The Consumer Voice in Europe

Cyber Resilience Act: cybersecurity of digital products and ancillary services

BEUC response to public consultation

Contact: **Cláudio Teixeira – digital@beuc.eu**

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

Co-funded by the European Union

Ref: BEUC-X-2022-051 - 25/05/2022

Why it matters to consumers

The number of digital services and connected devices is skyrocketing and they are increasingly interconnected and present in consumers' lives. Consumers expect the products they purchase to be safe and secure. Cyberattacks on connected devices put consumers at risk and endanger their privacy and security, even their physical safety. They can also lead to personality theft and have a financial cost. It is fundamental that the EU develops a strong horizontal legal framework to ensure that companies set up strong cybersecurity measures to protect consumers in this connected environment.

Summary

BEUC – The European Consumer Organisation welcomes the opportunity to respond to the public consultation on the Cyber Resilience Act (CRA). We fully support this initiative to improve cybersecurity protection for consumers in the EU. The CRA must introduce a new horizontal framework to adequately protect consumers from insecure products, notably by establishing mandatory minimum-security requirements for all connected devices.

In the age of the Internet of Things, when everything is connected, a cybersecurity incident is no longer an isolated affair: it can affect entire systems, disrupting economic and social activities and harming consumers in many different ways. Over the past years, BEUC members have demonstrated that too many connected products sold on the European market lack the most basic security features. These products are putting consumers at risk on a daily basis. However, despite the mounting evidence, little has been done to tackle this problem.

To ensure that consumers are adequately protected and can trust digital markets, there must be a solid guarantee that their connected products are both safe and secure to use. The CRA must ensure these products are secure by design and by default. It must put in place mandatory baseline cybersecurity requirements for both manufacturers and sellers of digital products and their ancillary services.

In particular, BEUC recommends the European Commission includes the following elements in the forthcoming CRA proposal:

- Common, mandatory cybersecurity rules applicable to all connected products marketed to/intended for consumers and their associated services.
- A broad scope and clear definitions covering all types of digital products and ancillary services. Rules should not exclusively focus on high-risk products.
- The principle that all connected devices intended for consumers are secure by design and by default.
- Mandatory baseline cybersecurity requirements should cover at least encryption, software updates and strong authentication methods.
- Mandatory cybersecurity certification for products to be considered high risk.
- Strong, effective enforcement mechanisms and clear provisions on remedies and means of redress for consumers when obligations are not respected.

1. Introduction

BEUC – The European Consumer Organisation welcomes the opportunity to respond to this public consultation. We strongly support the intention of the European Commission to deliver on the announcement made by President Ursula Von der Leyen in her State of the Union speech[1] in 2021 to propose a new Cyber Resilience Act (CRA). This new horizontal cybersecurity legislation should establish mandatory, minimum security requirements for all connected devices.

There has been a rise in the number of connected devices in recent years. Since the emergence of the first digital products connected to the Internet, the use of connected devices has become mainstream. All kinds of appliances are now becoming dependent on an internet connection to function. They are more interactive, easier to use, and with more functionalities than ever before. From household appliances to assist us with our daily chores to security cameras which protect our homes, and from the toys our children play with to the connected cars that we drive to work or even the medical devices that monitor our health, connected devices are playing a central role in virtually all aspects of our lives – even in those areas we once thought there would not be relevant to the digital sphere.

However, the widespread use of connected products without sufficient cybersecurity protection raises serious concerns from a consumer perspective. As the IoT ecosystem expands into all levels of our daily lives, it also increases the exposure of connected products and their users to cybersecurity risks. More connected products also mean more cybersecurity risks and vulnerabilities for their users, creating unprecedented opportunities for bad actors to take advantage of.

