DESIGNING CONNECTED DEVICES AND DIGITAL SERVICES TO BE SECURE

Challenges and potential solutions for European cybersecurity legislation from a consumer protection perspective

I. ABSTRACT

The level of cyber threats to consumer data and personal IT-infrastructures remains alarmingly high. Legislation for digital services and devices with respect to safety and security issues is still incomplete and too unspecific when it comes to concrete technical measures. To remedy this lack of regulation, the Federation of German Consumer Organisations (vzbv) proposes the following suggestions:

- An extension of the scope of the Directive on security of network and information systems (NIS Directive) to more types of digital services and to smaller service providers.
- A new horizontal law to tackle security issues of connected devices in the so-called Internet of Things for consumers.

Both legislative acts need to include references to reasonable baseline security measures as well as to international technical standards. Extending the scope of NIS Directive is expected to close the gaps left by the current directive and sector-specific legislation. The unique characteristics of connected devices as ‘cyberphysical systems’ lead to new challenges and call for a new horizontal legislative approach handling the novel risk induced by the Internet of Things. The two proposed approaches are likely to increase trust in connected devices and digital services and thereby stimulate the digital market in the EU.

II. NEW AND OLD CHALLENGES

The public consultation on the Directive on security of network and information systems (NIS Directive), which has just ended, offers a good opportunity to look more generally at the cybersecurity of digital services and connected devices from the perspective of consumers in the European Union (EU) - digital services and connected products are more important than ever in the private sphere. After the breakthrough of the personal computer in the 1990s and the internet in the 2000s, the phenomenon of ubiquitous computing[1] gained traction, with digital technologies playing an ever bigger role in people's lives. Alongside established and still growing services such as personal clouds, online marketplaces and social media applications, connected devices used in the Internet of Things (IoT) are being launched on the market in increasing numbers. Almost a third of people in Germany now have such products in their homes[2]. After all, the digitalisation of the home environment, in particular, offers huge potential for increasing energy efficiency, personal safety and convenience. In a smart home system[3], for example, a smartphone can be used to control the heating and optimise the amount of energy consumed[4], while various assistance systems are available to help the elderly and people with disabilities carry out routine tasks[5]. Internet-connected alarm and locking systems[6] enable homes to be monitored more comprehensively than with an analogue system and are more convenient because they can be controlled remotely from a digital device[7].

These digital offerings require an internet connection and a high number of sensors and actuators[8] fitted around the home. But this creates many new security risks. The confidentiality of personal data – and thus personal safety – may be compromised if locking systems are operated incorrectly, for example due to software defects or hacking. Intruders may exploit IT security flaws in locking systems to gain access to a supposedly secure home without having to physically break in[9]. For many years, weaknesses have been regularly uncovered in 'smart' toys that may enable an attacker to spy on a child's bedroom using a built-in microphone, for example[10]. The problems associated with connected devices

---

[1] Pipek, Volkmar: 'Ubiquitous Computing', Enzyklopädie der Wirtschaftsinformatik, 2020, https://enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Rechnernetz/Ubiquitous-Computing/index.html, 23 September 2020.

[2] Bitkom e.V.: 3 von 10 Deutschen haben ein smartes Zuhause ('3 in 10 Germans have a smart home'), 2019, https://www.bitkom.org/Presse/Presseinformation/3-von-10-Deutschen-haben-ein-smartes-Zuhause, 23 September 2020.

[3] Wikipedia: 'Home automation', 2020, https://en.wikipedia.org/wiki/Home_automation, 23 September 2020.

[4] Emmer, Wolfgang: Smarte Thermostate: Die besten Lösungen für smarte Heizungssteuerung ('Smart thermostats: the best solutions for smart heating control'), 2020, https://www.pcwelt.de/a/smarte-thermostate-die-besten-loesungen-fuer-smarte-heizungssteuerung,3443628, 23 September 2020.

[5] Verivox: Selbstbestimmt im Alter durch Smart Home ('Maintaining independence in old age with a smart home'), https://www.verivox.de/smarthome/themen/senioren/, 23 September 2020.

[6] DasHaus: Smarte Alarmanlagen: Mehr Sicherheit im Haus dank digitaler Technik ('Smart alarm systems: more security at home thanks to digital technology'), https://www.haus.de/smart-home/smarte-alarmanlagen-mehr-sicherheit-im-haus, 23 September 2020.

