ICT for Cyber Security in Business

R Hristev\textsuperscript{1} and M Veselinova\textsuperscript{1}

\textsuperscript{1}University of Plovdiv Paisii Hilendarski, Plovdiv 4002, Bulgaria

E-mail: veselinova@uni-plovdiv.bg

Abstract. In recent years, the financial value of the stored information repeatedly exceeds the one of the equipment which is needed for its storage. Therefore, the process of business development needs the implementation of up-to-date ICT for data security from cyber-attacks. The scalability of IT infrastructures in this direction leads to development of malware creators. Thus, file servers become inefficient and give away to private clouds. Attacks against data stored on file servers and workstations are becoming more widespread. Standard security methods (for example, backup) are not always secure enough and can also be the target of a cyber-attack if not properly managed. In addition, information from the time of the last backup to the time of attack will be lost. The paper aims to research and propose approaches which can be used for recovery of the information arrays. We consider some software for implementation of private cloud which correspond to the ISO 27001 standard. The methods for accessing data will be analyzed and the techniques by which clouds deal with some of cyber-attacks will be addressed.

1. Introduction

The article is dictated by the need to increase the security of data storage in the IT infrastructure of a company. The process of business development leads to the need of implementation of various information technologies to facilitate the work. One of the mainly used servers today are file servers. They are used by both small companies and large corporations.

One of the main applications of file servers is to store digitized company data. Another application of file servers is the need for an easy way to share information between company employees. Normally, the data stored in a company’s infrastructure exceeds the amount of hardware required for storage.

2. Is the data stored on file servers vulnerable?

As IT infrastructures grow, so does the amount of data stored, leading to an increase in the number of malware developers. In recent years, attacks targeting data stored on file servers and workstations have become more widespread. One of the most massive malware attacks ever occurred was WannaCry in May 2017. WannaCry attacked many hospitals, companies, universities, and government organizations in at least 150 countries, having more than 2,00,000 victims \[1\]. At the heart of this attack is an algorithm that encrypts the data on the workstation or file server, and a ransom is required to recover the information \[2\].

Ransomware is a type of malware that tries to block a user's access to a workstation or data. The purpose of ransomware is to block the victim from accessing their own resources by locking the OS or
encrypting certain files that appear valuable to the victim, such as photos, spreadsheets, or presentations [3]. A ransom is required to restore this access. The ransom in most cases must be paid in cryptocurrency, mainly bitcoins, thus making the payment virtually untraceable and the extortionists go unpunished. The value of the requested ransom and the reason for the payment depends on the type of virus. Ransomware detection techniques are observed in [4].

Antivirus software companies are investing more and more resources and efforts to develop software that helps to decrypt information, but it takes time. In order to decrypt the data are sought bugs in the virus's algorithm through which recovery tools can be developed. This is a long process in which users cannot use their information. There are dozens of ransomware for which no recovery tools have been developed.

Encrypting ransomware or so-called cryptoviruses are the most dangerous in terms of data. There are already dozens of such viruses with different names and various algorithms. The ransom is also different and depends from the virus that has entered the system, basically ranging between $300 and $2,000 to decrypt the information. The spread of cryptoviruses is achieved mainly with the help of Trojan horses and mass electronic messages.

In the general case, the encryption of the information is gradual and it is difficult for an ordinary user to immediately understand that his system is infected. More intelligent cryptoviruses encode a percentage of the files, only then inform the user that they need to pay a "ransom" to recover the information, while the other files are encrypted.

Cryptoviruses attack certain types of files. It depends from the type and version of the virus. More intelligent algorithms, in addition to local files, encrypt the files available on the attached network drives, and also scan the local network for unprotected resources - shared folders and drives with read and write permissions, which makes file servers vulnerable.

In addition to infecting different resources, cryptoviruses encrypt data in different ways - there are cryptoviruses that encrypt entire files and those that encrypt only the metadata of the files. If only the metadata of the file is encrypted, the process of decrypting and recovering the information is much easier.

Bit-by-bit hard disk scanning software does not work with cryptoviruses because, in addition to changing the file name and extension, they delete the original file as well as the shadow copies of the file available for the system. This type of software, even if it detects and "recovers" the files are generally broken.

