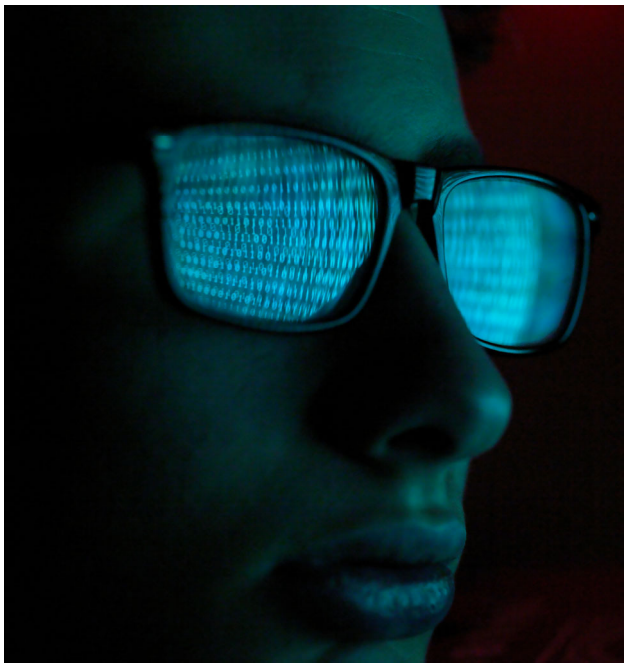
Cyber Security Update

PKF

Are you keeping pace with new and increasing Cyber Security threats in 2023?

As technologies advance, artificial intelligence develops, and algorithms become more complex it is not surprising that there is doubt from security executives that although legacy antivirus tools are still in widespread use as the main solution against computer virus attacks, whether they will hold up in the modern world and be able to deal with the increasing sophistication of malware and viruses.

Notably, the existing legacy antivirus software have been designed to recognise and deal with malicious code (which includes signature files) but the modern-day virus has become more covert in its entrenchment into systems and searches and utilises a 'zero-day vulnerability'. Notably, a 'zero-day vulnerability' is a vulnerability in a system's software (or the software of a device) that is known but is yet to be patched (updated to fix the security weakness). This is what modern viruses look for and there is growing concern that legacy antivirus software may not be able to deal with these types of threats.



Today an enormous amount of time is devoted by IT departments to administer and monitor signature-based anti-virus solutions (which are solutions which scan system files for evidence of malicious activity, typically monitoring inbound network traffic to find sequences and patterns that match a particular attack signature). Notably, on average it is estimated that an IT department will spend half a day every week doing nothing else but updating and patching (security) files to remove or reduce 'zero-based vulnerabilities'. And yet, only 8% of the IT security executives surveyed are confident that the legacy anti-virus solutions can detect and prevent modern malware threats.

As time moves forward, manually having to update and patch (security) files will be more and more time consuming and there is definitely a place to automate this process and' reduce the ground time'. There are concerns that if companies continue to manually perform this operation and it takes longer and longer to complete, that it could see them fall behind and be more susceptible to future virus threats.

Cyber Security Update

As time moves forward, manually having to update and patch (security) files will be more and more time consuming and there is definitely a place to automate this process and' reduce the ground time'. There are concerns that if companies continue to manually perform this operation and it takes longer and longer to complete, that it could see them fall behind and be more susceptible to future virus threats.

From the research conducted by Pulse (from 2020 to 2022), it found that updating and patching software by companies was not as complete as it had been in the past (which could reflect the increase sophistication of modern viruses and delivery method) and there was a fall in confidence from 81% to 65% that their current corporate anti-virus software was not adequate to deal with new threats.

It is expected that future applications and systems will respond to the 'zero-day vulnerability' and be developed using low-code solutions or machine learning where vulnerabilities in the software of systems and devices will be identified automatically and fixed.

PKF's Cyber Team based in Bangkok is confident that in the future, software for systems and devices with include next generation cyber security tools which will incorporate an element of automation to deal with modern virus threats. This will not only afford greater protection to a company's IT systems but significantly reduce the time that its IT department has to devote in ensuring the systems are adequately protected.