Connected devices typically process vast amounts of data about their users and their environment, which raises substantial concerns from a data protection and privacy perspective. In addition, many connected devices may pose direct safety threats to consumers, should they be hacked.[2]

For example, the proliferation of so-called ‘stalkerware’ - software that takes advantage of microphones and cameras embedded in products - allows malicious individuals to spy on consumers inside their homes or wherever they go. Spyware allows hackers to take control over consumers’ surrounding environment, by hacking their devices and monitor their security cameras,[3] shut down their cars[4], or even stop their connected pacemakers.[5]

Another kind of attack on the rise has been ‘ransomware’, which essentially locks users out of their computers and/or threatens them with the loss or compromising of their data against payment of a monetary ransom.[6] This kind of attack is particularly widespread, regardless of whether the victim is a student or a media company.[7]

[1] *"[W]e cannot talk about defence without talking about cyber. If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces. And we should not just be satisfied to address the cyber threat, but also strive to become a leader in cyber security. It should be here in Europe where cyber defence tools are developed. This is why we need a European Cyber Defence Policy, including legislation on common standards under a new European Cyber Resilience Act."* 2021 State of the Union Address by President von der Leyen: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

[2] This has recently become evident with the exposure of two critical security flaws, named 'Meltdown' and 'Spectre', in Intel computer processors AMD and ARM, which have been produced over the last two decades. https://www.cnet.com/news/spectre-meltdown-intel-arm-amd-processor-cpu-chip-flaw-vulnerability-faq/

[3] https://www.bleepingcomputer.com/news/security/new-hacking-tool-lets-users-access-a-bunch-of-dvrs-and-their-video-feeds/

[4] https://video.wired.com/watch/hackers-wireless-jeep-attack-stranded-me-on-a-highway

[5] https://www.wired.com/2016/03/go-ahead-hackers-break-heart/

[6] Ransomware is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. See definition: https://en.wikipedia.org/wiki/Ransomware

[7] https://ransomware.org/blog/first-big-ransomware-attack-of-2022-targets-large-portuguese-media-company/

Unfortunately, the increased risks and vulnerabilities derived from widespread connectivity and the rise in cyberattacks have not been followed by a substantial improvement of the security functionalities incorporated in the design of connected devices. Over the past years, BEUC members have shone a light on just how unsecure and dangerous some of these products can be.[8]

Moreover, the Internet of Things poses many other challenges for consumers besides cybersecurity.[9] For example, privacy and data protection, the artificial limitation of product lifecycles, lock-in effects and product liability and environmental and sustainability risks (e.g., due to the increased electronic waste). Also, connected devices have higher energy consumption due to their required networking components, with the need for continuous responsiveness of the devices via the network (idle mode) accounting for an exceptional part of their energy consumption.[10]

2. Market failure and the need for new horizontal cybersecurity legislation

Over the last years, European consumers have become aware and growingly concerned about the security of their products: a 2020 survey by the European Commission showed that 76% of consumers believed that there is an increasing risk of becoming a victim of a cybercrime, while 78% avoided disclosing personal information online because of cybersecurity-related issues.[11] In 2022, BEUC member Altroconsumo conducted a survey on the increase of connected devices at home: 69% of respondents said they feared their sensitive data could fall into the hands of private companies without their consent.[12]

Consumers have a legitimate expectation that the connected products that they purchase are safe and secure, ensuring both their cybersecurity as well as their physical safety. However, this is not what is happening presently.[13]

Consumer organisations were first to ring the alarm bell - yet not much has happened

Since 2016, testing conducted by BEUC members over the years has consistently shown that too many connected devices currently available on the European market come with multiple cybersecurity risks and basic flaws. An opinion from ENISA's Advisory Group also reached a similar conclusion[14]. More importantly, unlike what is popularly believed, one does not necessarily need to be a cybersecurity expert or an engineer to exploit these flaws.

[8] See below in Section 2, the outcomes of testing and surveys conducted by BEUC members across Europe on the cybersecurity vulnerabilities of connected devices.

[9] For additional insight on BEUC position on IoT and connected devices, please see our position paper: https://www.beuc.eu/publications/beuc-x-2021-091_protecting_european_consumers_in_the_world_of_connected_devices.pdf

[10] Friedli et al. (2016) projected that global standby losses would increase from 7.5 TWh in 2015 to 47 TWh in 2025, based on standby consumption of networked devices that are permanently connected to the power grid: https://nachhaltigwirtschaften.at/resources/iea_pdf/reports/iea_4e_edna_energy_efficiency_of_the_internet_of_things_technical_report.pdf

[11] European Commission, Special Eurobarometer 499, Europeans' attitudes towards cyber security, January 2020: https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=71905.

