

No data protection without data security

At the Internet Conference DLD, EU Digital Commissioner Günther Oettinger announced that by the end of the year, the European Union's data protection regulation, which had been long-awaited, should be adopted in the course of the unification of the digital market in Europe. This is intended to create a uniform legal framework for data protection throughout the EU. Data protectionists and the Federal Council are still skeptical about the draft so far, since it would not bring any more data protection in Germany.

But the need for data protection is more urgent than ever before: the NSA affair has not yet been forgotten, as the Paris terrorist attacks are discussing an encryption ban or at least access to intelligence services. And in 2014 the number of high-impact data scales has continued to increase, with a total of 580 million stolen records. Companies need to busy oneself with the question, how responsible they deal with sensitive data and how they can ensure that their data, as well as the data of their customers and business partners, are secure. Data protection is only an empty promise without effective data security. Unsafe data processing methods favor data protection violations. And in terms of data security, there is still a lot of catching up to be done in German companies, especially in medium-sized companies. The current DsIN safety monitor has shown that in German companies the degree of digitization is growing steadily, but security awareness is decreasing. A criminal lightness.

The Internet is part of the everyday work of almost all companies and the mobile connection of communications to the corporate networks is also increasing in the middle class. More and more sensitive information is processed and sent via the Internet and e-mail. In more than half of the companies (57 per cent) this is done without protection. Sixty percent of companies do not, or only partially, deal with the risks of Internet and e-mail communication. This also applies to the legal requirements for protection against access, misuse or manipulation. In principle, companies are just as negligent as sending business information via postcards or placing contracts on posters.

It is important to strengthen the risk awareness and understanding of weaknesses in the company. Decision-makers and employees have to be sensitized, which can happen by risks from the outside or through carefree action in the company. In particular, manufacturers of IT security solutions are also required to provide more awareness. Because there are easy-to-use solutions that make the exchange of files and the distribution of confidential documents highly secure. SSP Europe, for example, provides the official solution Secure Data Space, which encrypts the data by using triple crypt technology when downloading data over the Internet.

Günther Oettinger has pointed out in his lecture at DLD that European IT companies are no longer competitive. It certainly does not apply to IT security. Especially German suppliers currently have significant competitive advantages compared to US manufacturers, by which most German companies demur about built-in backdoors. These advantages are to be exploited in order to further strengthen data security and thus data protection in Germany.

The original article can be found at <http://www.sysbus.eu/?p=7560>