TeamViewer
Remote Management

WHITEPAPER

Verpassen Sie nie wieder einen Patch:

Reduzieren Sie Sicherheitsrisiken und schützen Sie Ihre IT-Infrastruktur mit automatisiertem Patch-Management

Inhaltsverzeichnis

Einführung:
Was ist eine Patch Management Lösung?

Damit Ihre IT-Infrastruktur stabil und sicher bleibt, sind regelmäßige Wartungen und rechtzeitige Updates für alle Computer und Geräte erforderlich. Wenn Sie es versäumen, Ihre Computer und Geräte zu aktualisieren, kann dies aufgrund veralteter Software zu erheblichen Sicherheitslücken führen.

IT-Organisationen stehen vor neuen Herausforderungen, wenn es darum geht, sicherzustellen, dass die Geräte immer auf dem neuesten Stand sind oder „gepatcht" werden, da die Zahl der Unternehmensgeräte, In der IT-Welt bezeichnet ein Patch eine Software oder eine Anwendung, die aktualisiert, optimiert oder von Fehlern korrigiert wurde und mittels eines Softwareupdates den Usern zur Verfügung gestellt wird. Um die Verfügbarkeit von Patches gezielt zu überwachen und vorhandene Patches zu installieren, ist eine effiziente Patch Management Lösung notwendig.

Mit einer Patch-Management-Lösung können Sie veraltete, anfällige Software erkennen und patchen.

Patching ist daher ein wesentlicher Bestandteil der IT-Sicherheit. Ohne sie werden Sicherheitsmängel niemals behoben werden, so dass Hackern oder Cyberkriminellen die Möglichkeit offen bleibt, Unternehmensdaten zu stehlen. Laut einer Studie des NIST sind 90 Prozent der erfolgreichen Angriffe auf Unternehmen auf bekannte Schwachstellen zurückzuführen und hätten durch korrekte und rechtzeitige Patches verhindert werden können.[1]

Bedeutung von Patch Management für Unternehmen

Cyber-Angriffe durch Malware können einen erheblichen Schaden für Unternehmen mit sich bringen. Datenverluste, Image-Schäden oder Produktionsausfälle kosten Unternehmen Millionen. Dabei steigt die Anzahl der Malware Varianten fast täglich an. Deshalb ist ein effizientes Sicherheitsmanagement der ITInfrastruktur notwendig.

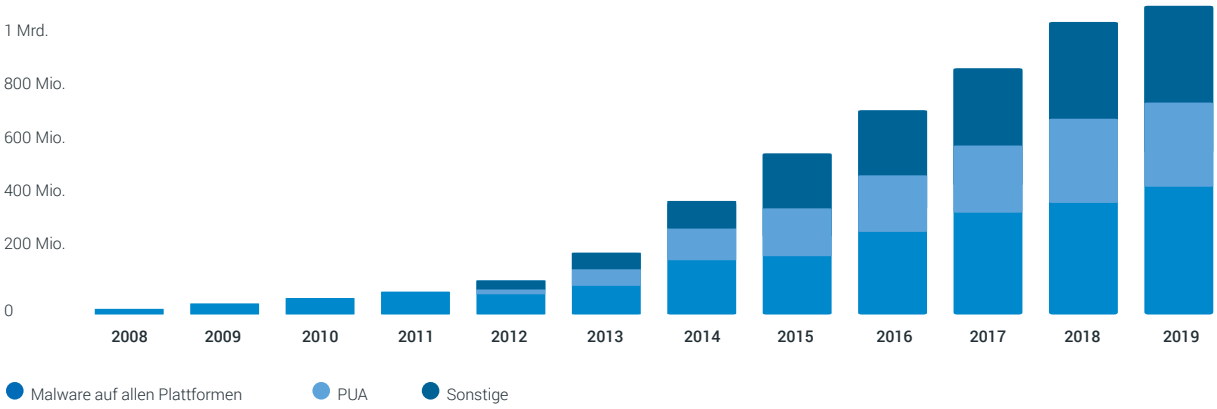

Abbildung 1: Gesamtzahl der bekannten Malware-Varianten *PUA (potentially unwanted application: Anwendungssoftware, die nicht eindeutig als Malware klassifiziert werden kann))[2]

