International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

UNCOVERING VULNERABILITIES: THE CONSEQUENCES OF SKIPPING FILE TRANSFER AUDITS

Rajendraprasad Chittimalla
Software Engineer
Team Lead, Equifax Inc

Abstract

The secure transfer of files within the organization is a big risk in today's digital world. File transfer is a common practice within organizations. These organizations don't understand the importance of file transfer audits and the consequences of skipping file transfer audits. This research emphasizes the importance and consequences of skipping file transfer audits. The consequences may include data breaches, unauthorized access to the file information, or the stoppage of operational work. These consequences can cause the reputational dump of any organization and financial loss as well. Multiple examples have been discussed in the papers which have caused the organizations to suffer a lot due to the lack of regular file transfer audits.

Keywords: file transfer audits, skipping file transfer audits, consequences of skipping file transfer audits

I. INTRODUCTION

In this Digital world, data is the backbone of any organization. The security of the data and sensitive information is uppermost. Any industrial organization relies on the seamless exchange of datato transfer financial[1] or intellectual properties to its clients. File transfer audits are used to ensure the safety of information. Most organizations skip these audits due to the lack of awareness which results in exposing systems and compromising the data confidentiality and security.

Let's start with the concept and purpose of File transfer Audits. File auditing monitors all the changes in the data, the attempts, and the addition to the data. It keeps a record of all the file transfer activity.

The purpose of this research paper is to focus on the security risks associated with skipping file transfer audits.

This research is going to make a huge impact on organizations skipping file transfer audits. The consequences of skipping file transfer audits could be data breaches, malware infiltration, and work inefficiencies. Organizations need to tighten up and move towards the habit of arranging regular file transfer audits. Also, the findings of this research remove all the misconceptions about the complexity of these file transfer audits.

II. LITERATURE REVIEW

File Transfer Audits are important for any organization to keep its data safe and secure. It doesn't matter if the organization is related to a health, financial, or insurance company. The cybercriminal can access and intercept the information. If the file is not handled properly once it's received, a data breach is possible. Your sensitive information could be in other's hands or could be in your competitor's access.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

File Transfer Protocol (FTP)[2] is used for the standard communication and transfer of files from the server to the client computer. Most organizations maintain the screen capture data to maintain the audit of all the FTP transactions. One of the best FTP tools to keep a record of the file transfer is Go Anywhere MFT. Using this tool, you can keep a record of all the file transfers and follow the audit trails. Moreover, by using such computer tools, you can easily access the older data within seconds which is not so easy when it comes to saving file transfer data in hard form.
There are also automated auditing tools available that enhance the accuracy of file transfer audits and remove the possibility of human error.

III. PROBLEM STATEMENT

Every organization understands the importance of file transfer audits but still, they neglect it. These organizations understand that the file transfer must be very safe and secure. It must not be breached to attack their reputation. The file transfer must be confidential and reach into the client's hands safely. But, still, these businesses neglect the conductivity of regular file transfer audits. This neglecting behavior by businesses leads to different vulnerabilities such as data breaches, anonymous access, and inefficient operational performances.
Moreover, this lack of file transfer audits not only just damages the reputation of the organization but also leaks sensitive information which has a direct impact on the legal and financial risks [3]. While there is a huge importance of File transfer audits, there is a huge gap in the reasons and consequences of skipping file transfer audits. So, this research emphasizes the vulnerabilities that arise while continuously skipping file transfer audits. The research paper examines and analyzes real-world case studies to come up with the best and most valuable results.

IV. UNCOVERING VULNERABILITIES

4.1.1. Denial of Service (DoS)

The biggest problem that a system might face is a Denial of Service attack as it restricts the user from doing any action and getting the appropriate result as feedback. It makes the system unusable for the user and causes total operational disruption.

4.1.2. Log4

It allows remote code execution and is the latest discovered vulnerability. It puts the sensitive information of the user or the organizational data itself at risk.

4.1.3. Java Remote Code Execution (RCE)

The arbitrary code can be executed on the respective server and with the execution of that chunk of code; an attacker can do unlimited violations including the complete takeover of the system.

4.1.4. Exploited Vulnerabilities

The other vulnerabilities can include the exploitation of unpatched systems. This can, in turn, result in data breaches and the loss of the user's data or the sensitive information that the organization is responsible for protecting.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

V. IMPORTANCE OF PATCHING & AUDITS

The vulnerabilities can only be neglected by adopting a patch option for applications. It's crucial to identify and react to the weak points of the system. The patching helps to avoid the full system failure and the audits support the system more by considering the latest changes in the patches. Here are the advantages these concepts provide to the organizations:

- Data Breaches: The sensitive information of the user or the organization comes at risk when the system is missing patching and audits.
- Operational Problems: The servers can be disrupted when the system is fully connected without any security patches and necessary gaps. The missing audits can leave the team clueless right till the end.
- Financial Loss: The revenue can be affected as it is directly linked to the user experience. Moreover, legal fines can put a heavy burden on the organizational budget.
- Brand Reputation Problems: The brand image can be destroyed if the user privacy policies are violated.