One of the standard methods for recovering data after this type of attack is backup, which is also not effective because the backup can also be encrypted by the ransomware. Recovery from backups is secure in cases where backups are stored in places that are not permanently connected to the local network or machine. This on the other hand means that it is impossible to implement automatic backups, just as in the event of this type of malware there will be data loss from the last backup to the time of infection.

3. Clouds and Shared Network Resources

Clouds have many advantages over shared network resources and file servers. We distinguish three main types of clouds: public, private, and hybrid.

Public clouds are a type of SaaS services. The most common of these are Google Drive, Microsoft One Drive, pCloud, DropBox, Amazon Cloud, Apple iCloud, and others. These types of clouds are good for storing and sharing insensitive data, but they are not a recommended option for storing and sharing sensitive and confidential information due to the lack of control over the servers on which the data is stored.

A hybrid cloud is an infrastructure that is a composition of two or more different cloud infrastructures (private, public, government) that have unique objects but are interconnected by standard or proprietary technologies that allow data or applications to be transferred between components.
In the private cloud, services and infrastructure resources are connected to a local area network. Users see the resources provided as SaaS services, but in fact an organization is needed to take care of the infrastructure. To protect them, they are shared on a local computer network. This means that in order for the files to be accessible, either the computer must be on that network or a VPN (Virtual Private Network) must be used. Also, the device's access to the shared resource must be set in advance.

On the other hand, information uploaded to the cloud can be accessed from both a computer and a mobile device, as long as it is connected to the Internet. The data can be accessed via a web browser, a file browser (via WebDAV), or synchronized with a local system disk using clients.

There are many advantages of private clouds, but some of the main ones are:

- Scalability;
- Protection;
- A high level of safety, as the system is released only for the needs of the organization and no one else has access to it;
- Easier management of the structure by users;
- Easy control of users' access to certain resources;
- If configured correctly, the private cloud complies with ISO 27001 - Information Security Systems.

The private clouds we will consider are ownCloud and NextCloud. In [5] there is short practical guide for setting up ownCloud and includes many advanced topics. There is discussion in [6] and [7] about NextCloud and how it can be used as a gateway storage and improvement of the software with new functionality.

Private clouds can be easily scaled according to the organization in which they are located, as organizations with up to 150 users can be taken over by a single server configuration, which has a web server, database, storage, etc., and the scheme will look like as shown in figure 1.

![Figure 1. Example for Single Server Configuration (Up to 150 Users)](image)

This scheme can be easily scaled. Figure 2 shows an example distribution of machines if the cloud is made up of two balancers, 4 web servers, 4 databases, etc. Such configurations are required for corporations with more than 5,000 users, and physical servers may not be located in the same location for disaster protection or proper resource allocation, such as users in the relevant office accessing the server in their local network, and the server on the other hand synchronize with the others.

Backup options for file servers usually involve creating backups, which in some cases is not a flexible enough way to protect. In case of infection with cryptovirus, this would lead to loss of data for the period from the last backup to the moment of infection. In such cases, private clouds undoubtedly provide great benefits such as versioning control and deletion confirmation.

The organization of files in private clouds is different compared to standard file servers. It is recommended to create one master user where the data will be stored and share it with other users when needed. When a user uploads a file to the private cloud of the concerned species, it becomes the property and is stored in the directory of the user who originally shared the common resources. For convenience, in addition to users, private clouds can also be organized with groups, thus sharing control can be much easier to be controlled by an administrator. The organization and schemes that can be created are different and depend on the specific infrastructure.

The example of distribution of machines in private cloud is shown in Figure 2.
Another big advantage of private clouds is that, unlike file servers, they can be easily set up and configured to comply with ISO 27001 - Information Security Determination Systems. To meet the standard, the data must be stored in encrypted form on the server, and the server must also be accessible via an encrypted connection. However, to meet the standard, more resources must be allocated in terms of the fact that encrypted files take up to 35% more disk space than unencrypted files.

