February 2015

SysAdmin Magazine

Securing File Servers

10 Tips against Data Breaches in File Servers

Quick Reference Guides:

File Servers

EMC Storage

NetApp Storage

Helpful How-tos:

Detect Excessive Permissions of "Everyone" Group in File Servers

Detect File Changes in a Shared Folder

SysAdmin Magazine

Contents

Securing **File Servers**

by Brian Svidergol

Microsoft-centric technology professional
focused on infrastructure solutions.

Today, IT administrators are spending more time securing their networks than ever before. In light of several high profile data breaches, many administrators are introducing security into every project. That is a good thing! There is a renewed investment in security. The bad news is that there is so much data to protect. Often, administrators find it difficult to prioritize their security efforts. Back in the early days of the Internet, many organizations only had a single location where their data was stored – in their data center. Today, data can be anywhere. This makes it a challenge to find it, back it up, audit it, and protect it. In this article, we will focus on protecting file servers. File servers have been used to store company data for a long time. And while solutions such as Microsoft SharePoint have knocked down the market share of file servers, file servers are still represented in virtually every company and store a treasure trove of sensitive data. What makes file servers a key target of hackers – whether an anonymous Internet hacker or a mischievous employee?

1. File servers have been around for a long time. Many companies introduced centralized storage of data on file servers long ago. OK, but why does that matter? Because once security wasn't part of most IT projects. High profile data breaches were unheard of. File servers were deployed as a matter of convenience, ease of use, and providing a good end user experience. File servers were all about sharing data and making it easy to do so. While most organizations have updated their file servers to newer operating systems, they often just migrate the data with the existing security remaining as is. Because of this, the security of file servers and of the data stored on them should be a critical area of concern.

2. File servers store all types of sensitive information. Many file servers have centralized shared folders for each department in a company. For example, you may have shared folders for HR, Accounting, Payroll, Engineering, IT, and Sales. This makes it a one-stop shop for hackers. In addition, file servers are often used to store the home folder data for users. Home folders often contain personal information and company information, archived email files, and documents that are works in progress. If a malicious person was looking for something sensitive, chances are that the person could find it on a file server.

3. File servers are easy to locate. Once you are inside a network, whether as an external hacker or as an internal employee or contractor, finding file servers is a simple task. If you have access to a client computer, you can often find file servers by looking at mapped network drives. If you are logged into an Active Directory Domain Services (AD DS) domain, you can also query AD DS with a 1-line PowerShell command to find the home folder path. That path will contain the name of the file server.

So far, we've established that file servers are targets for hackers, easy to find, and often hold a treasure trove of sensitive data. Now, let's discuss some of the steps you can take to secure your file servers.

I recommend removing the Everyone group altogether and then using a security group that represents the actual users that need access over the network.

Lock down share permissions

Share permissions are the permissions that control who can access a shared folder over the network. Share permissions combine with NTFS permissions to form what's sometimes referred to as "effective permissions". The default share permissions give the Everyone group read access. Back many years ago, an anonymous user was considered part of the Everyone group! Administrators often find it quick and easy to adjust the default share permissions and give change permissions (or Full Control permissions) to the Everyone group since they know that they'll be securing the folder with NTFS permissions. Instead, I recommend removing the Everyone group altogether and then using a security group that represents the actual users that need access over the network. Avoid catch-all groups such as Everyone or Authenticated Users because they might be in use for the NTFS permissions and giving access to users that do not need it.

Lock down NTFS permissions

Most administrators are familiar with NTFS permissions. And many administrators are familiar with the principle of least privilege which results in users and administrators getting the minimum necessary permissions to perform a certain task or to do their job. The common security issue for NTFS permissions on file servers revolves around AD DS security groups. Security groups are used to grant access to shared folders. It is common, especially after several years of service, for there to be security group sprawl. Too many groups. And lack of knowledge of who is supposed to be in which groups. These things often lead to undesired access, especially as employees move around between departments, and contractors come and go. The more people have access, the simpler it is for an undesired person to gain it. Also, don't forget the default NTFS permissions when you create a folder. Even on Windows Server 2012 R2, the default NTFS permissions give all local users on the file server and all AD DS domain users read access to the folder. That's why it is important to be careful with the share permissions. If you use the defaults on both share and NTFS permissions, you are giving everybody read access, and this means all of the data can be copied off!

Enable auditing

Auditing is a great tool, because it can tell you who accessed a file, who tried to access a file but failed, and who was the last person to access a file. But, I've found that only a minority of organizations have implemented auditing for their file servers. There are some challenges around auditing, as you may have experienced. For example, how do you deal with the massive amount of log data? How can you sort through that data to make use of it? How can you find out about an anomaly proactively instead of reactively during a security incident? Microsoft has made a lot of headway in these challenging areas though.

I've found that only a minority of organizations have implemented auditing for their file servers.

You can configure much larger event log sizes today, you can use event log subscriptions, and you can use System Center Operations Manager's ACS feature to centralize all of your logs. There are also third-party solutions to reduce the challenges and improve the administrative experience.

