**A6 Enterprises Ltd.**

NETWORK INSPECTION REPORT

Add a short description here

**Information available in audio.**

**PRESENTED TO**

Executivew Board

**PRESENTED BY**

St Patrick Currey

April 25, 2023

**Add Company Name**

**Network Scan Results**

After performing a basic network scan on the company's network, several potential security vulnerabilities were identified. These include:

Unpatched Operating System

Weak Passwords

Unsecured Network Access

Lack of Firewall

Unpatched

Operating

Systems

Several systems within the network were found to be running outdated versions of the operating system. This could allow hackers to exploit known vulnerabilities and gain unauthorized access to the network.

**Risks of Using An Outdated OS**

Legal Risks, such as lack of compliance with industry standards and regulations and liability for breaches

Performance risks such as incompatibility with new software and hardware, slow systems and frequent crashes and instability

Security risks. Outdated systems are especially vulnerable to ransomware such as Wannacry, worms and botnet attacks. Older operating systems are also more likely to have known vulnerabilities that attackers can exploit.

Weak Passwords

Many user accounts within the network were found to have weak passwords. This makes it easy for hackers to guess passwords and gain access to the network.

A WEAK PASSWORD PUTS YOU AT RISK OF

HAVING UNAUTHORIZED PARTIES ACCESSING

YOUR INFORMATION WHICH CAN LEAD TO

IDENTITY THEFT, THE LOSS OF CRUCIAL

RESOURCES AND DATA AND EVEN CRIPPLING

DATA BREACHES.

**EMAIL**

hello@reallygreatsite.com

Unsecured Wireless Netsworks

The wireless network was found to be unsecured, meaning that anyone can connect to the network without a password. This makes it easy for hackers to access the network and steal sensitive information.

**Add Company Name**

Lack of

Firewall

The network was found to be lacking proper firewall protection. This means that it is more vulnerable to external attacks and data

breaches.

Risks of Not Having a Firewall

Unlimited Public Access - Anyone can access the network and potentially have access to data and any devices linked to the network

Network Downtime - Without a firewall, it's easy for criminals to conduct violent attacks against the system, potentially shutting it down for extended periods of time

**Measures To Secure The Network**

Regular Patching: The company should ensure that all operating systems and applications are regularly patched to fix any known vulnerabilities.

Strong Password Policies: The company should enforce strong password policies, including requiring users to use complex passwords and changing them regularly.

Securing the Wireless Network: The company should secure the wireless network by using WPA2 encryption and creating a strong password. It is also recommended to set up a separate guest network for visitors to use.

Firewall Protection: The company should implement a firewall to protect the network from external attacks.

Plans to Monitor and Maintain The Network

**To maintain the security of the network, the following plan is recommended:**

**Regular Scanning: The network should be regularly scanned for vulnerabilities and security risks.**

**Security Updates: Operating systems, applications, and firmware should be regularly updated to ensure that they are secure.**

**User Awareness: The company should provide regular training to employees to increase their awareness of cybersecurity risks and best practices. Incident Response Plan: The company should develop an incident response plan to ensure that they can respond quickly and effectively to any security breaches.**