chess Helps You

Work From Anywhere

Securing Remote Workers

Due to Coronavirus

What can you expect?

In light of the recent Covid 19 pandemic, companies are enabling remote working at larger scales. For businesses to continue to operate, speed is vital in the current situation, and IT are faced with resource challenges to mass roll out remote access.

Often security is left as an afterthought and attackers take advantage of the newly created vulnerabilities in the system and the social panic.

Attackers will:

Target exposed services on public IPs

Try to gain access to Office365

Use phishing/vishing

Exploit vulnerabilities in home networks

What is the process?

While hackers tend to target vulnerabilities and not companies specifically, organisations with more than 100 employees would have a bigger attack surface.

With more people being enabled to work from home and using their own devices, this attack surface grows, and the IT team don't always have full visibility of it.

This makes protecting the organisation from cyber attacks more complicated – it's easier to protect and keep track of five known devices than to protect hundreds of known and unknown devices.

Security Vulnerabilities in Home Networks

Employees working from home can expose your network to a wider set of threats.

Home networks are predominantly insecure:

- People tend to use the default settings on their router which do not provide the highest level of protection
- With the increase of smart home appliances, the home attack surface is increased, and hackers can use your smart TV to gain access to your home network
- Children nowadays are often technically versed and can adjust settings to optimise their gaming experience but open the home network to attacks.

To protect your business system even if the home network is compromised, as an organisation, you need to ensure you have a secure baseline configuration for home use devices, advanced endpoint protection and multi-factor authentication in place to reduce the risk of an attacker gainining access to that system and into the office network.

What Can You Do?

1. Awareness

The best approach in the current situation is to test your remote access system through an external vulnerability test.

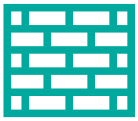
A Remote Access Penetration Test would not require any internal or physical access. The penetration tester would test your system from a remote location and try to gain internal access.
This will highlight the vulnerabilities that have opened up when you've rolled out remote work on large scales.

2. Get The Basics In Place

Endpoint

Choosing an advanced threat protection endpoint solution will help protect a device which has access to your business network but resides in an insecure home network.

Endpoint protection involves software which secure the endpoint devices which are linked to business networks as they can be exploited as a path to obtain internal access to the said system.



Next-generation Firewall

The firewall will act as a barrier between your network and the internet or outside intruders. It filters traffic, prevents intrusions and alerts of suspicious activity.

Next-generation Firewalls are a more advanced version of traditional firewalls which combine the functionalities of their traditional predecessors as well as additional ones such as in-line deep packet inspection, an intrusion prevention system, website filtering and antivirus inspection, etc.

Virtual Private Network (VPN)

A virtual private network solution may already be included as part of your Firewall solution and is one of the vital basics you need to have in place to protect your organisation's internal network.

A virtual private network is a solution which extends your organisation's private network and provides secure access to remote users' devices as if they are in the office.

Multi-Factor Authentication (MFA)

Hacking an organisation with a multi-factor authentication (MFA) solution in place requires more time and effort. Attackers tend to focus on 'low hanging fruit' and target glaring vulnerabilities within organisations' networks. For this reason, the hacker is more likely to move on to a less secure organisation without an MFA solution in place.

Multifactor Authentication is a security system which requires the user to verify their account
and access through multiple credentials independent from each other. This can include a combination of username and password and security token from the person's smartphone.

!

FREE personal PC and Mac protection for all Chess Sophos customers

For the duration of the COVID-19 global health concern, all Chess customers who are purchasing Sophos solutions can protect their employees' personal PCs and Macs for free with the Sophos Home Commercial Edition program.

Contact your Account Manager or call **0808 252 0755** for more information

About chess®

Chess is one of the UK's leading independent and trusted technology service providers, employing 480 skilled people across 6 UK sites, supporting a wide range of organisations.

By leveraging world-class technology, Chess helps you to connect your people, protect your data, grow your business, reduce your costs and work better together, which means your business, your people and your customers can thrive.

At Chess, we're passionate about our unique culture and our continuous investment in our people to be industry experts. We're extremely proud that our people voted us No.1 in 'The Sunday Times 100 Best Companies to Work for' list 2018, and we continue to celebrate more than ten years in the top 100.


WORK BETTER TOGETHER
PROTECT YOUR DATA
CONNECT YOUR PEOPLE
GROW YOUR BUSINESS
REDUCE YOUR COSTS
chess®
Help You

chess Helps You

Work From Anywhere

Contact Our Team Today

WorkFromAnywhere@ChessICT.co.uk

0808 252 0755

ChessICT.co.uk/

chess®