Global Information Assurance Certification Paper

Scott M Parrish

Security Considerations for Enterprise Level Backups

GSEC Practical (v.1.2f)

Security Considerations for Enterprise Level Backups

Introduction

Backing up your data is an essential security measure in today's computing environment. Data has gained intrinsic value, either in the manpower needed to generate that data or in the significance of that data to your customers. While data has become more significant it also grows, by some estimates as much as 100% per year. Data loss, both accidental and due to theft, costs hundreds of millions of dollars every year. When taken as a whole one thing becomes clear, your data must be protected.

Enterprise Level Backups

Enterprise level backups are becoming the fundamental way to safeguard your data. Gone are the days where you can have a tape drive hooked up to every machine in order to back it up. Now you might have 1 server backing up 20, 50, 100 or more clients, some backup solutions even allow thousands of clients on a single server. The primary reason for this is centralization: of media, of administration, of access. It is much easier to change 100 tapes on 1 machine than it is to change 1 tape on 100 machines. It is easier to collect data and spot problems from a central server than it is to monitor 100 machines.

Along with the greater ease in management that Enterprise Level Backups provide, comes a greater threat to security. Centralized service means centralized access. If an intruder gains access to your backup server he gains access to the collected data from all of that server clients. This is an important security risk, one that should be considered and planned for. Not every risk can be accounted for, good computer security is always a compromise between usability and precautions. A good overview of the security risks of Enterprise level backup can provide you with the groundwork needed to make the decisions for your environment.

Topics to be covered

Risks to your enterprise level backup security can be grouped into 5 areas. Physical security covers the presence of the Backup Server, its media library, and Media Storage. Client security covers the security measures needed on the client level, while Server Security covers those same measures for the Server. Network security involves the communication done between Server, Clients, and Library. Restore Security is for the process and human elements of restoring data.

Physical Security

The most straightforward way to get your data is to walk up and take it. It is easier to take 1 tape containing perhaps 20 gigs of data out of the building than it is to send it out with a network. Access to your Servers, your media library and your Media vault should all be carefully controlled.

Access to Servers

Gaining physical access to your server gives me all the advantages I normally have in gaining physical access to machines. It is easier to break into machines from the console than from anywhere else. Limiting physical access to the server removes the ability to make this sort of attack.

Access to Media Libraries

Most ELB solutions make use of media libraries. These libraries are made up of drives, storage for tapes and robotics used to move tapes in and out of the drives. They will often be located very near the servers themselves and will often be able to be secured in the same manner as the server. Another consideration to make is to use the locks of the libraries themselves. Locking the door of the library will make it harder for people to remove a tape or other media from the library and carry it off with them.

Access to Media Vault

A good location for your media vault should be a prime consideration of your ELB scheme. This location will hold multiple copies of every file kept by your ELB! It should be in a locked room or other similarly secure location, access to this room should be strictly controlled and even monitored if possible. Another primary security concern with media vaults is their proximity to the servers and other machines that they back-up. If a disaster happens and the building your servers are housed in is damaged, you don't want the backup of that data to be vulnerable to the same event. Try and locate your vault in a separate building from the data, Using a Fireproof vault or strict fire suppression methods are also good practices, though tend to be more expensive. Protecting your vault from excess heat, cold, humidity and chemicals will prolong the shelf life of your media and improve the reliability of your backups.

Media Labels and Audits

Today's library can hold hundreds of tapes at a time, making media tracking an important consideration. Most libraries work with a built in barcode reader. Each media is given a barcode label that is used to keep track of that tape. Media managers will use these barcodes to file tapes into the vault, so that it can be returned to library when it is needed for a restore, or when the data on that tape has expired.

A clear record should be kept of where each piece of media is at any given time, and periodic audits should be performed against those record. Missing tapes represent a potential security violation and strictest attention should be paid to who has access to those tapes and when. For large enterprise level backup schemes, consider a software package with barcode reader to automate the process of checking tapes out of the library.

Client Security

Client/Server communications generally follow one of two models.

In the server based model, the server accesses the client in order to initiate the backup session. The Server maintains and determines the schedules, and initiates sessions with the client. This method has the great advantage of being able to enforce

backup schedules, insuring that regular backups are done. However as this method provides for server to client access, there is also a potential vulnerability.

In the client based server, the client determines when the backups are supposed to happen and contacts the server when it is about to proceed. This method has several advantages, notably that the server has no way of initiating contact with the client, thus providing no new conduit for attack. On the other hand there is no server based way to enforce the schedule of backups, so timely and regular backups may not happen.

In addition to the software's method for client/server communication, there is also the consideration of administrative access. A centralized backup plan may require a shell for backup administrators to use. This shell would be used to stop and start services or daemons, troubleshoot failed backups, install software or retrieve data. While such shells are nearly critical to the ability to do centralized management of the backups, it also represents a clear security violation.

Access to Backup Client

Most client software includes the ability to perform data restoration, after all without the ability to restore data, backups aren't much good. This means however that anyone with access to the client software has access to the data backed up by that client. Strongly consider protecting access to the client software.

Server Security

Server security is crucial. You must consider the server as an open conduit to all information on the clients it backs up. You should plan on the server being a dedicated machine, with no other duties. This system should be well hardened to attack, its logs should be actively monitored on at least a daily basis and access to the machine should be granted to as few people as possible.

Server Access

In many backup solutions, a server will have access to all of the clients. It is essential to maintain a very tight guard around who has access to this keystone machine. If multiple users have access to the server, they should be required to login on a user account before switching to an account with greater privileges, and records and logs should be kept of when people log in. There should be no access to this machine at all that does not require a password to use. Passwords should have a short lifescycle (60 to 90 days) and changes should be enforced using a strict password policy. Protecting this machine with the most stringent security and access methods available should be and remain a top priority.

