©florian-pircher

en | de

Press release | 13.09.2017

Binding standards needed to keep network safe

EU Commission Cyber Security Strategy

The European Commission will today present a strategy paper on cyber security. The digitalisation of everyday life and the so-called Internet of Things requires more security for information technologies, as made clear by the May 2017 "WannaCry" incident.

Jan Philipp Albrecht, Vice Chair of the Civil Liberties, Justice and Home Affairs Committee, calls on the European Parliament to work towards mandatory minimum requirements, such as secure end-to-end encryption and secure default passwords.

"It is high time that we make the digital single market fit for purpose. The European Commission has long hesitated to submit its proposals for greater cyber security. The strategy lacks many key steps for more network security. Digitalization of everyday life requires clear rules and IT security standards for manufacturers of hardware and software. Minimum requirements, such as the end-to-end encryption of intelligent refrigerators and other networked appliances, identification of device quality on the Internet of Things, and secure pre-set passwords, are necessary safeguards of day to day digital life."

Julia Reda, Vice President of the Greens / EFA Group, calls for a rethinking of the handling of security flaws and the promotion of the autonomy of users when dealing with the Internet of Things:

"Member States and their intelligence services must be banned from keeping knowledge of security flaws to themselves or deliberately incorporating them into products. The EU needs to foster the search for such flaws in widespread free software. Commercial software vendors must be held liable for security flaws in their products in certain circumstances, such as failing to provide critical vulnerability updates as soon as possible, and neither providing access to the source code for an independent security check. The EU product liability directive has to be revised and extended to include software. The reporting obligation for significant disturbances of critical infrastructures such as electricity and water supply must also apply to other systems. In addition, critical device areas and infrastructures should be completely disconnected from the public internet to provide no target area for external attacks. If you buy a camera or a heater that can be connected to the internet, you should have the right to use it offline."

Notes

(1) For internet routers, for example, standard passwords are set which make internet access vulnerable to attacks. Secure default passwords minimize the risk of an attack.

Recommended

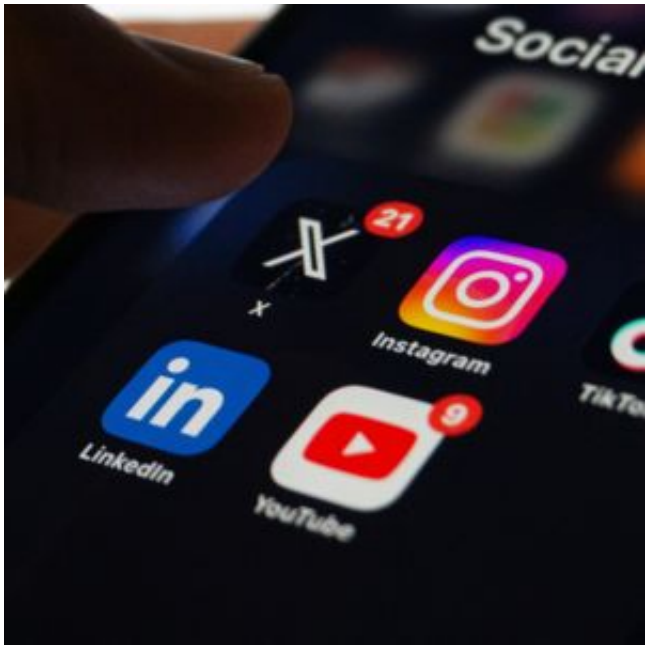
News

© European Union 2015 - EP Louise WEISS building: © Architecture Studio

Debriefing of the January 2025 Plenary Session

23.01.2025

Press release



X/Meta: Greens/EFA warn of Trump’s tech friends

21.01.2025

News

European Union

[Plenary Flash: 20-23 January]

20.01.2025

Study

Camilo Jimenez on Unsplash

[Politicians, parties, polls: Online Disinformation and…]

27.03.2024

Responsible MEPs

Jan Philipp Albrecht

Member

Felix Reda

Vice-President

Contact person

David Weir

Press & Media Advisor EN (English language press)

Please share

- E-Mail