Product

Data theft? What's that to me?

How can data get lost?

Accidentally
It happens so fast – a confidential document is attached to an e-mail message or copied to a USB flash drive without any intention of theft and thus slips by security systems like the firewall. Studies show that this is by far the most common cause of data loss.

Old hardware
From time to time, hardware must be exchanged for newer models. Or maybe you have leased your hardware and have to return it to the lessor? Often data on old hard drives is not deleted properly and falls into the wrong hands when hardware is exchanged.

Theft or loss of hardware
Do you know someone who has already lost a USB flash drive? Maybe even yourself? Or do you know somebody whose notebook was stolen during travel? The hardware is replaced easily, but the data might well be valuable beyond price in the hands of the wrong person.

Spyware
More than 80% of all malware circulating the internet today is designed to steal confidential data. Criminals make millions with it.

Hackers, criminal insiders and industrial spies
If your company is particularly innovative or processes other highly sensitive information, you could be in the focus of professional hackers and spies. This may not be the most common threat, but it is a particularly dangerous one because these criminals are deliberately aiming to harm you.

Almost every company or other organization processes confidential data. Most of these documents are stored electronically in company networks in the form of files. Examples of confidential files are:

- Documents (Word, Excel, PDFs etc.) containing personal data of employees or customers (name, address, date of birth, social security number, payroll information, credit card information, health records etc.).
- Price lists, marketing plans, proposals to and contracts with customers, NDAs
- Access information (password lists and the like)
- Research & Development documents
- Mergers & Acquisitions documents
- Protocols of board meetings

According to a study by the Ponemon Institute, every incident of data theft or unintentional data loss in the year 2009 cost a company an average of:

- in the USA: $ 6.75 million
- in the UK: £1.73 million
- in Germany: € 2.4 million (in 2008)

By far the largest number of damages (88%) is caused by unintentional negligence and mistakes and only 12% are acts of bad faith (Source: www.ponemon.org/data-security).

Costs are mainly incurred through:

- the loss of customers due to the loss of trust
- the loss of competitive advantages
- cost-intensive image campaigns required to repair the damaged image
- expenses for the legally required notification of the affected persons
- the payment of fines and penalties

Product

How can I protect myself?

- Create employee security awareness
- Protect all sensitive data in the network, on notebooks and on mobile storage devices by strong encryption (protects you also in cases of hardware exchanges)
- Restrict the use of mobile storage devices
- Allow only trustworthy applications access to sensitive data
- Central enforcement of security policies
- Automated encryption of confidential e-mail attachments
- Four-eye principle for the disclosure of critical data
- Logging of every access to sensitive data
- Prevent data leakage via FTP, web upload, screenshots, copy & paste

Meeting the legal requirements

Since the amendment of the German Federal Data Protection Act (BDSG) came into effect on September 1, 2009, companies are legally required to inform the affected persons or even go public in the case of a loss of personal data. If there were no sufficient protection systems installed, the law will presume negligence.
In the annex to §9, the BDSG mentions explicitly that encryption should be the medium of choice for meeting the legal requirements for electronic data processing.

Data Leakage Prevention

This term – DLP for short – describes software solutions preventing the unauthorized data leakage of company-sensitive information. Before deciding on a solution, it is therefore important to prioritize your own security requirements in order to make sure that the solution will solve the problem. Let the experts help you!

How much is your security worth to you?

Protection against data theft is a complex subject. It requires the knowledge of a specialist. Therefore, suitable solutions do not come for free – but, if worst comes to worst, they will be invaluable! Given the average cost of a data loss (see previous page), such an investment will pay off even if it prevents only one single data theft within a few years. In the end, it is your responsibility – you have to decide how much risk you want to take.

fide*AS*® – trust the Applied Security!

What our customers say:

„We looked at several encryption solutions. None of them were as easy to use and to deploy as fide*AS*® file enterprise . The apsec support team is outstanding, a rarity with the, 'get a sale and forget' type attitude of today. Highly recommended!

Jake Gaitan, IT Security Officer, Demmer Corporation

apsec protects knowledge. Knowledge is one of the key success factors of a company. We develop solutions to make your IT world more secure.

apsec offers knowledge. Put your requirements for encryption, data leakage prevention or digital signatures in the safe hands of our experts.

apsec works for you. We offer a full service, from business process consulting to software development and support for the whole system with only one goal – your satisfaction.

ddk-Software – Rådhustorvet 7,2 – 3520 Farum (Danmark)
www.ddk-software.dk – ddk@ddk-software.dk – Phone: +45 3927 0666

ddk-software