Best Practices for Maintaining the Security of Your Pharma Lab's IPV4 Network

Effectively securing the IPV4 network in your pharmaceutical laboratory requires having a good initial setup. We covered this in a previous blog, where we looked at seven essential security considerations when setting up an IPV4 network. The points in that blog can also help you improve the security of an existing network in your lab. What about ongoing security issues, however, and ensuring network security is maintained?

These are important questions as network security is not a one-time process. It is also not the sole responsibility of your IT team. Instead, effective network security is an ongoing process that requires effective policies and procedures. Also, everyone should understand their responsibilities in relation to network security, including lab technicians and other lab staff.

The following best practices will help you maintain the security of the IPV4 network in your pharma lab.

Disable Active Directory Logins that Are Not Needed

Regular maintenance of Active Directory logins is essential in pharmaceutical lab environments. At Westbourne IT, we regularly encounter situations where there are enabled Active Directory accounts of employees who have left the company. In some cases, the login credentials of these accounts are being used by other members of staff. That in itself is a security risk, but this risk is exacerbated when the privileges of the Active Directory account give the members of staff higher levels of administrative access than they should have.

Therefore, it is important to have robust procedures in place to disable Active Directory accounts whenever an employee leaves the company.

Conduct Regular Active Directory Auditing

Following on from the above point, it is also beneficial to conduct regular audits of Active Directory. During the audits, you should look to identify and resolve any potential security issues. Examples include:

- Are all enabled Active Directory accounts valid?
- Are all Active Directory accounts properly secured?
- Are all Active Directory accounts assigned to the right people?
- Have administrative privileges and access levels been properly assigned, particularly as employees change roles?
- Can you identify instances of employees sharing Active Directory login credentials?
- Are there generic user accounts, such as “User1" or LabMachine3”? If so, how can you change them?
- Are your multi-factor authentication processes fit for purpose and properly applied?
- Are all group memberships valid and are there any that should be removed?

Review Remote Desktop Rights

While it has use cases and benefits, Remote Desktop creates a number of security risks in pharmaceutical labs. That said, the use of Remote Desktop is often unavoidable. The best approach to enhance security is to keep the list of users tightly restricted.

The reality, however, is that employees come and go over time, with some people leaving, others changing roles, and others joining the company. Therefore, it is beneficial to regularly review the list of users that have Remote Desktop access, removing any that no longer need it.

Ensure Firewalls and Anti-Virus Software Are Up to Date

Firewalls, anti-virus software, and anti-malware software are essential components of any lab IT security strategy. However, these technical solutions are only effective if they are kept up to date. It's important to have processes in place to ensure you are running the latest versions.

Check Backup and Restore Processes

There should be regular backups running on your system as part of your disaster recovery protocols. However, it is not enough to just run backups on a daily basis. You also need to check the backup process is running properly, as well as checking your restore procedures. It is better to discover problems now rather than when you are in a disaster recovery situation.

Provide Staff Training and Create a Culture of Network Security

The people with access to your network represent the greatest risk and also, potentially, your greatest security asset. To enhance the security of your lab's network, you should provide regular training to ensure the team understands the risks and implications of network security, and the important role they as individuals play.

Pharma Lab Network Security – It's an Ongoing Process

The biggest factor in maintaining network security in your pharmaceutical lab is constant activity and vigilance. Network security is a process that is never finished, but you need to avoid situations where procedures are bypassed, and processes are delayed. The best practices outlined in this blog are a good starting point for improving the ongoing security maintenance of your network.