Another advantage of private clouds is that they can be accessed by any device with an Internet connection. In order for the files to be accessible, we only need to have an Internet browser, after which we can access the cloud. In cases where we use a file server, providing access is a bit more complicated, because in order to protect the information, the server is usually "visible" only from the local network in which it is located, and to access the stored information from a public network, VPNs are used. It is also possible to implement private clouds only in a local network if the stored data is too sensitive. In the other case, the cloud is "released" outside and can be accessed from anywhere. Also, private clouds, like public ones, can be accessed via synchronization software, and can also be mounted as disks via WebDAV.

4. Opportunities to Access Information Stored on Private Clouds

OwnCloud and NextCloud have developed desktop clients for Windows, Linux, and MacOS operating systems. File synchronization with the help of clients has its advantages and disadvantages. If the cloud is used by one user or is not implemented to share the same files and simultaneous work of multiple users on identical information arrays, then the desktop client finds an application.

The disadvantage of desktop clients is that they keep local copies on the machines on which they are installed and configured. Local copies are stored on the workstation in unencrypted form. The need to preserve local copies on the machine leads to the need for more disk space on it.

However, desktop clients are also used in situations where the same large files are shared between different users. Examples of departments in which the use of desktop clients could be useful are a prepress department, X-ray cabinets, and others.

If we consider the example with a pre-printed department that does not work with local copies or does not copy the necessary files to work on the local computer, then with an average file size of 200 MB, 200 MB of traffic is generated for each individual open file. When saving the file, it must be transferred to the server and then considered for saved, which in a prepress department consisting of even just 4 people is enough to load the network at times and slow down the work of other users. When using a desktop client, the user will generate 200 MB of traffic to the server once to save a local
copy of the server, and then it will be read by the local file system. When saving, we will not reduce the traffic to the server, but the synchronization of the file versions on the local computer and the server will become "invisible" to users and this will not hinder the work of other people on the server. Also, saving the file to a local disk will be faster than saving it over a network. Then the synchronization will take as much time as if we work through a mounted disk.

In the situation with X-ray cabinets, reading an X-ray/scanner from the local file system will be faster than reading from the server. Then there is no traffic for records.

Desktop clients are free and available on the official pages of the private cloud, which has been chosen to be integrated into the system. Once downloaded, it must be installed. The client is automatically added to the operating system startup. More than one user can be added to one client. They access the server via HTTP or HTTPS, depending on the server configuration. The client can be configured to synchronize all local file system folders available to the user, or only certain folders that are "visible" to the specific user.

WebDAV (Web Distributed Authoring and Versioning) as an extension was announced in 1996 by Jim Lighthead as an upgrade to the HTTP protocol. In fact, WebDAV is a new protocol that is based on HTTP but allows users to manipulate information arrays directly on the server. The protocol is used by ownCloud and NextCloud and can be used to mount disks in the operating system so that users can see and work with them, as with file servers. Because the other convenient access to work from a fixed workstation is to mount the disk via WebDAV, which is a relatively new protocol, some of the older software is not compatible with it and has problems saving files this way.

5. Information Recovery Methods
The main difference between file servers and private clouds is that file servers do not have data array protections, while private clouds have versioning control and double deletion, which in this case can protect us from cryptoviruses. In file servers, protection against such ransomware attacks is related to data backups. In the event of a cryptovirus attack, this would result in data loss from the last backup.

Version control can help us in few cases of ransomware infection. Some cryptoviruses do not delete the files, but encrypt only part of the file's metadata, not deleting the original copy but overwriting it without changing its name and/or extension. In such situations, unencrypted files can be recovered using the version control that is embedded in the described private clouds. This type of cryptovirus is not so scary because it makes it easier to decrypt and recover information, even if we do not have versioning control.

Double deletion can protect us from cryptoviruses that encrypt entire files and delete unencrypted data. In the double-delete approach, after the file is deleted, it automatically goes to Recycle Bin that is individual to each user. Deleted files will go to the Deleted files of the user who deleted the files, not to the Deleted files of the user who owns the files.

