PERFECTING YOUR PATCH MANAGEMENT STRATEGY

On May 12th of 2017, WannaCry ransomware slammed into corporate networks and rapidly crippled 300,000 computers in more than 150 countries within 24 hours. Banks, hospitals and communications firms worldwide felt the shock.

Per organization, damages ranged from hundreds of millions to billions of dollars.

The WannaCry attack's effectiveness stems from the fact that it operates as a network worm. The majority of ransomware attacks do not propagate this way, making this attack particularly insidious.

However, the panic, chaos and damages of four years ago were largely preventable. Information technology and cyber security professionals had overlooked this one agenda item...

Patching. Although Microsoft had released patches for the EternalBlue exploit (which facilitated the propagation of WannaCry) many organizations had failed to update software with patches. Taking the time to patch could have prevented many a corporate crisis.

In many organizations, patch management processes are inefficient. Create a mature patch management strategy that can make your organization more agile, secure, and compliant. See the following patch management tips.

1 Educate and involve stakeholders.

Ensure that system owners understand organizational policies and procedures with respect to patching.

2 Leverage vulnerability scanning.

A strong threat management program should use vulnerability scanning to detect exploitable weaknesses within an organization's applications, endpoints and IT infrastructure. Automated scanning can help alert security teams to vulnerabilities quickly and can facilitate patching, if needed.

3 Pre-test patches.

Ahead of rollout, ensure that patches operate correctly and will not lead to disruption.

4 Automate management and deployment.

Reduce the need for manual updates. Develop a policy-based patch management approach that is configured to automatically install the appropriate patches upon administrative approval. All-in-one automated patch management and deployment e sure swift delivery and installation of patches across an enterprise.

Nearly 60% of cyber attack victims report that a patch would have prevented a cyber attack.

5 Invest in solutions that offer virtual patching.

Some firewall systems offer virtual patching with protections that are automatically updated every two hours. Virtual patching speeds time to protect new and zero-day vulnerability announcements.

This is important, as threat actors can quickly exploit vulnerable systems before patches are applied. Virtual patching can give staff more time to test a patch, notify users, and schedule down-time if needed for patch application.

6 Implement programs that can catch drift.

Drift occurs when patched devices receive new application installations that unexpectedly nullify initial patches. As a result, the devices are no longer secure, despite the logging of appropriate patching.

7 Consider lifecycle management.

Lifecycle management services can reduce provisioning and critical patching time by 90%.[1]

8 Post-test patches.

For organizations, testing patches can be time consuming. However, failure to test patches could lead to adverse consequences. While some systems will enforce testing requirements, consider automating your testing.

9 Have a strategy for isolating infected systems.

Further, perform regular backups of data and system configurations and include redundancy in your system designs.

Software isn't static.

Poor patch management practices can lead to damaging and embarrassingly easy to prevent cyber attacks. Follow the recommendations outlined above in order to help protect your environment.

For more business and cyber security insights, please visit CyberTalk.org.

[1] Check Point, Lifecycle Management Services, https://www.checkpoint.com/support-services/lifecycle-management/