37:24_25.qxd 6/1/2018 11:18 PM Page 1

MAKING LIVES OF IT ADMINS EASY

ManageEngine's On-Cloud *Patch Management Plus* offering lends greater security depth and software efficiency to firms and organizations.

BY DIGITAL EDGE BUREAU

In quick succession WannaCry and GoldenEye strain of Petya ransomware wreaked havoc in the global digital space, which again proved how vulnerable firms and organizations have become to the nefarious designs of cyber criminals. The WannaCry attacks came to limelight when hospitals and specialty health clinics being run by UK's NHS (National Health Service) Trust came under huge ransomware attacks.

However, the attacks were not confined to UK alone; firms and organizations in over 150 countries became targets of the WannaCry ransomware epidemic. An estimated 300,000 computers were locked up across the globe. Using hacking tools named EternalBlue—which was originally developed by national security agency (NSA) for forensic purposes—cyber criminals unleashed one of the most pernicious ransomware attacks in recent times.

Upon detailed investigation, it was found that WannaCry ransomware exploited the vulnerability of un-patched Windows operating systems—including Windows 7, Windows XP, Windows 8, Windows 10, and Windows Server. However, computers running on Windows 7 and Windows XP were the most affected ones. The WannaCry advanced malware infected PCs running on Windows by locking users' files and data and demanding ransoms preferably in cryptocurrency. Microsoft urgently released patches which include updates for older versions of its operating systems. But the damage was already done.

One of the biggest takeaways for CIOs and IT administrators round the globe is that operating systems and other software applications must be patched with latest updates, which not only protect systems against cyber attacks, but also keep computers and servers running efficiently. Therefore, strong measures must be taken for updating software 'promptly' and 'on-time'. A miss can result in untold loss of data and reputation.

Yes, there may be many other reasons for cyberattacks, but an automated and centralized patch management system can prove to be mitigating the risk posed to organizations by ransomware attacks.

RAJESH GANESAN, DIRECTOR PRODUCT MANAGEMENT, MANAGEENGINE

The computer crime and intellectual property section (CCIPS) in its report corroborates that an average of over 4,000 ransomware attacks have happened every day since 2016. Many victims of ransomware have admitted that their failure to react and patch their computers and servers on time has made them fall prey.

ManageEngine brings solution

The Chennai-based ManageEngine, the real-time IT management division of Zoho Corporation, offers specific solution for automating patch management processes. The *Patch Manager Plus* is its flagship product that allows enterprises and organizations to keep their networks patched and effectively secured. Computers and servers can be patched from a single point of console. The *Patch Manager Plu*' supports all the major operating systems including Windows, Mac and Linux platforms. Also, ManageEngine offers patches to more than 250 third party software applications including Adobe and Java applications. For the company, India is a big and a very promising market for its *Patch Manager Plus* product. As the awareness around updating operating systems and other software applications grows, the company expects rapid rise in the demand of its flagship patch management solution. In the meantime, ManageEngine has introduced the cloud version of its *Patch Manager Plus* in the global as well as Indian market. The *Patch Manager Plus* on Cloud enables admins to automate the entire patch management process, from patch detection to deployment, without any infrastructure investment; thereby securing devices from multiple vulnerabilities and cyberattacks at less than a dollar per computer per month.

Interacting with Digital Edge, Rajesh Ganesan, Director of Product Management at ManageEngine, said, "With dynamics of digitalization fast changing and massive adoption of cloud technology, there is a greater need for automation in the endpoint management space, as endpoints are the major entry points of cyberattacks. ManageEngine's cloud-based patch management solution is engineered to meticulously look out for such threats".

The cloud version of *Patch Manager Plus* reduces the time and effort needed to deploy patches among the growing workforce on time thereby keeping the zero-day exploits and other vulnerabilities at bay. It also allows IT teams to remotely patch their servers, desktops, laptops and virtual machines from anywhere in the world.