[12] https://www.altroconsumo.it/organizzazione/media-e-press/comunicati/2022/internet-delle-cose

[13] In January 2014, security researchers uncovered that the first massive IoT botnet attack was performed by more than 100,000 poorly secured consumer connected products (such as smart devices like televisions or fridges) that had been affected without their consumers' knowledge. https://arstechnica.com/information-technology/2014/01/is-your-refrigerator-really-part-of-a-massive-spam-sending-botnet/

[14] https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

BEUC members have provided significant evidence that connected devices are sold without any cybersecurity features. Consumer groups have alerted and called on various authorities to act (e.g., consumer protection, product safety, data protection authorities). Unfortunately, the response from the authorities has been limited and inefficient.

For example, in 2016, the #ToyFail campaign, launched by our Norwegian member Forbrukerrådet, showed that a children's doll named Cayla could be easily hacked in just a few simple steps. Anyone could connect to the doll from a distance and directly speak to the children through the toy, thus putting the children's physical safety and privacy at risk.[15]

The next year, in 2017, Forbrukerrådet conducted a second campaign (#WatchOut)[16] which tested the security features of smart watches for children. The main function of these watches is to enable parents to keep in touch and track the real-time location of their children. Forbrukerrådet discovered serious security flaws, including the possibility for an attacker to track and contact the child directly or even alter the watch's geo-location ('location spoofing'). Later, in 2019, Icelandic market surveillance authorities recalled a similar type of smart watch for children, after discovering that its mobile app lacked a minimum level of security and could easily be used to have undue access to children).

In 2018, our Belgian member, Test-Achats (TA), launched the "Hackable Home" campaign. Having equipped a home with a broad range of smart devices, TA gave ethical hackers a week to take control of some products. Out of 19 connected appliances (such as a smart fridge, thermostat, printer, door lock, loudspeaker, robot vacuum cleaner), half of the products were considered to be vulnerable after just 5 days. In the case of the alarm system, hackers were able to monitor the camera images from a distance, disconnect the alarm sensors and even mute the smoke detector.

BEUC member Which? from the United Kingdom also conducted a similar test with smart gadgets – including an internet router, wireless surveillance cameras, a smart padlock and children's toys – 8 out of 15 tested appliances included at least one security flaw. The hackers went as far as taking control of the house's wireless cameras and were able to freely manoeuvre them to monitor the activity inside the house.[17]

In 2021, TA repeated the 'Hackable Home' exercise, this time with 16 connected devices (including smart televisions, smart vacuum cleaners, baby monitors, door locks and alarm systems). They found 54 different vulnerabilities. 10 out of the 16 connected devices had a serious or critical vulnerability.[18]

This worrying landscape is further confirmed by many other testing activities conducted by BEUC members. Which?[19] in the United Kingdom, Stiftung Warentest[20] in Germany, OCU[21] in Spain and Consumentenbond[22] in the Netherlands have also found security flaws in connected consumer devices.

[15] https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

[16] https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

[17]https://press.which.co.uk/whichpressreleases/the-hackable-home-investigation-exposes-vulnerability-of-smart-home-devices/

[18] https://www.test-achats.be/hightech/smart-home/presse/la-securite-des-appareils-domestiques-intelligents-est-une-veritable-passoire

[19]https://www.which.co.uk/news/article/the-smart-video-doorbells-letting-hackers-into-your-home-aRfBa5W1boxK

[20] https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/

[21] https://www.ocu.org/organizacion/prensa/notas-de-prensa/2017/juguetes-conectados-201217

[22] https://www.consumentenbond.nl/nieuws/2019/deel-beveiligingscameras-te-hacken

The results from our members research are clear: from 2016 to 2021, there have been no real improvements. The same basic problems remain:

- **Lack of password protection:** no password is required or weak default passwords are allowed.
- **Lack of encryption:** no encryption is used to ensure confidentiality of communications.
- **Lack of software updates:** updates are not provided after the products are introduced in the market, thus making them progressively more vulnerable.
- **Early obsolescence:** many products are no longer updated (risk of electronic waste due to surviving digital products manufactured made by reputably short-lived companies, growing more obsolete - and a security risk - over time).
- **No vulnerability disclosure:** lack of a contact point to report vulnerabilities.