Cyber-Angriffe wie z.B. im Jahr 2017 durch die Ransomware WannaCry, zeigen immer wieder, wie wichtig es ist seine Hard- und Software vor Angriffen zu schützen. Da heutzutage alle Systeme und Anwendungen großer Unternehmen über das Internet laufen, ist es für Kriminelle ein leichtes sich Eingang zu verschaffen. Dabei zeigen Erfahrungswerte das eine Antiviren-Software allein nicht ausreicht die IT-Infrastruktur vollkommen zu schützen. Denn Software beinhaltet Schwachstellen, da mit steigender Komplexität der Software Fehler in der Entwicklung unterlaufen.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) gab bekannt, dass „erfolgreiche Angriffe häufig auf Angriffe über unbekannte Schwachstellen und mangelndes Patch-Management zurückzuführen sind“[3], da die Anzahl kritischer Schwachstellen in IT-Standardprodukten in den letzten Jahren stark zugenommen hat.

Allein 2017 gab es mehr als 450 bekannte Sicherheitslücken, bei den 10 bekanntesten Anwendungen. Laut BSI, gibt es keine Anzeichen, dass sich die Lage in den nächsten Jahren ändern wird. 12.174 Sicherheitslücken wurden 2019 in den Top 50 der meisten genutzten Softwareprodukten verifiziert[4]

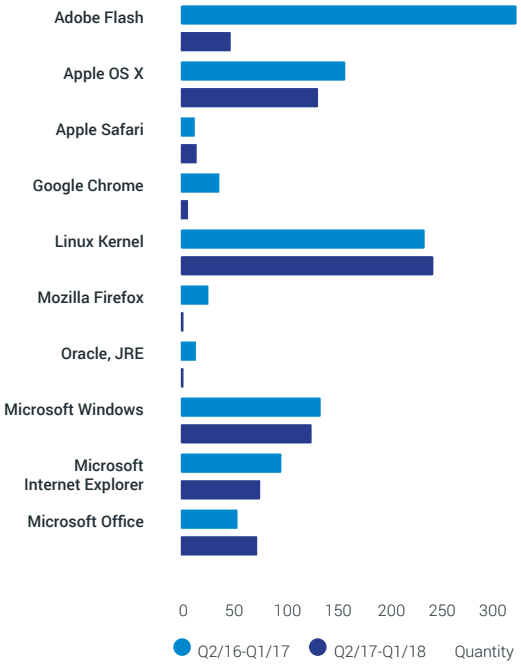

Abbildung 2: Kritische CVE-Einträge, Stand 31.03.2018 [5]

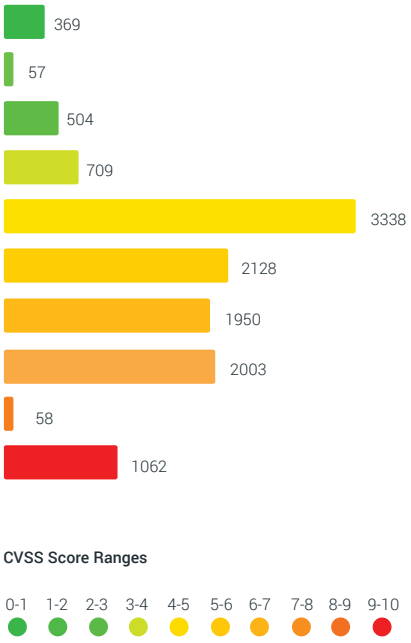

Abbildung 3: Verteilung der Sicherheitslücken im Jahr 2019 zum 30.10.19. Von unkritisch (grün) bis kritisch (rot) der TOP 50 [4]

90% der ausgenutzten Schwachstellen treten innerhalb von 40-60 Tagen nach der Veröffentlichung der Software auf. Dabei ist es die Aufgabe der IT-Administratoren schnell zu handeln. Der Patch muss bereitgestellt, getestet und ausgerollt werden. Dies ist für IT-Administratoren nicht nur ein enormer Zeitaufwand, sondern es ist auch ein nicht zu vernachlässigender Kostenfaktor.

Mit der Zunahme des Volumens der Schwachstellen ist das manuelle Patchen mühsamer und weniger praktikabel geworden, da es regelmäßig durchgeführt werden muss, um sicherzugehen, dass alle Geräte tatsächlich erfolgreich gepatcht wurden. Manuelle Patching-Prozesse erfordern auch manuelle Folgeprozesse, was die Zeit und die Ressourcen der IT-Administratoren zusätzlich belastet.

