WatchGuard

Vermeiden Sie verborgene Schwachstellen in Ihrem Netzwerk

watchguard.de

Inhaltsverzeichnis:

WatchGuard

Die Bedeutung des Patch-Managements in Unternehmen

Software-Patch-Management kann für Unternehmen und IT-Sicherheitsteams ein echtes Problem sein. Der Prozess der Identifizierung, Priorisierung und Bereitstellung von Updates beansprucht oft wertvolle Zeit und Ressourcen. Nicht nur IT-Teams stehen vor Herausforderungen, sondern auch Endanwender erleben Unterbrechungen, wenn Updates einen Neustart des Systems erfordern, was ihren Workflow stört. Infolgedessen werden viele Updates hinausgeschoben und kritische Patches übersehen, wodurch das Unternehmen anfällig für Sicherheitsbedrohungen wird.

Die Verschleppung von Patches ist jedoch mehr als nur eine kleine Unannehmlichkeit sondern stellt ein erhebliches Sicherheitsrisiko dar. Patches sind entscheidend, um Sicherheitslücken zu schließen, potenzielle Angriffe abzuwehren und die Einhaltung von Branchenvorschriften zu gewährleisten. Ohne eine solide Patch-Management-Strategie sind Unternehmen sehr anfällig gegenüber Schwachstellen, wodurch das Risiko von Cyberangriffen steigt. Um eine sichere, konforme und widerstandsfähige IT-Infrastruktur zu fördern, ist es wichtig, Patches zeitnah durchzuführen.

WatchGuard®

Schwachstellen in Zahlen

Die NVD (U. S. National Vulnerability Database) verzeichnete im Jahr 2023 insgesamt 28.831 Schwachstellen[1], gegenüber 25.081 im Jahr 2022, was einer durchschnittlichen Rate von 77 CVEs (Common Vulnerabilities and Exposures) pro Tag entspricht, die von Sicherheitsexperten, Forschern und Anbietern dokumentiert wurden. 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.

Die Analyse der Verteilung von Software-Schwachstellen in großen Unternehmen zeigt, dass Microsoft, Google und Apple zu den am stärksten betroffenen Anbietern gehören. Zwischen 2021 und 2022 entfielen mit 60 von 246 dokumentierten Fällen rund 24 % der ausgenutzten Sicherheitslücken auf Microsoft. Es folgen Google und Apple, die mit 30 bzw. 29 Fällen jeweils für etwa 12 % der ausgenutzten Sicherheitslücken verantwortlich sind.[2]

Die meistbenutzten Anwendungen von Drittanbietern sind das Hauptziel für Hacker. Etwa 45 %[3] der kritischen Common Vulnerabilities and Exposures (CVEs) wurden nicht gepatcht. Anwendungen wie Google Chrome, Mozilla Firefox, Microsoft Office, Apache, VMware, ERP-Systeme (SAP, Oracle) und Atlassian[4] sind häufige Ziele. Daher reicht es nicht aus, nur die Betriebssysteme 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 dann weiter 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.

WatchGuard

Quellen:
1. The National Vulnerability Database (NVD)
2. Google - Analysis of Time-to-Exploit Trends
3. Help Net Security - 45% of critical CVEs left unpatched in 2023
4. CISA - Top Routinely Exploited Vulnerabilities

