WatchGuard

Schwachstellen- und Patch-Management

watchguard.com

Inhaltsverzeichnis

WatchGuard

Die Bedeutung des Patch-Managements in Unternehmen

Software-Patches sind für IT-Administratoren in der Regel sehr lästig. Ihre Priorisierung und Bereitstellung ist eine zeitraubende Aufgabe, nicht nur für sie, sondern auch für die Anwender. Computer und Server müssen oft neu gestartet werden, was mit Arbeitsunterbrechungen einhergeht. Updates werden daher häufig aufgeschoben und empfohlene Patches ignoriert. Was wie eine harmlose Aktion aussieht, kann jedoch für Unternehmen schwerwiegende Folgen haben.

Ebenso können IT-Administratoren nur mit größten Mühen gewährleisten, dass auf allen Systemen in ihrem Netzwerk die notwendigen Patches installiert sind. Software-Patches und -Updates sind unverzichtbar, wenn es darum geht, die Cybersicherheit eines Unternehmens zu gewährleisten, da sie verhindern, dass Software und Systeme anfällig für Sicherheitsbedrohungen sind.

WatchGuard®

Schwachstellen in Zahlen

Im Jahr 2020 wurden insgesamt 18.103 Schwachstellen (durchschnittlich 50 CVEs Tag) von Sicherheitsexperten, -forschern und -anbietern gemeldet.[1] Angesichts dieser Zahl überrascht es kaum, dass Unternehmen mit begrenzten IT-Ressourcen große Schwierigkeiten haben, ihre Infrastruktur zu warten und zu schützen.

Patch-Management kann viel Zeit und Ressourcen in Anspruch nehmen. Häufig ist es keine leichte Aufgabe, die eigenen Geräte und Anwendungen zu überblicken, Patches zu priorisieren und Programme und Systeme, selbst die kritischen, zeitnah zu patchen. Unternehmen müssen Patches so effizient wie möglich verwalten können, da sie sonst ihre Produktivität und ihre Cybersicherheit massiv beeinträchtigen könnten.

24,1 Prozent[2] der Schwachstellen entfallen auf fünf Unternehmen: Software in the Public Interest (SPI), SUSE, Oracle, IBM und Microsoft.

Die meistbenutzten Anwendungen von Drittanbietern sind das Hauptziel für Hacker. Laut dem Common Vulnerabilities and Exposures (CVE)[3]-Index weisen Anwendungen wie Java, Adobe, Google Chrome, Mozilla Firefox und OpenOffice die höchste Anzahl an Schwachstellen auf. Es ist daher zu wenig, Betriebssysteme einfach nur zu patchen.

Man sollte auch die Tatsache berücksichtigen, dass es immer mehr Angreifer gibt, die über die notwendige Kompetenz verfügen, Schwachstellen schneller aufzuspüren. Haben sie diese entdeckt, setzen sie Programme zur Automatisierung der Ausnutzung dieser neuen Schwachstellen ein, die weit verbreitet werden und manchmal sogar viral gehen. Das Ergebnis dieser Verknüpfung aus Bedrohungen, Schwachstellen und Konsequenzen stellt ein erhebliches Risiko für Unternehmen dar. Doch so überraschend es sein mag, es sind nicht die unentdeckten Schwachstellen, die die größte Gefahr darstellen.

Quellen:
1. SCMagazine – Vulnerabilities hit record high in 2020, topping 18,000
2. Cybersecurity alert – TechRepublic
3. attack.mitre.org – MITRE

