datto | BUSINESS MANAGEMENT

RMM & Patch Management:

The First Line of Defense Against Cyberthreats

Cybersecurity has been a topic of discussion among IT professionals for quite some time, but a managed service provider's, or MSP's, responsibility to maintain secure environments has increased rather dramatically over the past decade as threats have become more commonplace.

Today's cybercriminals are continuing to leverage social engineering[1] emails as the top attack vector. According to the Anti-Phishing Work Group's[2] Q1-2019 report[3], the total number of phishing sites from Q4-2018 to Q1-2019 increased by 30%. In addition to the rise in phishing, ProofPoint's Q1-2019 Quarterly Threat Report[4] states emails with malicious URLs exceeded those with emails containing malicious attachments by 5 to 1 and are up 180% versus Q1-2018. Users are closer than ever to be within a single click from the threat. A single mistaken click on an email URL redirecting an unsuspecting user to a fake website will lead to executing code to exploit a vulnerability.

Security professionals all agree that a comprehensive security strategy is multi-faceted, incorporating perimeter hardening, end-user education, software patch management, and disaster recovery planning. It is also becoming more complex to proactively prevent attacks from occurring. Threats, like strains of ransomware, adapt as prevention measures mature and new technologies emerge making it difficult for businesses, especially smaller ones with limited resources, to remain ahead of the criminals.

However, the problem needs to be addressed head-on. As Gartner states, "Cybersecurity risk, if not treated appropriately, translates into business risk, reputation loss, regulatory breaches and general disruption of operations." The cost of disruption is too significant, and often orders of magnitude higher than prevention when responding to an event after it has occurred.

Technology vendors are doing their part to ensure vulnerabilities are fixed as quickly as possible, usually releasing an update within hours of learning about it. A well-documented case study on this is the WannaCry[5] outbreak of 2017. Microsoft learned of the vulnerability within the Windows Operating System on March 14, 2017, and released security bulletin MS17-010[6] that same day marked as CRITICAL. The global outbreak transpired two months later, compromising 230,000 computers in 150 countries in 24 hours. The malicious code that exploited the vulnerability fixed by Microsoft was in the wild for almost a month before the attack occurred. When the dust settled, there were at least 300,000 devices that had not received the critically flagged update from Microsoft.

High-profile attacks, like WannaCry, raise awareness among businesses and MSPs are often the ones looked to for providing the strategic guidance and tactical measures to secure the IT environments for their clients. To adequately do this, MSPs need to approach their client security engagements thoughtfully. Failure to do so may establish a false sense of security and potentially expose-clients to costly disruptions.

Getting Started with Patch Management Services

An MSP has the opportunity to build out a line of services that can be bundled or delivered à la carte. The types of services might include

- Vulnerability Assessments & Management
- Patch Assessments & Management
- Secure Configuration Assessments
- Application Security Testing
- Compliance Assessments & Management

According to Gartner, the goal of proper patch management services is, "to mitigate the risks of security breaches or performance issues by standardizing the patch management processes across the entire organization." The service may start by defining a baseline of compliance across the managed environment. From there, determine the minimum versions of required business applications that need to be in place and then identify the gaps and path to remediation. Spend adequate time to understand the risks associated with other business applications and what the contingency plan is if a patch is unable to be deployed or results in a disruption.

In many cases, the MSP will want to test your patches in a sandboxed environment, lab, or against a small population of risk-tolerant devices. Before deployment, MSPs should confirm their targets have verified backups, especially if they are devices vital to operations such as servers. Verify everyone involved understands the primary and contingency plans and is ready to respond if the deployment fails. Following the successful deployment, re-evaluate the environment and confirm compliance. Identify non-compliant anomalies and build a follow-up plan to remediate. The last stage is to report the results to stakeholders.

Building a service around patch management requires a combination of program process documentation and technology toolsets to deliver effectively. MSPs should position it to their clients as an on-going and comprehensive discipline, not a short-term project. All stakeholders should understand the frequency of updates, the targeted devices subject to receiving updates, and how to define and measure compliance.

Leveraging the power of a fully automated, policy-based platform, like Datto RMM[7], will position MSPs to systematically deploy patches for typical business applications as soon as they become available helping to close the window of exposure for known and zero-day vulnerabilities. Datto RMM will also generate easy-to-understand reports, bringing clear visibility to the sites and devices with the highest risk. Being able to have a conversation, backed by data, further establishes the MSP as a strategic partner who is proactively looking to prevent downtime and maintain the clients' best interests.

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

©2019 Datto, Inc. All rights reserved.

1. https://www.datto.com/blog/5-types-of-social-engineering-attacks
2. https://apwg.org/
3. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
4. https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q119-quarterly-threat-report-0528.pdf
5. https://www.datto.com/blog/why-are-ransomware-attacks-like-wannacry-so-effective
6. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
7. https://www.datto.com/business-management/datto-rmm