CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER DEFENSE MEDIA GROUP
InfoSec Knowledge is Power

eMAGAZINE

Over 130+ Packed Pages This Month...

Sources of Majority of Breaches

Securing the IoT Supply Chain

Cloud Adoption Security Issues

Evolution of Enterprise Security

Privilege Security for the New Perimeter

What Recent Data Leaks Tell Us

Best Vulnerability Scanning Tools

...and much more...

CYBER DEFENSE GLOBAL AWARDS
CYBER DEFENSE MAGAZINE
2018
WINNERS

NOVEMBER 2018

MORE INSIDE!

One step closer to complete endpoint security

By Srinivasa Jagan, Product Analyst, ManageEngine

Hackers are making it tougher for IT security experts to safeguard every endpoint. Security enhancements have now assumed center stage, as attackers are working hard to sneak through security loopholes. The focus has moved away from attacking operating systems and has shifted to applications and mobile as well. Patching all vulnerable endpoints in a quick, easy and comprehensive manner is the best way forward to guard against cyberattacks and data thefts. Time, manpower and budget are important factors in these difficult times. As manual patching is no longer viable, IT managers should choose to automate their security to manage all third-party patches on priority.

Automated Patch Management

Prevention is always better than cure. Automated patching software eliminates human errors and delays and helps IT departments prevent vulnerabilities leading to malware attacks. In a typical IT environment such as that in a financial institution, individually patching thousands of connected computers would take too long despite hotfixes available in time. It is ideal to eliminate manual intervention and use an automated process to check for and automatically deploy critical new patches as they are released. Once the patch configuration policy is initiated, the security shield is always on.

Cloud-Based Patch Management

Adopting cloud-based architecture for automated patching brings several advantages. It eliminates the investment in infrastructure and the effort in managing the day-to-day detail. Cloud deployments are faster, lighter and also bring on-demand computation and enhanced storage. Having the right patch management software that is configured to support an exhaustive list of third-party applications, including all essential enterprise apps, is crucial.

Multi-Factor Authentication

While many organizations are moving from on-premise solutions to third-party cloud-based patch management, it is important to secure cloud resources. This is where multi-factor authentication (MFA) can help, especially when cloud applications and data are accessed by several users. MFA requires more than one parameter to log in, such as a one-time password, smart cards or biometric authentication. These additional layers help prevent a data breach and render brute-force attacks ineffective.

Capable and Alert Incident Response Team

A skilled incident response team brings an organized approach to remedy potential attacks after a security breach or when a vulnerability is discovered. The right incident response limits damages and restores normalcy when restricted data is accidentally spilled onto the public domain. Also, it is crucial to address all security incidents within 48 hours.

An incident response team should have an incident response team manager who delegates and prioritizes tasks when incidents happen. Cybersecurity experts then assess the damage level and act quickly to mitigate it. Threat researchers constantly monitor potential unauthorized access and work with the above teams to analyze past and present attacks to prepare for the future. Above all, incident teams should also have a complete alert system to spot any abnormalities and nip all problems in the bud.

Well-Defined Security Policies

Well-defined authorization policies are vital to prevent misuse of information. Therefore, assigning full read/write/audit access to multiple technicians and restricting unauthorized users, such as technicians, from accessing patch management should be done carefully. Companies should acquire an endpoint security solution that provides strong and secure access to a virtual private network (VPN), takes care of the client's firewall settings, and uses an agent to stop man-in-the-middle attacks. A strict VPN access policy prevents security breaches from outside attacks when laptops are lost or when a VPN is accidentally enabled to previous employees.

Awareness Increases Security

A recent IBM survey revealed that 60 percent of all cyberattacks are caused by insiders, often unintentionally, owing to a lack of awareness. All employees should be aware of security policies and issues and should be trained on security and privacy practices. Ease of use and advanced technology are also essential for robust patch management. Better usability minimizes errors and provides a smooth experience that improves productivity and efficiency. A mobile user interface or console will also help employees and administrators immediately be aware of and respond to any evidence of a cyberattack.

With too many endpoints and too little time, even the best IT pros struggle to keep up with troubleshooting. Enterprise endpoint security is the key to keeping your enterprise compliant and secure. This blend of user-friendly patch management solutions that goes hand-in-hand with a security-focused employee mind-set will free up IT teams to deal with other pressing needs. Adopting such technologies and practices will help organizations ensure their networks stay safe from all possible threats.

About the Author

Srinivasa Jagan is a product analyst at ManageEngine, a division of Zoho Corp. He brings a demonstrated history of working in the information technology and SaaS industries, and growing up with numbers and chess, he possesses a critical eye for detail. For more information on ManageEngine, the real-time IT management company, please visit www.manageengine.com;

follow the company blog at http://blogs.manageengine.com, on Facebook at http://www.facebook.com/ManageEngine and on Twitter at @ManageEngine.