Bekannte Schwachstellen, Hochrisiko-Schwachstellen

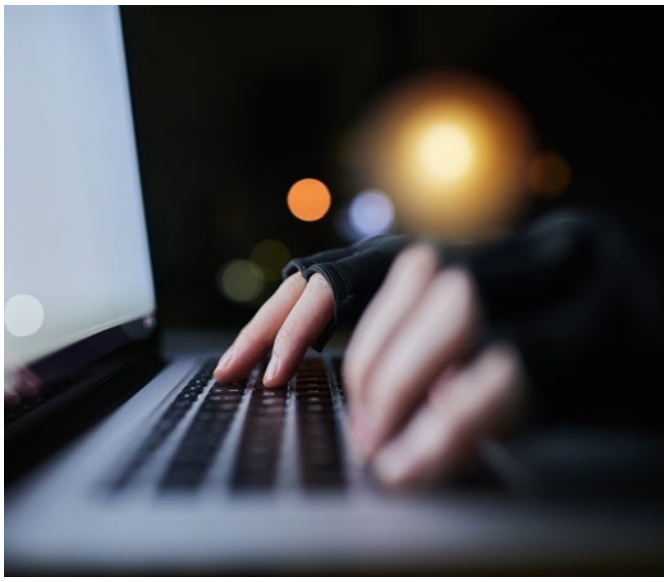
Derzeit ist die Ausnutzung von Schwachstellen weiterhin die häufigste Ursache der meisten Sicherheitsverletzungen. Bekannte Fälle wie WannaCry, Petya und BlueKeep, die weltweit für Chaos sorgten, sind noch in aller Munde. Nur wenige Angriffe erfolgen aufgrund tatsächlich unbekannter Schwachstellen (Zero-Day-Angriffe), die meisten sind auf bekannte Schwachstellen zurückzuführen.

Im vergangenen Jahr haben Hacker typischerweise bekannte und behobene Schwachstellen für den Zugriff auf nicht gepatchte Systeme ausgenutzt, wobei viele von diesen Schwachstellen in den letzten zwei Jahren bekannt wurden.[4] Dagegen waren in letzten zehn Jahren nur etwa 0,4 Prozent der Schwachstellen Zero-Day-Schwachstellen.

Man sollte sich vor Augen führen, dass Hacker für die Durchführung ihrer Angriffe auch Zugang zu öffentlichen Exploits haben. Sie zögern nicht, diese auszunutzen, da sie genau wissen, dass die meisten Unternehmen ihre Systeme nicht patchen. Tatsächlich nutzen 80 Prozent der erfolgreichen Angriffe Schwachstellen aus, für die es bekannte Patches gibt, die nicht angewendet wurden.

Vor diesem Hintergrund ist klar, dass Unternehmen ihre Anstrengungen auf die Kontrolle und Minimierung bekannter Schwachstellen konzentrieren sollten, die immer wieder ausgenutzt werden; sie stellen ein größeres, realeres Risiko dar als sonstige Arten von Bedrohungen.

Die Zeitspanne zwischen dem Bekanntwerden einer Schwachstelle und ihrer Ausnutzung hat sich ebenfalls erheblich verkürzt. Unternehmen müssen daher gegen die Zeit arbeiten, um Patches zu installieren, bevor Cyberkriminelle ihre Systeme über eine Reihe von Angriffsvektoren gefährden können.



57 Prozent der Opfer von Cyberangriffen sagen, die Anwendung eines Patches hätte den Angriff verhindert. 34 Prozent geben an, vor den Cyberangriffen von der Schwachstelle gewusst zu haben.[5]

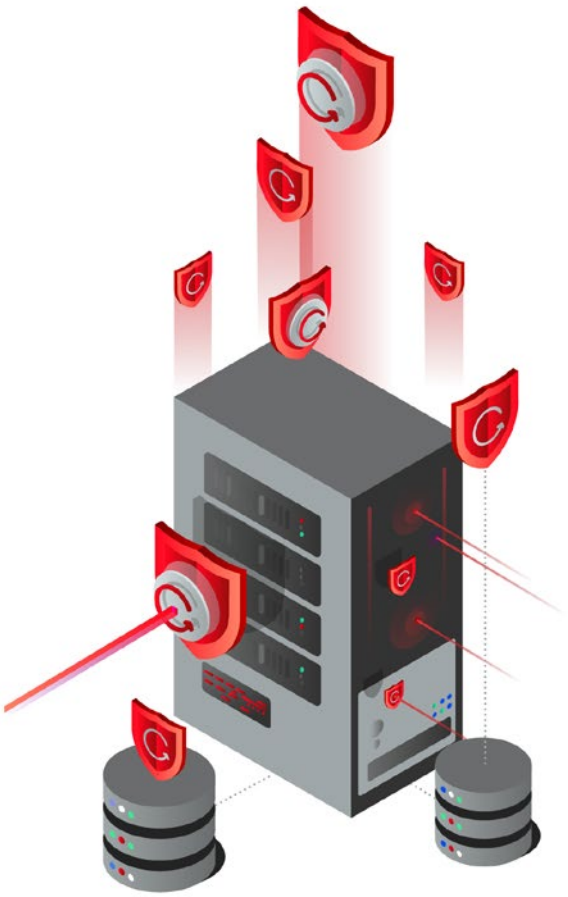
Quellen:
4. Cybersecurity & Infrastructure Security Agency – CISA
5. Cost and consequences of gaps in vulnerability response – Ponemon

