How software and network security measures can help keep systems secure

Passwords

Using passwords in an organisation would have to be suitable and secure, and would have to go by a policy going by the fact that passwords should not be written down, should be changed periodically (every 90 days), to as little as every seven days, strong passwords must be used. Also passwords should be absolutely random or even nonsense, but should be memorable to the person able to use the password.

Levels of access to data

Network systems and servers provide control over the levels of access to data. This can be by controlling certain users’ access to files and data on a network, for example only users who have certain privileges can be able to either view information, change and update information, or to be able to create new files, folders or data sets.

Diskless networks

Diskless networks do not store files on drives, USB devices or any other external drive, all files are saved on a network file server, or in recent technology, are saved by cloud computing. This prevents data being stolen as it is mostly caused by copying data from a computer and storing it on a mobile storage device. Workstations tend to not have files stored on devices, and would have a BIOS configured in order to prevent others from adding new devices into the workstation.

Disaster recovery

Disaster recovery is the process of regaining data that has been damaged or lost. This can be done by having **backup systems**, **whole system replacement**, and **tiers of recovery**.
Backup systems ensure that if data have been lost or damaged, that a user can be able to retrieve their files from this system from an external source and reuse them as normal. Whole system replacement takes place when you have not planned or experienced a system disaster.

Audit logs

These are used to keep documentation of network and database activity, having records of who has done what, where they did it and when. The audit log could have simple references to the service being accessed along with the system identity of the user. The main purpose of the audit log is to maintain detailed records of how a system has been used, when issues occurs, enabling system administrators to track the causes can be done with audit logs, and they’re also used to work with monitoring systems so that alarms can be enabled and placed on a system, alerting system administrators to suspicious activity.

Firewall

The reason for having firewalls is to block unauthorised access from entering the network. For example firewalls prevent access from unwanted users from accessing a company’s intranet blocking them from gaining the company’s information, and also provide protection from malicious threats. More than one firewall can be installed in a company, as it offers more security.

Software updating

Software updating ensures that your system is safe from likely faults and vulnerabilities, making sure that the system is safe from hackers, and by also preventing them from accessing the network. This process can be automatic, keeping users up to date on how their system is.

Backups

Having backups ensures that data is safe and secure, and that data can be restored when needed. It is essential to have a managed backup system in case of system failure. When it comes to network administrators, it is essential that they do at least one back up each day, for example if a company were to have a system failure and have all their data lost, they’re able to retrieve all their files as they have backed up their data already.