[7] Schreiber, Manuel: Elektronisches Türschloss nachrüsten und per Smartphone steuern (Smart Home) ('Adding an electronic door lock controlled by smartphone (smart home)'), 2018, https://www.chip.de/artikel/Elektronisches-Tuerschloss-nachruesten-und-per-Smartphone-steuern-Smart-Home_139974455.html, 23 September 2020.

[8] See Wikipedia: 'Actuator', 2020, https://en.wikipedia.org/wiki/Actuator, 23 September 2020.

[9] Whittaker, Zack: Security flaws in a popular smart home hub let hackers unlock front doors, 2019, https://techcrunch.com/2019/07/02/smart-home-hub-flaws-unlock-doors/, 23 September 2020.

[10] Stiftung Warentest: Wie vernetzte Spielkameraden Kinder aushorchen ('How connected smart toys eavesdrop on children'), 2017, https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/, 23 September 2020.

therefore relate not only to digital *cybersecurity*[11] but also to physical *product safety*. These two aspects are mutually interdependent, because if a connected device is hacked, its product safety is also compromised. Consumers therefore face new threats alongside the more familiar ones, as there are still regular reports of web servers and traditional end-user hardware, such as routers, being hacked[12]. And consumers are rightly concerned. In a recent survey by the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv), 76 percent of respondents said that they were worried about their personal data potentially ending up in the wrong hands[13] and 75 percent reported experiencing a security incident in the past twelve months[14].

Whereas most large companies have complex IT security infrastructures and expert staff, the protection afforded to individuals' data and systems is relatively poor. For example, the authentication process for digital services still tends to be password-based and is therefore insecure[15]. Many connected devices are not protected at all or are merely secured by a password that is easy to ascertain. There is often no secure authentication process either[16].

[11] Cybersecurity is used here as an overarching term for data security and IT security, i.e. the confidentiality, availability and integrity of digital data as well as the availability of IT systems and their functions. Cf. Wikipedia: 'Information security', 2020, https://en.wikipedia.org/wiki/Information_security, 23 September 2020.

[12] See the latest attack on Twitter accounts: tagesschau.de: 17jähriger nach Twitter-Hack festgenommen (17-year-old arrested after Twitter hack'), 1 August 2020, https://www.tagesschau.de/ausland/twitter-festnahme-hack-101.html, 23 September 2020.

[13] vzbv: Erwartungen und Erfahrungen der Verbraucherinnen und Verbraucher. Erkenntnisse der Marktbeobachtung des vzbv ('Expectations and experiences of consumers. Findings from the vzbv's market survey'), 2020, https://www.vzbv.de/sites/default/files/downloads/2020/06/16/ergebnisbericht_it-sicherheit_0.pdf, slide 6, 6 October 2020.

[14] Ibid. slide 7, 6 October 2020.

[15] Many providers, such as Google, do not activate this function by default: Google: Stronger security for your Google Account, 2020, https://www.google.com/landing/2step/, 22 September 2020.

[16] Alladi T., V. Chamola, B. Sikdar and K. R. Choo (2020): 'Consumer IoT: Security Vulnerability Case Studies and Solutions', in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pages 17–25, doi: 10.1109/MCE.2019.2953740, page 20 onwards.

III. SECURITY REQUIREMENTS FROM A CONSUMER PERSPECTIVE

The security problems described above often occur because data is stored and sent unencrypted and users' login details are not secure enough. It is therefore obvious that the risks to which consumers are exposed in the digital sphere and when using connected devices could be dramatically reduced with relatively simple technical security precautions. This means it should be mandatory for all digital services and connected devices to be designed with fundamental security features (*security by design*) and for their factory settings to be such that consumers do not have to undertake complex configuration in order to make them secure (*security by default*). Given that the security of digital services and connected devices is constantly changing, providers must make security updates available on an ongoing basis to ensure that they meet the latest security standards.

VZBV'S POSITION

Digital services and connected devices need to meet the following security requirements *by design* and *by default*:

- Encrypted transmission and storage of data
- Secure authentication procedures (e.g. two-factor authentication)
- Sufficiently strong password protection for applications and data
- Regular provision of security updates over a long enough period of time.