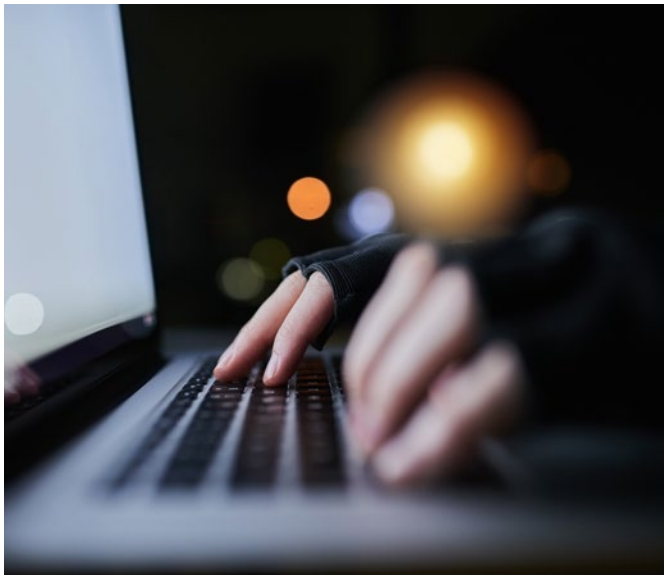
Bekannte Schwachstellen, Schwachstellen mit hohem Risiko

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.

In den letzten Jahren haben Cyberkriminelle in erster Linie ältere Software-Schwachstellen ausgenutzt und sich insbesondere auf ungepatchte, internetfähige Systeme konzentriert. Diese Cyberkriminellen erzielen in der Regel den größten Erfolg mit bekannten Schwachstellen innerhalb der ersten zwei Jahre nach ihrer Offenlegung, da die Wirksamkeit dieser Schwachstellen tendenziell abnimmt, sobald die Systeme aktualisiert werden.

Das rechtzeitige Patchen von Software kann bösartige Aktivitäten erheblich stören und Angreifer dazu zwingen, komplexere Strategien zu nutzen, wie die Entwicklung von Zero-Day Exploits. Darüber hinaus priorisieren diese Angreifer häufig weit verbreitete und schwerwiegende CVEs (Common Vulnerabilities and Exposures), da sie kostengünstige und wirkungsvolle Möglichkeiten für die Ausnutzung von Schwachstellen bieten. Tatsächlich stellte die Cybersecurity and Infrastructure Security Agency (CISA) fest, dass Kriminelle im Jahr 2022 häufig ältere, nicht gepatchte Software-Schwachstellen ausnutzten, von denen einige seit über zwei Jahren bekannt sind.

In Anbetracht dieser Tatsachen ist es klar, dass Unternehmen ihre Bemühungen auf die Kontrolle und Abschwächung bekannter Schwachstellen konzentrieren sollten, die immer wieder ausgenutzt werden und eine größere und realere Gefahr darstellen als andere 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 % der Opfer von Cyberangriffen sagen, die Anwendung eines Patches hätte den Angriff verhindert. 34 % geben an, vor den Cyberangriffen von der Schwachstelle gewusst zu haben.[5]

Quellen:
5. Cost and consequences of gaps in vulnerability response – Ponemon

Lebenszyklus einer Schwachstelle

Zeitfenster zum Ausnutzen von Schwachstellen:

Der „Zeitpunkt des Exploits“ bezieht sich auf das früheste Datum, an dem ein Exploit für eine bestimmte Schwachstelle verfügbar wird. Ein Exploit umfasst alle Hacker-Tools, Viren, Daten oder Befehlssequenzen, die entwickelt wurden, um diese Sicherheitslücke auszunutzen.

Schwachstelle entdeckt:

Der Entdeckungszeitpunkt bezieht sich auf das früheste Datum, an dem eine Schwachstelle als Sicherheitsrisiko identifiziert wird. Dieses Datum bleibt der Öffentlichkeit unbekannt, bis die Schwachstelle offiziell bekannt gegeben wird.