Use encryption

For highly sensitive data, locking down share permissions, NTFS permissions, and enabling auditing aren't enough. You also need to encrypt the data. At a minimum, you should consider encryption of the most sensitive data. There are multiple encryption solutions available for file servers, shared folders, and individual files. Some, such as Active Directory Rights Management Server (AD RMS), are client facing technologies that allow users to dictate who can access specified documents and when. Other technologies, such as BitLocker, are backend technologies that are deployed and maintained by administrators while users are unaware of their presence. Each type of technology is geared for specific threat vectors. For example, if somebody gains access to your data center or server room and physically steals the file server or the hard drives, BitLocker can protect against that. If somebody gains access to the Payroll shared folder and copies all of the Excel spreadsheets to a remote FTP server, AD RMS can protect against that. Often, combining solutions is the best course of action because it protects against the most threats.

Consider looking at ways to implement monitoring and alerting to address your file servers.

Monitor and alert, especially for unusual activity

In my experience, most companies have some type of monitoring. Whether it be a small and simple solution or a complex one, most companies are covered. However, rarely do I see the type of advanced monitoring and alerting that would alert an administrator if an unauthorized person attempted to access a highly sensitive shared folder. Part of the layered approach to protecting your file servers and thus your data is having real-time monitoring and alerting that can warn you of an impending danger. If somebody performs a port scan of your entire IP range, you are likely to be alerted. If somebody shuts down your email server, you are likely to be alerted. But, if somebody tries to access 35 shared folders that they don't have access to, will you be alerted? Not likely. If somebody accesses a sensitive shared folder as a service account, will you be alerted? Not likely. Consider looking at ways to implement monitoring and alerting to address your file servers.

Implement Dynamic Access Control and automated file classifications

DAC was introduced in Windows Server 2012. As the name implies, it automates access control, dynamically. You can also use it in a manual or semi-automated way. However you use it, it can help prevent unauthorized access to your data. DAC works by implementing centralized rules that define access conditions. For example, if you are a member of the HR security group and you are in Toronto office, then you can read and write to the HR file share. But DAC supports much more complicated conditions that take into account the type of computing device being used, and AD DS attribute data. DAC becomes more powerful when it is combined with the enhanced and automated file classification which is available in Windows Server 2012 and Windows Server 2012 R2. Automated file classification continuously runs and classifies your data based on classifications that you configure. For example, if it finds files with credit card numbers, it can flag those as personally identifiable information and DAC can be configured so that only specific HR people can access that data. Similarly, you can classify driver's license numbers as sensitive and invoke an automatic AD RMS action to encrypt the data based on an existing template. This happens in the background, seamlessly. These couple of topics alone could take up a chapter of a book so if you aren't familiar with them yet, you should take a look.

Besides the obvious technical stuff, there are other ways to help protect your file servers. And these areas are what I call the "indirect access methods". The indirect access methods are often the simplest way to gain access to areas of your network. So, when you are configuring your environment, you need to keep these things in mind:

Be careful with password resets

If Joe works on the Payroll team, he probably has access to the payroll data. Just about anybody could deduce that. Including the contractor named Bob working at the Helpdesk. Bob is curious about salaries. So he decides to reset Joe's password a few minutes after Joe leaves for the day. Then he signs in as Joe and starts browsing the Payroll shared folder. How do you protect against something like that? First, limit password resets as much as possible. For example, anybody that has administrative access to IT systems or sensitive company data can only have their password reset by Helpdesk Level 3 which is limited to a few highly trusted individuals.

Be careful with group memberships

If Sally works on the Sales team as a manager, she probably has access to sales forecasts and pending deals. If our friend Bob is looking to see if now is a good time to buy a bunch of the company stock, would having access to the sales forecasts and pending deals be of value to him? Yes. How would he gain access? From what he heard, Sally is constantly working so resetting her password is likely to raise some red flags.

Security is all about a multi-layered approach.

But, Bob takes a quick look at her group membership and discovers that she is a member of a group named Sales Managers and a group named Sales. He adds himself to both of those groups and then begins perusing the Sales shared folder. Once he finds what he wants, he removes himself from the groups. How do you protect yourself against something like that? One way is via auditing, monitoring, and alerting. Another is to have a group owner and every time a membership change takes place, the group owner is notified. If Bob knew that every time a group membership changed, it was logged and the group owner was notified, he probably wouldn't add himself to those groups.

Watch out for fake malware

Fake malware, for lack of a better term, is gaining in popularity. Its only goal is to elevate itself. A malicious outsider wants to gain access to corporate data. An outsider sends fake malware via e-mail to a few people inside the company. The fake malware gets activated and starts purposely hogging the memory and CPU. Helpdesk connects remotely or sends out a desktop technician to investigate. The fake malware records remote connections and logs keystrokes for all local activity. Then it spreads by using the Helpdesk or desktop technician credentials. The goal is to continue along until some high profile targets have been acquired. In most cases, an AD DS domain administrator is the goal. How do you protect against this? Not easily. And certainly not with a single solution. As you've probably heard, security is all about a multi-layered approach. In some high security organizations, malware is investigated offline. In this example, an offline investigation by the desktop technician would've prevented the attack, assuming that he found the fake malware and removed it. Email is a large attack vector for these attacks, so preventing malicious attachments and educating users can also go a long way.

