Realtime
publishers

The Essentials Series: New Techniques for Creating Better Backups

Avoid Making Headlines by Securing Your Backups

sponsored by

ARCserve®
More than Backup

by Eric Beehler

Copyright Statement

© 2009 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Avoid Making Headlines by Securing Your Backups

In March of 2005, a large, multi-national banking company lost backup tapes. Those tapes contained information about 1.2 million federal employees, including personal data about US Senators. In July of 2008, a popular retailer potentially exposed information about 650,000 customers because the company charged with securing the backup tapes reported them missing. In January of 2006, a major hotel chain lost a tape containing the personal data of 206,000 customers. In March of 2009, a major police department in a large city suspected 80,000 police identities could be compromised when data tapes were found stolen by a pension fund director of communications. These are just a few examples of a seemingly rising trend. The loss of data is not the only thing these companies have in common. They also shared the unenviable spotlight of the press and had to admit to their customers that their identities were possibly compromised.

In all these incidents, whether an inside job or an external theft, the data on the tape was easily readable. No encryption was employed to protect that data and there were obviously issues with security of the physical media. Thus, once a stolen tape is loaded, it can be read without any further hacking necessary. Once the tape is out, the data is free and clear for the taking.

As companies become more aware of their responsibilities for data and have to deal with the data retention requirements from legislation such as the Sarbanes-Oxley Act, they are realizing that old backup methods assume that only authorized personnel have access to tapes. The storage retention requirements and realities, such as the need for readiness to mount a disaster recovery, means there are more tapes with more data in more places. With the sensitivity of the data and continued scrutiny of companies who hold that data, administrators need to be vigilant because they are the ones on the front line of data defense.

Enforcing Your Policies

Although the technical solutions for backup security are important and help thwart attacks and loss, they are not the total picture. In fact, it is what we do as people that get an organization half way to true backup security. Take a look at your current IT policies. Often there is coverage of accounts, networks, permissions, and physical access, but backups are often left out. Even if there are policies that speak specifically to backup, the exposure to backups is usually so confined to specific IT personnel that it’s barely given a second thought, which puts the onus on administrators to get this area of security right. Without policies and enforcement of those policies specific to data backup, we’ll all continue to see stories about massive data breaches due to poor backup security.

Tracking Data Security and Access

First, develop a policy around where your tapes are stored. Tape storage is becoming an increasingly difficult thing to deal with now that some data has to be kept for upward of 7 to 10 years. Tape storage locations and containers should be clearly marked with pertinent information such as dates, backup system, and data center.

Even more important, access controls need to be established to those locations. This means no more tubs in closets or unlocked doors. Access to tapes should be just as stringent as access into a data center or network closet. An access control list (ACL), much like the kind on a file system, allows you to create an audit trail to understand who has what and why.

If there isn't a clear method to go about removing and destroying old tapes, one needs to be established. Sometimes tapes will show error or be labeled as too old to use. Those tapes need to enter a process of verifiable destruction. Degaussing—exposing the tape to a strong magnetic field—is a common practice. A challenge with tape destruction is that different tapes have different requirements to be considered "destroyed." Follow best practices for the specific kind of tape. A quick wave of the magnet isn't usually sufficient to destroy all the data. In addition, create an audit trail and have someone verify proper procedure is being followed. Many third-party companies that handle data offsite backup archiving can also handle data tape destruction, but be careful about handing off that responsibility to a third party. If you do, there should be regular audits of that process at least once a year.

Tapes that were used to store sensitive information should be pulled from rotation and not reused in a different capacity. Tapes that need to be reused often—for example, as differential backups—should be separate from archive tapes. Do not resell media unless there is a verifiable process for erasing data. Letting sensitive data out the door on EBay won't seem like such a frugal decision when a security breach is discovered.

Media Handling/Chain of Trust

There are plenty of reasons to use a third-party company for archive tape storage, including storage space, proper climate controls, and access to data for disasters. When using a third-party company, make sure there are policies in place for security. When allowing those third parties on site, make sure there are specific protocols for how they retrieve those items and ensure you audit what is going out the door. Also, there should be specific people identified as those who can retrieve tapes. Those tapes should be in sealed containers that have been cataloged. Finally, never use a third-party company without a way to audit their activity.

In house, use specific assignment of duties in order to make it clear whose job it is to handle tapes and who has access to sensitive data. Also, credentials for backup and restores must be handled as carefully as the domain administrator account. These credentials give access to data that has the same impact as handing a person domain access to all your servers. Document who has access to what and keep that documentation up to date. Also document any backup and restore testing, as these audits are proof of how your process is working.