WatchGuard

Patch-Management

A) WAS PATCH-MANAGEMENT BEDEUTET

Dieser Begriff bezeichnet den Prozess, bei dem Unternehmen, genauer gesagt deren IT-Abteilungen, Patches (Änderungen im Code oder in den Daten) herunterladen und installieren. Sie optimieren und sichern damit Software, Computer, Server und Systeme. Das Ziel ist die Gewährleistung der Funktionsfähigkeit dieser Komponenten. Gleichzeitig sollen Sicherheitslücken minimiert werden. Wenngleich dies eine einfache Aufgabe zu sein scheint, können die meisten Unternehmen nur mit Mühe erkennen, welche kritischen Patch-Updates sie zuerst installieren müssen. Daher ist die Priorisierung von Patches für Administratoren entscheidend. Tatsächlich dauert es laut Ponemon im Durchschnitt 97 Tage, bis Unternehmen Anwendungen oder Systeme patchen.[6] Die durchschnittliche Zeit bis zu einem Cyberangriff nach der Veröffentlichung eines Patches für eine kritische Sicherheitslücke beträgt jedoch 43 Tage,[7] d. h. es besteht eine durchschnittliche Risikolücke von 59 Tagen.



Quellen:
6. State of Endpoint security risk 2020 – Ponemon
7. Cost and consequences of gaps in vulnerability response – Ponemon

WatchGuard

B) WELCHE ARTEN VON PATCHES GIBT ES?

Es gibt verschiedene Arten von Patches, und jede von ihnen dient einem bestimmten Zweck: der Korrektur eines Fehlers oder der Behebung einer konkreten Sicherheitslücke. Hier einige Beispiele: Hotfix, Service-Patches, Wartungsversionen, Monkey Patches usw.

In diesem Dokument konzentrieren wir uns auf die beiden Arten, die unserer Ansicht nach am wichtigsten sind, da sie kritische Sicherheitslücken beheben sollen, die häufig das Ziel von Angreifern sind. Sie sind somit für Unternehmen und Sicherheitsexperten von größter Relevanz.

- **Sicherheitspatches wirken sich sowohl auf Betriebssysteme als auch auf Drittanbietersoftware aus:** Ein Sicherheitspatch ist eine Änderung, die an einer Anwendung oder einem Programm vorgenommen wird, um Bugs oder Fehler zu beheben, die Sicherheitslücken verursachen. Die Anwendung dieser Art von Patch verhindert die Ausnutzung von Schwachstellen. Ferner sorgt sie dafür, dass Bedrohungen Schwachstellen in einem Gerät gar nicht mehr, oder nur noch in geringem Maße, missbrauchen können. Patch-Management ist Teil des Schwachstellen-Managements: die zyklische Praxis der Identifizierung, Klassifizierung, Behebung und Abschwächung von Schwachstellen (Sicherheitsrisiken).

- **Service Pack (SP) oder Feature Pack (FP):** Dies sind wichtige Patches, die eine Sammlung von Updates, Korrekturen oder Funktionserweiterungen für eine Software umfassen. Sie lösen in der Regel viele anstehende Probleme und enthalten gewöhnlich alle Patches, Hotfixes, Wartungs- und Sicherheitspatches, die vor dem Service Pack veröffentlicht wurden.

