PLUG THE GAP

Andrea Babbs *highlights the advantages of securing access control with vulnerability and patch management*

The 2021 World Economic Forum report has found that cybersecurity practices in place across organisations are becoming outdated due to increasingly sophisticated and frequent cyber crimes occurring. Consequently – and unfortunately unsurprisingly – businesses of all sizes are finding it difficult to keep up with the innovative modern security market.

Traditional methods used to protect businesses from cyber attacks now fail to meet the security needs of the modern hybrid IT world. Entry points are left unsecure for attackers to leverage as employees work away from the support and guidance of IT teams. Therefore, it is of utmost importance for IT teams to strengthen endpoint security across the business to successfully control these threats and secure access control. There is an array of tools that can help to do this, such as vulnerability and patch management.

Desktops, mobile phones and laptops are all examples of end-user devices which need to be protected at all times as part of a business endpoint security. This was much easier prior to COVID-19 when traditionally workforces were in office environments and IT teams were physically available to monitor individual devices. They could ensure that applications were up to date, ensure that the right software was installed, and double check that there was no malicious activity on the device.

However, now in the modern hybrid working environment, remote users are away from the immediate help of their IT teams. In turn, new endpoint vulnerabilities have emerged. This is a consequence of employees working on personal devices, browsing on potentially dangerous websites and working on open and unsecured networks.

"A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error and attackers will look to exploit any of them, often combining one or more, to achieve their end goal" – NCSC, Government UK.

And, it's clear that cyber security attackers are taking advantage of these new hybrid working security risks – with new research carried out by the British Chambers of Commerce (BCC) and Cisco revealed that more than half of UK firms believe remote working has left them open to cyber attacks. These new endpoint vulnerabilities could 'leave the door open' for data leaks and ransomware attacks to occur, with attackers gaining unauthorised access to the business network.

Businesses can enable two-factor authentication in order to control access

REDUCING RISK

To reduce these risks, endpoint security must be prioritised. Modern security strategies must be compliant against the complexities of hybrid working environments, with endpoints secure regardless of if the employee is working at home or in an office-based environment. So where do businesses begin to ensure they have the right tools and technologies in place?

A study by the Ponemon Institute found that 68 percent of businesses have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastructure. The same survey also found that 55 percent of professionals consider smartphones to be among their most vulnerable endpoints, with other particularly vulnerable endpoints including laptops (50 percent) and tablets (24 percent). This demonstrates how important it is for organisations of all sizes to protect its endpoints, as they are a key entry point for attackers.

There are a number of ways endpoints can be secured. Firstly, organisations can ensure that staff members have strong passwords that meet the necessary requirements or have rules in place for workforces to operate only on protected networks. As an extra layer of protection beyond just a username and password, businesses can enable two-factor authentication in order to control access as users will need to have the necessary evidence, such as a code, to gain entry on the device. Both these methods are a fundamental starting point for maintaining access control, as only those that have had their identity verified can access company data.

Other examples include uninstalling unused software, applications and datasets; keeping programmes up to date; having an antivirus software in place; and requesting IT team approval for new downloads to ensure they are trustworthy and not malicious. But in the modern cybersecurity landscape, technology solutions including patching and vulnerability management are key in going one step further to protect and secure each endpoint.

Patching is one of the most crucial things organisations can do to reduce cyber threats. The principle of patching is to ensure that all applications and softwares are up to date and have the most current security protection installed. Frequent new vulnerabilities in software are discovered frequently and patches are a response to this. By updating the software with a 'patch,' it will enable businesses to plug any potential gaps before cyber attackers can target them. Updates also include bug fixes, additional new features and aim to improve the overall software.

As emphasised by the UK National Cyber Security Centre: "Exploitation of known vulnerabilities in software remains the greatest cause of security incidents. Patching the process of applying updates from software developers, hardware suppliers and vendors, to either enhance functionality or to improve security is one of the most important things you can do to mitigate vulnerabilities."

