Prevention First

Patch Management: Racing to win against cybercriminals

Digital Security
Progress. Protected.

According to the recent news in cybersecurity, numerous companies are **falling victim to both known and previously fixed vulnerabilities**. Recently, one of them suffered a data breach, affecting more than 30 million customers, that was connected with a software vulnerability that had been fixed just one week prior to the attack.

While negligence in cybersecurity is reprehensible, this blog won't be flogging companies forlate patching or for not taking security seriously enough. The truth is that applying patches across big enterprises, and even within smaller organizations, is not just about clicking a single button to upgrade everything; there's a lot more to it.

And the scale of this problem is huge. According to the latest Verizon Data Breach Investigations Report, exploitation of vulnerabilities is the third-most-used vector to access an organization.

The good news is that there are professional tools that can carry part of a business' burden by increasing the prevention mechanisms in its security strategy. Specifically, ESET Vulnerability & Patch Management (V&PM), a capability within our diverse ESET PROTECT Platform, uses an automated tool that detects vulnerabilities and applies the latest patches for apps and operating systems across all endpoints.

Facing Goliath

In general, companies worldwide take an average of between 82 and 208 days to patch vulnerabilities. When it comes to critical vulnerabilities, the situation is not much better: High-severity vulnerabilities still take 146 days to patch, on average.

And things are getting worse. In the United Kingdom, the number of businesses with patch management (policy application) software security updates executing within 14 days of patches being made available fell from 43% in 2021 to 31% in 2023, according to a survey conducted by the UK Department for Science, Innovation and Technology.

Here is a quick reminder of what a delayed patching task may cause:

- **Ransomware encrypting business data and demanding a ransom.**
- **Data breaches disclosing sensitive information about clients, employees, or business partners.**
- **Long-term persistence in accessing information about targeted business systems and activities.**
- **Severe cyber incidents that can lead to loss of customers' and business partners' trust.**
- **Delayed patching that also brings with it both compliance risks and insurance issues**

One of the key reasons why managers leave their companies vulnerable to preventable cyberattacks is that **patch management processes have become complex and time-consuming tasks**.

The 2022 Ponemon Institute report about the state of vulnerability management in DevSecOps found that 47% of security leaders have a backlog of applications that have been identified as vulnerable — it's like David facing Goliath.

More than 65% of those security leaders say their backlogs contain 100,000+ vulnerabilities, and **54% say they were able to patch less than 50% of them**.

And Goliath is only growing larger. In April 2023, MITRE ATT&CK's List of Common Vulnerabilities and Exposures (CVE) surpassed the 200,000+ records milestone, and, by the end of February 2024, the number had grown to more than 225,000.

Patching is anything but child's play

The barrage of vulnerabilities is not the only thing that businesses need to deal with. The sheer complexity of IT services and applications creates other challenges that are amplified by a growing number of employees doing their jobs remotely.

Variety of systems and applications gets too wide – **Businesses now run on multiple operating systems and third-party applications of different vendors**. This makes finding security gaps, and the applications of patches, more difficult.

There are more hybrid workers – Since the COVID-19 pandemic erupted, the number of hybrid workers has risen significantly. For example, in pre-COVID USA, 4.7 percent of employees were working from home at least once per week. In 2023, it was 28.2 percent. For companies, this means more Bring Your Own Device (BYOD) employees.

Applying patches is demanding – Before applying patches, businesses need to test for errors or side effects, and schedule deployments to avoid disruptions to internal workflows. After the patches are applied, the work is still not done. **IT admins need to monitor patch effectiveness**, check to see if all relevant devices are updated, and deal with post-deployment issues, if needed.

Patching needs to be prioritized – Because of a gargantuan number of published CVEs, released patches, and updates, companies need to assess risks and prioritize their patching.

Shortage of IT resources – With the increasing number of cyberattacks, CVEs, cloud computing, and remote work, the burden on IT teams is higher than ever. More than one-third of IT teams lack effective tools (43 percent) and resources (38 percent), according to a 2022 study.

Relieving the burden via automation

On the bright side, as IT is becoming increasingly complex, the **solutions helping to mitigate the burden on professionals are also becoming more comprehensive**. They can't solve everything, but they can give businesses a much-needed boost in the race over who will either patch or exploit a vulnerability first.

Here are some benefits of Automated V&PM:

- **Automated patching across all endpoints.**
- **Automated scanning of endpoints' software & third-party applications + instant reporting and visibility of vulnerabilities.**
- **Vulnerability reports of most vulnerable software and devices.**
- **Possibilities for configuring auto-patching, setting a patching strategy, and defining time slots for when patching should occur.**

ESET Vulnerability & Patch Management provides all of these. And what is more, businesses can manage their patching via ESET PROTECT, which centralizes and automates multiple IT security and management tasks to **decrease complexity of IT processes, especially addressing that backlog of vulnerabilities**.

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach, powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researcher**s. ESET protects your business so it can unlock the full potential of technology.

EXPLORE

ESET®

Digital Security
Progress. Protected.