In a short article like this, I can only touch on many of the topics in a brief way. As you can imagine, most of the bullets in my list can be extrapolated into very long articles by themselves. But, the goal is really to bring some attention to these areas and encourage administrators to use the information as a starting point to securing their environments.


New Release
Netwrix Auditor 6.5
Detect & Prevent Breaches
Learn More: netwrix.com/go/auditor6.5

How to Detect Excessive Permissions of Everyone Group in File Servers

Native Auditing vs. Netwrix Auditor for Active Directory

Security breaches do not only originate from external attacks but also stem from internal factors, such as negligence on the part of IT staff. Members of Everyone group can be granted excessive permissions by mistake. This will allow them to copy, distribute, modify, or delete files on file servers which, in turn, can lead to crippling consequences for the organization, including exposure of sensitive data. That's why it is highly recommended that existing permissions of Everyone group are audited on regular basis.

Native Auditing

1.

We need to know what folder(s) group "Everyone" has access to. Run the following script in Powershell filling up "File Share Path" and ".csv File Name and Path" parameters.

```
dir -Recurse | where { $_.PsIsContainer } | % { $path1 = $_.fullname; Get-Acl $_.Fullname | % { $_.access | where { $_.IdentityReference -like "Everyone" } | Add-Member -MemberType NoteProperty -name "File Share Path" -Value $path1 -passthru }} | export-csv ".csv File Name and Path
```

2.

Open created .csv file via Microsoft Excel and check which folders group Everyone has access to.

3.

In order to find out other user or group permissions just type the name instead of word "Everyone" in the script.

Netwrix Auditor for File Servers

1.

Run Netwrix Auditor → Managed Objects → File Servers → File Servers → Reports → State-in-Time Assessment → Permissions → "Basic Account Permissions by Folder" report → Specify the following settings:

UNC Path – Specify a path to your shared folder using \\fileserver\share

Account – Everyone

Show Subfolders – Yes

Show Folders With Permissions – All

Show Account With Permissions – Access

Show Users with Permissions - All

2.

Click "View Report". You can export this report in PDF, XLS and DOC format.

3.

In order to know other user or group permissions just type the name in "Account" field.

Ten Simple Ways to **Prevent Security Breaches** in File Server 2012

by Krishna Kumar
10+ years in IT Industry specializing in designing, implementation and administration.

File server is the central location in any network containing all kinds of information which is saved and shared by users within the organization. There is no restriction on the type of information used and shared. Since it is one of the most common reach out place for the users in the organization, file server has become one of the critical systems in the organization. Protecting file servers is very important, as it can be accessed by many users simultaneously and sometimes by organizations worldwide as well. Accessibility and performance of the file servers can affect the productivity of the users. Microsoft has introduced some new features to protect Windows file server from any kind of security breach. Given below are the ten simple ways to prevent security breaches in Windows file server.

1. Implement Distributed File System (DFS)

DFS implementation helps to share the load and provide increased availability of the file server. DFS secures files and folders through NTFS and share permissions. It allows access only to those files or folders, for which a user has an appropriate NTFS or shared folder permissions.

2. Assign permission to group and avoid "full control" permission

Always assign permissions to group and avoid giving permissions to individual users. This allows the administrator to provide more control over the permission model. Provide least permission whenever and wherever possible and do not provide "full control" NTFS permission on folders/files, unless necessary.

3. Enable firewall with logging

Configure and enable Windows firewall with logging using an advanced security node. Enabling firewall protects connection from unauthorised sources through different ports and logging details on dropped packets or successful connections and can also help monitor and troubleshoot in case of a security breach.

4. Dynamic Access Control

This is a new useful feature which allows the administrator to centrally apply access control and permissions based on the defined rules. You need to identify and tag the data considered sensitive and once this is done, you can allow or deny access to specific resources. Dynamic Access Control also provides control over the permission and security of the data on a more granular level.

5. Physical security and Branch Cache

It is important that file servers are physically secure. It is recommended not to keep an individual file server in a small branch office which can be easily exposed to robbery. We can also make use of the Branch Cache feature to cache only specific data: the content is encrypted by default, and data is protected from any kind of threat.

Since file server contains a lot of sensitive information, you should audit WHO has accessed WHAT and WHEN.

6. Antivirus protection

Since the file server can be accessed by many users, it is an easy target for malware attacks. This can impact the accessibility and performance of the file server and also affects other network client machines. Updating the server with the latest antivirus version can protect it from most kinds of malware threats.

7. Update with the latest rollups and service packs

Microsoft releases security rollups and service packs quite frequently. These patches are based on the latest vulnerabilities and threats, so it is recommended to review these rollups and service packs regularly to keep the environment secure.

8. Enable BitLocker

BitLocker is a native tool for data encryption and protection. Data is stored on the disk subsystem of the file server and the disk system can fail for various reasons. Replacing a failed disk allows user to continue accessing the file contents. But we don't know if data can be recovered from a failed hard as well, and it can be very expensive for the organization. This kind of threat can be prevented by BitLocker: no data can be extracted from the disk or even from a failed disk, once it has been detached from the server.