There are certain regulations that can affect how you develop and follow policy. For example, Health Insurance Portability and Accountability Act (HIPAA) compliance requires a chain of trust be established when sharing patient data with third parties. Thus, with data passed off or shared with a third party, there must be a guarantee that confidentiality and data integrity will be maintained. Often, by understanding who has access and who has specific duties in the backup environment, there will be very few questions you can't answer if a question of security arises. A fully documented backup and restore plan that is audited is always a best practice and is a requirement with certain types of data.

Unauthorized Backups

Finally, avoid unauthorized forms of backup. Several data breaches that have been made public show that large repositories of sensitive data made it to a laptop, a USB drive, or external hard disk. These types of backup need to be tightly controlled. A large database of customer data copied to a USB flash drive cannot be allowed. Consider using solutions such as Group Policy to prevent use of unauthorized external devices. This is possible in Windows XP and more fully in Windows Vista. Using laptop hard drive encryption can help limit exposure to lost laptops, but policy should make it clear that this kind of data should be kept in the safety of internal servers.

Take Advantage of Security Tools

The fact is there are security features, such as encryption and access control, already available to most administrators. For those that don't have them, they are usually just an upgrade away.

Encryption

The primary method of securing backup tapes is through encryption. Encryption allows the backup tape to be secured the same as when a laptop hard drive is encrypted to prevent stolen data, a Web site provides encryption to protect personal information, or an email is encrypted to ensure only the recipient can read it. Instead of easy access to the data, there is now a complicated, often impenetrable layer of protection that can't be opened without the keys.

Implementing Encryption

Encryption is often employed for data that is expected to be outside the walled network and in the public. When thinking of backups as potentially having that same issue, you'll find encryption absolutely necessary at least for key data. To implement, you'll want to review how your specific backup software implements encryption, but there are some key things to know. First, the type of encryption, or cipher, usually speaks to how strong the encryption is. The first instinct may be to use the strongest encryption possible, but there is a price to be paid. The stronger encryption requires more calculations and, therefore, more CPU cycles to process. This can stretch out the backup time as well as the stress on those servers. Depending on the options, some backup software will allow you to choose where the encryption will happen and some offer additional hardware, such as an add-in processing card or an appliance, to offload encryption processing.

Performance Considerations

Performance impact can be measured by taking stock of performance before and after enabling encryption. Look at statistics such as CPU, memory, and time to complete a backup. It's better to start small and ensure you can back up and restore properly before relying on this method. Once files are encrypted, if the key is lost or the proper procedures not followed, the data will be inaccessible even though you have the physical media. Understanding the performance impact is an important factor if you are going to use agent- or client-based encryption before the files are transmitted. If you are considering a hardware-based solution that will enhance encryption speed, factor in the cost of the key versus performance gained.

Also note that encrypted data is sufficiently random, so it does not compress well. In fact, encryption usually adds 5 to 7% to the size of a file. Enabling compression using the backup client software will gain better performance than tape-based backup compression. If you are relying on the built-in function of tape drive compression, such as the kind that comes with the LTO-3 tape drive, consider disabling that and enabling the compression of your backup software client. This is, of course, another process that will add to CPU overhead, though it's not usually very significant on modern server hardware. Consider what a one-to-one compress ratio will do to the available capacity of the backup solution to gauge impact.

Key and Password Management

Before turning on encryption, the proper procedure must be considered. This is especially important in regards to key management. This is where many organizations fall short. As with a password on a post-it note stuck to a monitor, the keys do no good if everyone knows them or can access them easily. Often with client-based encryption, the keys are created per backup client agent. Thus, a best practice is to manage either one passphrase very well or reduce risk by using multiple passphrases, assuming a single-key encryption method. Either way, usually the management of these passphrases is a manual process, done through a spreadsheet and restricted access to the file. Some software includes centralized key management, which offers enhancements to automate and protect those keys. Ensure you are exploring the available options and make a decision on how to limit access to encryption keys.

Another consideration for managing keys is ongoing key changes. If a key is compromised or an employee who had access to the keys is leaving the company, best practice is to change the passphrases that are used. This means creating a key log, which tracks when keys were issued, to which servers, and who had access to those keys. When the key is changed, it only applies to data backups moving forward. All keys used for previous backups are still valid, so you must keep those keys available and accessible in case those backups are needed.

