Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Non-Malicious Destruction of Data

Protecting the data employees need to do their jobs is of vital importance to every company and should be viewed by any Information Technology professional as the top priority. While outsider threats to the integrity of the network must be given a high priority, we must not forget that often the greatest threat to the company is from the inside. Malicious and nonmalicious damage by users still represents the greatest threat to the integrity of the network and the data that resides on that network. Accidental destructio...

Copyright SANS Institute
Author Retains Full Rights

AD

Name: **Saffet G. Ozdemir**
Version #: **SANS Security Essentials Version 1.2f**
Title: **Non-Malicious Destruction of Data**

© SANS Institute 2001, Author retains full rights

Non-Malicious Destruction of Data

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In today's competitive market with slim profit margins and tight deadlines no company can afford for whole departments, or small groups of employees, to be unproductive for even short periods of time. Protecting the data these people need to do their jobs is of vital importance and should be viewed by any Information Technology professional as the top priority.

While outsider threats to the integrity of the network must be given a high priority, we must not forget that often the greatest threat to the company is from the inside. Malicious and non-malicious damage done by users still represents the greatest threat to the integrity of the network and the data that resides on that network. Accidental destruction of data is almost unavoidable given that nearly every office employee must use a computer at some point in the execution of their normal duties. Moreover, employees or consultants within the company are in a unique position to do the most malicious damage by knowing which files are likely to create the greatest disruption when sabotaged and by having access to those files on a regular basis. Additionally, temporary employees and consultants are less likely to protect the company's data through observance of established security and integrity procedures. Since their role in the company is temporary, they may simply have been given inadequate training in company security procedures

In a 1999 survey of 300 Windows NT systems managers, 88 percent said accidental deletions were the leading cause of lost data while 69 percent of IT managers said they had suffered a critical loss of data due to the same cause. In the same survey, of the 48 percent of respondents who said backups were inadequate, 55 percent said data is lost between backups and 26 percent said backups are not always reliable. [3] Overall, 64 percent had tried to recover data from backup only to find the backup was faulty. [5] While this survey is now nearly two years old, there is no reason to think this very common problem has simply disappeared. Not only are there more users every year, and more automation of formerly manual tasks, the general skill level of the users typically lags behind the growth curve of both hardware and software. [1]

In the case of malicious activity, the opportunity for damage by an insider is substantial. Moreover, an insider seldom requires specialized knowledge in order to inflict this damage. The attack of an insider may be restricted to deleting a few files needed by a rival employee within the organization, or may be directed at the organization itself, perhaps by corrupting or deleting an important sales tracking database. In a 1999 joint survey by Computer Security Institute and the Federal Bureau of Investigation, 55% of respondents reported malicious insider activity. [4]

While traditional tape backup schemes are essential, they are also inadequate in a number of areas. Specifically, failures can result during the backup and recovery process and time is lost in recovery of vital files. Additionally, many backup strategies do not include user files on local hard drives. Finally, there is often a significant delay between the time data is created and the time at which it is backed up. Destruction of data collected during this time delay is irrecoverable and often results in time-consuming procedures to recreate the data, assuming it can even be accurately recovered. Inevitably, some of the data will be permanently lost. When the World Trade Center was the target of a terrorist attack, none of the transactions for a brokerage firm had been backed up for the current day. This information had to be reconstructed from trade tickets and notes, which had survived the bombing. Much of this 'paper backup' had already been relegated to the wastebasket. When a small newspaper in North Carolina caught fire, most of the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

news articles and nearly all of the advertising from the previous and current day had to be reconstructed from memory.

Regardless of whether the loss is restricted to one department or even the laptop of a single hard working sales representative, the result is expensive and time-consuming.

Areas of Vulnerability

Proprietary Software

Software in larger corporations will be comprised of a variety of "off the shelf" standard products and special in-house applications developed to meet the specific needs of the company. In the case of custom software, protection of the software itself is required. Also with custom in-house software, two situations must be provided for. Firstly, appropriate version control must be maintained. Secondly, strong testing standards and code review are needed to insure the software does not corrupt or destroy vital data.