9. No Internet access

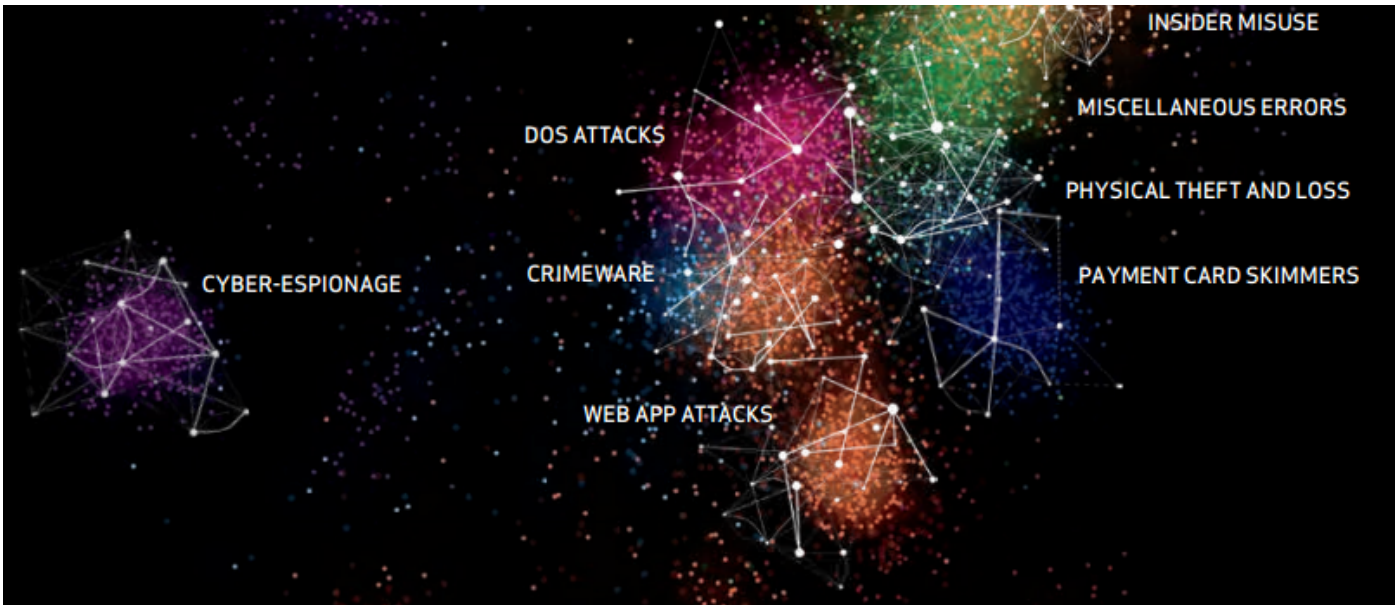
Protect file servers from Internet access and thus prevent potential damage to the server. It also stops file servers from installing any unauthorised third party application, which can impact performance and accessibility of the server.

10. Enable file server auditing policy

Since file server contains a lot of sensitive information, you should audit WHO has accessed WHAT and WHEN. This will help administrators analyse the environment for any kind of vulnerabilities and threats.

Verizon 2014 **Data Breach Investigations Report**: Change Auditing is on Guard against **Insider Misuse**

According to the report's analysis, change and configuration auditing proved necessary for maintaining security and protecting IT infrastructure against internal threats and data leaks.



The Verizon Annual Data Breach Investigations Report is one of the most expected computer security reports of the year. Based on actual incidents of data breaches, the Verizon Data Breach Investigations Report shows the actual state of IT security by analyzing the trend in security incidents. One of its chapters, "Insider and Privilege Misuse," is devoted to describing the mechanisms used for compromising organizational intellectual property. According to the Verizon 2014 Data Breach Investigations Report, corporate information is one of a company's most valuable assets, and the company's ability to control access to sensitive data and its dissemination inside and outside of the company can determine its superiority over competitors, and therefore, its future in the market. That is why corporate information is often compromised by unscrupulous employees for personal benefit or for other reasons. Michael Fimin, CEO of Netwrix, the #1 provider of change and configuration auditing solutions, takes a close look on the Verizon 2014 Report's chapter on insider threats to follow the main points stated by the Report and explain why tracking changes is so necessary for strengthening security and protecting systems against insider misuse.

The commentary is provided by Michael Fimin, CEO of Netwrix Corporation.

The majority of security breaches have resulted from privilege misuse: 88% of information leaks are attributed to granting incorrect access rights. Granting access privileges to certain employees is an inevitable need, but taking these accounts under control is also a must. “Most insider misuse occurs within boundaries of trust necessary to perform normal duties,” confirms The Verizon 2014 Report. Therefore, preventing privilege misuse is difficult, and the only way to stay secure is to grant access rights only to those with a business need and to keep an eye on their activities. Monitoring IT systems is easier with comprehensive change and configuration auditing solutions that allow you to track changes made to access rights, and thus have complete control over sensitive data and security configurations.

“The main thing we could do is enable continuous tracking of malicious user activities. Having deployed an auditing solution, one can ensure security by continuous analysis of authorized and unauthorized changes made to system configurations and sensitive data.”

