The Consumer Voice in Europe

Ref.: BEUC-X-2018-024/UPA/cs 16 March 2018

Subject: Cybersecurity Act - Consumers need mandatory security by design and by default

Dear Rapporteurs and shadow rapporteurs,

I write on behalf of BEUC, The European Consumer Organisation, in view of the ongoing discussion on the European Commission's proposal for a proposal for a Regulation on ENISA, the 'EU Cybersecurity Agency" and on information and Communication Technology Cybersecurity ('Cybersecurity Act').

All sorts of connected devices are already pouring into consumers' homes, pockets, cars and offices. While the arrival of the Internet of Things brings many benefits to consumers, it also comes with a tremendous increase in exposure and risk to problems linked to cybersecurity. More connected products translate in more vulnerabilities for hackers to exploit. The latest European Commission barometer survey shows that 86% of consumers believe that the risk of becoming a victim of a cybercrime is increasing.

Products that go onto retailers' shelves must be secure, but that's not the case today

The biggest downside of the Internet of Things for consumers today is the lack of security of connected products and services. Currently, many popular connected devices already available to consumers are designed and manufactured without ensuring the most basic security.

Several of our members have made this evident:

- Our Norwegian member Forbrukerrådet discovered serious security flaws in popular GPS smart watches, for example the possibility for an attacker to easily change the geo-location of the watch ('location spoofing') as well as track and contact the child directly.[1]

- An investigation from our UK member Which? revealed that four out of seven connected toys tested could easily be hacked and enable anybody to use the toy to communicate with a child.[2]

[1] Ref.: https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf
[2] Ref.: http://press.which.co.uk/whichpressreleases/which-issues-child-safety-warning-on-connected-toys/

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.beuc.eu • www.twitter.com/beuc
TVA: BE 0422 071 051 • EC register for interest representatives: identification number 9505781573-45

- Our members Test-Achats/Test-Aankoop[3], Stiftung Warentest[4] and OCU[5], from Belgium, Germany and Spain respectively, 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 mechanism.

In conclusion, today European consumers are increasingly exposed to unsecure connected products which put their safety, privacy and economic interests at risk.

The Commission's 'Cybersecurity Act' proposal will not tackle this serious problem …

Unfortunately, the European Commission's proposal for a 'Cybersecurity Act' missed the opportunity to ensure a high-level of security for consumer-oriented connected products.

By setting up a framework for the establishment of a *voluntary* certification scheme, the European Commission's proposal fails to effectively improve the security features of connected products, which is so urgently and quickly needed.

… and it is therefore crucial that the European Parliament amends it to introduce mandatory cybersecurity by design and by default principles

We call on the European Parliament to amend the European Commission's proposal to establish mandatory principles of security by design and by default.

In our view, these principles must be substantiated around a set of **minimum binding security requirements that would work as the legal basis for all connected products to comply with. Such requirements would include often simple yet very important security features such as: software updates, strong authentication mechanisms and encryption.**

Establishing such a legal basis is important for consumers but also for market surveillance and other public authorities to be able to enforce such rules effectively on the market.

Like with many other areas, the Internet of Things has developed, and permeated consumers' lives faster than our legal framework could keep pace. That means that the EU cannot wait any longer to establish a regulatory solution for this problem. Voluntary certification alone will not be a successful policy response due to a lack of incentives for producers to invest in security.

Thank you for taking our concerns into consideration. To illustrate our recommendation, we have attached a proposed amendment to the Cybersecurity Act jointly developed with ANEC that you can find in Annex to this letter.

We remain at your disposal should you have any questions or wish to receive further feedback.

Yours sincerely,

Ursula Pachl
Deputy Director General

[3] Ref.: https://www.test-achats.be/action/espace-presse/communiques-de-presse/2017/interconnected-toys
[4] Ref.: https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/
[5] Ref.: https://www.ocu.org/organizacion/prensa/notas-de-prensa/2017/juguetes-conectados-201217

Raising standards for consumers

The Consumer Voice in Europe

Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency" and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

Article 43a (New)
Security by design and by default

Commission Proposal	BEUC Proposal
	1. Taking into account the state of the art, producers and service providers shall ensure the security by design and by default of their ICT products and services. **Producers and service providers must ensure that the software running on their ICT product or service is secure and does not have any known security vulnerability considering the state of the art technology at the time.** **ICT products and services must implement the following technical measures:** **(a) ICT products and services must be provided with up to date software and must include mechanisms to receive secure, properly authenticated and trusted software updates on a regular basis;** **(b) remote access capabilities of the ICT product or service must be documented and secured against unauthorized access during the installation at the latest;** **(c) ICT products shall not have the same default hardcoded standard passwords for all devices;**

	(d) Data stored by ICT products and services must be securely protected by state of the art methods such as encryption; **(e) ICT products and services shall only accept high-security methods for authentication.** **2. Producers and service providers must notify the competent authority of any known security vulnerabilities as soon as they are discovered. In addition, they must provide a timely repair and/or replacement to overcome any new security vulnerability discovered.** **3. ICT products and services placed on the market shall comply with the obligations in paragraph 1 during their foreseeable and normal period of use.** **4. The Commission shall by means of implementing act, and in cooperation with ENISA, adopt detailed rules on the specificities of the security requirements provided in paragraph 1**. **5. Where the market surveillance authorities have reasons to believe that the ICT product or service does not comply with the requirements laid down in this Regulation, they shall without delay require the relevant producer or service provider to take appropriate corrective action to bring the product into compliance with those requirements, to withdraw the product from the market, or to recall it within a reasonable period, commensurate with the nature of the risk, as they may prescribe.** **6. Where the producer or service provider does not take adequate corrective action within the period referred to in paragraph 5, the market surveillance authorities shall take appropriate provisional measures to**

	prohibit or restrict the product being made available on their national markets, to withdraw the product from that market or to recall it. **7. Market surveillance authorities shall organise appropriate checks on product compliance and oblige the producers or servide providers to recall non-compliant products from the market. When identifying the products that will be subject to compliance check, national certification authorities shall prioritise high risk products for consumers, products embedded with new technologies and/or products with high selling rates.**