

Safeguarding Data Loss

When large companies and organizations run inventory checks of their electronic devices, managers often end up scratching their heads. How can it be that – like in the song – suddenly only 90 company laptops can be located instead of the original 100? Theft or absentminded employees are just two of a number of possible explanations. Over time, companies can lose track of mobile devices in the everyday “chaos” of the enterprise. If a device changes department, location, or user – and this might happen several times in the span of just a few months – it is often subsequently listed as “missing.” The danger is that confidential data on those devices can get into unauthorized hands and be sold to third parties or exploited for someone’s own ends.

Protect your data as a security precaution

Losing data is every company’s worst-case scenario. To prevent it from happening, devices at risk and critical documents should be protected right from the start. Professional encryption solutions protect data with a security shield to stop people from accessing data that they’re not supposed to. Inventory management solutions can help keep track of everything, and introducing company-wide security policies make employees aware of possible security threats. Doing this not only protects confidential data, but also prevents having surprising numbers of devices disappear.

Increasing numbers of security breaches and “missing” equipment

In a recent U.S. study, the Ponemon Institute found that the number of incidents of data security breaches had increased by more than 30 percent in 2005. The study reported that more than 90 percent of these incidents were a result of the loss or theft of digital information. And there was another bitter pill for the companies concerned to swallow. When the data abuse became public knowledge, 60 percent of all their customers either terminated their contracts or at least considered doing so.

When the U.S. Department of Trade announced in the spring of 2006 that it had lost 1,137 laptops in the past few years, there was a big outcry in the media. An especially embarrassing aspect was that 249 of these devices carried personal data about U.S. citizens who hadn’t been notified. Until the story came out, the Department of Trade wasn’t even aware that so many computers were missing. If the data on those laptops had been encrypted, a lot of trouble and anxiety would have been averted.

Encryption means no more worries about mislaid data

The larger the company, the harder it is to trace where mobile devices currently are. Sometimes it’s only a case of laptops, PDAs, or USB sticks moving to a different floor in the same building, but when entire departments move, it can mean a new site or even a different country. Inventory management solutions can help track where devices are and which devices are no longer in use. And even though the hard drives on retired equipment can be overwritten several times to protect confidential documents, or the special deletion software now available to prevent data from being reconstructed can be run on the devices, neither of these approaches can guarantee 100 percent security. However, if the devices had already been equipped with encryption protection, the disposal wouldn’t require any extra effort or expenditure. Disposal costs would be reduced, as would the worry that data could inadvertently end up in the public domain if there should be a lapse in security at the disposal company. Professional security software for mobile devices also ensures that a hard drive that has been removed from one computer cannot be read in another.

Tips for choosing an effective encryption solution

The best encryption software for mobile devices uses secure algorithms, such as the well-established AES algorithm. This algorithm also allows for installation at a later stage and can be used on several different operating systems. Additional criteria when selecting the software are low maintenance requirements, transparent and automatic operation, a high degree of stability, and a short test phase. The more thought a company puts into its security policy, the better and faster it will then be able to meet this list of requirements.

Efficient software for administering data security must provide simple mechanisms for the uniform, central configuration of all relevant security rules. The more comprehensively these rules are structured results in the fewer potential sources of error and the less training and planning needed. Sector-based encryption concepts are the easiest to use because they cover the entire data storage medium. In contrast to file-based or directory-based systems, only a few standardized rules, encompassing large client groups, need to be defined. And another important thing: professional security solutions provide protection that is more extensive and of a higher quality than an operating system's own tools. They offer other advantages, too: Security policies can be enforced across platforms, the entire hard drive can be encrypted, removable media can be backed up, and heterogeneous PC environments can be supported.

Integrated concepts support due diligence

Knowledge is the best defense against the risk of devices disappearing. Employees can be taught security rules to observe and which forms to complete in order to protect devices and the network – as well as to be reminded to keep a watchful eye on mobile devices. Management and executives are legally required to provide careful and secure data management. For example, the State of California has enacted legislation that applies to all companies that conduct business operations in California (even firms based outside of the United States). When a data security breach is identified, businesses are required by California Senate Bills 1386 and 1950 to notify all individuals involved. In Germany, one of the requirements of KonTraG (Control and Transparency in Business Act) is that businesses are obliged to implement efficient risk management. Since a substandard IT security system can cause enormous economic damage, company management must provide for an adequate level of security. Under Section 7 of the German Federal Data Protection Act (BDSG), a company is liable, irrespective of who is actually to blame, for any damage caused by unauthorized or incorrect collection, processing, or use of personal data by third parties. Only in cases where the company has taken due diligence does the obligation to pay damages or compensation not apply.

To improve the care management and employees take in dealing with end devices, mobile devices, and servers, and when exchanging data with business partners, the IT department must define company-specific processes and standards in its security policy. This policy must be implemented and regularly reviewed. The challenge of implementing security policies throughout the enterprise, in particular in a heterogeneous IT infrastructure, can only be met by using an integrated IT security concept and comprehensive IT security solutions. These solutions should offer reliable protection independent of the platform, and meet both company-specific and legal requirements. A well-devised and implemented inventory plan will make employees attentive to this important issue. The planning will take time and effort at the beginning, but once the framework is in place and the selected software has been rolled out, fears of losing critical data will be a thing of the past.