VI. REASONS FOR SKIPPING FILE TRANSFER AUDITS

Now, that we understand the importance of file transfer audits, we are going to look at the reasons for skipping file transfer audits.

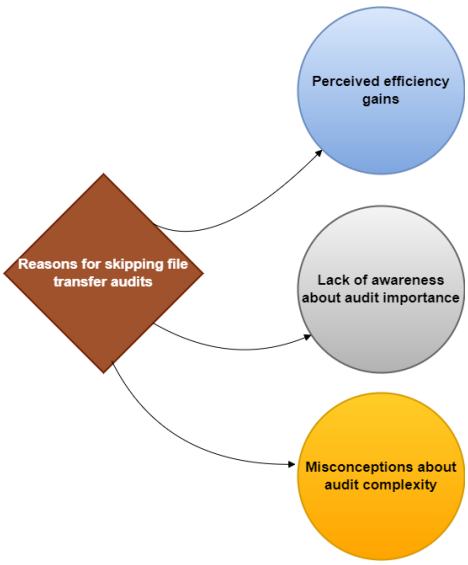

Figure 1: Reasons for skipping file transfer audits

Even though, companies understand the importance of file transfer audits, then why are they unable to do it on time? What are the reasons behind skipping file transfer audits?

Perceived efficiency gains:

Most of the organizations skip file transfer audits to save cost and time. They rather keep working on their operations instead of improving the efficiency of the work. The organizations are on tight deadlines, therefore, they skip the file transfer audits to save from the cost and increase in operational burden. What these organizations don't understand is that this small investment in file transfer audits is saving them from greater costs and operational delays.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

Lack of awareness about audit importance:
One of the other reasons for skipping file transfer audits is the lack of awareness about its importance. Most of organizations are unaware of its importance and maintaining their data security on the traditional ways. It is important to create awareness in such organizations about file transfer audits and how the organization can protect itself from data breaches, and protecting confidential information.
Organizations need to arrange seminars and training sessions to create awareness about how file transfer audits work and what is important in securing organizational assets.

Misconceptions about audit complexity:
Most of the organizations skip file transfer audits by understanding that the process is complicated and technical. They skip the audits by considering that it require specific knowledge, cost, and enough time. Such misconceptions are most common in small organizations where it's limited IT resources.
But nowadays, there are many auditing tools which make it possible to automate the audit process [4] which results in less cost and time consumption.
Moreover, there are third-party audit companies that perform the audits within a very limited time, saving the organizational time consumption on audits.

VII. LIMITATIONS

7.1 Variable Audit Practices

The organizations can have distinctive practices to handle the audits. Therefore, the effectiveness is dependent on the methods adopted by the respective members. The difference can be in methods of audit, its frequency, and scope make it challenging.

7.2 Difference in Organizational Response

The response to data breaches and emergencies can differ between organizations. Also, contributing factors like organizational size, type of industry, and existing security measures can play their role in the management.

7.3 Consequences are Unimaginative

It's difficult to exactly point out the consequences of skipping the file transfer audits due to the distinct nature of the data. Also, other factors might be effective such as inadequate encryption, human error, and broader security.

7.4 Lack of Standards

There are no standard metrics to measure the impact of file transfer audits and how skipping it can cause serious problems for the organization. There is no universal measurement set for the ability to assess and compare the consistency across different organizations.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

VIII. CONSEQUENCES OF SKIPPING FILE TRANSFER AUDITS

Although there is a huge importance of file transfer audits, organizations are adopting the habit of file transfer audits. But, there is a missing part about the consequences of skipping file transfer audits. So, this research paper fills the gap by covering all the consequences of skipping file transfer audits.

Increased vulnerability to unauthorized access:

Studies reveal that organizations skipping file transfer audits faced unauthorized access attacks to their sensitive information. One of the most popular financial institutions faced the data breach attack, which resulted in the information leak of millions of their customers. This all was due to the lack of file transfer audits.

Higher risk of data breaches:

One of the consequences of skipping file transfer audits is the risk of data breaches. The file transfer data usually consists of financial information, customers' personal information, or even companies' sensitive information. Without regular file transfer audits, outdated security protocols or unauthorized access could be ignored which results in cyber-attacks.

Data breaches resultin reputational damage that allows your competitors to have an upper hand over you. Moreover, there is a good chance that the sensitive information lands in the hands of your competitors which is not good for your business.