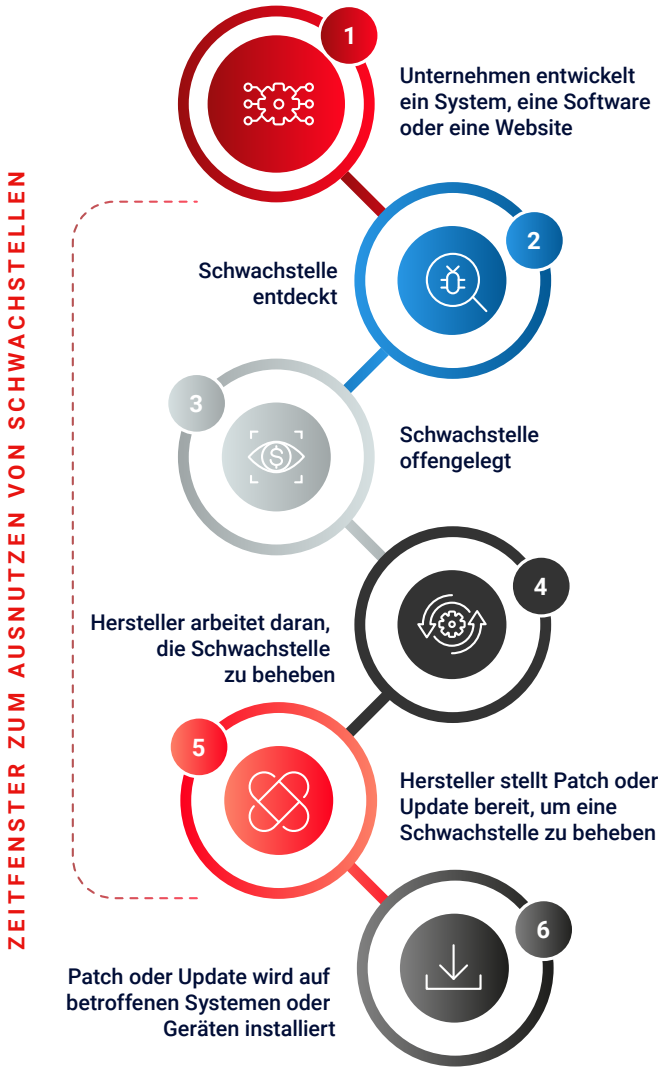
Schwachstelle offengelegt:

Den meisten Unternehmen fällt es schwer, alle Sicherheitsquellen für neue Bedrohungen zu verfolgen. Daher sind sie auf spezialisierte Anbieter angewiesen, die ihnen klare und detaillierte Informationen über Schwachstellen geben. Der Zeitpunkt der Offenlegung ist das erste Datum, an dem eine Schwachstelle öffentlich in einer vertrauenswürdigen, unabhängigen Quelle diskutiert wird, auf die jeder zugreifen kann.

Patching:

Der Zeitpunkt, an dem ein Patch verfügbar wird, ist das früheste Datum, an dem der Softwareanbieter einen Fix, eine Zwischenlösung oder einen Patch veröffentlicht, um Schutz vor der Ausnutzung der Schwachstelle zu bieten. Leider werden Patches oft erst veröffentlicht, nachdem die Schwachstelle veröffentlich worden ist.

Der Lebenszyklus einer Schwachstelle besteht aus verschiedenen Phasen, die jeweils einen Zustand und die damit verbundene Risikoexposition darstellen.[6]



