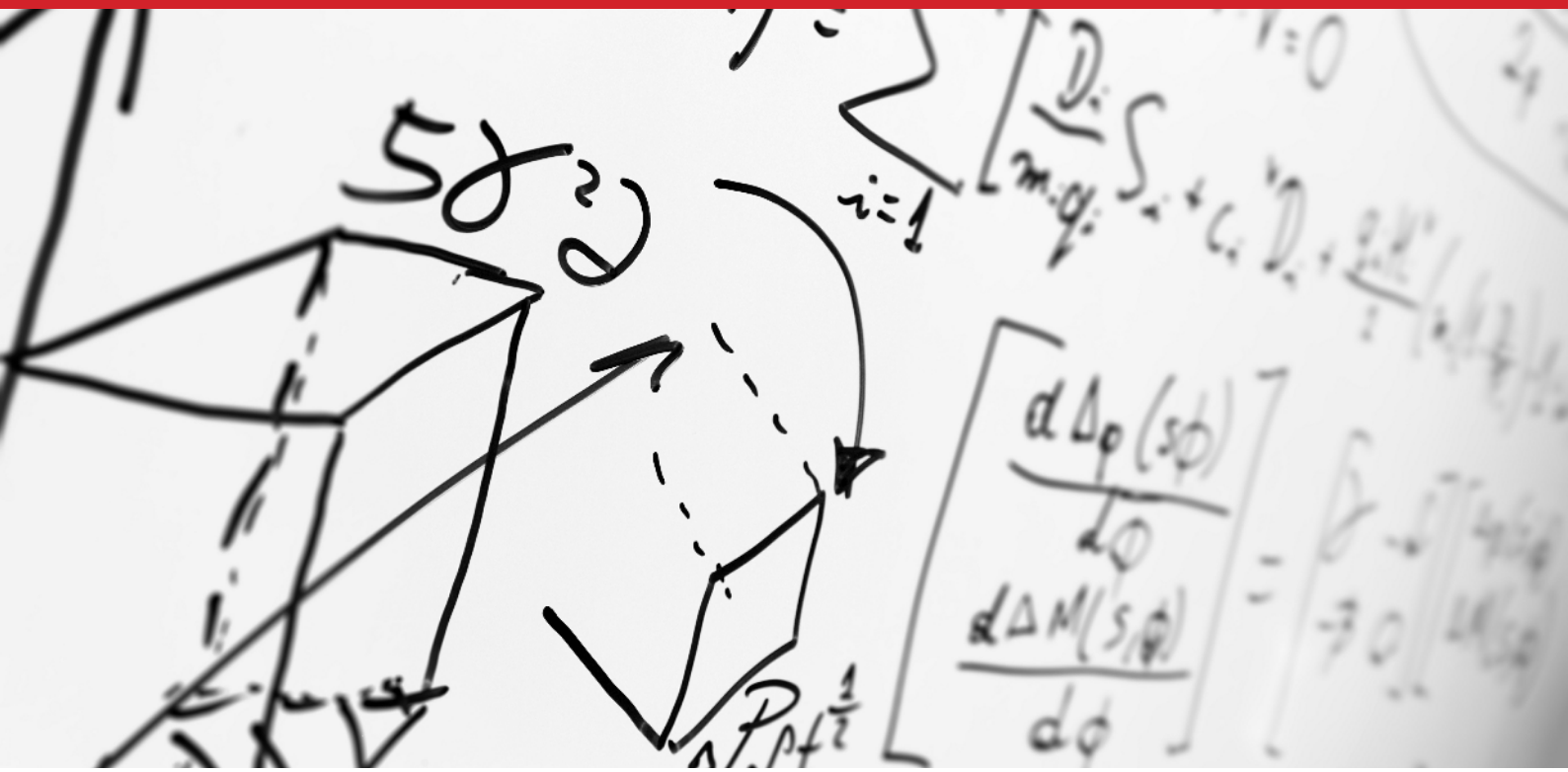
Leaving the Backdoor Open: Patch Management

Until recently, patch management was barely a consideration for many organisations. Instead, 'install and forget' was the common approach to deploying systems. In fact, many systems were rarely or never patched. Of course, the rise of cybercrime and myriad of threats has changed all that, or has it? Incredibly, 44% of security breaches occur after vulnerabilities have been identified and solutions found. A report by BMC and Forbes Insights found that many months often elapse before identified security vulnerabilities are fixed, leaving organisations needlessly exposed.

The devastating financial and reputational costs of a security breach are well documented. At the same time, the risk of a breach has increased exponentially. That's why patch management is now regarded as a critical part of an integrated defence strategy.

The Cost of Complexity

The rapid evolution of IT systems has meant increased complexity, more points of entry and a greater attack surface ripe for exploitation. Today's IT professionals must look beyond core systems, and safeguard enterprise business applications, remote sites, desktop operating systems and mobile devices. At the same time, businesses have become far more reliant on technology for everything. Even short periods of unplanned downtime can cause disproportionate harm.



