The Invisible Threat To UK Businesses

As a vast amount of the country's workforce are now working from home due to the ongoing coronavirus crisis, Ian Vickers, CEO of cloud-computing service METCloud weighs in on the best practices to avoid another invisible threat – cyber-attacks.

As the coronavirus crisis continues, a large percentage of the UK's workforce have been given no choice but to operate from their own homes. Given the fast-paced nature of this ever-evolving event, many businesses were required to introduce this new way of working at a rapid pace. This means that in many cases, businesses had little or no time to consider the strength of its cybersecurity infrastructure.

Unfortunately, cybercriminals are already taking advantage of this unprecedented situation in a bid to defraud many companies out of huge sums of money; with a significant spike in cyberattack attempts reported over the past weeks, according to the National Cyber Security Centre.

While companies can invest in services to protect its systems, it still remains vital that all staff are kept up to date on best practice and cybersecurity developments. This enables them to be vigilant to threats and understand how their role plays a part in keeping the company safe against breaches, during this crisis and beyond.

Regular, short and informative meetings to keep cybersecurity at the forefront of employee's minds is far more effective than long, intensive sessions. By keeping everyone engaged, staff are more likely to maintain a vested interest in the company's cybersecurity measures.

Cyber-attacks continually evolve. Therefore, employees should always be aware of the new ways cyber criminals may try to infiltrate a breach in the infrastructure. Make sure to communicate this and ensure that all staff have someone to go to, should they want to raise an issue or ask a question.

Relying on one password to gain access to important programmes and resources can be risky. By introducing a multi-factor authentication, a business can cut the risk of others gaining unauthorised access to important and sensitive resources. This process is achieved by filling two or more security verifications (e.g. security question, PIN, facial recognition or fingerprint scan) before access is granted.

Password practices should still be improved. Although users should refrain from using the same password across multiple platforms, many still do because it is easier to remember. This is where password management programmes will be invaluable in protecting the cybersecurity interests of a company.

A word of warning - make sure that the master password for these programmes aren't easily guessed. Follow the suggested guidelines from The National Cyber Security Centre, that recommends three random words.

Recent events have vindicated the importance of cloud computing. With a reported 775 per cent demand upsurge for Microsoft Azure services last month, there is very little debate on whether businesses should consider cloud computing. The service not only makes the transition from office work to remote smoother; it also provides clever collaborative tools for the teams.

By allowing the staff to reliably access data from a remote server, rather than their individual devices, cloud computing allows better protection against damage/loss, less physical overheads and maintenance to the company.

Phishing emails are becoming increasingly crafty as cybercriminals are becoming increasingly savvy with getting users to click on suspicious links. Of late, they have taken to masquerading as trusted contacts where they ask recipients to review ‘documents’. When clicked, these malicious files have been known to cripple entire networks and breach the security of other contacts linked to the affected user.

It is important to continually advise the workforce to avoid clicking on any suspicious emails. If they seem suspicious, it is best to contact the sender by other means to verify the authenticity of the email.

Remote desktops allow multiple end users to connect to the server and its resources remotely. Hence, patch updates are imperative in ensuring the integrity of its performance and security. Users are inclined to ignore prompts and messages to perform these updates, proving it to be detrimental to the overall health of the system.

It is best to schedule these updates when the user logs off for the day and allow these critical processes to take place.

As companies become more reliant on technology, it is becoming more evident that the responsibility of cybersecurity lies in everyone within the business.

While there are countless cybersecurity resources available, a company’s cybersecurity strength lies within its people. It is important to ensure best practice measures are continually communicated and maintained within the workforce.

Met Clod 19th May

Ian Vickers CEO Cloud computing