To recover the files, the computer network must first be cleaned from the ransomware, after which the deleted files can be recovered by the user who became infected from a section in the "Deleted files" in the web interface. The main problem here is that in order to be able to recover files after cryptovirus infection, we need to have a large disk space set aside. More specifically, if in our organization we have 1 TB of data that we store and we have activated the module for storing information on the server in encrypted form, which can increase its size by up to 35%, then the server will store 1.35 TB. When the system is infected by this type of virus, it will encrypt the current files, which can further increase their size, and the size of the encrypted files depends on the used encryption algorithm. In the general case, the size does not increase by more than 50%, i.e. encrypted files from the cryptovirus will not exceed 2.02 TB. Once the files are encrypted, the original, unencrypted files for the user will be moved to "Deleted files", i.e. the space that the infected and uninfected files will occupy is a total of 3.38 TB. This means that we need to have approximately 2 TB of free cloud space to be able to ensure seamless recovery of information. If we do not have such space after the server disk is full, the procedure is performed by the queue method and files from
"Deleted files" are deleted, following the rule the first one entered in the Deleted File will be deleted first.

In such situations and reducing this large space that needs to be kept free, the considered private clouds have developed a "Ransomware protection" add-on that can be useful. Once activated, the add-on makes a blacklist with extensions and prevents attachments from files with such extensions. If a user tries to upload a file with an extension that is defined in the module, the server will not allow it, thus avoiding the need for additional space. Extensions of the more well-known cryptoviruses have been introduced in the module, but this will not protect the system from everyone. It is recommended that the module is always kept up to date. If we do not set aside space and the system is infected with a cryptovirus, the extensions of which are not described, then the damage will be big and eventual data loss is also possible.

The Ransomware protection module will help us to the point that we can minimize the upload of infected files to the server. This will not stop the attacking virus from deleting the original copies, and they must be restored by Deleted Files.

6. Integration of Private Clouds in an Existing IT Infrastructure

Moving from a file server or shared directories between users to a private cloud can be a heavy task. If this is taken into account, ownCloud and NextCloud are almost identical and have minimal differences, which is normal because they are designed by the same team. The choice between NextCloud and ownCloud is difficult. Once the cloud to be integrated has been selected, it must be picked a server on which it will be installed and configured. When calculating the required components, attention should be paid to:

- Number of users who will use the private cloud.
- number and size of files that will be stored on the private cloud;
- the number and size of files that are expected to be added for private cloud storage for one year.

When the computing power required to deploy a private cloud in an organization's existing IT infrastructure is considered, it must be installed on the hardware or virtual machine. The next step is to transfer the existing data to the selected private cloud. It is recommended to create primary users for the system on which the files are initially stored and from which users are shared with others so that when working with people in the private cloud, file ownership is always with the primary users. This will allow the user to be easily deleted from the system when leaving a company employee, without deleting his files (except those in "Deleted Files"), without the need to transfer ownership of files, which can be done by the console. There are two ways to move data from the file server or shared directories to the private cloud in the easiest way. The first is by mounting the main user via WebDAV to a server and manually copying the data. The second method involves the use of a synchronization client. When configuring a synchronization client with a new user, a local directory is set in which the files will be stored. This way, this directory can be a disk, a file server folder, or a shared directory. The important thing here is to choose the option that indicates where to save the local files. This will cause the synchronization client to automatically upload them to the private cloud, and if the option is not selected, files located in the specified directory will be deleted.

Once the files are already available on the private cloud, it should move on to adding new users and sharing the files with them. Here the hierarchy of users should be considered, who should have access to what data. For proper configuration and flexibility of the hierarchy, the realization of groups and the organization of users in groups can help a lot. Note that a user can be a member of more than one group.

One of the main questions that needs to be answered is, "How do users work with their files?" The answer will extract important information on how to configure user access to the cloud. The two described private clouds have identical options for accessing data - through a browser, synchronization client and WebDAV. Some organizations may need a combination of different methods to access the data. There is no one-size-fits-all rule to configure user access to files.
Thus, we can conclude that the supporting points for the implementation of a private cloud in an existing IT infrastructure are:

- choice of type of private cloud;
- calculation of the required computer power (processors, memories, disks, network provision);
- installation and configuration of the selected private cloud.
- transfer of existing data to the private cloud.
- adding users and creating a hierarchy.
- sharing the information with the new users.
- configuring workstation access to the private cloud.

