Your Key to Cloud Data Protection

Press Release

Pfungstadt, 7 January 2019

Data theft in the Bundestag: Would it have been preventable?

Which security measures make sense for the protection of sensitive data?

Correspondence from German Chancellor Angela Merkel, the mobile phone number of Jan Böhmermann or private holiday pictures of ZDF journalists - these and similar sensitive data were published in December via a Twitter account and are freely accessible. The data contained both older and current information as well as personal data such as names, mobile phone numbers, e-mail addresses, credit card details or chat histories. All parties in the Bundestag are affected except AfD, journalists from ARD and ZDF, entertainers, musicians and actors. The Federal Office for Information Security (BSI), the Federal Office for the Protection of the Constitution, the Federal Criminal Police Office and the Federal Intelligence Service are currently investigating how the data could be stolen. “Nobody can prevent data from being stolen, but it is possible to prevent attackers from using the stolen information by taking appropriate security measures,” says Elmar Eperiesi-Beck, Managing Director of eperi GmbH.

What could such security measures look like? “In the event that data is stolen from servers and published, an encryption solution that does not even allow IT administrators access to unencrypted data will help,” says Elmar Eperiesi-Beck. Even if the data were stolen via a cloud application such as Salesforce or Office 365, additional encryption would be the only protection. “Encryption is one of the most effective ways to protect valuable data. In combination with pseudonymization, it is ideally suited to transform personally identifiable data into meaningless text, so that no conclusions can be drawn about the person concerned. This applies equally to data in use, in transit and at rest.” Only those who have access to the cryptographic keys can read the encrypted data.

So when it comes to protecting cloud data, encryption is the best way to protect critical data from unauthorized access by third parties, criminals or administrators in external data centers. “All email communications, appointments and other sensitive data stored and processed on the cloud platform should always be protected from attackers by encryption and pseudonymization,” Elmar Eperiesi-Beck advises. This also makes it possible to implement the strict requirements of the European Data Protection Regulation (GDPR) and other laws.

eperi GmbH
Gutenbergstraße 4-6 / 64319 Pfungstadt / Germany
T +49 6157 98 950 00
F +49 6157 98 950 29
W info@eperi.com / eperi.com
Managing Director: Elmar Eperiesi-Beck

About eperi
eperi GmbH is a leading provider of cloud data protection solutions, and has 15 years of experience in the field of data encryption for web and SaaS applications. These solutions enable internal and external data protection and compliance requirements to be enforced at a centralized location, and ensuring that customers as cloud users are given sole control of all data protection processes.
www.eperi.com

Note to editors:
Elmar Eperiesi-Beck is available for interview requests by telephone. If you are interested, please call 06157-98950 15.

Press Contact
Michaela Ohlsen
michaela.ohlsen@eperi.com
+49 6157 98950 15