It is a surprising finding that among companies’ employees, who have been granted privileged access rights and may become guilty of information leak, anyone can be suspected of committing a crime, including managers and executives. “We saw more insider espionage targeting internal organizational data and trade secrets than ever before,” says the Verizon 2014 Report. Moreover, the Report states that 71% of data breaches happened during business hours, with violators operating right in front of their colleagues while using corporate LANs.

The Verizon 2014 Report identifies the perpetrators of insider misuse but also states that, in addition to insider threats, a company may face dangers from external attacks. Companies should not extend complete trust to partners or former employees. Situations in which a former employee continues to exploit still-active accounts are not as rare as they might seem.

“Besides, monitoring suspicious activities of all former employees might become a best practice. Only if you quickly react to malicious activities and have complete visibility across the entire IT infrastructure, you can be better prepared against possible security breaches.”

The Verizon 2014 Report also identifies the assets usually affected by insider misuse. The survey states that in roughly half of incidents, the valuable information is stolen from databases and file servers - all places where data is stored, uploaded, and shared among employees. Therefore, these repositories should always be under control. Because they store sensitive, business critical data, it is always a good decision to audit SQL servers, file servers, and SharePoint on a regular basis to prevent unauthorized access and modification of content.

Having described who misuses organizations’ intellectual property, how it happens, and which resources are compromised the most, the Verizon 2014 Report raises the issue of security violation discovery and investigation. The report states, “Discovery methods for the majority of breaches have traditionally been dominated by external signals.” Therefore, in most cases, an external contractor is able to notice an information leak.

Breaches are discovered mostly by other employees, and only 9% of IT organizations use IT auditing to detect and investigate security violations. Nevertheless, comprehensive auditing solutions are able to track changes to user content and permissions across the entire IT infrastructure.

It generally takes companies days to weeks to discover security incidnts. However, quite a few breaches revealed themselves only years later. Continuous monitoring of IT systems helps to reduce discovery time from days to hours, thus providing a quick reaction to a security violation and a better chance to find a misuser.

"Simply by deploying a change and configuration auditing solution, IT organizations get complete control of what is going on in their IT systems. Knowing who did what, when, and where allows detecting and investigating security incidents via analysis of unauthorized or malicious changes to system configurations."

When a data leak is detected, identifying the root cause of a security incident may become tricky if the investigation is not performed by a trusted third party. Otherwise, unscrupulous employees may attempt to conceal their wrongdoing by presenting false investigation results.

"Automated audit acts here as an incorruptible judge. Showing changes made to user content and permissions as well as arranging these changes into readable reports with just one click provides unbiased information and reliable investigation results."

While it is almost impossible to watch the activity of every employee, Verizon outlines several recommendations to strengthen security and minimize the risk of insider data leaks. The report states that knowing what data is stored and who has access is a positive practice. This will not prevent a security breach, as access rights have already been granted, but will help ensure that only those who need sensitive information have it.

Another good practice is the regular review of user accounts activity to react to malicious changes made by employees. This practice also works to address security concerns regarding former employees. Disabling their accounts as soon as they leave the company helps prevent data leaks and reduces the risk of a security breach.

Watching for data exfiltration is another practice recommended by Verizon. Common places exposed to security breaches are file servers and SharePoint, which makes them a "pain point" in organizational workflow. Therefore, file servers and SharePoint are good places to enable auditing to track changes to user content and permissions and provide real-time reporting on demand.

The last recommendation made by Verizon is to make all employees aware their activity is being monitored. Regularly publishing anonymized reports of access audits will force end-users to control their actions and become more responsible toward sensitive information with which they are working.

Summing up the results of the Verizon 2014 Data Breach Investigations Report, it is obvious that tracking changes made to security configurations and sensitive data is a key point in preventing insider data leaks. Deploying a change and configuration auditing solution allows to have complete visibility across the entire IT infrastructure by knowing who changed what, when, and where ensures that the security policies established in the organization are working and simplifies root cause analysis in case a security breach occurs.

For a full report, please visit
verizonenterprise.com/DBIR/2014

How to Detect File Changes in a Shared Folder

Native Auditing vs. Netwrix Auditor for Active Directory

Accidental or malicious modifications to files of sensitive information, including simple access and read events, may easily result in serious and obviously unwanted repercussions for the company, including reputation damage, a loss in revenue or legal penalties.

Native Auditing

1. Configure audit settings in your shared folder's properties->advanced security settings-> auditing tab.
2. Configure Domain controllers policy GPO. Enable "Audit object access" policy setting for success and failure.
3. Optionally for Windows Server 2008-2012 configure granular audit policy. Set "Audit File System" and "Audit Handle Manipulation" settings to success and failures.

Netwrix Auditor for File Servers

1. Simply get information about all changes from Scheduled User Accounts Changes Report in your mailbox.

See Real-Life Use Cases:

netwrix.com/go/shared_folder

Top 10 Free Tools for Change Auditing and Password Management

Track changes to Active Directory, Exchange, file servers, manage passwords and troubleshoot account lockouts at absolutely no cost.

The following freeware tools can save you a lot of time and make your network more efficient – at absolutely no cost. Some of these tools have advanced commercial versions with additional features, but none of them will expire and stop working when you urgently need them.