7. Private Cloud or File Server

The private clouds discussed in this article have much greater capabilities than the file server. A file server is a centralized storage space that is accessible to all authenticated users as in table 1. Initially, the file server is used to store data without any security mechanisms implemented to protect data integrity. The system administrator must take care of the protection of the system himself and develop scenarios and mechanisms for quick and easy recovery of information after external interventions.

Clouds deal with many of these problems, and in addition to storing information, they have a user authentication system that can be used to determine if a user can only read the file, edit it, and share it with other users, which in the case of file servers can only be done by a system administrator. The data can be stored in encrypted form on the server, as well as be accessed through encrypted communications, so as to meet ISO 27001 - Systems for determining the security of information. In addition, by default they have versioning control, which can not only protect the data from some types of ransomware, but also from a malicious user who deletes the data itself in a file. Also another feature that significantly improves security is the double deletion, in which for the irretrievable deletion of data from the server, for a well-calculated infrastructure. Once deleted, the files are actually moved to the Deleted Files.

The main disadvantage of private clouds in compared to file servers is that for the storage of the same data and the work of the same number of users with the system require more computing resources. Integrating the private cloud can be a difficult task for which we need more qualified staff.

|                              | NextCloud | OwnCloud | File Server |
|------------------------------|-----------|----------|-------------|
| File Storage                 | Yes       | Yes      | Yes         |
| Access rights                | Yes       | Yes      | Yes         |
| Controlling the type of access of individual users to the data | Yes | Yes | No |
| Encrypted data storage       | Yes       | Yes      | No          |
| Versioning Control           | Yes       | Yes      | No          |
| Double Deletion              | Yes       | Yes      | No          |
| Computing power              | Bigger    | Bigger   | Less        |
| High qualified administrator | Yes       | Yes      | No          |

8. Conclusion

Ransomware has become one of the most urgent issues in the digital world. It is clearly, that protecting against ransomware is a difficult task. The private clouds considered in this article are open source solutions through which we can better protect our data by storing it according to ISO 27001 -
Information Security Determination Systems. The article describes approaches by which user data can be recovered after being encrypted by a ransomware attack. The main advantages of using the considered solutions in comparison with the standard file servers are also described. An approach for integrating a private cloud into an existing IT infrastructure is presented. A comparison of the positive and negative sides of the private clouds and file servers discussed in the article is made.

9. References

[1] Savita Mohurle, Manisha Patil, A brief study of Wannacry Threat: Ransomware Attack 2017, *International Journal of Advanced Research in Computer Science*, Volume 8, No. 5, May-June 2017, ISSN No. 0976-5697.

[2] Ronny Richardson and Max North, Ransomware: Evolution, Mitigation and Prevention, *International Management Review*, Vol. 13 No. 1 2017.

[3] J. P. Tailor and A. D. Patel, “A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control,” *Int. J. Res. Sci. Innov.*, vol. IV, no. November, pp. 2321–2705, 2017.

[4] SH Kok, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam, Ransomware, Threat and Detection Techniques: A Review, IJCSNS *International Journal of Computer Science and Network Security*, VOL.19 No.2, February 2019, pp. 136-146.

[5] Aditya Patawari, *Getting Started with OwnCloud*; Packt Publishing Ltd.: Birmingham, UK, 2013.

[6] Sachin Kariyattin, Suresh Marru, Marlon Pierce, Evaluating NextCloud as a File Storage for Apache Airavata, *Proceedings of the Practice and Experience on Advanced Research Computing - PEARC ’18*, (2018), Article No.: 87, Pages 1–4, doi:10.1145/3219104.3229270.

[7] J. B. Nurdin, E. Mulyana and Hendrawan, “NextCeph: Nextcloud Platform Based Application for Ceph Cluster Management,” 2019 *IEEE 13th International Conference on Telecommunication Systems, Services, and Applications* (TSSA), Bali, Indonesia, 2019, pp. 25-30, doi: 10.1109/TSSA48701.2019.8985460.