Several elements explain the general lack of security of smart products and related services. First, for many manufacturers and service providers, their objective, is first and foremost, to place their product on the market. This must occur as fast as possible (‘short time to market’) and, therefore, cybersecurity is often ignored.

In addition, manufacturers and vendors who focus on products of lower digital complexity (or products which are traditionally unconnected and only recently have been converted to be ‘smart’ e.g. toothbrushes, dolls) are unlikely to have the necessary skillset to guarantee the product’s adequate cybersecurity. Therefore, they often fail to account for possible cybersecurity issues when importing and reselling connected products. Moreover, the law does not establish liability of manufacturers and sellers for damages caused by the lack of cybersecurity of connected products. This means that taking responsibility for the cybersecurity aspect of digital products is not being incentivised by legal liability.

Ultimately, the conclusion is that the current EU legal framework does not adequately ensure the cybersecurity of connected products and does not provide the necessary incentives to provide for basic security of connected products. Therefore, we need additional legislation.

3. EU legal framework: interplay with other relevant legislation

As previously stated, the current EU legal framework is not fit to address the cybersecurity risks stemming from connected products and the IoT environment. The regulatory framework is fragmented over different pieces of legislation that contain cybersecurity relevant provisions, for example the Radio Equipment Directive (RED) and the General Data Protection Regulation (GDPR).

Also, the main European legal instrument related to cybersecurity, the Cybersecurity Act (CSA)[23], only focuses on voluntary certification schemes. There are no baseline mandatory cybersecurity requirements for connected products and associated services established in EU law. Also, the relevant existing legislation is limited in its scope and does not give consumers the protection and rights that they need, including in terms of remedies and redress if something goes wrong.

In the era of connected devices, users are no longer safe if the cybersecurity of their digital products or services is compromised. For example, the connected toys tested by our members would be considered safe according to today’s product safety legislation, yet

[23] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

there are serious cybersecurity risks that might endanger the physical safety of their users. Consumer product legislation such as the RED, the General Product Safety Directive (GPSD) or the Toys Safety Directive (TSD) do not cover security risks generated through connected products. Although the recent review of product safety legislation with the General Product Safety Regulation (GPSR) proposal acknowledges that the cybersecurity features, among other aspects, of a product can also be taken into account to assess a product's safety, it still falls short to adequately protect consumers,[24] due to its limited scope and the absence of baseline mandatory minimum cybersecurity requirements.

Although we welcome the recent adoption of the delegated act on the application of the essential requirements in Article 3(3), (d), (e) and (f), of the RED,[25] this directive remains an intermediary solution. The delegated act is an important step to improve the security of connected devices, but has a few important shortcomings:

- **Scope**: the RED does not cover all consumer IoT devices, with a study from the European Commission showing that only 70% of connected devices are covered (for example, wired devices are out of the scope).[26]
- **Entry into force:** the delegated act will only enter in force as of 1 August 2024, in order to allow European Standardisation Organisations (ESOs) such as ETSI, CEN and CENELEC to draft and adopt the relevant standards.
- **Continuous conformity**: the RED rules do not require devices sold on the market to be secure during their lifespan - the rules only require the product to be secure when it is ‘placed on the market’. There is no obligation regarding the provision of updates during the product’s lifecycle.
- **Vulnerability disclosure**: the RED does not put in place rules on vulnerability disclosure. Several of our members have reported that manufacturers of connected devices do not provide a contact point to report vulnerabilities, which makes it harder for consumers, organisations, and for other ethical hackers to engage in a constructive conversation with the manufacturers.

The Cybersecurity Act (CSA) was a missed opportunity to address most of the issues and problems previously pointed out, due to the voluntary nature of the certification framework it introduced (Article 56 (2)). The CSA has shown that, without a binding framework, there is simply no guarantee companies will join a certification scheme or that the overall security of connected products would increase.[27]

The role of the General Data Protection Regulation (GDPR) is also limited in relation to cybersecurity. Strong authentication mechanisms, such as unique passwords, would be required to ensure the security of personal data processing and to make harmful attacks more difficult. However, the GDPR also lacks legal certainty as it only uses a risk-based approach for security safeguards. Additionally, the enforcement powers that the GDPR gives Data Protection Authorities have important limitations when it comes to market surveillance. Data Protection Authorities, for example, cannot order the withdrawal of a noncompliant connected product from the market.