1. Change Notifier for Active Directory
Tracks changes to Active Directory (AD) users, group memberships, OUs, permissions, and provides visibility into what's happening inside your AD.
Free Download

2. Change Notifier for Group Policy
Tracks every change made to your group policy objects (GPOs), including GPO links, audit policy, password policy, and software deployment changes, and fills major gaps found in native auditing tools.
Free Download

3. Account Lockout Examiner
Alerts on account lockouts, helps troubleshoot these events, and analyzes their potential causes. The accounts can be unlocked via Netwrix Account Lockout Examiner console or mobile device.
Free Download

4. Change Notifier for Exchange
Reports on what's happening inside your Exchange servers, and tracks both configuration and permission changes with "before" and "after" values.
Free Download

5. Password Expiration Notifier
Automatically reminds your users to change their passwords before they expire so you can avoid password reset calls. It works nicely for users who don't log on interactively and never receive standard password change reminders at logon time (e.g., VPN users).
Free Download

6. Change Notifier for File Servers
Tracks changes to files and shares permissions, detects deleted and newly-created files, and reports on file-access attempts. This freeware tool strengthens security of your Windowsbased file servers.
Free Download

7. Password Manager
Allows users to reset forgotten passwords and unlock their accounts through a convenient, web-based, self-service portal and integration with the standard Windows logon produre. The tool supports up to 100 users.
Free Download

8. Change Notifier for SQL Server
Detects changes made to your SQL Server configurations, including database creation and deletion, changes to database users, roles, and schemas. It also reports "before" and "after" values for every change, and sends daily reports showing all changes made.
Free Download

9. Change Notifier for VMware
Allows you to control changes in your virtual environments. It notifies you about changes to VMware virtual machine settings, creation and deletion of virtual machines. It also sends daily reports of all changes made in the past 24 hours with "before" and "after" values.
Free Download

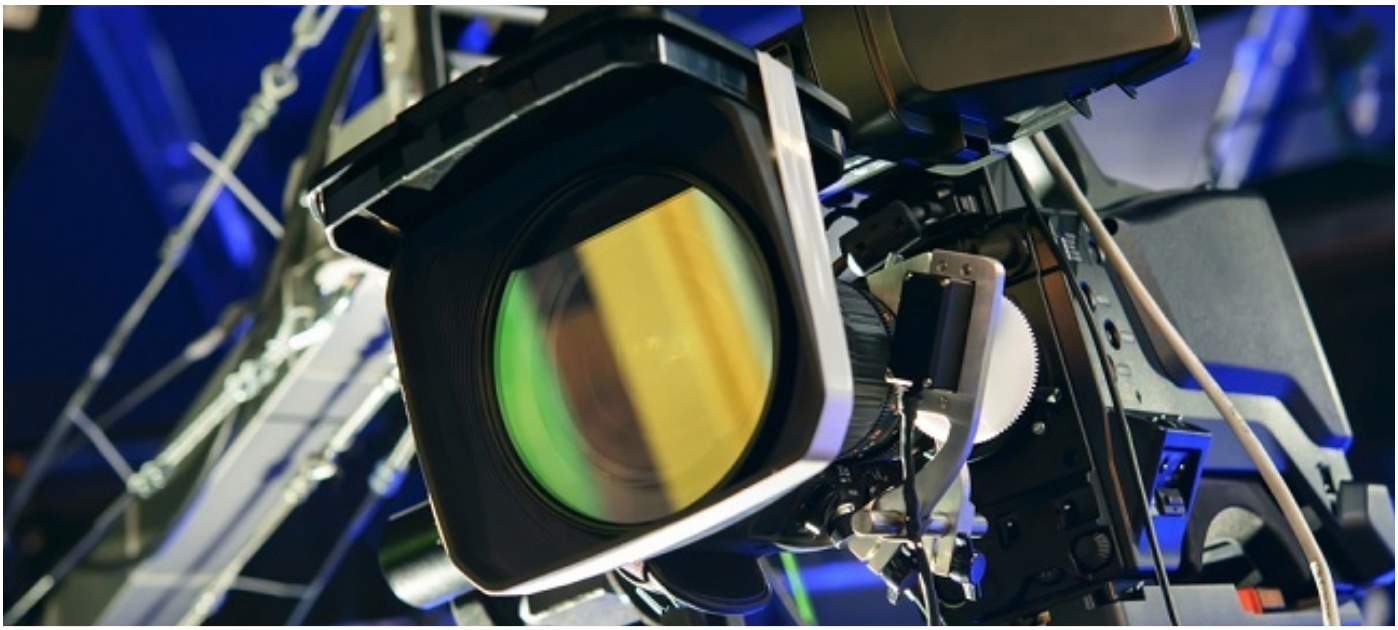
10. Change Notifier for Windows Server
Alerts you about changes made to your Windows Server configurations, including installed software and hardware, services and scheduled tasks. It sends summary reports listing changes of the last 24 hours with "before" and "after" values.
Free Download

JOHN BAGLEY
Award-winning professional writer and independent consultant

Sony Pictures **Hacker Attack**: Lesson Not Learned

by Jeff Melnick
Pre-Sales Engineer at Netwrix Corporation

2014 was one of the hardest years in the history of IT security: we became witnesses to dozens of breaches followed by loss of sensitive data, payments, tears and suffering of numerous users. In December, the Internet exploded with the news of the Sony Pictures hack, which took place in the end of November, but remaining hot due to policital implications. However, let us stay away from politics and try to investigate what happened from the technical side.