Shared Data

Shared data resides exclusively on the network and is in use by multiple employees much of the time. Shared data undergoes regular updates and may be shared not only by many users, but also by many departments. This data may be accessed and maintained via a packaged software product or by in-house software developed specifically to meet the demands of the company. Frequently, this data is accessed by multiple applications simultaneously. Loss or corruption of shared data can severely impede the work of many people and departments. The ability to quickly and reliably recover this data is essential. Moreover, data that is updated constantly throughout the day should be subjected to more than a daily backup. For example, let us say we have a database accessed by several dozen users resulting in a few hundred transactions in a given hour. Corruption and loss of that database at any time of the day, and then attempting to recover that file from the previous night's backup results in the loss of every transaction made during the current day. The users must then attempt to reconstruct the lost work, which therefore results in hours of lost productivity and general worker frustration. [6]

User Data

User data is local data that individuals require to complete specific tasks and it is not usually created or updated in a multi-user environment. More often than not, this data is kept on the local hard drive of the user's workstation. User data encompasses such things as word processing documents, single-user databases of limited scope, spreadsheets, etc. The importance of this data is often given low priority since its loss or corruption does not affect the operations of an entire department or group of many users. However, in many corporations the user data represents the bulk of the information created in the course of a business week. While a single document may seem to be of limited importance, the effects of its loss can be great if it happens to be required by the CEO for the next meeting of the board of directors and its creation required the labor of

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

one individual over a week's time. And what is the cost of losing every document on the hard drive? [6]

Mobile Users

Many corporations now have significant numbers of mobile users employing laptops. These employees are often disconnected from the network for extended periods of time, working exclusively with the laptop and connecting only periodically to the network for synchronization or sharing of data. Frequently the mobile user's only reason for connecting to the network is for accessing e-mail. Even if these users are making regular backups of their data, it may be difficult to retrieve the information in an emergency. The user may lose or corrupt an important file while on the road at a time when the appropriate I.T. staff is not available to assist in recovery. An additional area of vulnerability to the company occurs if the employee is suddenly terminated or suffers an accident. In this event the company may not even have the appropriate access to the data or the backups. Finally, what is the company to do if the laptop is stolen? Unless the user had the foresight to transfer all files to the network during one of their connections, the data is lost forever.

Telecommuters

It is projected that by 2004, nearly 21% of workers will telecommute some or all of the week. Further, mobile data collectors are predicted to make up 14% of the workforce. [7] Already there are in excess of 23 million people who work at least one day a week outside the traditional office. Many of the same problems regarding data integrity and protection, which affect mobile users also affect telecommuters. Regardless of whatever company policy may be, inevitably some work related information will reside on the computer in the worker's home. While this also presents unique security risks, we are primarily concerned in this article with maintaining and protecting the integrity of the data, whether it be documents, spreadsheets, or important notes the worker maintains on their daily activity. Firstly, it is important that files on the computer in the home be adequately backed up. Secondly, it is vital that the company have access to at least a copy of that work related data. In some cases, the computer in the home office of the telecommuter may not even belong to the company – but the data they are working on does. The risk to the data on a home computer is far greater than the risks presented in a traditional office environment. Theft, fire, flooding, and mishandling are very real dangers.

Approaches

True Test Environments for Software

In too many organizations there is no means of thoroughly testing new or updated software prior to deployment. At best, the testing environments are limited in scope and function. This can result in compromising the integrity of vital data when the inadequately tested software is deployed for use in the enterprise. In addition, the software may have unexplored security holes, which are not apparent in limited test circumstances. For effective testing of new software, it is necessary to maintain a complete testing platform, which mirrors in nearly every respect the live

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

environment. While this can sometimes represent added expense, it is less costly in the long run than compromising data that may or may not be recoverable. Ultimately, Quality Assurance is a sound foundation for Information Assurance.

Insuring Adequate Backup of Local User Data

A frequent solution to backing up data on workstation hard drives is to warn the user to copy files to the network. While some users may be diligent in this respect, most are not. Unfortunately, it is when the user is the busiest and working the hardest that this simple precaution is often overlooked. "Making them pay the price" of their negligence by having to re-enter their work is hardly the optimal solution. Ideally, local hard drives should be backed up frequently and transparently, without the intervention of the workstation user. In the event of an accidental deletion, the user should have the ability to quickly and easily restore the lost file without requiring specialized expertise and most definitely without having to rely on the Recycle Bin. Should a hard drive in a workstation crash, it should be possible to recover **all** files the user was working on.