[24] While clarifying that cybersecurity risks having an impact on the safety of consumers “are covered by the concept of safety” under the new GPSR proposal, Article 7(1) (h) states that shall be only considered, among other aspects, the “appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product”. Recital 22, Article 7(1), (h), proposal for a Regulation on General Product Safety: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10381_2021_INIT&from=EN

[25] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.007.01.0006.01.ENG&toc=OJ%3AL%3A2022%3A007%3ATOC

[26] While covering wireless connected products, it leaves out of the scope devices which rely on wired Internet connectivity (e.g. broadband via cable, DSL, etc.): https://ec.europa.eu/docsroom/documents/40763/attachments/2/translations/en/renditions/native

[27] See BEUC position paper on cybersecurity for connected products here: https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

4. Horizontal rules with broader scope and very limited exclusions

BEUC welcomes the plan to introduce the CRA. This new horizontal cybersecurity law must ensure that all connected devices intended for consumers are secure by design and by default by establishing mandatory, minimum, security requirements for all digital products and ancillary services. In this regard, we highlight the importance of ensuring that the CRA has a broad scope to cover all relevant products and services. The CRA should cover all digital products and their ancillary services, including tangible digital products (wireless and wired hardware) and intangible digital products (embedded and non-embedded software), throughout their whole lifecycle.

Any exclusions to the scope should be strictly limited and adequately justified, ensuring that obligations apply to all relevant products and services. In this regard, we call on the Commission to ensure that digital products covered by other legislation at EU level are not automatically excluded from the scope of the CRA. It is the only way this legislation can provide the horizontal legal framework that is necessary.

Digital cloud services should also fall within the scope of the CRA. These services are increasingly important to our economy and society, as well as very popular and important for consumers. A successful cyberattack on cloud services would have a severe impact, as consumers rely on them for multiple purposes, from the common use of cloud data storage e.g., becoming default storage for smartphone photos, to device-syncing, both for personal and professional use. Following the massive increase of demand for this kind of services since the pandemic,[28] excluding them from the CRA would create an important loophole in terms of consumer protection.

5. Mandatory requirements: cybersecurity by design and by default

Consumer trust in the digital environment relies on a solid guarantee that the products they acquire are both secure and safe to use. As previously mentioned, this is currently not the case. The shockingly low levels of cybersecurity of the majority of digital products translate into a lack of trust among consumers and leaves them exposed to high security and safety risks, as well as potential negative economic consequences.[29]

More and more products are becoming interconnected, forming part of the same network e.g., home devices, PCs, security cameras, toys, thermostats. In this new reality, there is a clear risk for consumers. All it takes is for one device to be vulnerable for the entire network of devices to become compromised. And unfortunately, it is the objects that consumers are most likely to keep permanently connected and synced at home which are the easiest ones to hack.

Consumers must be able to rest assured that the connected products they purchase, or services they use, are secure and protected from software and hardware vulnerabilities. For this to happen, providing security by design and by default must become mandatory. The CSA did introduce the principle that products should be secure by default and by design as a cybersecurity objective of certification schemes, yet it fell short by not making such schemes mandatory.[30] The CRA should go further and make this principle mandatory: from their very inception, all connected products should already include cybersecurity

[28] https://www.marketwatch.com/press-release/global-consumer-cloud-storage-services-market-expected-to-grow-usd-32902-million-business-statistics-development-data-forecast-period-2022-2028-2022-04-14

[29] https://www.which.co.uk/news/article/data-breaches-how-your-personal-details-end-up-in-the-hands-of-criminals-aWs6A1p3VSOJ

[30] Article 51 (i), Cybersecurity Act: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

functionalities according to their potential risks ('security by design'), and their default settings should always be the most secure ones ('security by default').