No one knows (except for the hackers) how exactly they broke through and when it happened first. Most hacks like this begin with a phishing attack, which involves sending emails to employees to get them to do one of the following: click on malicious attachments, or visit websites where malware gets downloaded to their PC automatically. Or they may have just hacked the company's partners to make their phishing more trustable.

Sony didn't learn the lesson of 2011, when the PlayStation Network was down for a few months. Moreover, they hid the fact that they had been hacked in the beginning of the year, and 47.740 e-mail addresses and birth dates of those who signed up to the Sonypictures.de newsletter have been compromised. Probably, the main attack started from the Sonypictures.de breach, and hackers had access to Sony Pictures network for about a year stealing sensitive information and preparing their destructive strike.

Again, like in 2011 Sony made hackers' work much easier by storing passwords in a folder named "Password." 140 files containing thousands of private passwords, stored in plaintext documents without protection of any kind - is this for real? Having accessed data, hackers wiped out all

infrastructure using *Trojan Destover malware*, which is capable of wiping disk drives and MBR. Wiping systems are an effective way to cover up malicious activity and make incident response more difficult.

So how does the Destover work? The Destover droppers install and run EldoS RawDisk drivers to evade NTFS security permissions and overwrite disk data and the MBR itself. On the first run, it creates the 'Backup and Restore Management' Windows brmgmtsvc service, adds its own executable and sets a startup '-i' switch. It also drops several copies of itself and starts each of them with a different switch: -m, -d, and -w. All of them try to connect to three IP addresses, process execution continues regardless of connection.

-m overwrites MBR, creating 'usbdrv3.sys' and starts usbdrv3 service 'USB 3.0 Host Controller'. Creates filehandle with 64k strings of '0xAAAAAAAA' also connecting to all other drives and overwrites them

-d overwrites data on all logical drives with '0x0df0adba' 20k chunk with the exception of not .exe or .dll ones which are forced for deletion

-w stops the Windows Terminal Services, writes contents with JPG, HTML and WAV info ("Hacked by" page) out to 'c:\windows\iissvr.exe' and starts this process which listens on Port 80 and serves these files, after a two hour sleep, the original service restarts the machine with a call to ExitWindowsEx(EWX_REBOOT|EWX_FORCE, 0) which forces an exit but delays the shutdown while system state file creation occurs

Here are the Command and Control IP addresses utilized by this malware:

203.131.222.102
217.96.33.164
88.53.215.64
200.87.126.116
58.185.154.99
212.31.102.100

Block them on your firewall or IPS.

Sony did not secure their network, but it is hard to find out whether this means that Sony lacks security practices or this attack was inevitable. Securing a corporate network as large as Sony's is really difficult. Joseph Demarest from FBI's Cyber Division said that "the level of sophistication" of Sony Pictures attack was extremely high, the malware would have slipped or probably gotten past 90% of Net defenses that are out there today.

In most cases you can't avoid an attack if the hackers are real professionals, but they can't steal terabytes of information within seconds or even hours. Sony did not detect information leakage; probably they didn't intently check their outbound bandwidth or audit their systems. Now we all see what the cost of such bad IT security behavior is.

So what IT Security specialists can do to lower down the chance of being hacked?

1. First and foremost – **work with your employees**, perform security trainings where you will explain people best security practices like how to manage their passwords. Warn people about phishing, social engineering. Be warned about rogue employees, try to detect or predict them as soon as it is possible.

2. Secondly, **regular backups** allow a company to recover from a destructive hacker attack in a short period of time, decreasing production downtime.

3. Finally, there is a need to **invest more in IT security**. It seems like a needless expense until a disaster strikes. But when it strikes, cleaning up the mess will cost you millions. Implement best security practices, (updates, tools, appliances, procedures etc…) make regular penetration tests, audit your systems, and always be prepared.

Quick Reference Guide

File Server Auditing

How to enable logging of important changes to files on a File Server in security event log

File Shares Audit Settings

- Navigate to the required file share, right-click it and select "Properties"
- Select the "Security" tab > "Advanced" button > "Auditing" tab > Click "Add" button
- Select Principal: "Everyone"; Select "Type: All"; Select "Applies to: This folder, subfolders and files"; Select the following "Advanced Permissions": List folder / read data; Create files / write data; Create folders / append data; Write attributes; Write extended attributes; Delete subfolders and files; Delete; Change permissions; Take ownership
- Click "OK" three times

Event ID Reference (2003/2008 - 12)

- 560/4656 - A handle to an object was requested
- 567/4663 - Object access attempt
- 4670 - Permissions to an object were changed
- 564/4660 - An object was deleted

Audit Object Access Policy

Run **gpedit.msc** > Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy > *Audit object access* > Define > Success and Failures

Granular Audit Policy (Windows Server 2008 - 12)

Run gpedit.msc > Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies > Object Access

- *Audit File System* > Define > Success and Failures
- *Audit Handle Manipulation* > Define > Success and Failures

