ambersail

SECURE REMOTE WORKING

Remote working is now the norm. It offers many benefits including flexible working arrangements and greater staff productivity.

However, there is a catch. If not set up properly, opening your networks to Internet based access can lead to very serious security issues.

HERE ARE FIVE KEY CONSIDERATIONS TO STAY SECURE.

1.

Do you control what devices are connecting to your network?

Any device that is remotely accessing your network needs to be securely configured. Make sure that software is regularly updated with security fixes. The integrity of every remote device is key when protecting your company networks. There should be no exceptions.

Pay special attention to people using their own equipment to access the network. These devices can often be shared with other family members who might not be security aware.

If devices are being used to access confidential materials, ensure that your remote access solution allows you to carefully control what can be accessed from the device. Alternatively, issue company-owned devices that can offer restricted use.

2.

Physical data protection

People might download local copies of sensitive data for convenience. This should be actively discouraged or control of data storage will be lost. In many cases, core GDPR principles have been neglected leaving a company open to embarrassing data leaks and heavy fines.

Remote devices should always be fully encrypted to protect data and reduce risk.

Users should always lock screens when stepping away from a device. Open screens provide direct access to sensitive company networks. Also consider a company policy that ensures team members are aware of their surroundings. Accessing confidential systems from a crowded coffee shop may not be a good idea.

3.

Strong User Authentication

As access is via the Internet, securely signing into the network is very important.

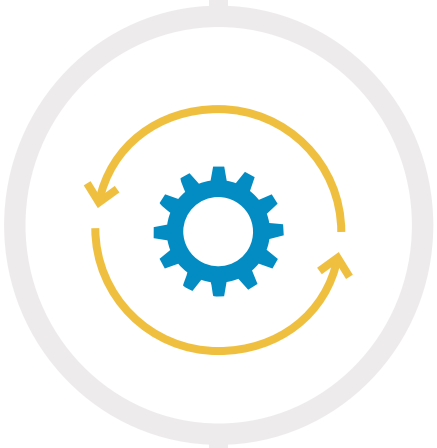
Two factor authentication remains a strong and secure method for sign in. It requires that at least two "factors" are offered to authenticate a user. These are two of:

Something you know – such as a password

Something you have – such as a token or client certificate

Something you are – such as a biometric input like a fingerprint

Many users will already be familiar with two factor authentication. Examples are phone-based fingerprint readers or facial recognition systems.

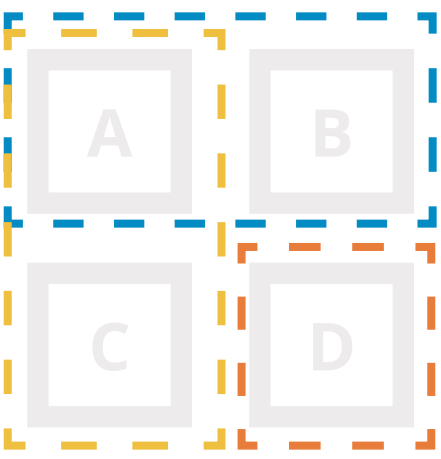


4.

Keep your remote solution updated

Ensuring that software is continually patched and updated. This is critical. Systems must be monitored for security flaws and updated as part of a regular schedule. Critical flaws should be patched as soon as possible once discovered.

Remove all default accounts. Any remaining default credentials must be changed to a strong alternative. Ensure that user passwords are strong. Ensure that cryptographic settings are in place so that data is encrypted both on the device, and in transmission over the Internet.



5.

Is your network too open?

If you have a flat, open network it might be time to consider a redesign. Segmentation is a technique to section a company network off into smaller, protected networks. Networks that can be controlled to allow access to only the right people.

Segmentation is a Defence In Depth strategy used by many companies to protest sensitive data. Imagine your remote access solution and internal network get compromised. It will be far harder for an attacker to find valuable data if it is protected in its own controlled subnetwork.

As with everything in the security world, there is no "silver bullet" which can solve all problems and stop hackers. Instead a "defence in depth" approach must always be taken to enforce security.

Remote working is here to stay. Always remember that it provides communication to people over the public Internet. This introduces risk that must be managed to avoid serious security issues.

More here: www.ambersail.com/vpn-penetration-testing/