Ability to Quickly Recover Deleted Files

It is not uncommon that a user accidentally deletes files on the network. While it is easy enough for a user to undelete files on their local workstation, it is not so easy for them to recover the network files. If the user fears retribution for the careless act, the user may not even inform anyone immediately that the inadvertent deletion occurred – assuming the user is even aware at the time of what he or she has done. Even assuming there is a recent and accurate backup of the file, the intervention of I.T. staff is generally required to recover the file and that can consume more time than the worker can afford. Clearly, this does not meet the 'availability' criteria for proper Information Assurance. In an ideal world, deleted or corrupted files should be recovered with relatively little effort and in as short a time as possible. The recovered files should contain the most up-to-date information possible, not simply what was in the file at the end of the previous business day, which, unfortunately, is usually desperately inadequate.

Summary

Any backup solution must protect the enterprise and the individual users within the enterprise from lost productivity, lost or corrupted data, and time consumed in resuming normal operation. The solution must protect the data in the event of damaged hardware, bad software, and user error. This protection must be extended to all users within the enterprise, regardless of their physical location or work circumstances. In addition to protecting the data, a good backup solution will also allow for repair of corrupted software. Any solution that is to be successful should be of limited complexity and as much as possible allow users at least some limited ability to recover their own work under circumstances that may be less than ideal. The salesperson sitting in a hotel room at midnight ought to be able to recover that important file absolutely required for a presentation the next day.

Examples of Potential Solutions

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Managed Client Backup

Managed Client Backup [8] is a software suite which provides backup solutions to cover both workstations and mobile users. Features include file versioning, unattended backup, and user-initiated drag-and-drop restore. Not only does this solution take the responsibility for backing up the workstation out of the users' hands, it also gives them restoration control without requiring the intervention of skilled and expensive I.T. staff.

File versioning provides the added benefit of being able to 'roll back' through previous versions of the same file. Should the integrity of a file be compromised, it is possible to simply move back through the versions until a correct version is located. Data trickling insures that backups are current and not simply images of the file from the night before. Resume and Reconnect features protect the mobile users, offering them a higher level of protection than might otherwise be possible. The backup procedures are policy driven and not dependent on the user following a set schedule or performing any specialized tasks.

Ontrack RapidRecall

The Ontrack RapidRecall suite [9] offers a host of utilities for efficient, accurate, and timely backup and data recovery. The core of this software makes an image of every user's PC on a designated server. This snapshot of each PC is then updated every day.

A backup module transparently backs up all user data at every PC. This data is then stored on a centralized server on the network. A module called iRoam allows users to retrieve files via a web browser through an Internet connection or on the company's intranet. This is a convenient tool for both mobile users and telecommuters.

The Heal application is used to repair software on a PC. The software problem may be due to a corrupted application, a virus, or bad configuration settings. Regardless of the problem, Heal allows the users to repair the damage themselves or it can be restricted to the use of I.T. personnel only.

Storactive LiveBackup

Storactive LiveBackup [10] provides continuous, real-time backup of important data, insuring that data on the backup remains current. Files on workstations are backed up automatically and transparently as they change. Moreover, LiveBackup protects data from loss even when disconnected from the network, allowing laptop and remote users to be protected against data loss. Users have the ability to restore their own files. Administrators maintain centrally managed backup policies, insuring that backup procedures are consistent and enforced.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[1]Drew Robb: Surveys: Human error is the culprit in data loss
Government Computer News 09/06/1999
http://www.gcn.com/vol18_n029/enterprise/553-1.html

[2]Ninety Percent of survey respondents detect cyber attacks 03/22/2000
Computer Security Institute
http://www.gocsi.com/prelea_000321/htm

[3] Mitch Wagner: User Errors are Key Reason for Data Loss, Survey Says
Today's News 10/29/1999
http://www.internetwk.com/story/INW19991029S0002

[4] Statement for the Record of Louis J. Freeh, Federal Bureau of Investigation 02/16/2000
Federal Bureau of Investigation
http://www.fbl.gov/pressrm/congress/congress00/cyber021600.htm

[5] Deletions are Bigger Threat Than Viruses
Microtimes Magazine
http://www.microtimes.com/202/induanal202a.html

[6] New technologies, enlightened administration and just plain old-fashioned luck
ComputerWorld 3/06/2000
http://www.idg.net/go.cgi?id=311005

[7] Telecommuting (or Telework): Alive and Well or Fading Away?
International Telework Association and Councel 06/2001
http://www.telecommute.org/aboutitac/alive.shtm

[8] Managed Client Backup
http://www.caworld.com/proceedings/2000/storage_mgmt/tsi08sr/sld002.htm

[9] Ontrack
http://www.ontrack.com/rapidrecall/modules.asp

[10] Storactive Inc
http://www.storactive.com

© SANS Institute 2001, Author retains full rights

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**