Indeed, it is now agreed by cybersecurity experts that the implementation of certain security measures by design and by default would help remove many of the risks stemming from connected products. For example, in the case of the #ToyFail campaign by Forbrukerrådet, the protection of the Bluetooth connection of the Cayla doll through a strong authentication mechanism method e.g. unique password, could have prevented access to the doll by unauthorised persons.

To ensure a high-level of security by design and by default, the CRA must, at the very least, introduce mandatory baseline cybersecurity requirements, which should be transversal to all digital products. At the very least, the **mandatory baseline cybersecurity requirements** should cover **security updates, stronger authentication mechanisms and encryption.**

These requirements should serve as a conditional prerequisite which product manufacturers must comply with before being allowed to place their product on the market, therefore effectively protecting consumers.

Security updates

Products should be secure during a minimum period of time which should correspond to the legitimate expectations of the consumer and the expected lifespan of the product and its associated services. When put on the market, connected devices should be protected against any known vulnerabilities and security updates must be made available in a timely manner for the duration of the expected lifespan of the product and in line with consumers' expectations. Moreover, security updates should be easy to install, regardless of whether the user of the product is tech-savvy, thus not leaving out the most vulnerable consumers.

Furthermore, transparency of software updates should be improved: as far as technically possible, security updates should be provided separately of functionality updates e.g. linked to the operating system. Presently, it is not clear what the proposed updates contain or for what purpose they are necessary e.g. to improve security, install new OS functionalities or some other 'hidden' features. In fact, consumers even struggle with unexpected impacts on their products after installing certain updates.[31] Manufacturers should therefore clearly explain the reason behind each update (functionality or security) as well as its product impact.[32] In addition, the end-of-life policy must be clear to the consumers before purchase, explicitly mentioning the period until which updates will be provided.[33] Technical support should also be available to the consumer during the lifespan of the product.

In addition to committing to security updates, information on update policy should be made clear to consumers. In 2020, BEUC Dutch member Consumentenbond conducted research on the update policy by manufacturers for their smart products. In total, they surveyed 86 manufacturers producing 18 different kinds of products: only 22% had a clear update policy in their website, while only 14% of manufacturers mentioning a minimum duration period

[31] In May 2022, BEUC Italian member Altroconsumo conducted a survey on rise of connected smart devices at home: one third of respondents experienced functioning problems with smart devices, with 30% of those stating to have encountered malfunctions immediately after installing updates: https://www.altroconsumo.it/organizzazione/media-e-press/comunicati/2022/internet-delle-cose

[32] In November 2020, the Italian Antitrust Authority found that HP, since (at least) the end of 2016, misled consumers, encouraging updates to new firmware while omitting its impact on the use of non-original ink/toner cartridges, in order to falsely persuade consumers not to use third party cartridges. Recently, Test-Achats, OCU, DECO Proteste and Altroconsumo, our Belgian, Spanish, Portuguese and Italian members respectively, asked HP to pay damages to consumers: https://www.euroconsumers.org/Activities/printergate-euroconsumers-asks-hp-to-compensate-printer-owners-up-to-eur150

[33] See BEUC position paper on durable and repairable products and the changes needed for a successful path towards the green transition here: https://www.beuc.eu/publications/beuc-x-2021-061_durable_and_repairable_products_beuc_position_paper.pdf

for providing (at least security) updates online e.g. "our smartphones receive security updates for at least 24 months after market introduction", an extremely low number.[34]

Strong authentication mechanisms

Consumers often have several digital accounts, whether it is for online shopping or social media profiles. These accounts are often also linked to various connected products. Should one of these account's access data be hacked, there is a risk of losing access and control over your own account, potentially resulting in financial loss and misuse of personal data for fraudulent purposes.

Secure authentication methods should therefore be required in every connected device. In particular, unique and complex passwords should be the default setting of connected products. Consumers should be required to choose strong passwords in case they want to change the default one.

In addition, the provision of two-factor-authentication methods for users - an identity check using two different, independent procedures - should be mandatory, as these provide a more secured two-step verification, offering effective protection against such unauthorized access.

