HEXAGON IT

Protecting Business & Client Data when Remote Working

Guidance and recommendations for ensuring home & remote working is secure

Home working has become the new norm as a result of the Coronavirus pandemic.

Even as restrictions are relaxed, it won't be possible to return to busy office workspaces any time soon.

There'll need to be strict social distancing and hygiene protocols in place for the near future with the possibility that further lockdown restrictions are introduced.

Organisations will need to plan to return to full working capacity effectively with less office space to cater for safe working conditions.

Home working is here to stay not just due to Coronavirus restrictions, but also from employee demand.

Many people will want the option of working part of their week at home.

Flexible working practices increase productivity and staff engagement and improve retention.

Businesses that embrace this will flourish.

They'll attract and retain the best staff and they'll stay responsive to client needs wherever their workforce is located.

However, there are major cyber security and data protection risks associated with this new way of working if you don't put the right protection in place.

They fall into 3 areas:

1. insecure user devices and home networks

2. data breach from loss of information control

3. hackers accessing company networks and data through weak or stolen passwords

1 INSECURE DEVICES AND HOME NETWORKS

The Risk

Home working takes end user devices and laptops and desktops out of the safety of the office.

They're using a home network which is shared with other members of the household.

Other computers on home networks are highly likely to contain malware and work computers may also be used for non-work purposes.

Allowing home workers access via a vpn risks spreading malware and compromising your business network and servers.

Vpn connections are like a very long network cable. Once connected the local machine becomes part of your business network as if it was in the office.

Threats on that machine or on the home wifi can travel across the vpn and infect your network and servers without you knowing.

The Solution

Assume the computers home workers are connecting from are insecure and are on insecure networks..

1. Implement reverse proxy for remote and virtual desktop connections

Enable vpn'less connection for work purposes. RDP connections through open ports are not secure and allow attackers to use these open ports to attack networks.

Implement a reverse proxy to handle internal connections from the internet. The reverse proxy acts as a middle man only passing valid requests to and from internal servers and pcs. No direct network connection is made, The home pcs can only talk to the proxy. This can be for RDP, file access and email access.

There are a number of tech companies supplying applicances capable of working as a reverse proxy such as Kemp Technologies, Nginx and Citrix.

We've implemented cloud Citrix ADC (formerly Netscaler) appliance which our customers use to create proxy'd secure home working whether to office pc's or cloud hosted desktops.

2. Use secure file sharing service

Secure file sharing services allow users to access work documents without having to connect to the business network.

They allow access to files from office pcs, roaming laptops, tablets and mobiles. Other useful features include versioning and secure sharing with thried parties such as allowing view only and limited time access.

Low end services such as Dropbox and Onedrive lack stability and security features. Egnyte offers additional functionality.

We provide Citrix Content Collaboration (formerly Citrix Sharefile) to customers. This allows secure document and file sharing on any device, versioning and secure sharing.

Plus it integrates with Citrix containerisation (see 2) to ensure you maintain control of business information wherever it is.

Recommendation

Reverse proxy:	Citrix ADC
Secure File Sharing	Citrix Content Collaboration

We're able to provide both of these as services from our secure cloud.

2 DATA BREACH FROM LOSS OF INFORMATION CONTROL

The Risk

Home working means data has to leave the safety of the office or data centre.

To work effectively staff will copy files to local computers to work on before copying back to the work drive. The problem is, the file is still local and is rarely deleted even though it's not needed.

This leads to an uncontrolled spread of data with no way of removing copies. This could be client information as well your business data.

The Solution

There are two ways of ensuring business and client data is controlled. The best solution may be to use a mixture of the two.

1. Keep files and documents in the office or data centre

Rather than needing to copy documents to the local computer to work on, virtual desktops allow staff to work without files being copied locally.

Using MS Remote Desktop of Citrix Virtual desktops, files and documents are kept cenrally with staff able to view and work. Either connect to your desktop in the office or a virtual desktop in the cloud.

Add additional policies to stop data being copied locally and prevent local printing.
Ensure a reverse proxy method (see 1) is used to connect to the remote desktop. This requires an always on internet connection.

2. Use containerisation to protect documents & file copied to local pcs and devices

Containerisation allows business and client data to be controlled whether it's on a laptop, home pc, tablet or mobile.

Corporate data is stored in a secure container which is controlled by the business. Only authorised users can access the container which can be locked and wiped remotely.

This allows documents to be kept on laptops and other devices for work with central, automated policies to remove documents/files when no longer needed.

Once the laptop/device is no longer needed for work puposes or is lost or stolen the container and all contents is removed.

This is great for allowing personal devices to be used for work, keeping control of coporate data without compromising personal data. Containers can protect corporate emails in the same way allowing personal devices to receive and send work emails.

Recommendation

Solutions such as Soti, MobileIron and Citrix Endpoint Management.

