Security

This page covers the importance of security for Filecoin storage providers, including the need to mitigate potential security threats and implement appropriate security controls.

Being a Filecoin storage provider involves more than just storing customer data. You are also responsible for managing Filecoin wallets and running systems that require 24/7 uptime to avoid losing collateral. This means that if your network or systems are compromised due to a security intrusion, you risk experiencing downtime or even losing access to your systems and storage. Therefore, maintaining proper security is of utmost importance.

As a storage provider, you must have the necessary skills and expertise to identify and mitigate potential security threats. This includes understanding common attack vectors such as phishing, malware, and social engineering. On top of that, you must be proficient at implementing appropriate security controls such as firewalls, intrusion detection and prevention systems, and access controls.

Additionally, you must also be able to keep up with the latest security trends and technologies to ensure that your systems remain secure over time. This can involve ongoing training and education, as well as staying informed about new threats and vulnerabilities.

In summary, as a Filecoin storage provider, you have a responsibility to ensure the security of your customer's data, your own systems, and the Filecoin network as a whole. This requires a thorough understanding of security best practices, ongoing training and education, and a commitment to staying informed about the latest security trends and technologies.

Network security

When it comes to network security, it is important to have a solid first line of defense in place. One effective strategy is to implement a redundant firewall setup that can filter incoming traffic as well as traffic between your VLANs.

A next-generation firewall (NGFW) can provide even more robust security by incorporating an intrusion prevention system (IPS) at the network perimeter. This can help to detect and prevent potential threats before they can do any harm.

However, it is important to note that implementing a NGFW with IPS enabled can also have an impact on your internet bandwidth. This is because the IPS will inspect all incoming and outgoing traffic, which can slow down your network performance. As such, it is important to carefully consider your bandwidth requirements and plan accordingly.

System security

A second layer of defense is system security. There are multiple concepts that contribute to good system security:

- Host-based firewall (UFW)
- Implement a host-based firewall on your systems (also called UFW on Ubuntu), which isiptables
- based.
- SELinux
- Linux comes with an additional security implementation calledSELinux
- (Security Enhanced Linux). Most system administrators will not implement this by default because it takes additional consideration and administration. Once activated though it offers the highest grade of process and user isolation possible on Linux and contributes greatly to better security.
- Not running as root
- It is a common mistake to run processes or containers asroot
- . This is a serious security risk because any attacker who compromises a service running as root automatically obtains root privileges on that system.
- Lotus software does not require root privileges and therefore should run under a normal account (such as a service account, for instance calledlotus
-) on the system.
- Privilege escalation
- Since it is not required that Lotus runs as root, it is also not required for the service account to have privilege escalation. This means you should not allow thelotus
- account to usesudo
- .
-

Previous Network Next Storage

Last updated7 months ago