The Different Types of File Protection:

1. Access Control List (ACL)

An ACL is a set of rules for allowing or denying access to certain resources. Resources in this case may be files, networks, or devices.

They prevent intrusions or unwanted traffic to protected resources from unauthorized users. Only users with the proper permissions are granted access. Others are denied.

2. Encryption

Encryption is the backbone of cybersecurity. It is central to file protection by maintaining the confidentiality of file contents. They protect data by turning the file’s content into a ciphertext that only authorized parties can decrypt and decipher. Protects sensitive data from being exposed in case of theft or unauthorized access.

3. Auditing and logging

Auditing trails and system logs provide a means of tracking file usage. It enhances file protection by providing a measure of non-repudiation to hold people accountable for file operations. It captures file actions performed like changes, deletions, transfers, and unauthorized access.

4. DAC

Discretionary access control (DAC) is an access control method that allows users to manage permissions for their resources, letting system or data owners decide who can access them and at what level.

Anyanwu, C. (2024, September 4). What is An ACL? Access Control Lists Explained. freeCodeCamp.org. https://www.freecodecamp.org/news/a-deep-dive-into-access-control-lists/

Fathauer, M. (2024, December 9). What is an Access Control List (ACL)? Basics & Best Practices. Ping Identity. https://www.pingidentity.com/en/resources/blog/post/access-control-list.html

Digital Guardian. "What Is File Protection? How It Works & Different Types." Fortra’s Digital Guardian, 13 Nov. 2023, www.digitalguardian.com/blog/what-file-protection-how-it-works-different-types.

https://www.digitalguardian.com/blog/what-file-protection-how-it-works-different-types

User and group management is an important part of computer systems because it limits who can access the system and what data they will have access to. By arranging users into the right groups and partitions, you can assign correct permissions and the level of access they have to the correct groups. And by separating users and defining different access levels a system can restrict access to sensitive data and system resources, reducing the risk of accidental or malicious misuse.

Solanki, A. (2024, December 4). *Understanding user and group Management: A simple guide*. NetworkHunt. <https://networkhunt.com/understanding-user-and-group-management-a-simple-gui/>

*Managing and configuring users and groups in Windows*. (n.d.). https://library.mosse-institute.com/articles/2023/09/windows-users-and-groups/windows-users-and-groups.htm

Labeling data flow diagram is important because descriptive texts identify the type of data being moved. And because of that, labeling provide clarity and accuracy in understanding what and how data moves within a system. Proper labels on processes, data stores, and data flows makes everyone involved in the project understand clearly what information is being transferred and how it is being processed.

<https://www.ibm.com/think/topics/data-flow-diagram>

<https://www.lucidchart.com/pages/data-flow-diagram>