Earlier this year, our German member vzbv conducted a survey covering a total of 16 industry sectors, to determine how often their digital services offered users an option to choose two-factor authentication solutions and whether these solutions were optional, pre-set, or mandatory. After examining over 200 different digital services offered online, to check the types of two-factor authentication offered and how secure they were, vzbv found that only a few and already regulated industry-specific areas (such as finance) offered comprehensive options for two-factor authentication.[35] Even in sectors which process sensitive data, consumers received very limited protection with a second authentication factor only when they registered. Given the potential for financial loss and fraud involving the sectors surveyed, this is a concerning landscape.

Encryption

Presently, a substantial number of connected devices and digital services do not have the most basic encryption protection. All companies, manufacturers or service providers, should ensure that the data which are transmitted and stored in their digital products and services is properly encrypted. Moreover, the communication between connected devices and servers, the manufacturer/service provider and third parties should also be encrypted.

Encryption is not only an essential safety and security tool in the design of digital products: it is often a product's last barrier of defence against malicious interference. Therefore, even if cyberattacks succeed in breaching passwords and access users' information, there is a possibility that these encryption systems can ultimately succeed in protecting information by preventing hackers from accessing the content of the data and causing further harm.

Mandatory cybersecurity certification

The baseline security requirements should be complemented with mandatory cybersecurity certification for those connected products which could be considered to be of high-risk. The criteria used to determine which products can be considered high-risk should include not only the sensitivity of the data processed by these products, and the risks entailed by their normal use, but also the potential dangers that these devices may represent in case of a successful cyberattack, including potential physical harm for consumers.

[34] https://www.consumentenbond.nl/nieuws/2022/fabrikanten-informeren-onvoldoende-over-updates

[35] https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten

The potential harm of connected products therefore merits detailed scrutiny and active market surveillance e.g. self-driving cars may be hacked in order to harm its passengers[36]; products for children can have its inbuilt microphone, camera and speaker used to gain unwanted access to children; electricity control or heating systems of smart homes can be hacked to compromise the safety of those who live in it; door locks, surveillance/security products can be made vulnerable to harm those it intended to keep safe[37].

System updates and sustainability

In addition, businesses should also be incentivised to act more sustainably and produce longer lasting digital products to address the growing environmental and sustainability risks, in particular the increase of electronic waste. Besides recycling and adequate disposal policies, manufacturers of digital products should not only design hardware that can be easily exchanged once outdated or broken, but also ensure that the software of their products is adequately and regularly updated with vital system updates.

This is a growing concern given that, in some cases, manufacturers no longer provide security and functionality updates, in what is a deliberate effort to push consumers to discard their products to exchange them for newer ones[38] – planned obsolescence.[39]

A recent report by Which?, BEUC's member from the United Kingdom, found that connected devices could be obsolete after as little as two years, should manufacturers choose to stop providing vital software updates – despite these connected devices being far more costly and having a far greater life expectancy.[40] Moreover, when manufacturers are no longer able to provide updates to a particular product line, it would be also important to implement measures to ensure that the user has, and can easily exercise, their 'right to repair'. [41]

6. Strong, effective enforcement and redress

BEUC has consistently raised concerns regarding the lack of enforcement of relevant EU law in relation to connected devices. Having strong, swift enforcement and effective redress mechanisms is fundamental for consumers. Manufacturers and sellers must be held accountable if a cybersecurity flaw on a device places consumers in danger or causes them harm. Moreover, consumers must be able to address and complain to a public enforcement authority - which should take the necessary enforcement steps to prevent any harm from happening - and to seek appropriate redress (should harm materialise).

However, under the current EU legal framework, there are no clear cybersecurity rules enabling public enforcement authorities to be competent to step in. There are also no overarching rules in place that allow or require national enforcement authorities to actively remove from the market insecure, unsafe devices from a cybersecurity standpoint. Although the RED directive does include market surveillance mechanisms, the scope of the products covered by the RED is limited, not covering all connected devices. For example, wired products are not covered. Moreover, the RED rules do not ensure that a device is secure during its lifespan, as they are limited to when the product is 'placed on the market'.

