorities to withdraw unsecure products from the market.

ANEC and BEUC recommendations:

- For high risk connected products (e.g. self-driving cars, products for children, smart home and security products, smart cities systems, medical devices), the application of minimum security requirements should be complemented with mandatory cybersecurity certification.
- The proposal should clarify how the European Commission will prioritise the products and services for which it will request ENISA to prepare a candidate scheme.
- Cybersecurity requirements should always aim for the highest level of security for consumers and where appropriate establish additional elements for products in which higher standards of security are needed due to the object of protection.
- National authorities should be able to withdraw from the market products that do not comply with the current proposal and/or the certification schemes in place.

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