

O&O Study: Data in the USA and Germany Not Securely Deleted

Just because files are deleted, does not mean they are gone. How do Germans and U.S. Americans stack up when it comes to data protection? For their study "Data Data Everywhere", O&O Software purchased around 400 used storage volumes with the goal of finding out whether the contained files really were securely deleted. Once again alarming results: Olaf Kehrer and his team were able to restore private and company data with very little difficulty.

Berlin, September 3 – Windows Vista has raised the bar for computers in terms of required system performance. It is no wonder that many users choose to purchase a new PC and sell their old one. Hoping to strike a chord with users in this sort of situation and others, O&O Software purchased a large number of used data storage volumes to test in their new study. From 2006 to 2007, O&O Software purchased 395 storage volumes via online auctions in both Germany and in the USA, allowing for an international comparison.

Included in the 395 storage volumes consisted of 115 memory cards, USB Sticks and digital cameras, as well as 280 hard disk drives. Of the 280 hard disks, 59 were defective and were not included in the analysis, as the reconstruction of data in such cases would have been too complicated. On the remaining 221 hard disks, 72 (33 %) had already been securely deleted, making it impossible to recover any deleted data. However, 149 hard disks still contained data or had "only" been formatted.

The study's author, Olaf Kehrer, elaborates: "This means that 67 % of the hard disks contained personal or company data that could be reconstructed. In total, 17 million files with a total size of 2.4 Terabytes were recovered from those drives. These files included a large number of Word documents and Excel spreadsheets as well as 60 complete e-mail mailboxes of previous hard disk owners. Additionally, a number of private photos and videos were found, some of which contained bizarre pornographic material."

Of the 115 memory cards, USB Sticks and digital cameras tested, 32 were securely deleted, about 27.8 percent. 72.2 percent of this set, 83 storage devices, had not been professionally deleted, making the reconstruction of those contained files an easy task.

Data Data Everywhere 2007: Sensitive Data Visible to Everyone

The analysis of the recovered files were shocking for the study's authors. It was possible with very little difficulty to recover private letters, informative resumés or frivolous e-mails that would cause serious damage if they fell into the wrong hands. Cybercriminals on the Internet go through enormous trouble, using Spyware and Trojan viruses, just to get their hands on this sort of data and use it against unsuspecting users.

U.S. Americans did not behave much better than the Germans in terms of data security. Of the 80 purchased hard disks originating in the USA, 12 were defective and not included further in the analysis. Of the 31 intact hard disks, data could be reconstructed, about 45 percent of those hard disks tested. Olaf Kehrer: "On the hard

disks originating in the USA, a large number of explosive findings were made, including photos from soldiers in Iraq and U.S. military information. If data, such as the web access information for the US Air Force we found, were misused the damage would be devastating. Considering that we only purchased 80 hard disks from the USA, this is a surprisingly high quota."

What many computer users do not know is that mobile memory cards use the same file system as Windows hard disks. For this reason, a basic solution is simply not enough. With the right tools, deleted files can easily be recovered. 72.2 percent of the tested memory cards were not securely deleted. On 83 memory cards, the authors of the study could excavate 1.8 GBytes of images, around 3,100 in total. The photographs included shots of very intimate situations that could have only been possible using a camera's auto-shutter function.

Why don't users delete their data securely?

Over the last few years, the IT media have warned about the dangers of insecurely deleted data falling into the wrong hands. Despite the heightened awareness by some in the media, it would appear that company and private users have still not taken this issue to heart.

The study "Data Data Everywhere" states that that the biggest reason for this is simply lack of awareness. Olaf Kehrer: "When deleting data and formatting partitions, Windows gives the impression that the all files are completely destroyed. This is simply not the case. At home, in companies and in governmental organizations this is an extremely pressing issue. IT professionals have to make sure that the their colleagues know that files need to be securely deleted."

Old hard disks do not simply get thrown away these days, but rather find themselves quickly for sale on online auction blocks, such as eBay. This makes it possible for unauthorized users to easily access and recover deleted data that were thought to have been deleted. A further risk can be found at the repair shop. If a computer is sent in for repair with the original hard disk, users would be well-advised to require a signed statement from the repair shop promising not to read or copy any contained files. Of course, the most secure way to prevent such data theft is to remove the storage media before the computer is sent for repair.

Olaf Kehrer: "Naturally the ignorance of many users is not to be underestimated. Many sellers of user hard disks know full well about the dangers of recovering deleted data and, perhaps due to laziness or apathy, still pass them on to the customer."

Secure Solutions: Securely Deleting Data

This study on data security by O&O Software highlights not only the problems with this issue, but rather the solutions as well. It is clear that the simple formatting of a storage device is not enough. The encryption of the data on hard drives increases security, but still is not a serious obstacle for professionals who can use a number of methods to get at the data. Although very resource intensive, the physical destruction of a hard disk using large magnets or a drill is very secure. However, a secure deletion software - such as O&O SafeErase - offers a more accessible solution for private and corporate users.

The Study Results for "Data Data Everywhere" are available as PDF for immediate download (<http://www.oo-software.com/dde2007/>).

Homepage: <http://www.oo-software.com>

Study Download: <http://www.oo-software.com/dde2007/>

(6555 characters for release).

About O&O Software

O&O Software GmbH has been developing "Tools for Windows" since 1997. Customers include home users, SMEs, public institutions and global business groups. These tools are effectually sold directly and by using our partner network and are available in more than 50 countries. The product portfolio includes applications for performance optimization, system administration, data restoration and the secure deletion of data. O&O products have been judged as technologically leading in numerous tests. You can find more information and free trial versions of all products on our website. O&O's products include O&O BlueCon, O&O CleverCache, O&O Defrag, O&O DiskImage, O&O DiskRecovery, O&O DiskStat, O&O DriveLED, O&O FormatRecovery, O&O MediaRecovery, O&O RescueBox, O&O SafeErase, O&O ToolBox and O&O UnErase.

Press Contact

Andrea Strehsov

O&O Software GmbH, Am Borsigturm 48, 13507 Berlin, Germany

Tel.: +49 (0)30 4303 4303, Fax: +49 (0)30 4303 4399

E-mail: press@oo-software.com

Members of the media can find additional information and imagery online in the O&O PressCenter at <http://www.oo-software.com/en/press/>