C) WELCHEN ZWECK HABEN PATCHES?

Patches sollen Schwachstellen oder Sicherheitslücken beheben, die nach dem Start einer Anwendung oder eines Softwareprodukts festgestellt wurden.

Ungepatchte Software kann alle Endpunkte für Exploits anfällig machen und damit Hackern eine großartige Gelegenheit bieten, erfolgreich Angriffe zu starten. Software-Patches sind für Administratoren und Sicherheitsexperten ein wichtiger Bestandteil ihrer Tätigkeiten.

Im technologischen Bereich und speziell im Softwarebereich kommt es häufig vor, dass eine Anwendung, nachdem sie einmal auf den Markt gekommen ist, repariert oder sogar modifiziert werden muss. Es ist daher eine gute Idee, einen Prozess zu entwickeln, der dem Software-Lebenszyklus ähnelt, bei dem verschiedene Phasen festgelegt werden. So hat man die Möglichkeit zur Analyse, Bewertung und regelmäßigen Anwendung von Patches, um eventuell auftretende Probleme zu lösen.

Lebenszyklus des Patch-Managements

Das Patch-Management kann das wirksamste Werkzeug zum Schutz Ihres Unternehmens vor Sicherheitslücken und das am wenigsten kostspielige sein, sofern es effizient implementiert wird. In diesem Abschnitt erläutern wir, wie Sie ein routinemäßiges Patch-Management-Verfahren einführen. Ihr Ziel sollte es sein, dieses in den Standardbetrieb Ihres Unternehmens zu integrieren. Dieser Zyklus oder dieses Verfahren ist in sechs Phasen gegliedert[8]:

Identifizierung von Geräten und Basissoftware

Die Identifizierung von Geräten und der darauf installierten Basissoftware sowie deren Patch-Level ist eine komplexe Aufgabe, die jedoch sowohl die Sicherheit als auch die Betriebsfähigkeit verbessert. Mit einer solchen Basis können Sie Änderungen am System ohne Risiken vornehmen und haben die Möglichkeit, zu einem früheren bekannten Funktionszustand zurückzukehren, falls bei der Installation eines Updates oder Patches ein Problem auftritt.

Verfügbarkeit:

Die aktuelle Liste der Patches muss auf der Grundlage des Inventars der Geräte und der Software überprüft werden, um festzustellen, von welchem Patch diese jeweils betroffen sind.

Anwendbarkeit:

Patches, die veröffentlicht werden, sind nicht immer für alle Geräte gültig. Daher sollten Sie unbedingt prüfen, ob ein bestimmtes Update für die Geräte in Ihrem Prozess geeignet ist.

Beschaffung:

Es ist nicht immer einfach, die Update-Datei von einer offiziellen Quelle zu erhalten und zu überprüfen, ob der Patch legitim ist. Die Verwendung von Hashes ist bei Patches, die sich auf Steuersysteme beziehen, nicht üblich.

Validierung:

Die Validierung dient der Sicherstellung, dass das Update keine negativen Auswirkungen auf den Prozess haben wird. Um den Patch oder das Update zu validieren, müssen nach den Rollout-Phasen Test-Assets eingesetzt werden. Mit der Validierung soll geprüft werden, welche Auswirkungen das Update haben könnte, z. B. Änderungen an Firewall-Richtlinien, Einstellungsänderungen usw.

Rollout:

Im Validierungsprozess muss ein Rollout-Paket erstellt werden. Das Paket muss die Aktualisierungsdateien und Installationsanweisungen sowie eine Liste der Geräte enthalten, bei denen das Rollout durchgeführt werden soll.