Quellen:
6. Research Gate: 0-Day Patch Exposing Vendors (In)security Performance

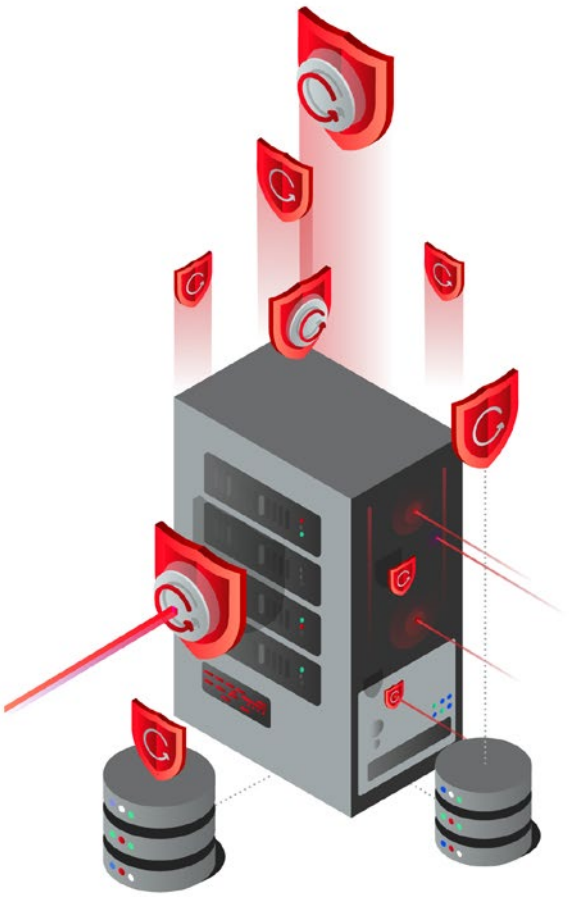
Patch-Management

A / WAS PATCH-MANAGEMENT BEDEUTET

Unternehmen, insbesondere ihre IT-Abteilungen, verwenden einen bestimmten Prozess, um Patches – Code- oder Datenänderungen – herunterzuladen und zu installieren, die Software, Computer, Server und Systeme aktualisieren, optimieren oder schützen sollen. Ziel ist es, die korrekte Funktion dieser Komponenten zu gewährleisten und eventuelle Sicherheitslücken zu schließen.

Obwohl dies eine einfache Aufgabe zu sein scheint, stehen viele Unternehmen vor Herausforderungen bei der Bestimmung, welche kritischen Patch-Updates für die Installation priorisiert werden sollten. Daher ist die Priorisierung von Patches für Administratoren unerlässlich.

Sicherheitskennzahlen können nützlich sein, um die Effektivität einer Sicherheitsstrategie zu bewerten. Beispielsweise liegt die durchschnittliche Zeit für das Patchen einer Schwachstelle – bekannt als Mean Time to Patch (MTTP) – zwischen 60 und 150 Tagen. Darüber hinaus benötigen Sicherheits- und IT-Teams in der Regel mindestens 38 Tage, um einen Patch bereitzustellen.[7] Diese Verzögerung stellt eine große Chance für Cyberkriminelle dar, Zero-Day-Schwachstellen auszunutzen.



Quellen:
7. Infosec - Time to patch: Vulnerabilities exploited in under five minutes?

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 Patches 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 Bereich der Technologie, insbesondere bei Software, sind für Anwendungen oft auch nach dem Start Korrekturen oder Updates erforderlich. Aus diesem Grund ist ein strukturierter Prozess, ähnlich einem Software-Lebenszyklus, mit definierten Phasen für Analyse, Test, Validierung und regelmäßige Patch-Anwendung, unerlässlich. Durch diesen Ansatz wird sichergestellt, dass Probleme zeitnah und effektiv angegangen werden, wodurch die Software sicher, stabil und auf dem neuesten Stand bleibt.

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 fünf Phasen unterteilt.[8]

Identifizierung und Bestandsaufnahme:

Beginnen Sie mit der Identifizierung und Auflistung aller Ressourcen innerhalb der Netzwerkinfrastruktur eines Unternehmens. Dieser Prozess umfasst eine detaillierte Bestandsaufnahme von Servern, Workstations, Netzwerkgeräten und Softwareanwendungen, einschließlich ihrer aktuellen Patch-Level. Diese Aufgabe kann zwar komplex sein, erhöht jedoch die Sicherheit und Bedienbarkeit erheblich und schafft eine Grundlage für die nachfolgenden Phasen.

Entdeckung und Bewertung:

Im nächsten Schritt werden automatisierte Tools und Technologien zur Durchführung von Schwachstellenscans eingesetzt, um potenzielle Schwachstellen und Sicherheitslücken in den Netzwerkressourcen zu identifizieren. Tools zur Schwachstellenbewertung suchen systematisch nach bekannten Schwachstellen in Betriebssystemen und Softwareanwendungen sowie nach anderen Problemen, die von Kriminellen ausgenutzt werden könnten. Während der Bewertung ist das Risiko jeder identifizierten Schwachstelle zu evaluieren, indem der Schweregrad und die potenziellen Auswirkungen auf den Unternehmensbetrieb und die Daten untersucht werden. Priorisieren Sie das Patchen je nach Schweregrad und ordnen Sie die Schwachstellen anhand der CVSS-Skala unter Berücksichtigung ihrer Wichtigkeit, Ausnutzbarkeit und der möglichen Auswirkungen auf Ihre Geschäfte.