We recommmend Citrix Endpoint Management. It enables containerisation of documents, file and emails. It links with Citrix Content Collaboration (secure file sharing) and can secure corporate email through Citrix ADC.

We host containerisation for our clients based on Citrix Endpoint management together with Citrix ADC, and Citrix Content Collaboration.

3 HACKERS ACCESSING COMPANY NETWORKS AND DATA THROUGH WEAK OR STOLEN PASSWORDS

The Risk

Opening up business networks to allow mass remote working increases the risk of hackers accessing your data and systems.

Once hackers have access they can steal data, install keyboard logging and email watching malware to track activities or encrypt your files and demand a payment to unencrypt.

Staff who regaularly work remotely will be aware of the risks of weak passwords and will often have limited privileges. Staff who are normally office based often have higher privileges and less awareness of the risks of weak passwords.

Hackers have access to millions of username and password pairs from hacked websites.

The Solution

Implement 2 factor authentication.

After entering your username and password you're prompted for an additional step. The easiest is confirmating a prompt on your mobile phone. Once you've done this you complete your login.

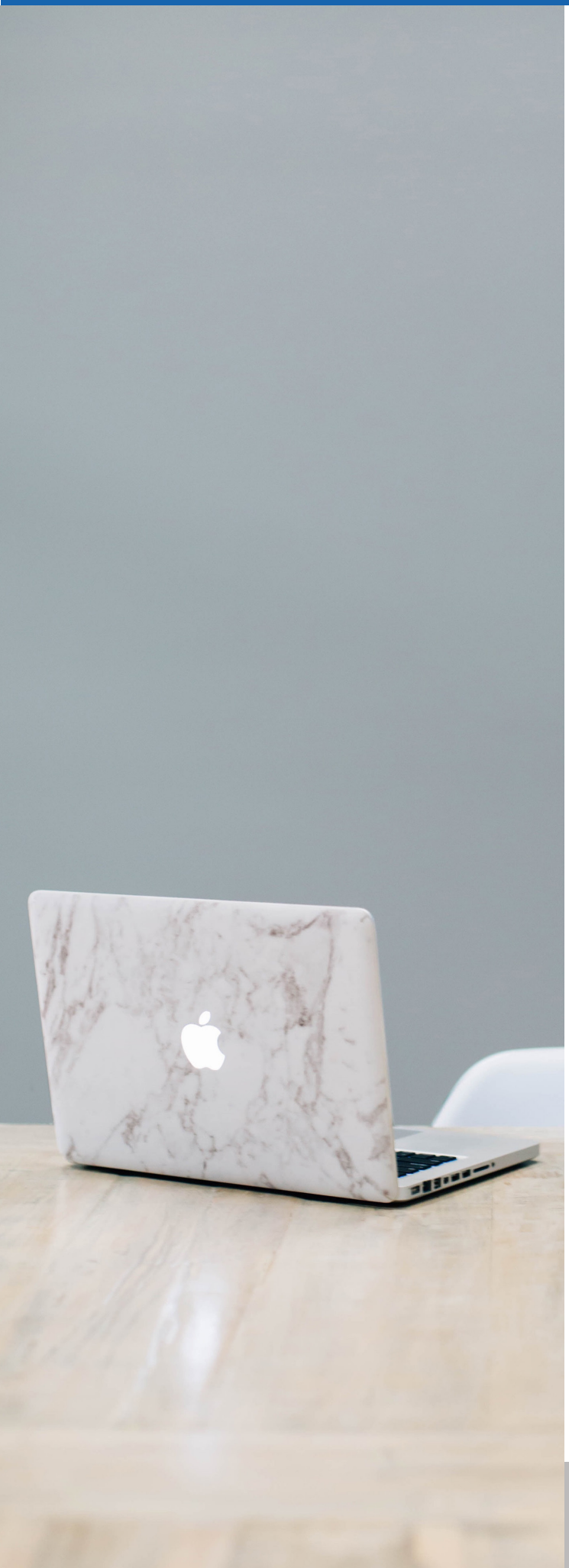
This removes the ability for hackers to access your system by using stolen or guessable username and passwords.

Recommendation

There are many 2 factor authentication providers including Azure.

We recommend and use Duo for a couple of reasons.

Duo great support for temporary login if you lose your mobile or the battery's dead.
Also, Duo allows offline login. With Azure, if you don't have an internet connection, you won't be able to login.



Home and remote working opens up great possibilities for flexible working practices but it also significantly increases the risk from cyber threats and data breaches.

It's possible to mitigate against these and create a secure, productive remote working platform for your workforce.

The technology is available but not simple to implement and manage.

Contact us to explore how our ready built solutions can help you quickly move to a secure, flexible digital workspace.

Rapidly enable your staff to work anywhere, anytime on any device without compromising cyber security or data protection.

Steve Barnett

Email: steve@hexagon-it.co.uk

HEXAGON IT