Encrypted Data

One way to safeguard data from prying eyes is encryption. Encrypting data allows it to be stored with less concern about who can access it.

One simple method is to buy a hardware encryption interface for your data library. These attach to the SCSI cable that connects the server and library and do a hardware

level encryption (Or decryption) on all data passing through the cable. Tapes are written with encrypted data, and are subject to being decrypted the same way, making them useless for thieves. This method is fairly software independent allowing you to use any number of different packages to administer your backups.

Some software packages will allow encryption at either the client or the server level. Client side encryption safeguards your data at the client level, preventing access to that data without a password or software key. Server side encryption provides many of the same features as a hardware solution, As data is written to storage it is encrypted with a password or key.

Another method is to use a file or file system level encryption package. These encrypt the data as it's stored to hard disk preventing even other people with access to that system access to those files. This can be an especially good solution if there are only a limited number of files or systems that need this level of protection.

Access to Data

You can access backup data from most if not all backup solutions. If there are super sensitive files that even the backup administrators should not have access to you should consider either a personal backup solution for those machines or providing a method to encrypt that data before it arrives at the backup server.

Network Security

An often overlooked aspect of enterprise level backup security is the network. The network will carry data between client, server and library and is potentially a huge security hole.

Eavesdropping

In many Backup solutions, communication between a client, server and library will be open. That means that every file backed up over the network will be sent in the clear! If your network has a high security integrity and a secure firewall in place than this likely won't be any problem. If you are doing backups over a wan or on machines that are outside the firewall you should consider using a VPN between Server and Client, while this will degrade the performance of the throughput, it will also guarantee that no one is able to pull your data off of the network.

SAN Security

Storage Area Networking is an increasingly popular choice for providing both storage and backup services. The most important thing to remember about SAN security is that SAN is a network, and is vulnerable to the same sorts of vulnerabilities and attacks that more conventional computer networks are. SAN resources should be protected by physical security and the hosts on the SAN should be expected to meet stringent security requirements. As SAN continues to grow in popularity, it will become a better target for malicious attackers. Any good practices begun now will continue to protect you into the future.

NDMP limitations and potential

An emerging protocol that directly affects network backups is Network Data Management Protocol or NDMP. NDMP is used primarily to provide a backup solution for Network Attached Storage (NAS). Most NAS manufacturers use a proprietary operating system for their devices that precludes them from being supported by most Enterprise level backup schemes. NDMP provides a protocol based access to the data on the NAS and thus allows it to be backed up by any software that supports the protocol.

There is a serious flaw in the NDMP protocol. While the specification allows for MD5 digest authentication for credentials, it does nothing to protect the data stream itself. Additionally MD5 digest is not required so it is possible to present credentials such as a password in clear text. So any client on the appropriate network can eavesdrop on the data stream and extract the full contents of any file being backed up. This is a serious vulnerability

Employee Security

Backups without the ability to do restore are a waste of perfectly good tape. Backup operators and administrators may have access to great amounts of confidential data and. While there are very few technical considerations when providing for employee security, there are a number of human based factors.

Access to Restores

While clients are capable performing their own restores, most often it is a job function of the Backup administrator to do them. In a large organization, the backup administrator is unlikely to know everyone he will receive requests from and so some sort of identity verification must be performed.

One simple method is to create a Code-Word challenge. Create a file in the top directory of the backup and make the file readable only by those people allowed to request restores. Write a small script that is executed when the backup is performed to randomly place 3 words in the file. Then require anyone requesting a restore to provide those three words.

More sophisticated methods may include forms or manager signatures. Be careful to strike a useful and workable balance between authentication and efficiency.

Backup administrator

Most security comes down to having responsible people. A Backup administrator is going to have access to a large amount of your data, be sure you can trust him. Simple things like pre-employment background and reference checks can reveal potential problems. Regular operational audits can ensure that all the correct processes are being followed. Making sure you are putting your trust in the right person will go a long way to preventing any security problems.

Conclusion

While technical and usability concerns are extremely important to selecting an enterprise level backup solution, security is worthy of consideration. Defending your data in every way possible means protecting the servers that backup that data.

Resources

Cook, Rick. "Encrypting Backups for additional security" Searchstorage Tips: Backup. July 24, 2001
http://searchstorage.techtarget.com/tip/1,289483,sid5_gci756807,00.html (Aug 26, 2001)

Edatafinder.com. "SmartGuide for Background Checks". © 2000
http://www.edatafinder.com/htmlsmartguides/BackgroundChecks.html (May 28, 2001)

Element K Journals. "Close the door on hackers--secure your network" Windows NT Professional July, 1999
http://www.elementkjournals.com/ntp/9907/ntp9971.htm (Aug 27, 2001)

Enhanced Software Technologies. "11 Common Backup Mistakes and How To Avoid Them" eLinux: Linux Technology Solutions. © 2000
http://www.elinux.com/articles/bru.jsp (Aug 24, 2001)

Network Working Group, NDMP Initiative. "NDMP Version 4 Protocol". April, 2001
http://www.ndmp.org/download/sdk_v4/draft-skardal-ndmpv4-02.txt (Aug 22, 2001)

Ontrack Services. "Cost of Data Loss" Data Recovery Center. © 2000,2001
http://www.ontrack.com/datarecovery/cost.asp (Aug 25, 2001)

Quantum Corporation. "Best Practices" Prove It, Planning and Preparedness.
http://www.dlttape.com/proveIt/steps/plan/best/ (Aug 24, 2001)

Radding, Alan. "SAN security: not a big problem – yet" Storage Networking World Online. May 25, 2001.
http://www.snwonline.com/implement/san_security_5-28-2001.asp?article_id=28 Aug 22, 2001)

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event