[36] https://www.which.co.uk/news/article/we-hacked-a-ford-focus-and-a-volkswagen-polo-aQ3dE0O2FLgQ

[37] https://www.which.co.uk/news/article/more-than-100000-wireless-security-cameras-in-the-uk-at-risk-of-being-hacked-a0vVp2v8zNqx

[38] In December 2020, Test-Achats and OCU, BEUC's Belgian and Spanish members respectively, launched class action lawsuits against Apple over the planned obsolescence of the Apple iPhone. See https://www.test-achats.be/actions-collectives/apple-iphone

[39] https://www.howtogeek.com/731791/what-is-planned-obsolescence-and-how-does-it-affect-my-devices/

[40] https://press.which.co.uk/whichpressreleases/a-fridge-too-far-the-smart-appliances-that-cost-a-grand-more-but-may-only-last-two-years/

[41] BEUC's detailed position on the "right to repair" can be found here: https://www.beuc.eu/publications/beuc-x-2021-091_protecting_european_consumers_in_the_world_of_connected_devices.pdf

Given this visible gap, we note that some data protection authorities (DPAs) have found enough freedom to act against cybersecurity breaches[42], although this is not (only) a data protection problem. However, there are no practical effects for consumer redress, as the maximum that DPAs can do is order companies to stop processing data. The consequence is that dangerous products remain available on the EU market: there are no product recalls, no refunds, or compensation for consumers.

The CRA should therefore ensure that national authorities are empowered by clear cybersecurity rules to conduct effective market surveillance and enforce effective sanctions against manufacturers whose products do not comply with this legislation and/or the certification schemes in place.[43] They must also, in particular, have the power to withdraw from the market digital products that do not comply with legal security requirements and/or certification schemes. In addition, cooperation between national authorities and consumer protection organisations should also be encouraged to create synergies towards a better market screening, raising awareness and prevent violations of CRA obligations.[44]

Moreover, consumers must also benefit from clear remedies and means of redress. The EU should set relevant provisions to ensure that consumers have a clear right to seek adequate compensation against any damage or loss suffered due to a cybersecurity flaw of a device, in accordance with Union and national law. Following the example of the latest digital legislation, in particular the Digital Services Act (DSA) and the DMA (Digital Market Act), the CRA must be also added into the annex of the EU Representative Actions Directive (RAD), so that in case of mass damages, consumers can group together to introduce legal actions collectively.[45]

In conclusion, BEUC has consistently called for stronger horizontal provisions that can ensure a higher level of protection for consumers regarding cybersecurity in the context of connected devices. For further detailed information about BEUC's position on cybersecurity and connected products, please see our position paper on "Cybersecurity for Connected Products"[46], as well as our position paper on "Protecting European Consumeres in the World of Connected Devices".[47]

ENDS

[42] *« Credential stuffing » : la CNIL sanctionne un responsable de traitement et son sous-traitant*. 27 January 2021, available at: https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant

[43] Following the work of BEUC member in the United Kingdom, Which?, the House of Commons is currently considering legislation - Product Security and Telecommunications bill (PSTI) - to tackle insecure connected devices, which would introduce cybersecurity requirements and the enforcement of effective sanctions for non-compliance: https://www.which.co.uk/news/article/uk-government-announces-crackdown-on-insecure-products-awalK2U3pf4H

[44] BEUC German member, Verbraucherzentrale Bundesverbands (vzbv) has recently signed, in May 2020, a Memorandum of Understanding with the German Federal Office for Information Security (BSI) where they commit to cooperate for the period of three years with the aim to work together towards raising awareness of consumers and actively preventing violations of EU law on digital consumer protection: https://www.vzbv.de/meldungen/verbraucherschuetzer-kooperieren-mit-bundesamt-fuer-sicherheit-der-it

[45] 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. See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020L1828

[46] See BEUC position paper on "Cybersecurity for Connected Products": https://www.beuc.eu/publications/beuc-x-2018-017_cybersecurity_for_connected_products.pdf

[47] See BEUC position paper on "Protecting European Consumeres in the World of Connected Devices": https://www.beuc.eu/publications/beuc-x-2021-091_protecting_european_consumers_in_the_world_of_connected_devices.pdf

60 YEARS YOUNG YEARS STRONG

BEUC The European Consumer Organisation

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EISMEA. Neither the European Union nor the granting authority can be held responsible for them.