However, there are drawbacks to patching. It can be a very costly, repetitive and manual process, which means that errors can be made. Additionally, with hundreds or thousands of applications installed across the workforce, it can be difficult to maintain up to date and precise inventories across larger businesses. Often, automatic updates can be turned on to ensure that the most up to date software is running – but this may not always be possible. Additionally, new challenges from remote working have meant that it has become more difficult for updates to be made across systems, especially when the process is done manually by IT teams. Consequently, older, unpatched devices are more vulnerable to malicious applications than devices that have had patches deployed – as demonstrated by the 2019 Ponemon Institute Vulnerability Survey, which found that 60 percent of breach victims were breached due to an unpatched known vulnerability where the patch was not applied.

> **IT TEAMS ARE UNDER HUGE PRESSURE TO ENSURE ENDPOINTS DON'T PROVIDE VULNERABILITIES**

Maintaining robust network security requires constant attention because new vulnerabilities and patches are appearing with increased frequency. However, rather than conducting this process manually, there are patch management and automation solutions which can minimise this burden. IT teams can instead be alerted that an update is needed and deploy the required patches in real-time – in turn, minimising any possible security threats and overall bettering the network security.

A large number of cyber attacks are the result of attackers exploiting publicly disclosed vulnerabilities to enter a businesses network and systems, with the NVD database holding over 8,000 vulnerabilities published in Q1 of 2022 – a 25 percent increase from the same period the year prior. In turn, IT teams are under increased pressure to implement a comprehensive security strategy that ensures endpoints don't provide vulnerabilities.

Therefore, another tool that has been recognised as one of the ten steps for organisations to protect themselves by the National Cyber Security Centre is vulnerability management. A good vulnerability management process should include multiple stages, from identifying, evaluating, fixing and reporting the vulnerabilities. This process will help to support businesses to understand which risks need to be prioritised – especially as some vulnerabilities may be more difficult to fix than others or have more of a detrimental impact if leveraged by an attacker.

▶

By deploying vulnerability management solutions, IT teams will have enhanced visibility of the network and device vulnerabilities and can frequently monitor the company's operating systems and applications for possible weaknesses. Ongoing scans will identify any existing faults in the IT infrastructure, including outdated software that should be patched, providing IT teams with a holistic view of the network. This proactive approach aims to close the security gaps that exist before they are taken advantage of.

IT IS VITAL TO STRENGTHEN ENDPOINT SECURITY ACROSS THE BUSINESS TO SECURE ACCESS CONTROL

Today's modern security landscape requires a layered cyber security strategy, which comprises a number of tools and solutions to maximise a business' security posture. This can become both complicated and costly for IT managers who are overseeing a variety of different security tools and technologies.

Nevertheless, solutions are available that combine both patch and vulnerability management tools into one platform, with automated processes in place to help harden and secure existing business endpoints. This provides a streamlined and cost-effective solution for IT teams by having a single, comprehensive platform in place, which can monitor and manage all potential end points for a cyber attack. It also removes the complexities of having various tools across the organisation in turn meeting the productivity needs of IT teams by enhancing visibility of any risks and weaknesses in the business' network and maintaining control over users' access.

The two tools go hand in hand to provide enhanced security for organisations' endpoints. Vulnerability management can provide visibility to IT teams on the endpoints, which could cause a threat for the business and once identified can then be patched using patch management – mitigating the risk through a combined approach. By engaging in both vulnerability and patch management best practices, organisations can take a proactive approach to vulnerability remediation and access control to endpoints.

Cyber criminals continue to relentlessly identify any vulnerabilities and weaknesses in a business' network. The modern security landscape is more sophisticated and high risk than ever before, particularly with the rise of hybrid working. In order for organisations to keep its network protected and maintain access control, preserving a strong network security posture is crucial for survival. Two fundamental principles that must be considered as part of an endpoint protection strategy are both patch management and vulnerability management. These solutions – especially combined – will help ensure businesses are constantly vigilant of potential risks to its endpoints, and firmly close any open doors to cyber attacks ●

Andrea Babbs has worked in the IT Industry for over 20 years. During that time she has worked for IT Security Vendors and Resellers dealing with email, endpoint and web security. Andrea is currently Country Manager and Head of Sales for VIPRE Security Limited, where she manages the UK and Irish business.

More than half of UK firms believe remote working has left them open to cyber attacks