Quellen:

8. A Practical Methodology for Implementing a Patch Management Process- SANS Institute

Planung und Tests:

Die Zeit von der Erkennung der Schwachstelle bis zur Ausnutzung hat sich verkürzt und IT-Teams unter Druck gesetzt, Produktionssysteme schnell zu patchen und gleichzeitig hohe Verfügbarkeit und Qualitätstests sicherzustellen. Sobald Sie geplant haben, welche Patches wann aufgespielt werden sollen, beginnt die Patch-Testphase, die auf repräsentativen Computern und nicht auf kritischen Systemen wie Servern mit sensiblen Daten durchgeführt werden sollte. Dieser Ansatz trägt dazu bei, eine reibungslose Bereitstellung über andere Systeme hinweg zu gewährleisten und das Risiko von Unterbrechungen wichtiger Abläufe zu minimieren.

Abhilfe und Schadensminderung:

Eine rechtzeitige Behebung ist unerlässlich, um das Zeitfenster für Angreifer zu minimieren. Konfigurieren Sie bei der Anwendung von Patches die Kritikalität der Software und planen Sie eine Aufgabe zur Patch-Verteilung (Datum/Uhrzeit) für die sofortige oder regelmäßige Ausführung. Steuern Sie auch Neustarts von Computern und legen Sie Ausnahmen außerhalb der Stoßzeiten fest. Wenn keine sofortigen Maßnahmen möglich sind, sollten Sie Abhilfestrategien in Betracht ziehen, wie das Isolieren von Computern, das Deinstallieren von Patches (Rollback) oder das Implementieren zusätzlicher Sicherheitskontrollen, während nach einer dauerhaften Lösung gesucht wird.

Monitoring und Reporting:

Das Patchen einer Schwachstelle bedeutet nicht unbedingt, dass sie behoben ist. Diese Phase erfordert eine sorgfältige Kontrolle, um sicherzustellen, dass Schwachstellen nicht mehr ausgenutzt werden können und keine Nebenwirkungen auftreten. Ein gutes Tool für das Schwachstellenmanagement sollte alle Aktivitäten und Ergebnisse dokumentieren und eine historische Referenz schaffen, die bei Compliance-Audits hilft. Entscheidend für eine effektive Kommunikation ist auch die regelmäßige Berichterstattung. Berichte sollten identifizierte Schwachstellen, ihren Schweregrad, Minderungsstrategien und Ihre allgemeine Sicherheitslage zusammenfassen. Dieser fortlaufende Prozess betont die kontinuierliche Verbesserung, um die sich entwickelnde Bedrohungslandschaft anzugehen und die Wirksamkeit Ihres Sicherheitsprogramms zu bewerten.

Entdecken und schließen Sie Lücken in Ihrer Sicherheit

WatchGuard Patch Management ist eine Lösung, die den komplexen Patch-Management-Lebenszyklus für Betriebssysteme von Windows, macOS und Linux sowie für 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.
- Einhaltung von Vorschriften wie PCI DSS, HIPAA oder der DSGVO, die regelmäßige Patches erfordern. Identifizieren und verfolgen Sie, wie viele Geräte in Ihrem Netzwerk konform sind, und überwachen Sie, welche Computer erfolgreich gepatcht wurden und deren Updates aktuell sind, um sie vor Cyberbedrohungen zu schützen und gesetzliche Vorgaben mühelos zu erfüllen.

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.

Reduzierung der Angriffsfläche

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.

Patchen Sie Ihre Systeme noch heute!

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

Teilenr. WGCE67452_111424