Essential Security Considerations When Setting Up an IPV4 Network in a Pharmaceutical Laboratory

When we are talking to pharmaceutical labs about IPV4 networks and security, we are often asked the question “how much security is enough”. When setting up a new network in a pharma laboratory, the best approach is to implement as much security as possible while allowing your lab functions and processes to continue unimpeded.

In the area of network security, there is always this trade-off between usability and security. It's important IT systems, processes, and workflows facilitate the operation of your lab while being as easy as possible for users. However, from a security point of view, it's important to lock everything down as much as possible.

How do you get the balance right? The following seven essential security considerations will help. They particularly apply when setting up a new IPV4 network in a pharma lab environment, but they are also relevant if you are reviewing the security of an existing network.

Network Segmentation

One of the most effective steps you can take in securing your IPV4 network is to segment it. Network segmentation is usually achieved through the deployment of a router or by designating a separate VLAN for your lab environment.

Segmenting your network is all about reducing your attack surface.

Labs in the pharmaceutical industry are becoming more digitalised with the increasing use of technology. This digitalisation brings a range of benefits, but one of the downsides is an increased attack surface.

Segmenting your network will help prevent issues on the corporate network from impacting your lab's network, while also preventing data on the lab network from unintentionally getting onto the corporate network.

Disable Unnecessary Protocols

Disabling unnecessary protocols on your IPV4 network also reduces the attack surface in your lab. For IPV4 networks, you should consider disabling IPV6, as it is susceptible to man-in-the-middle type of attacks. For example, attacks that interrupt data transfers, putting data at risk.

Disabling NTLM is also beneficial, although this isn't possible in all situations. Where it is not possible to fully disable NTLM, you should consider creating exception lists to limit NTLM access to specific servers.

Secure Your Physical Cabling Layout

One way an attacker might try to access your lab's network is by physically attaching a rogue device. You can make this considerably more difficult by only enabling ports and wall points that are in use. Restricting port usage on your corporate router to a whitelisted MAC address also helps.

Secure Wi-Fi Connections

It is becoming increasingly common in lab environments to enable network access via Wi-Fi. While convenient, Wi-Fi access creates additional security risks. One of the ways you can mitigate these risks is by implementing MAC address filtering, thereby restricting Wi-Fi access to devices that have been authorised and validated.

Consider Carefully Your Use of Remote Desktop

Remote Desktop is a very useful tool in a range of situations, including in IT and lab equipment support. However, Remote Desktop creates security risks. As these risks cannot be eliminated, the best approach from a security standpoint is to not use Remote Desktop.

In situations where you have to use Remote Desktop, you can reduce the risk it poses by enabling Network Level Authentication and tightly restricting the users who have access.

Enable Admin-Level Multi-Factor Authentication

Accounts that have administrative functions on your network should have multi-factor authentication (MFA) enabled to prevent credential sharing. MFA also mitigates the risk of theft.

You should also set accounts on your network, particularly admin-level accounts, to lockout after a set number of incorrect logins. IT service desks can reinstate locked accounts, minimising any negative impacts of this important lab environment security feature.

Disable USB Ports for Storage Devices

While USB ports are useful, including for IT support staff, they are also a potential physical entry point for attackers, particularly attackers who want access to the data on your network. Therefore, the network security of your lab will benefit if you disable storage devices and USB sticks on USB ports.

Getting Network Security Right from the Start

IPV4 network security in a lab environment is an ongoing process that requires constant vigilance, robust procedures, and regular reviews. That said, properly securing your network when it is first being set up will provide you with a strong level of underlying security that will protect your systems and data. The considerations in this blog should factor into your decision-making.