PB.W-01-414 Kapitel 2: In die Zukunft wirtschaften

Antragsteller*in: OV Maxvorstadt/Schwabing/Freimann
Beschlussdatum: 08.04.2021

Änderungsantrag zu PB.W-01

Von Zeile 413 bis 417:
Zertifizierungen und wollen vor allem die KMUs sehr viel stärker durch ein dezentrales und unabhängiges IT-Beratungsnetzwerk unterstützen. Wir ~~stärken unabhängige Aufsichtsstrukturen~~fördern die Sensibilisierung für IT-Sicherheitsrisiken, die freie Wissensvermittlung und ~~schaffen neue Sanktionsmechanismen~~den internationalen Wissensaustausch zur Stärkung der IT-Sicherheit für Bürger*innen und die Wirtschaft. Die IT-Sicherheit gefährdende Maßnahmen, wie das Schwächen von Standards für IT-Sicherheits-Verfahren (z.B. Verschlüsselung) sowie den Handel und das staatliche Offenhalten von Sicherheitslücken, wollen wir beenden und eine Meldepflicht schaffen. Für die Nachhaltigkeit von IT-Produkten soll für technisch langlebigere Produkte eine Verpflichtung zu einer angemessenen, risikoorientierten und benutzerfreundlichen Bereitstellung von IT-Sicherheitsupdates eingeführt werden, wie z.B. für Smartphones, Internet-of-Things-Geräten mit Netzanschlüssen.

Begründung

1. IT-Sicherheit sollte durch Sensibilisierungsmaßnahmen, Wissensvermittlung, (internationalem) Wissensaustausch, Hilfestellungen und positive Anreize gefördert werden. Das Ausnutzen von Sicherheitslücken erfolgt inzwischen 'industriell' oder als 'Service', die Betrüger sind bereits international vernetzt und wirken über Grenzen hinweg. Aufsichtsstrukturen und Sanktionen sind weniger hilfreich, maximal als Ultima Ratio bei nachhaltiger Ignoranz, Vorsatz oder grober Gefährdung anderer.
2. Die IT-Sicherheit wird nicht nur durch das 'Horten' von Schwachstellen, sondern genauso von häufigen 'staatlichen' Forderungen nach dem Aufweichen von Standards für IT-Sicherheits-Verfahren, z.B. Verschlüsselung. In der Vergangenheit wurden durch derartige Maßnahmen (z.B.: EXPORT-Verschlüsselung durch die USA) Schwachstellen eingebaut, die die IT-Sicherheit allgemein gefährdet haben (z.B. Schwachstellen erst ermöglicht haben). Notwendige Überwachungsmaßnahmen sollten Daten dezentral abgreifen, nicht die Bürger*innen und die Wirtschaft gefährden.
3. Für die Nachhaltigkeit für langlebigere IT-Produkte ist es unumgänglich die Hersteller zu verpflichten, benutzerfreundliche Sicherheitsupdates zur Verfügung zu stellen. Dies sollte abhängig von dem Wert und der voraussichtlichen Nutzungsdauer für alle Geräte mit Kommunikationsschnittstellen (z.B. Ethernet, WLAN, Mobilfunk, Bluetooth, NFC) erfolgen, da diese einem höheren Risiko ausgesetzt sind. Darunter fallen auch Geräte mit Fernwartungszugängen. Der Zeitraum sollte sich danach richten, wie lange das Gerät im Markt angeboten wird, nicht wann es eingeführt wurde.