Prove it

In the ‘olden days’ the office front door was locked and we went home safe in the knowledge that it was secure. In today’s digital world of mobile phones and cloud servers far more is needed.

The switch to home working caused by the coronavirus crisis resulted in a lot of security issues, with strong office system firewalls being replaced by poorer home computer security. Office password regimes with their usual strict security protocols were diluted by poorer technology in the home, leaving some firms vulnerable to data breaches and malware.

Most computer servers, whether in offices, in the Cloud or on the Web are protected by firewalls, antivirus programmes and a collection other security safety tools. Whilst these all remain vital, their effectiveness in a Cloud based world is becoming less certain. Adopting a no nonesense zero trust approach is beginning to make more sense.

New security doctrines that require proof of identity before granting access are growing in popularity, with zero trust policies on the rise. This is beginning to be adopted by more firms throughout the world. By defining who has access to the firm’s resources you build a better security regime.

Zero trust authentication is still evolving and developing new strengths by going another step further in approving the computer device the user is accessing. The use of bring your own device (BYOD) has been responsible for a lot of cyber and data breaches over the years and so by identifying the machine the user is accessing delivers another layer of security.

Firms have been learning from their mistakes in ‘lockdown’ and beefing-up home working security, even introducing ‘password policies’ for home workers. This is helping to create a regime of ‘best password practice’ and the adoption of new rules at law firms and other organisations.

Zero trust environments demand that individual machine and or device identities verify which machine is being used by which employee. Having a firewall is all well and good but now that most firms have multiple machines in and outside their office walls, especially as so many employees are working from home today, this is now not enough.

The practice of password reuse by employees working from home is beginning to diminish and moving towards office style security. Many coronavirus related cyber security breaches were the result of bigger break-ins at large service providers like Amazon, Google and others, where thousands if not millions of passwords had been stolen. Cyber criminals simply ran through these stolen passwords until they found a match. By introducing stricter policies on passwords massively reduces the chances of this happening.

Whilst system administrators and or office and practice managers should have their password management regimes under control, it is worth reviewing and reinforcing password security standards. Having a 'password policy' in place, whether formalised in a written document or not, should include at least the following basic standards to ensure employees working from home keep their firm's data safe.

- Passwords should be a least 8 numbers and characters long. In other words, complicated, using special symbols, capitals, and numbers.
- Password should be unique – no duplicates.
- Passwords should always have at least two-factor authentication where the user receives an authentication code to their mobile or similar device.
- Incorrectly entered passwords should have a disabling mechanism after a number of attempts, forcing the user to call-up the admin, office or practice manager.
- Passwords should facilitate access to ONLY those duties performed by the employee. This helps prevent access to more sensitive data requiring stricter controls.
- A 'Review Regime' is helpful, where 'permissions' are reviewed and down or upgraded as appropriate. Employees who used to have access to particular types of data, might have left the firm or no longer require the same level of access, and others may need to be upgraded owing to a promotion or new role.

Since most of home working today accesses the firm's Cloud based services or internal servers, it is vital that this is limited to only those with permission. Adopting a no nonesense zero trust approach is an emerging standard where everyone is treated with suspicion. Until a user can prove that they are who they say the are, access is denied. A platform like this can be applied to the Cloud, Webservers, mobile phones, travelling sales reps and homeworkers with each required to confirm their credentials

Creating a stronger sense of security that is real and active promotes greater productivity as well as delivering a deeper and longer lasting security within the firm. In an increasingly mobile and digital world where almost everything is transmitted digitally, and more often than not from outside the comparative safety of the office network and cloud systems, zero trust protocols need to persist.

On a zero trust platform everyone is treated the same – with suspicion. Until a user can prove who they are through a software defined perimiter (SDP), access will not be granted. A zero trust platform can be applied to the Cloud, Webservers, mobile phones, travelling sales reps and homeworkers with each required to confirm:

1. their identity – authentication
2. they are on a sufficiently secure connection
3. they are authorised to access the resources they need
4. which device they want access from
5. where they are – on a business network or café wi-fi

There are useful Web links to learn more about passwords and how to protect data. The National Cyber Security Centre Website at https://www.ncsc.gov.uk/guidance/using-passwords-protect-your-data is particularly good, offering a 'Small Business Guide' on cyber security and how to apply this to your firm.

One of the most common mistakes made by firms is forgetting or simply not bothering to change the manufacturers' default passwords that smartphones, laptops, and other types of equipment are issued with. This is an essential task before distributing phones and other digital devices to staff that ensures cyber criminals do not break in on day one. The site also has advice on encryption, authentication, secure lock-ups for mobiles and tablets, phishing, and keeping smart phones safe. The NCSC also have useful guides on passwords and other related topics.

Microsoft's Website at https://support.office.com/en-gb/article/password-policy-recommendations-for-office-365-9fa2539a-2211-41fd-85a0-bc37b9619ca4 also offers good advice on ways to manage your passwords, how to resist common attacks as well as containing them and understanding human behaviour.

A zero trust policy trusts nobody, even the Chief Executive must 'prove their identity'.

For further information about zero trust platforms
Phone: 01342 301325
Email: thebureau@the-bureau.co.uk