DetailHomeNewsDetail

01/07/2019

Draw consequences from hacker attack©

geralt / pixabay.com The current hacker attack on public figures demonstrates the vulnerability of digital communication and affects trust in open communication in a democracy. This underscores the vital importance of privacy and data security to modern democracy, as well as the need to be prepared for and then respond effectively to the possibility of such unauthorized disclosure of personal data. Mobile phone numbers or e-mail addresses may not be viewed as particularly politically sensitive or in need of confidentiality protection. The motivation of the person responsible may also be based more on the need for recognition than on fundamental considerations. The point, however, is that individuals must have the power to decide who should know their personal data and who should not. Informational self-determination must be guaranteed regardless of the quality of the personal data.

The state commissioner for data protection and freedom of information in Rhineland-Palatinate, Prof. Dr. Dieter Kugelmann, emphasizes the need for self-data protection: "Everyone must be aware that everyday communication using modern means of communication requires a certain amount of attention because you are dependent on service providers and technical infrastructures," says Kugelmann. "But if you stick to a few basic rules, such as data economy and take precautions such as encryption and care when choosing passwords, there is no reason to be misled by free communication as a central element of democracy."

With regard to the specific case, there are still uncertainties. In any case, the data come from very different sources. They affect public figures, who are often more likely to disclose data because they are in the public eye. However, these people draw the line between private and public themselves and have a particular interest in their private data remaining private. The State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate examines, within the scope of his responsibilities and in cooperation with other authorities, whether and how quickly the data can be deleted or at least blocked. Since some of the data is stored outside of Europe and already mirrored, international cooperation is required. He also examines the extent to which the penal provisions of data protection laws apply.

The unauthorized publication of personal data of many public figures makes it clear once again that communication via the Internet harbors risks. Risks exist for privacy and the preservation of communicative retreats, because a large amount of data

is transmitted and stored in a way that is sometimes difficult to control, without the person concerned being able to keep track of it and have the power of disposal. However, as far as the power of disposal of the individual is sufficient, particular care should be taken to transmit as little as possible, especially sensitive data, to ensure appropriate encryption of data and security of transmission paths and to use providers of services that guarantee a high standard of data protection. The aim must be to enable free communication and at the same time avoid risks or at least reduce them as much as possible.

Further information:

Possibilities of self-data protection in the InternetUse cloud storage safelySecurity of passwords

return