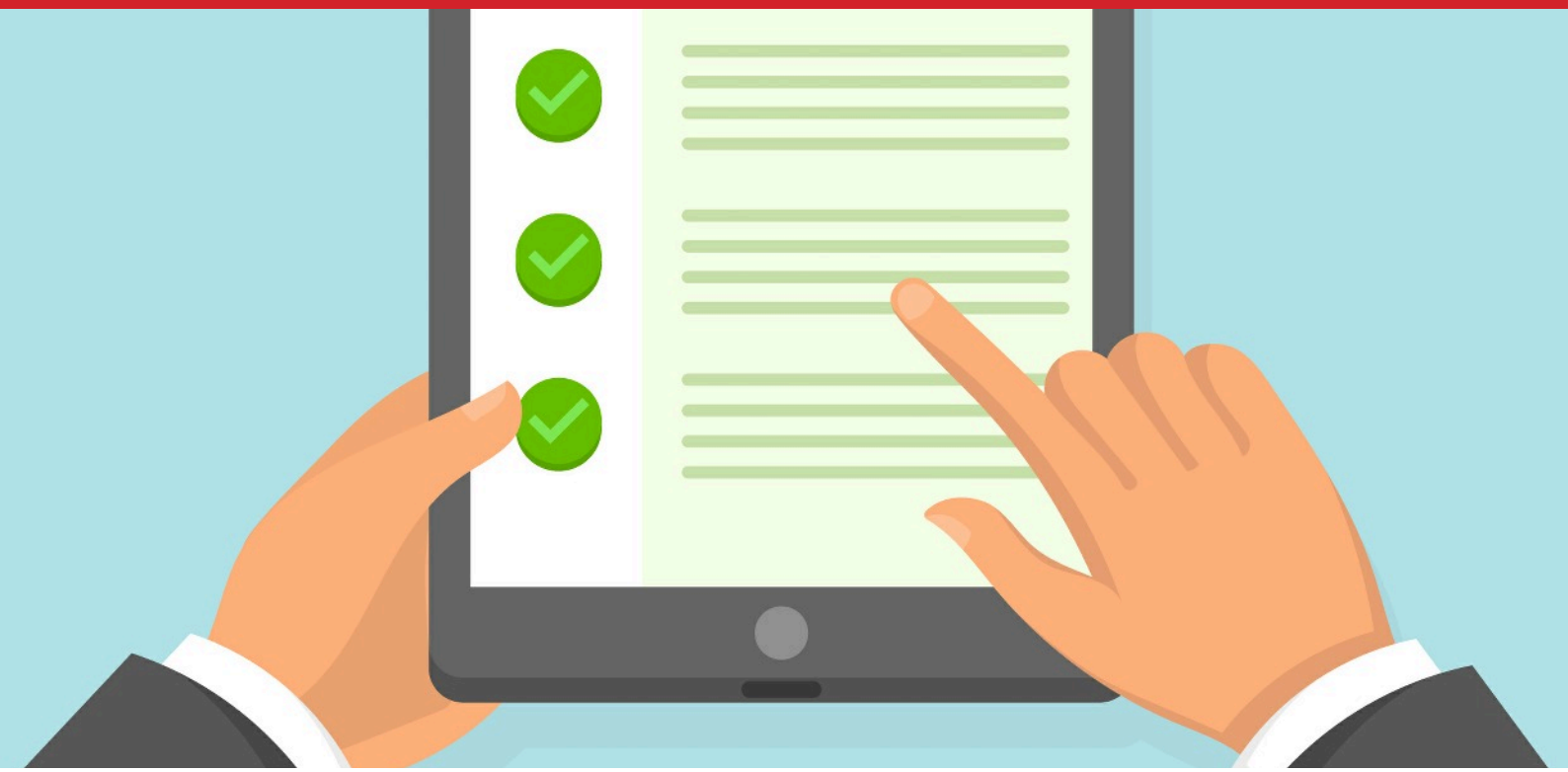
Erroneous Task

So, what does good patch management look like and how do you manage it? The key objective of a patch management program is to create a consistently configured environment that is secure against known vulnerabilities in all systems and applications. This sounds simple enough. However, in reality patch management can become a complicated, time-consuming and erroneous task, even for smaller businesses with limited IT infrastructure.

There are many software solutions available to help with patch management but this is only part of the solution. To be successful, patch management requires a combination of people, process and technology.

Where Are You Now?

At this point, many organisations turn to IT frameworks such as ITIL (Information Technology Infrastructure Library) to provide a structure and best practice for executing effective patch management. We would recommend you review your patch management strategy. Does it include the right components of people, process and technology? If not, then this is something you should tackle quickly before it becomes a bigger issue.



IT Audit

It might seem obvious, but a good place to start is by conducting an audit of all your IT systems and endpoints. You can only manage IT assets you know are part of your network, so understand what you have, where it's located, what operating systems and applications are running.

Rationalisation

You might want to think about standardising hardware and software choices, making everything easier to manage. You will also want a list of all the security controls you have in place. In this way, you'll know what requires attention when alerted of a vulnerability. You might also want to think about doing a risk assessment, so you can prioritise your workload.

Rationalising your IT will help make it more manageable, but replacing kit or applications because they're going end of life is seldom immediately necessary. Vendors typically continue support, security upgrades and patches for years. Once again, having the right people and processes in place will help you make informed decisions that support your business.

Patch Staging

When a patch becomes available, you should resist the urge to push it out across your network immediately. Sometimes, patching a system can have unforeseen consequences and cause

problems. Doing a quick Google search and checking IT forums, for example, can provide an early warning that something is wrong with a patch and offer possible solutions. We would recommend you adopt a patch staging process, whereby patches are applied gradually across your organisation rather than in one go.

Contact Us Now

If you would like any help or guidance, our UK service desk is ITIL aligned. We also provide comprehensive patch management solutions for our customers, removing the burden and enabling them to concentrate on doing business.

About Us

Modern Networks provides IT and telecoms managed services to over a thousand commercial properties and hundreds of enterprise clients. Our services including computing, enterprise anti-virus, business collaboration software, networking, infrastructure cabling, data backup, storage, VoIP telephony, WiFi, broadband and mobility solutions. All services are fully managed, continually monitored and expertly supported by our UK service desk.

Images courtesy of freepik.com and msteffen, flickr.com