# FACTSHEET

# Ensuring cybersecure consumer products

## Connected consumer products: insecure by default?

The number of devices connected to the internet is due to reach over 75 billion by 2025 according to some estimates. From internet connected dolls to Bluetooth powered coffee machines, products that are linked to the internet are increasingly used in people's homes, places of work and when they travel. Yet many of these products are not at all cybersecure.

Lack of cybersecurity can have serious consequences for consumers. For example, compromised devices such as connected toys or cameras can pose risks of surveillance or blackmail. But cybersecurity failures can also harm consumer's physical safety, for instance when a hacked smart door lock allows intruders to enter one's home. And when a connected medical device or car is hacked, it could actually have fatal consequences.

The Advisory Group of ENISA, the European Cybersecurity Agency, in 2019 published an opinion on 'Consumers and IoT Security'. It highlights that the general lack of security of connected products is due to a great extent to the fact that manufacturers have no legal obligation to respect minimum security requirements. Since there is no regulatory nor economic incentive, the market fails to provide appropriate measures. The opinion contains recommendations on how ENISA can contribute to improve the security of connected devices.

## Evidence abounds

**Product tests by BEUC member groups have unveiled wide-spread and serious problems, for example:**

- In 2019, BEUC's Danish member Forbrugerrådet Tænk uncovered security flaws in smart door bells, creating risks of break-ins.
- In 2016 and 2017, our Norwegian member Forbrukerrådet identified failures with connected toys and smart watches for children. In both cases, strangers were able to easily hack the product and directly speak to the children.
- In 2018, Test Achats/Test Aankoop from Belgium installed 19 popular smart home devices (a smart fridge, alarm system, door lock...) and challenged two ethical hackers to find security vulnerabilities. Within five days, they found bugs in more than half the products.
- In 2020, an investigation by UK consumer group Which? revealed that cheap smart plugs found on online marketplaces contained critical security issues that expose people to hackers, and design flaws that could even start a fire.

With the number of connected products exploding, more and more devices amass huge amounts of often sensitive consumer data. This also increases the potential for damaging data breaches and fraudulent activities.

Despite the fact that since many years consumer organisations have alerted authorities and policy makers at national and EU level about the risks for consumers and society, no effective measures have been put in place to date.

BEUC The European Consumer Organisation

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme

## EU laws not up to speed

Despite the serious risks outlined above, the EU still lacks solid legal requirements to ensure the cyber security of all connected consumer products available in our shops.

The EU's Cybersecurity Act (in force since June 2019) does not remedy the situation because the framework for certification schemes it introduced is only voluntary for business, not mandatory. Moreover, the European Commission will roll out these voluntary schemes incrementally over time, so any potential positive impact will still take time to materialise.

The General Data Protection Regulation (GDPR) also contains rules related to the security of personal data processing but has its limits. If strong authentication mechanisms like unique passwords are implemented to ensure the security of personal data, harmful attacks are made more difficult. However, the GDPR does not give data protection authorities the powers to mandate the withdrawal of an unsecure connected product from the market.

The Radio Equipment Directive could potentially address some of the problems identified. However, the Directive's security relevant provisions are not fully applicable and effective because a complementary EU secondary act (so-called delegated act) has not yet been adopted by the European Commission. Even after its expected adoption in the first half of 2021, the Directive will not ensure security by design and by default of all connected consumer products.

## EU laws not up to speed

EU consumers clearly need a horizontal cybersecurity law that provides a catch-all safety net. This would make sure that all products not covered by any specific legislation have to respect a number of minimum security requirements. Such a law would require all connected products to be secure by design and by default. It would also give enforcers the necessary tools to oversee connected products put on the market and effectively take action when they do not meet the minimum security requirements.

### LACK OF ENFORCEMENT

Because of the current lack of clear rules, cybersecurity flaws in consumer products are not addressed by national enforcement authorities. In 2016, security flaws with the connected toy "My friend Cayla" that put children at risk were detected by our Norwegian member Forbrukerrådet. Consumer organisations alerted all relevant authorities but no effective measures were taken. On the ground of an anti-spying law, consumers in Germany were asked to destroy the toy – but were left without redress or compensation.

## What minimum cybersecurity requirements do we need:

The security requirements which manufacturers of connected products should respect are at least:

- **SECURITY UPDATES:** When put on the market, IoT products should be protected against any known vulnerabilities. Security updates must be made available for the duration of the expected lifespan of the product and in line with consumers' expectations.
- **STRONG AUTHENTICATION:** Unique and complex passwords should be the default setting of connected products and consumers should be required to choose strong passwords in case they want to change the default one.
- **ENCRYPTION:** Companies must encrypt the data which are transmitted and stored by products and services they produce.