If a backup system is using a multiple-key system, the rules change a bit. Instead of having a single key for each system encrypting data, the encryption management layer takes care of managing that key, also known as a key quorum. It then sets up access for administrators through their own credentials and passwords. So, even if tapes were taken and that person had credentials to the encryption system, they still would not have access to the system that contains the encryption keys. How this is configured and managed varies by backup vendor, but the concept is the same. This kind of system adds to the safety of the keys but can involve additional cost and complexity.

If the backup software doesn't integrate an encryption feature or the cost for encryption is too much of a hurdle because of extra licensing or hardware requirements, there are alternatives that allow for encryption of select data. Some applications and databases may already be encrypting sensitive data. Many databases, for example, are able to encrypt select data. Some applications may encrypt data as a rule. Re-encrypting this data does not cause harm during backup, but when trying to understand exposure without encryption, see if sensitive data is already being encrypted.

Also consider where encryption is needed most. Encryption introduces another layer of security, and that involves more chance for error. If you don't need encryption to backup certain data, perhaps you should consider leaving it out. If you think about it, backup of Web servers, QA application environments, and Windows C: drives tend to avoid any sensitive data. It could be much easier, faster, and more efficient to use encryption on certain file shares, databases, and email, among other potential targets.

Giving Backup Software Proper Access

The internal threat isn't just limited to the backup tapes but also in how the backup software accesses the server that contains sensitive information. Great pains are often taken to limit access to these systems, but then the backup software needs administrative access to everything. An account that is authorized to back up entire servers can leave a big hole in the case that someone gets a hold of those credentials for nefarious purposes. Set the backup account so that it does not have interactive logon rights. Even though it will need to access all files on a Windows file server, for example, avoid just putting that account in the local Administrators group where it can have access to everything. In a Windows environment, use the domain-specific Backup Operators group instead. If you need to use local administrator rights, consider a separate account per server to limit exposure. With this, you'll still want to make sure to track all accounts and their uses.

Do not use real user accounts or a general administrator account to back up servers. Use service accounts created specifically for that role. Often an administrator's user account will be in use without anyone's knowledge and then cause problems later when a password expires. Using a general administrator account for backup can expose you to pain when the credential has to be changed or in the event of a lockout of an important account like the domain administrator. Plus, an all-encompassing account like the domain administrator will cause far more problems if used to hack and expose your environment. Know the accounts you are using and use them only for the purpose of backups and restores; reducing your security threat and possible problems.

For a DMZ network segment, there is generally more risk because the servers come in direct contact with Internet traffic. First, proper lockdown for a server in this environment is a must. You might even be using a different domain. What isn't common is a separate backup environment for those DMZ servers. As with anything in the DMZ, make sure only the needed ports are open in the firewall between the DMZ and internal network or the backup software. These ports are easily found from the vendor of the backup software. Next, ensure that a different set of service credentials are used for the backup agents in the DMZ. If those servers were ever compromised, they should never be able to have direct access to servers in the internal network. In fact, if ever there were a time to use a separate service account per server, those in a DMZ are the servers to consider.

Databases are an interesting consideration because most databases come with their own method for creating a file backup. Most backup vendors have special agents that will interact with a database and back it up without those separate jobs. When using a built-in backup job in SQL Server, for example, the backup agent isn't the only access to worry about. The SQL Server Service account, when running as a domain account, also needs read and write access to a folder on the server in order to place those files in a backup location. It's also an option for SQL Server to use a proxy account to run the backup job. The backup agent can then apply further encryption at a file level before backing up the files to tape. This time, there are two backups to consider and two accounts to track access for. With these kinds of applications, the chain of backup needs to be tracked so that access needs can be tracked as well.

Don't Forget Your Data When It Hits Tape

Administrators have a choice to make when it comes to backup security: Will they be proactive or reactive? A reactive stance assumes the risk to a data breach is low and the likelihood anything will happen is not high enough to worry about. These people are in danger of making it on the news. The proactive administrator will be able to track where their data resides, whether it's on disk or tape. The proactive administrator will be able to refer to audits to ensure the company's data is being handled properly. They will be confident that data involved in a tape loss or theft will still be protected because of encryption. In addition, they will be able to ensure that unauthorized users do not have access to sensitive data through the backdoor of backup. In fact, the proactive administrator will be able to use this web of security tracking and encryption to sleep better.