Potential for malware infiltration:

Another consequence of skipping file transfer audits is malware infiltration. Any malware software could be introduced to the system during file transfer by an external or internal source. Therefore, it is crucial to scan the files before file transfer to stay safe from malware attacks. If this malware gets to the system successfully, it could corrupt the data or lead to a system shutdown [5].

Examples of real-world consequences:

One of the examples of real-world consequences of skipping file transfer audits is the data breach of a financial organization. This high-profile incident occurred due to the lack of file transfer audits. The financial organization lost the data of millions of its users, which not only resulted in reputational damage but also broke customer's trust and led to legal penalties.

Another example is the manufacturing organization. The company suffered from operational delay and damage because of skipping the file transfer audits. The files were corrupted, which resulted in a delay of production and caused financial losses.

These examples highlight the importance of file transfer audits to prevent data leaks and protect organizational reputation.

IX. UNCOVERING VULNERABILITIES IN FILE TRANSFERS

File Transfer is a common practice in all industrial organizations. It is very important to conduct File transfer audits to protect industrial sensitive information. Following are the practices used by the organizations to transfer data, and the vulnerabilities caused by file transfers without regular file transfer audits:

Remote Code Execution (RCE):

One of the vulnerabilities of skipping file transfer audits is that the attacker executes the data on the client-server which results in data manipulation or data theft. Therefore, if the files transferred

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

during the application process are not completely validated, it results in different attacks that allow attackers to steal information or leave malware in the system.
Same is the case with Log4j java library which allow attackers to take full control of the system and manipulate information.
Example:

```
importos
importhashlib
defvalidate_file(file_path, expected_hash):
    "Validate the integrity of the transferred file using its hash."
    withopen(file_path, 'rb') asfile:
        file_hash = hashlib.sha256(file.read()).hexdigest()
    returnfile_hash == expected_hash

deftransfer_file(source_path, destination_path, expected_hash):
    "Transfer a file with validation to prevent RCE vulnerabilities."
    ifnotvalidate_file(source_path, expected_hash):
        raiseValueError("File validation failed. Transfer aborted.")

    withopen(source_path, 'rb') assrc_file:
        withopen(destination_path, 'wb') asdest_file:
            dest_file.write(src_file.read())

    ifvalidate_file(destination_path, expected_hash):
        print("File transferred and validated successfully.")
    else:
        raiseValueError("File validation failed after transfer.")

# Exampleusage
source = 'data/source_file.txt'
destination = 'data/destination_file.txt'
expected_hash = 'expected_sha256_hash_of_the_file'

try:
    transfer_file(source, destination, expected_hash)
exceptValueErrorase:
    print(e)
```

Snapshot 1: Data Transfer without Vulnerability

In this above example, 'validate file' compares the hash with the expected hash before and after file transfer, which ensures that the data is safely transferred without any RCE vulnerability in the middle.

Denial of Service (DOS):
DOS attacks are another example of vulnerabilities in file transfers. It makes operations stop and disturbs customers' trust. These DOS attacks cause downtime in applications and sometimes lead to application crashes.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

Dependency Management Flaws:
Software dependencies are managed by tools such as DNF. It is important to configure dependencies properly; otherwise, it causes the system to lead to insecure software installation. Such mismanaged dependencies cause security issues; therefore, regular file transfer audits are required to manage things properly.
Example:

```
set-e

# Updaterepositorymetadata
sudodnfmakecache

# Installspecificversionsofcriticaldependencies
sudodnfinstall-ypackage1-a.b.cpackage2-x.y.z

# Verifytheinstalledversions
dnflistinstalled|grep-E'package1|package2'

# Checkforsecurityupdates
sudodnfupdateinfolistsecurity

# Applysecurityupdates
sudodnfupdate--security-y

# Exampleofdependencyvalidation
if!rpm-qpackage1|grep-q'a.b.c'; then
    echo"Package1 mismatch. Expected a.b.c"
    exit1
fi
if!rpm-qpackage2|grep-q'x.y.z'; then
    echo"Package2 mismatch. Expected x.y.z"
    exit1
fi
echo"Dependencies are installed and validated successfully."
```

Snapshot 2: Validation of Dependencies

In this example, the specific script validates that the dependencies are installed correctly. By regular file transfer audits, organizations can prevent the risk of RCE, DOS, or dependency management attacks.

X. RESEARCH IMPACT

The impact of this research focused on the consequences of skipping file transfer audits. This research contributes to the field of academic knowledge by exploring multiple aspects of cyber security such as file transfer audits. While there's a huge amount of data available on data security, there was a lack of information on the consequences of skipping file transfer audits. Therefore, this research paper adds depth of knowledge and provides valuable resources for future studies.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

Figure 2: Consequences of reading file transfer audits

Moreover, organizations can now add a policy of having regular file transfer audits into their regulations for data security. It also enhances the cybersecurity culture within the organization. Based on all the evidence and recommendations, the cyber team can now focus more on the security protocols and cover all the gaps for information safety.