Security Event Log Settings

- Run **eventvwr.msc** > Windows Logs > Right-click "Security" log > Properties: Set retention method to "Overwrite events as needed" or "Archive the log when full"
- Open *Event viewer* and search Security log for event id's listed in the Event ID Reference box
- To specify the action taken to the file, search for *Accesses* string in each event

For Detailed File Server Auditing, Try Netwrix Auditor - netwrix.com/go/trial-fs

- **Change auditing**: detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™**: scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years and more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

EMC Storage Auditing

How to enable logging of important changes to files on EMC Storage in security log

File Share Audit Log Configuration

- Navigate to the CIFS root shared folder, right-click it and select “Properties”
- Select the “Security” tab > “Advanced” button > “Auditing” tab > Click “Add” button
- Select Principal: “Everyone”; Select “Type: All”; Select “Applies to: This folder, subfolders and files”; Select the following “Advanced Permissions”: List folder / read data; Create files / write data; Create folders / append data; Write attributes; Write extended attributes; Delete subfolders and files; Delete; Change permissions; Take ownership
- Click "OK"

Event ID Reference

- 560 – Object open
- 562 – Handle closed
- 563 – Object open for delete
- 564 – Object deleted
- 567 – Object access attempt

Audit Object Access Policy

Run **GPMC.msc** (*url2open.com/gpmc*) on your domain controller > open “Default Domain Policy” > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy > *Audit Object Access* > Define > Success and Failure

Security Event Log Settings

To be able to increase the security log size, you must move it from the Data Mover root folder. To do this, perform the following procedure:

- Create a new file system where the security log will be stored
- Mount this file system on a mount point, e.g. /events
- Make sure that it is accessible via the “\\<Celerra_name>\C$\events” UNC path
- Run **regedit**, navigate to File > Connect Network Registry… > specify the file server (Celerra) name > Navigate to “*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security*” and change the “*File*” value to “*c:\events\security.evt*”
- You may need to restart the corresponding Data Mover for changes to take effect

After moving the log from the root folder run eventvwr.msc > Action > Connect to another computer > Celerra name > Select Security log > Properties > Define:

- *Maximum event log size to 4000000*
- *Overwrite events as needed*

Search Security log for event id’s listed in the Event ID Reference box.

For Detailed EMC Storage Auditing, Try Netwrix Auditor - netwrix.com/go/trial-fs

- **Change auditing**: detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™**: scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years and more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

NetApp Storage Auditing

How to enable logging of important changes to files on NetApp Storage

Set System Access Control Lists

- Navigate to the CIFS root shared folder, right-click it and select "Properties"
- Select the "Security" tab > "Advanced" button > "Auditing" tab > Click "Add" button
- Select Principal: "Everyone"; Select "Type: All"; Select "Applies to: This folder, subfolders and files"; Select the following "Advanced Permissions": List folder / read data; Create files / write data; Create folders / append data; Write attributes; Write extended attributes; Delete subfolders and files; Delete; Change permissions; Take ownership
- Click "OK"

Event ID Reference

- 560 – Object open
- 562 – Handle closed
- 563 – Object open for delete
- 564 – Object deleted
- 567 – Object access attempt

Full list of events can be found here:

url2open.com/ontapauditing

Configure CIFS Auditing

Connect to NetApp storage using ssh client.
Event auditing is turned off by default. If you want to turn auditing on run "options cifs.audit.enable on". Then enable gathering of:

- File access events, run "options cifs.audit.file_access_events.enable on"
- Logon/logoff events, run "options cifs.audit.logon_events.enable on"
- Local account management events, run "options cifs.audit.account_mgmt_events.enable on"

When enabled audit log file will be created once a day or when it becomes 75% full of 384mb size, this can be adjusted:

- Set size of log in bytes, run "options cifs.audit.logzise 524288-68719476736"
- Set % threshold run "options cifs.audit.autosave.onsize.threshold 75%"

Default audit log file location etc/log on storage, it's possible to change it if you run "options cifs.audit.saveas <fullpath>"

Audit Event Logs

Copy log files from the /etc/log folder and run eventvwr.msc > Action > Open Saved Log

Search Security log for event id's listed in the Event ID Reference box

For Detailed EMC Storage Auditing, Try Netwrix Auditor - netwrix.com/go/trial-fs

- **Change auditing**: detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™**: scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years and more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

Insider Threat Detection with Netwrix Auditor

Detect Suspicious Activity in at Early Stages

Receive Alerts on Critical Changes

See System Configuration at Any Roint of Time

Learn More: netwrix.com/go/insider_threat

Next Steps

Try #1 Change and Configuration Auditing Platform:

Free Trial: setup in your own test environment
netwrix.com/go/completevisibility
Test Drive: virtual POC, try in a Netwrix-hosted test lab
netwrix.com/go/test_drive
Live Demo: product tour with Netwrix expert
netwrix.com/go/live_demo
Contact Sales to obtain more information
netwrix.com/go/contact_sales

netwrix.com | netwrix.com/social

Corporate Headquarters: 8001 Irvine Center Drive, Suite 820 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749
EMEA: +44 (0) 203-318-02

netwrix
#1 for change auditing