Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

Patch Management

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Patch Management – Was ist das?

Patch Management ist ein Prozess im Bereich Cybersicherheit, der darauf abzielt, Sicherheitslücken und Schwachstellen in Software und Computersystemen zu **identifizieren** und zu **beheben**.
Dies geschieht durch das regelmäßige **Aktualisieren** von Software, Betriebssystemen und Anwendungen mit sogenannten Patches. Patches sind kleine **Software-Updates**, die Fehler beheben, die Leistung verbessern oder neue Funktionen hinzufügen.

Wie funktioniert Patch Management?

Der Patch-Management-Prozess beginnt normalerweise mit der **Überwachung** von Systemen und Anwendungen auf **verfügbare Updates** und Sicherheitspatches. Sobald ein Update verfügbar ist, wird es **getestet**, um sicherzustellen, dass es keine negativen Auswirkungen auf das bestehende System hat. Nach erfolgreicher Prüfung wird der Patch auf die betroffenen Systeme angewendet, um die **Sicherheitslücke zu schließen**.
Es gibt verschiedene Arten von Patch Management, die sich je nach Umfang, Automatisierungsgrad und Anwendungsgebiet unterscheiden:
Beim **manuellen Patch Management** werden Patches von IT-Administratoren oder Benutzern manuell heruntergeladen, getestet und auf die betroffenen Systeme angewendet. Manuelles Patch Management ist zeitintensiv und erfordert eine hohe Aufmerksamkeit, um sicherzustellen, dass alle relevanten Patches installiert werden. Dieser Ansatz ist bei kleineren Unternehmen oder Einzelpersonen häufiger anzutreffen, kann jedoch bei größeren Organisationen mit vielen Systemen und Anwendungen schnell unpraktisch werden.
Automatisierte Patch-Management-Systeme verwenden Software-Tools und -Lösungen, um den Prozess der Identifizierung, Installation und Überprüfung von Patches weitgehend zu automatisieren. Diese Systeme können Updates und Patches automatisch aus vertrauenswürdigen Quellen herunterladen, auf Kompatibilität testen und sie dann auf die betroffenen Systeme anwenden. Automatisiertes Patch Management ist effizienter und weniger fehleranfällig als manuelle Methoden, erfordert jedoch immer noch menschliche Überwachung, um sicherzustellen, dass die Automatisierung korrekt funktioniert und keine Probleme verursacht.
Bei **zentralisiertem Patch Management** werden Patches und Updates von einer zentralen Stelle innerhalb einer Organisation verwaltet und verteilt. Dies ermöglicht eine bessere Kontrolle und Überwachung des Patch-Management-Prozesses und gewährleistet, dass alle Systeme und Anwendungen konsistent und zeitnah aktualisiert werden. Zentralisiertes Patch Management kann sowohl manuell als auch automatisiert durchgeführt werden, wobei in größeren Organisationen meist eine Kombination aus beiden Ansätzen verwendet wird.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Chancen gibt es?

Patch Management hilft, Sicherheitslücken und Schwachstellen in Software und Computersystemen zu beheben. Durch das Schließen dieser Lücken wird das **Risiko von Cyberangriffen**, Datendiebstahl und anderen sicherheitsrelevanten Vorfällen **reduziert**.

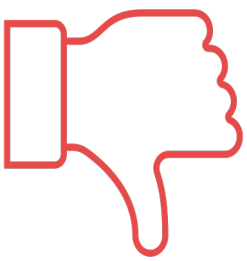
Patches beheben oft Schwachstellen, die von Malware wie Viren, Trojanern oder Ransomware ausgenutzt werden können. Durch die Aktualisierung von Systemen und Anwendungen wird das **Risiko einer Malware-Infektion verringert**. Patch Management trägt zur Stabilität und **Leistungsfähigkeit von Computersystemen** bei, indem es sicherstellt, dass bekannte Fehler und Probleme behoben werden. Dies führt zu weniger Systemabstürzen, Leistungsproblemen und Ausfallzeiten.

Ein proaktives Patch Management ermöglicht es Unternehmen, ihre **IT-Ressourcen effizienter einzusetzen**, indem es die Zeit reduziert, die für die Behebung von Sicherheitsproblemen und Systemausfällen aufgewendet wird.

Welche Risiken gibt es?

Manchmal kann ein Patch Probleme verursachen oder mit anderen Softwarekomponenten oder Systemen **inkompatibel** sein. Dies kann zu Systemabstürzen, Leistungsproblemen oder sogar Datenverlust führen. Daher ist es wichtig, Patches vor der Installation **sorgfältig zu testen** und zu überprüfen.

Bei manuellem Patch Management kann es zu **menschlichen Fehler**n kommen, z. B. wenn ein Patch übersehen oder falsch angewendet wird. Diese Fehler können zu Sicherheitslücken und Systemproblemen führen. Es kann vorkommen, dass für bestimmte Schwachstellen oder veraltete Software keine Patches verfügbar sind. In solchen Fällen müssen Unternehmen möglicherweise **zusätzliche Sicherheitsmaßnahmen** ergreifen oder auf alternative Lösungen umsteigen.



Wem nutzt Patch Management?

Ein strukturiertes Patch Management ist eine **Pflichtaufgabe** für Organisationen jeder Größe und Branche, da jedes Unternehmen, das Computersysteme, Netzwerke und Software verwendet, potenziellen Sicherheitsrisiken ausgesetzt ist. Die spezifische Vorgehensweise und die verwendeten Tools können jedoch **je nach Größe, Ressourcen und technischen Anforderungen** der Organisation variieren.

Manchmal kann die **Auslagerung** von Patch Management an externe Dienstleister eine praktikable Option für Unternehmen sein, die ihre IT-Sicherheit verbessern möchten, ohne die internen Ressourcen dafür aufzubringen. Bei der Auswahl eines Anbieters ist es wichtig, dessen Expertise, Sicherheitsmaßnahmen und Datenschutzrichtlinien sorgfältig zu prüfen, um eine effektive und sichere **Patch-Management-Strategie** zu gewährleisten.

Fazit

Ein umfassendes Patch Management allein garantiert keine vollständige Sicherheit. Unternehmen müssen weiterhin **proaktive Sicherheitsmaßnahmen** ergreifen und sich auf **mehrere Verteidigungsebenen** verlassen, um einen umfassenden Schutz zu gewährleisten.

Um Cybersicherheitsrisiken zu minimieren, sollte Patch Management als Teil eines umfassenden Sicherheitsansatzes betrachtet werden, der auch andere Schutzmaßnahmen wie Firewalls, Intrusion Detection und Prevention Systeme sowie regelmäßige Sicherheitsüberprüfungen umfasst.