WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

Key points on the draft of the German Federal Ministry of the Interior on the draft of a cybersecurity strategy for Germany
(dated: 9 June 2021)

Berlin, 30 August 2021

The German Federal Ministry of the Interior (BMI) had already published and discussed the key points of the Cybersecurity Strategy 2021 (CSS21) in April of this year. Within its cybersecurity strategy, the German federal government sets out the priorities and objectives for the activities of public authorities and in the area of IT security policy.

eco commented on the key points and explained that they could represent helpful ideas and approaches for improving cybersecurity in the state, society and the economy if they are applied correctly, and no other aspects are included in the strategy that counteract them. In particular, measures should be refrained from that systematically exploit vulnerabilities in IT systems by public authorities as a contribution to improving IT security.

On 9 June, the BMI presented a preliminary draft for the CSS21, which supplements the key points and expands the topics addressed. This draft contains several aspects that require detailed consideration from the Internet industry's point of view. eco addresses these aspects in the following key points.

- **Re 8.1.8 Responsible handling of vulnerabilities – Coordinated Vulnerability Disclosure**

eco considers the immediate reporting of vulnerabilities that become known to security authorities to the respective manufacturers or developers to be a central factor in improving and guaranteeing IT security. eco considers a strategy that provides for the systematic withholding of vulnerabilities, especially involving the BMI, to be extremely critical. eco supports the efforts of the BMI to establish legal certainty for persons and organisations that discover vulnerabilities and report them.

- **Re 8.3.1 Improve the German federal government's options for averting cyber attacks**

According to the plans of the BMI, the German federal government's options for countering cyber attacks are to be made possible and expanded through amendments to the Basic Law. eco urgently warns that the legislature is tangentially affecting an area that is sensitive to fundamental rights and that telecommunications secrecy is thus also to be weakened. In particular, it should be conclusively clarified beforehand to what extent danger prevention is to be understood and under what conditions it is to be made possible.

- **Re 8.3.7 Intensify criminal prosecution in cyberspace**

eco recognises that criminal prosecution in the area of crime through the use of IT must be intensified, as must criminal prosecution in the case of attacks on IT. eco considers this to be a central challenge in the area of IT security that the state must address in the coming years. However, it is problematic in the present formulations and designs that the state does not address this in a meaningful, proportionate and fundamental rights-protecting way. eco is clearly against the use of Trojans on a large scale and calls on the legislator to develop less invasive measures with clear legal boundaries. eco rejects an obligation for companies to cooperate in the installation of malware on users' end devices.

- **Re 8.3.8 Promote responsible handling of 0-day vulnerabilities and exploits**

eco considers the question discussed here about the right time to report 0-day vulnerabilities to be obsolete and not expedient. Vulnerabilities should be reported immediately to the respective manufacturers by public authorities as soon as they become known to them. Together with the manufacturers, a way should be sought to eliminate the vulnerability immediately and thus minimise the risks for citizens. The retention of vulnerabilities by state authorities for other purposes is considered irresponsible and counterproductive for IT security by eco. In this way, public authorities not only undermine IT security, but also damage the trust of citizens in state institutions.

- **Re 8.3.9 Ensuring security through encryption and security despite encryption**

One of the central points of criticism of the German government's last cybersecurity strategy (CSS 2016) were the goals of "security through encryption" and "security despite encryption". After these theses did not appear in the previous consultations on the cornerstones of the now present security strategy, there was hope that the federal government would have refrained from this heavily criticised approach. The demand that has now been reintroduced is considered unacceptable by eco. The systematic weakening of encryption - whether through the exploitation of vulnerabilities or even through demands for "key management" or "access options" - is a threat to the security, integrity and confidentiality of communication. Particularly in view of the fact that corresponding considerations appear in the draft CSS 2021, eco reiterates: A built-in vulnerability to circumvent encryption or comparable solutions represents a danger for all users of corresponding devices or software. eco resolutely rejects the involvement of manufacturers or providers, as contemplated by the CSS 2021.

- **Re 8.3.11 Strengthen the digital sovereignty of the security authorities by strengthening ZITiS**

As early as the 2016 Cybersecurity Strategy, eco considered the tasks and function of the German Central Office for Information Technology in the Security Sector (ZITiS) to be problematic. It was unclear how ZITiS penetrates into IT systems and which requirements and obligations to protect the fundamental rights of all citizens must be observed in doing so. The Cybersecurity Strategy 2021 now provides for an expansion of ZITiS's tasks and powers, although these central questions have still not been conclusively clarified. eco pleads here for a thorough examination of the tasks and powers of ZITiS and of the legal basis on which ZITIS acts.

- **Re 8.3.12 Increase the level of cybersecurity through strengthened intelligence through strengthened advance reconnaissance**

The CSS2021 envisages an intensification of intelligence and intelligence activities. Against the background of the problematic experiences of the past years and the recent legislation within the framework of the German Federal Intelligence Service Act (BND-Gesetz), the extent to which this proposed intensification will actually lead to a practical contribution to a practical improvement of the IT security situation for society and the economy must be

critically examined. eco calls for a critical review of the goals and objectives for intelligence services and, in particular, for stricter rules for activities relating to telecommunications networks and Internet infrastructures.

About eco

With more than 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust, and ethically-oriented digitalisation. That is why eco advocates for a free, technology-neutral, and high-performance Internet.