WatchGuard

Quellen:
8. Patch management in control systems – INCIBE-CERT

Schützen Sie Ihre IT-Infrastruktur mit WatchGuard Patch Management vor bekannten Schwachstellen

WatchGuard Patch Management ist eine Lösung, die den komplexen Patch-Management-Lebenszyklus für Betriebssysteme und Drittanbietersoftware vereinfacht. Infolgedessen wird die Angriffsfläche verringert und die Fähigkeit zur Verhinderung und Eindämmung von Vorfällen, die durch Systemschwachstellen verursacht werden, verbessert.

Die Lösung ist in die Endpoint-Security-Lösungen von WatchGuard integriert, d. h. es werden keine neuen Agents oder Management-Konsolen benötigt. Sie bietet zentralisierte Echtzeit-Einblicke in den Status von Schwachstellen, Patches, ausstehende Updates und nicht mehr unterstützte bzw. End-of-Life(EOL)-Software auf Computern und Servern sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks. Mit den enthaltenen Management-Tools können Sie die Erkennung, Planung, Installation und das Monitoring der kritischen Patches und Updates, die Ihr Unternehmen benötigt, automatisieren – alles in Echtzeit und in einem einfachen, intuitiven Format.

Wichtige Vorteile und Funktionen von WatchGuard Patch Management

- Prüfung, Überwachung und Priorisierung von Updates für Betriebssysteme und Anwendungen. Sie können den Status ausstehender Patches und Updates für das System und Hunderte von Drittanbieteranwendungen anzeigen und sogar Patches zurücksetzen.
- Verhinderung von Vorfällen durch systematische Reduzierung der durch Schwachstellen verursachten Angriffsfläche. Die Verwaltung von Patches und Updates ermöglicht es Ihnen, Schwachstellen vorzubeugen.
- Eindämmen und Entschärfen von Angriffen, die Schwachstellen ausnutzen, sofortige Anwendung kritischer Updates von der Cloud-Konsole aus. Die Konsole korreliert Funde mit Schwachstellen und minimiert so die Reaktions-, Eindämmungs- und Behebungszeit, indem Updates bei Bedarf von der Konsole aus angewendet werden. Darüber hinaus können Sie über die Konsole betroffene Computer vom Netzwerk isolieren und sowohl reale als auch potenzielle Angriffe eindämmen.
- Reduzierung von Betriebskosten, da keine Agent-Implementierungen oder Updates auf Endpoints notwendig sind. Daraus folgt eine Vereinfachung der Verwaltung ohne Überlastung der Computer oder Server. Minimierung des Aufwands für Remote-Updates über die Cloud-Konsole. Sofortige, automatische Visualisierung von Sicherheitslücken, Updates und EOL-Anwendungen.

WatchGuard

Das Patch-Management ist ein Prozess, der regelmäßig durchgeführt werden muss und so umfassend wie möglich sein sollte, um effektiv zu sein. Allerdings sollten nicht alle Systeme gleich behandelt werden; jedes Unternehmen muss seine Anlagen priorisieren und sicherstellen, dass die kritischsten zuerst geschützt werden.

Gleichzeitig muss garantiert werden, dass Patches auf allen Rechnern installiert werden und nicht nur auf den für das Unternehmen wertvollsten oder wichtigsten. Darüber hinaus machen Patches nicht nur einen Arbeitsaufwand seitens der Systemadministratoren nötig, sondern erfordern möglicherweise auch die Unterstützung des Unternehmens, um ein bestimmtes Wartungsfenster zu vereinbaren.

Angriffsschutz

Adaptive Sicherheitsarchitektur

Vorhersagen/Vorwegnehmen

Entdeckung von Sicherheitslücken, ausstehenden Patches und Updates sowie EOL-Anwendungen

Prävention

Automatisierte Patch-Zeitpläne und Austausch von EOL-Anwendungen

Reaktion

Patching aller anfälligen Endpoints

Erkennen und eindämmen

Eindämmung von Angriffen durch Patching in Echtzeit

WatchGuard®

Erfahren Sie, wie WatchGuard Patch Management Ihnen helfen kann, das Schwachstellenmanagement durch die Optimierung von Updates und Sicherheitspatches zu vereinfachen.

Weitere Informationen finden Sie auf unsere Website

WatchGuard

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB www.watchguard.com/de