XI. FUTURE DEVELOPMENTS

Thefuture of file transfer audits is advancing with the technological revolution. Many automated file transfer audits are now on the market. The utilization of Artificial intelligence in File transfer audits has made things smooth and easier for the audit teams. It has become easier to identify the irregularities which was not very efficient with manual methods. Moreover, AI has made it possible for the systems to learn from their previous data which has directly reduced the burden on the shoulders of IT teams and provided more accuracy.Blockchain technology[6] is revolutionizing which has a secure file transfer future. This technology can ensure the authenticity of the transferred files.

XII. CONCLUSION

The given writing can be concluded in the following:

- There is so much information on the internet about the importance of file transfer audits. Still, many organizations don't adopt the habit of regular file transfer audits.
- The lack of audits reflects the bigger consequences that organizations are not aware of. The consequences of skipping file transfer audits are far more dangerous. A small leak of information could bring the whole business to its knees.
- This research focuses on the consequences of skipping file transfer audits to understand this more in-depth.

International Journal of Core Engineering & Management
Volume-6, Issue-08, 2020 ISSN No: 2348-9510

- There could be a cyberattack on the system, where attacks can steal the private information of the company. Sometimes, the attackers crash the system, causing the company to stop its operations and cause downtime.
- Multiple examples have been discussed above related to such incidents where the organization not only lost its reputation but also faced legal penalties for its data leak.
- By identifying and eliminating malware and cyber-attacks, the organization can maintain operations and work smoothly.
- By regular file transfer audits, the organization can safeguard its valuable information and confidently protect its assets.
- Therefore, it is important to conduct regular file transfer audits to avoid such incidents. These audits[7] will identify the malware and unauthorized attempts to access the data.

REFERENCES

1. C. Brandon Brown CPA, "Audit and Control of Electronic Funds Transfer," EDPACS, vol. 23, no. 10, pp. 1-6 , 1996.
2. P. Zabihollah Rezaee, A. Sharbatoghlie, P. Rick Elam and P. Peter L. McMickle, "Continuous Auditing: Building Automated Auditing Capability," A Journal of Practice & Theory , vol. 21 , no. 1, p. 147–163, 2002.
3. D. J. B. Ferrey, "Auditing the Operating System," EDPACS, vol. 10, no. 10, pp. 1-8, 1983.
4. M. C. A. V. Rafael Belchior, "TOWARDS SECURE, DECENTRALIZED, AND AUTOMATIC AUDITS WITH BLOCKCHAIN," AIS Electronic Library, 2020.
5. N. C. H. James V. Hansen, "Control and Audit of Electronic Data Interchange," Management Information Systems Research Center, University of Minnesota, vol. 13, pp. 403-413 , 1989.
6. M. N. Hossain, S. B. University, S. M. Milajerdi, J. Wang, R. Sekar, S. Stoller and V. Venkatakrishnan, "SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data," in Open access to the Proceedings of the 26th USENIX Security Symposium , Aug 2017.
7. B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security & Privacy, vol. 9, no. 2, pp. 50-57, Jun 2010.
8. Jaquith, The Definitive Guide to Quantifying, Classifying, and Measuring Enterprise IT Security Operations, Pearson Education, Mar 2007.
9. F. Yamaguchi, F. ’. Lindner and K. Rieck, "Vulnerability Extrapolation: Assisted Discovery of Vulnerabilities using Machine Learning," Technische Universitat Berlin, Germany and Recurity Labs GmbH, Germany.
10. M. Z. S. &. B. Z. Chernyshev and , "Healthcare Data Breaches: Implications for Digital Forensic Readiness," Jounal of Medical Systems, vol. 43, Nov 2018.
11. F. Yamaguchi, A. Maier, H. Gascon and K. Rieck, "Automatic Inference of Search Patterns for Taint-Style Vulnerabilities," in 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, May 2015.
12. V. B. Livshits and M. S. Lam, "Finding Security Vulnerabilities in Java Applications," 14th USENIX Security Symposium.
13. F. Yamaguchi, C. Wressnegger, H. Gascon and K. Rieck, "Chucky: exposing missing checks in source code for vulnerability discovery," in CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Nov 2013.
14. M. Dowd, J. McDonald and J. Schuh, The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Pearson Education, Nov 2006.

15. H. Perl, S. Dechand, M. Smith, D. Arp, F. Yamaguchi, K. Rieck, S. Fahl and Y. Acar, "VCCFinder: Finding Potential Vulnerabilities in Open-Source Projects to Assist Code Audits," in CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Oct 2015.