These security requirements are very important for digital services and connected devices, as well as for the software installed on them. Providers should be obliged to comply since data that has been encrypted before transmission cannot be read by unauthorised third parties, or at least not easily. If mobile connected devices, such as smartphones, are stolen, any data stored on them is only secure if it has been encrypted. And only secure authentication can prevent devices controlled via a network connection from being accessed by someone with ill intentions who has managed to work out a weak password. This applies both to access to connected devices and to the use of web-based services that are linked to connected devices and store data about device usage and about their owners on the provider's servers. However, many other digital services in the form of web applications for consumers also lack adequate security. Web mail services, social media applications, online marketplaces and other services that process sensitive data need to ensure that authentication, data transmission and data storage is secure, as described above.

IV. EXISTING LEGISLATION

Until now, existing European legislation containing provisions on IT security and data security[17] has focused on the "functioning of the internal market"[18] and the protection of critical infrastructure. The rules on data protection– first and foremost the General Data Protection Regulation (GDPR) – are an exception since the main purpose of data protection

[17] We believe the following are relevant and have discussed them here: NIS Directive, Cybersecurity Act (Regulation (EU) 2019/881), General Data Protection Regulation (Regulation (EU) 2016/679), Directive on privacy and electronic communications (2002/58/EC), European Electronic Communications Code (Directive (EU) 2018/1972), Radio Equipment Directive (2014/53/EU), Product Safety Directive (2001/95/EC).

[18] NIS Directive, article 1 (1).

is the “protection of natural persons with regard to the processing of personal data”[19]. Legislation governing IT security and data security, such as the Cybersecurity Act and the NIS Directive, are primarily aimed at protecting public goods. The protection of individual consumers’ interests with regard to the security of their personal IT systems, connected devices, digital identities and data is not always given due attention, as the following overview shows.

1. NIS DIRECTIVE

The NIS Directive obliges the providers of cloud computing platforms, digital marketplaces and search engines to take “appropriate and proportionate technical and organisational” security measures to protect their systems[20]. In the event of a security incident with a substantial impact, the competent authorities must be notified[21]. Although the Directive constitutes the first horizontal regulation of IT systems’ cybersecurity, and thus represents progress from a consumer protection perspective, vzbv believes there are various gaps in the protection offered, for example:

- The NIS Directive’s definition of ‘digital services’ only covers the three service offerings mentioned above. Social media platforms are excluded[22]. This is extremely problematic because these services also process huge volumes of user-generated and personal data and play a huge role in personal and, in some cases, business communications. Cyberattacks, such as identity theft or data theft, can therefore cause enormous financial losses and have severe consequences for the affected person’s social existence.
- The NIS Directive does not cover connected devices and systems or other types of hardware (routers).
- Only “substantial” damage affecting more than a certain number of users has to be reported[23]. Moreover, the provider only has to notify the authorities, not its affected customers. The authorities themselves do not have to pass on information to affected individuals. Unlike in the GDPR[24], in other words, data subjects do not have a right of information.
- The NIS Directive explicitly excludes small and medium-sized enterprises (SMEs) from the aforementioned provisions in article 16[25].

The provisions in the NIS Directive therefore lack adequate consumer protection and security requirements as listed above for digital services and connected devices (see section IV) as, with regard to digital services, the Directive is aimed at protecting the economy as a whole and is not focused on the security interests of private end users.

---

[19] 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, article 1 (1).

[20] NIS Directive, article 16 (1).

[21] Ibid. article 16 (3).

[22] Ibid. annex III, article 4 (17), (18), (19).

[23] Ibid. article 16 (4).

[24] GDPR, article 34. This provision only applies if it can be assumed that an incident relates to personal data. The loss of other data with a material or immaterial value to the user is not covered, nor is the malfunctioning of digital services or products.

[25] NIS Directive, article 16 (11).

2. OTHER LEGISLATION

A number of other laws require the providers of digital services and products to secure their infrastructure. The Radio Equipment Directive, which essentially applies to connected devices too, requires that general safeguards are incorporated in order to protect personal data[26]. By contrast, the scope of the General Product Safety Directive[27] is not defined in such a way that it could also cover connected devices, nor can the term 'safety' currently be construed to include not only physical and chemical product safety but also cybersecurity issues[28].

