Introduction

With the increasing use of technology, businesses have become more reliant on computer systems and networks. However, with this reliance comes an increased risk of cyber-attacks and security breaches. It is important for businesses to understand the potential risks and have measures in place to mitigate against them. This report will provide guidance on the provided network and address some of the major issue of it.

Outdated operating systems and computers.

One of the biggest risks in this network is the use of outdated operating systems and computers. These systems can be vulnerable to attacks, which can result in loss of data, legal proceedings, and financial loss. To protect against this risk, the business should update all computers to actively supported and patched operating systems. This will ensure that the systems are up-to-date and protected against known vulnerabilities.

In addition to updating the operating systems, the business should also implement regular security updates and patches. This will ensure that any new vulnerabilities are addressed, and that the system remains secure.

Server located on ground floor.

Another risk in the network is that the server is located on the group floor. If a server is located on the ground floor, there is a risk of flooding and easier access by unauthorized individuals. This can result in damage to the server hardware and data loss, as well as unauthorized access to sensitive information.

To mitigate against this risk, the business should consider relocating the server to a higher floor or a more secure location. This will ensure that the server is protected from flooding and is more difficult to access by unauthorized individuals.

In addition, the business should implement access control measures such as key card or biometric authentication. This will ensure that only authorized individuals have access to the server room. It is also important to ensure that regular backups of data are taken and stored offsite. This will ensure that in the event of a disaster, the data can be recovered.

Lack of network segmentation

Another risk for the business is the lack of network segmentation. If personnel can access all network devices on the network, there is a risk of unauthorized access to sensitive information, malware or virus infection, and difficulty in identifying the source of an attack.

To mitigate against this risk, the business should segment the network to restrict access to certain devices and information. This will ensure that only authorized personnel have access to any sensitive information. It is also important to implement proper access controls and authentication measures to prevent unauthorized access. Regularly reviewing and monitoring network access logs will also help identify any unauthorized access attempts.

Weak Authentication

The use of a single 15 character password for key network services is not strong enough and makes the system vulnerable to brute-force attacks. This can result in unauthorized access to sensitive information, data theft or loss, and system disruption or downtime.

To mitigate against this risk, the business should implement multi-factor authentication for key network services. This will ensure that even if a password is compromised, an attacker would still need to provide additional authentication factors to gain access. Enforcing password complexity and length requirements, as well as implementing password rotation policies, will also help ensure that passwords are strong and not easily guessable. Using password managers to generate and store complex passwords, and monitoring and logging failed login attempts, will also help identify any unauthorized access attempts.

Use of Telnet

The use of telnet for remote access to network equipment is not secure and should be replaced with more secure protocols like SSH. This can result in unauthorized access to network equipment, data theft or loss, and network disruption or downtime.

To addition to use of SSH Implementing access control policies to limit access to authorized users, monitoring and logging remote access sessions, and conducting regular security audits and vulnerability assessments will also help identify and mitigate any security risks.

Open Source Software

While open-source software can be secure, it may not receive the same level of support as commercial software. This can result in potential security vulnerabilities, data breaches, and legal issues as the source code of the software is openly viewable and vulnerabilities can be easily found

To mitigate against this risk, the business should regularly monitor and update open-source software for security vulnerabilities. Implementing additional security measures such as firewalls and network monitoring, and considering using commercial software for critical systems, will also help ensure that the system remains secure.

Wireless Security

While WPA2 is technically relatively strong protocol, it is still vulnerable to attacks like password cracking and rogue access point attacks. This can result in unauthorized access to the wireless network, theft or loss of confidential data, compromise of network security, and disruption of business operations.

To mitigate against this risk, the business should use strong and complex passwords for the wireless network. Implementing a wireless intrusion detection system to detect rogue access points, regularly updating firmware and security patches for all wireless APs and using additional security measures like MAC address filtering and disabling SSID broadcast will also help ensure that the wireless network remains secure.

Conclusion

In conclusion, the existing network face a few security risks by implementing the measures outlined in this report, the network can mitigate against these risks and ensure that their systems remain secure. However, the business will need to regularly review the network against new and emerging threats to endure the network’s protection is up to mark.