Your Key to Cloud Data Protection

MEDIA ALERT

Insufficient protection for German citizens' sensitive data: Eperi urges stronger focus on data encryption in the cloud

Data protection professionals are very worried about German data. About 40 government agencies store data with external cloud providers, according to figures from a meeting of the Bundestag's internal affairs committee that were published by the broadcaster hr-info. Against this backdrop, many people are asking questions about how secure this data really is. In early April 2019, it emerged that bodycam data from the German federal police force was being stored in Amazon Web Services (AWS), the cloud service provided by Amazon. The internal affairs committee subsequently uncovered additional cases in which data about German citizens was stored on servers whose data protection-related legal framework is questionable.

European data protection regulations, like the EU's GDPR, also apply to non-European providers delivering cloud services within Europe. However, the US Cloud Act – which enables US authorities to access this data – also applies to these cases, even if the data is not stored in the US. This would not be allowed on European providers' servers or would at least be significantly more difficult from a legal standpoint. Konstantin von Notz, a member of the Bundestag from the Green party, has therefore published a podcast on hr-info in which he urges the federal government to develop a European solution to the problem of storing sensitive official data that would comply with current standards in Germany.

The cloud server's location is not the real problem

"The current discussion about unauthorized access to data is only looking at one side of the problem," warns Elmar Eperiesi-Beck, CEO and founder of the German encryption specialist Eperi. "Even if the data is stored at a German cloud provider, that still doesn't automatically guarantee data protection. As long as the data is stored in unencrypted form in the cloud, the cloud providers can still access it."

In Eperiesi-Beck's view, the subject of data encryption in the cloud is often seriously neglected. "Nobody can completely block access to data stored in the cloud by third parties. But what organizations definitely can do is to prevent unauthorized people from misusing that data – by protecting it with data encryption and pseudonymization. With the lack of clarity around the legal situation, companies and public authorities urgently need to tackle the issue of cloud data encryption, because prevention is the best protection against the fraudulent use of data."

German specialist in data encryption with a focus on the public sector

Eperi is a German specialist in data encryption with more than 15 years' experience. The Eperi Gateway solutions were developed on the basis of close cooperation with Germany's Federal Office for Information Security (BSI). The company counts multiple public authorities among its customers, including the Federal Network Agency. Eperi is a founding member and partner of the BSI's Cyber-Security Alliance and is also a member of TeleTrust, a German and international IT security association.

Further information

Journalists interested in this topic are welcome to contact Eperi to fix up an interview with Elmar Eperiesi-Beck.