The Directive on privacy and electronic communications stipulates that technical measures be put in place to ensure the security of communication services and networks[29]. However, the scope of this Directive only covers communication services such as those offered by internet service providers, and not over-the-top telecommunications services such as instant messaging. Security requirements for such services are set out in the European Electronic Communications Code. The technical requirements are defined in slightly more detail than in the NIS Directive; for example, the Code suggests that data be encrypted, although it does not make this mandatory[30]. The GDPR also requires controllers responsible for the processing of personal data – such as operators of web mail services – to implement measures to protect the data that they process[31]. However, it does not stipulate that any of the security measures listed in section IV be implemented.

At EU level, there is thus no legal framework that requires the principles of *security by design* and *security by default* to be applied to the design of all digital services and connected devices across all sectors or that sets out the technical requirements in sufficient detail.

> **CONCLUSION**
>
> *Security by design* and *Security by default* for devices and services used by consumers have not been made mandatory by any existing EU legislation to date. EU legislation does not sufficiently regulate the security requirements to be met by digital services and connected devices.

V. POTENTIAL LEGISLATIVE SOLUTIONS

1. NIS DIRECTIVE

There is no horizontal EU legislation on cybersecurity that adequately regulates the digital services used by consumers. The best way of filling the resulting gaps in the legislation, for example pertaining to social media applications, is by updating the NIS Directive. The scope of the Directive should therefore be extended to include smaller firms and further types of digital services, not least social media applications, for which there is little regulation

---

[26] Directive 2014/53/EU 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. Ibid. article 3 (3) e.

[27] Directive 2001/95/EC on general product safety.

[28] See vzbv: Sichere Produkte stärken das Verbrauchervertrauen ('Secure products boost consumer confidence'), 2020, https://www.vzbv.de/sites/default/files/downloads/2020/10/05/20-10-01_vzbv_positionspapier_produktsicherheit.pdf, 6 October 2020, page 14.

[29] Consolidated text: Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Ibid. article 4.

[30] Directive (EU) 2018/1972 establishing the European Electronic Communications Code. Ibid. article 40.

[31] GDPR, article 32.

elsewhere. In addition, the legislation needs to be more in-depth and contain more specific technical details.

VZBV'S POSITION

- The scope of the NIS Directive needs to be extended to cover further digital services, such as social media platforms, and smaller firms.
- The disclosure requirement needs to be broadened so that data subjects have to be notified in the event of a security incident, even if only a few people are affected.
- To protect consumers, the security requirements for digital services that have to be met *by design* and *by default* need to be set out in more detail.

2. REGULATION OF CONNECTED DEVICES

As cyberphysical systems, connected devices require their own legal framework because the integration of physical products with connected IT systems creates completely new challenges in terms of cybersecurity. To ensure continual conformity, the standard of security at the time that a device is placed on the market must be maintained by means of a mechanism for installing the manufacturer's security updates. A number of issues in this context can be resolved by modernising and expanding the General Product Safety Directive[32].

VZBV'S POSITION

A new horizontal legal framework for connected devices needs to be created that includes the following cybersecurity requirements:

- Obligation to ensure security by design and security by default
- Encrypted storage and transmission of sensitive data
- Secure authentication mechanisms
- Provision of security updates throughout the expected lifetime of the product to ensure that it continues to meet the latest security standards
- Specific technical standards setting out security measures in more detail (the European Commission needs to continue to drive the development of such standards for connected devices).

As shown by the technical risks and potential threats for consumers that were described earlier, the current legal situation is in urgent need of change. This is required not only to ensure information privacy – a very important personal right – but also because of macroeconomic factors. Firstly, the avoidance of IT security incidents is financially beneficial as, in the long run, preventive measures are cheaper than the cost of remedying the material damage done by cyberattacks. Secondly, increased confidence in connected devices and digital services among potential customers will boost the digital economy and is essential for its continued growth. After all, IT systems to be used in sensitive private spheres only have a chance in the long term if they are trustworthy and reliable. This can only be achieved with a legal framework that defines mandatory security requirements for digital services and connected devices aimed at consumers.

[32] Sichere Produkte stärken das Verbrauchervertrauen ('Secure products boost consumer confidence'), page 14 onwards.