For some, it is the ultimate comfort, for others a nightmare: The concept “Bring your own device”, the professional use of private mobile devices, challenges companies in security.

On thin ice

After some time, the pressure was too big. A long period the management level of the company blocked the suggestion to not give oars out of hand, but then the smartphone fundamentalists triumphed. Under the shorthand symbol BYOD the result leaves clear traces on the electronic premises: “Bring your own device" counts today despite controversial views to the most important trends at the workplace. The professional use of portable private hardware at work is considered as an improvement of life quality in the job.
More and more employees renounce the use of company models and use better their own, well-known mobile devices. Because they demonstrate more comfort in the zone between parking, coffee machine and desk. Thus, the one-time strict limit is lifted in favor of a completely new paradigm of use, characterized by convenience. “The personal demands more flexibility for everyday life as well as these modern technologies are habit in their private use.”, head of Security Services SSP Europe GmbH Dr. Dieter Steiner says. The advantages of BYOD are obvious: The user uses a terminal of his choice and is familiar with the operating system. Productivity is also improved, because the user can always do his work from any location.

A study by the market researchers of Ipsos, on behalf of IT specialist Citrix, underlines the fact: Every second out of five companies, which drives the BYOD rail in Germany, is experiencing productivity gains of more than 20 percent. In addition, the stressed company budget can be saved as the cost of purchasing hardware is reduced. What can be better than techno fans, who pay device from their own money. This is not the only reason that even careful managers look at the matter quite positively- finally the course also fits into the general austerity. Where before the workforce had to run storm, thus the yes-word from above is in many places only formality. According to the market researchers of Gartner, around half of the managers expect from their experts the use of own equipment at work. In practice, however, things are much more differentiated. IKEA Austria goes different ways: All 2800 employees can access by their own device at different service of the company. Private alternatives of laptops are undesirable, because they are provided by the company.

In the case of telephones and tablets, on the other hand, there is the possibility to use own devices that can be billed at the same time via the company. “The option is barely used- probably also because we have a very good standard for company equipment", says Daniel Bleyer. The deputy IT manager of IKEA Austria is basically concerned about the use of electronic mail: there are no special IT requirements, because the e-mail software, which is used here, is a self-contained system."

Despite such well-being solutions, other pages of BYOD can hardly be covered. In terms of data security, companies generally move on thin ice. As a result of the tricky quantitative starting situation, the Sopra Steria Consulting Company advises: Two thirds of the companies have already switched to the BYOD fraction. In companies of more than 1000 people, this practice is particularly widespread- which in principle offers a very broad attack field. Some responsible persons make criminals their highly dubious game easily, however it is because of cluelessness, lack of competence or pure ignorance. According to Sopra Steria Consulting,

40 percent of the companies are not constantly upgrading devices with security updates. Guidelines for safe use are just as bad as the necessary regular safety checks in about one third of the factories. “Mobile working not only creates flexibility, but also risks”, warns the Head of Information Security Solutions at Sopra Steria Consulting Gerald Spiegel. Than without security measures the business use of private devices creates the risk of unintentional data leakage, because the users themselves do not always carry out regular updates or separate significant company data from their private information.
Prophylaxis, however, is not a piece of magic: The IT department must set clear guidelines for the use of BYOD and raise awareness among employees; It should also clearly define which apps may not be used. “Central solutions for data exchange must also be offered. In addition, companies can use mobile device management to manage their mobile devices”, emphasizes Steiner.

As this step is required. BYOD does not have to be the center of attention, as the fast food company McDonald's proves. “There is a separate policy which Security requirements for such solutions regulates", noted Human Resources Director Ursula Riegler. In principle, demand is not very large in the company- however, because most of the employees have mobile phones as well as service laptops with private use.
Perhaps the whole challenge for some board rooms is soon history anyway. A counter-reaction comes from the USA. There, the BYOD traffic lights are increasingly switching to red, says the international industry association “Computing Technology Industry Association " (CompTIA). The deniers rely heavily on internally deployed devices in order to be able to implement security strategies more freely. Even if colleagues were tweeting their frustration about this development over the company via companies mobile phone- or then just over the private tablet.

The original article can be found at https://www.secure-data-space.com/wp-content/uploads/2017/04/2017-04-24-Profil-Auf-d%C3%BCnnem-Eis.pdf