Wenn es sich um einen manuellen Patching-Prozess handelt, kann es je nach Komplexität des Systems notwendig sein, sich bei der Implementierung der Patches auf die Endbenutzer zu verlassen. Dies wirkt sich in der Regel auf den Erfolg der Patch-Implementierung aus.

Das Patchen der Server-Seite ist relativ einfach, weil die IT die volle Kontrolle darüber hat, aber auf der Client-Seite treten die meisten Schwachstellen auf (~95 Prozent), und es ist schwierig, die Clients auf dem neuesten Stand zu halten. Logistische Probleme kommen ebenso in die Quere wie der menschliche Faktor; die Leute verzögern Patches, weil sie ihre Arbeit nicht unterbrechen wollen. Aus diesen Gründen wird beim Patchen oft nachlässig agiert, denn obwohl Patches oft seit langem verfügbar sind, werden sie aus Zeit- und Kostengründen nie implementiert. Wenn hier jedoch nicht richtig gepatcht wird, spielt das Cyber-Kriminellen in die Hände und Schwachstellen werden systematisch ausgenutzt.

Durch diese Schwachstellen kann es also zu schwerwiegenden Sicherheitslücken in einer Anwendung oder einem IT-System kommen. Deshalb stehen Unternehmen heute vor der großen Herausforderung, ihre ITInfrastruktur besser zu organisieren und zu verwalten. Hier ist Patch Management die optimale Lösung, ITAdministratoren zu entlasten und die Performance, Effizienz und Effektivität der IT-Infrastruktur zu steigern. Denn eine effiziente Patch Management Lösung untersucht welche Patches für die Systeme am besten geeignet sind, automatisiert das Verteilen und Ausrollen der Patches und stuft sie nach Dringlichkeit ein. Patch Management führt demnach nicht nur zu einer besseren Patch-Bereitstellung, sondern minimiert auch manuelle Schritte und verringert das Risiko menschlicher Fehler.

Risiken eines schlechten Patch-Managements

Kostspielige Systemausfallzeiten

Verlorene Glaubwürdigkeit bei Kunden

Lange Sanierungszeiten

Fragwürdige Datenintegrität

Negative PR

Unsichere IT-Umgebung

Vorteile von Patch Management

Das regelmäßige und automatisierte Patchen erhöht die Sicherheit der IT-Systeme und die Integrität von Netzwerken erheblich. Dies ist der offensichtlichste Vorteil von Patch Management. Jedoch bring eine effiziente Patch Management Lösung noch weitere wichtige Vorteile mit sich, die für Unternehmen von Nutzen sein können.

Steigerung der IT-Produktivität und Reduzierung ungeplanter Ausfallzeiten

Die manuelle Patch-Verwaltung ist für IT-Administratoren sehr zeitaufwändig. Die Identifizierung von Schwachstellen, die Feststellung, welche Endpunkte Patches benötigen, und schließlich deren Rollout und die Sicherstellung, dass die Patches ordnungsgemäß auf die betroffenen Computer und Laptops angewendet wurden, nimmt viel Zeit und Ressourcen in Anspruch.

Darüber hinaus verursacht dies ungeplante Ausfallzeiten für Mitarbeiter, die Zugang zu ihren Geräten benötigen. Eine automatisierte Patch-Management-Lösung hilft daher nicht nur den IT-Mitarbeitern effizienter zu arbeiten sondern minimiert auch ungeplante Ausfallzeiten für Mitarbeiter.

Ermöglicht Sicherheit und Daten-Compliance zur Risikominimierung

IT-Compliance schützt Unternehmen vor Strafen oder potenziellen Imageschäden. Risiken entstehen dabei u.a. durch Sicherheitslücken und können z.B. Datenschutz-Richtlinien verletzen indem Mitarbeiter- oder Kundendaten offengelegt werden.

Das hat oftmals Kundenabwanderungen oder negative Publicity zu Folge. Eine effektive Patch-Strategie wirkt diesen Risiken entgegen und sorgt für Vertraulichkeit als auch für Integrität.

Vorteile

Schnelle und lückenlose Aktualisierung der Systeme

Automatische Anwendung von Patches zur Behebung von Software-Schwachstellen

Computer zentral verwalten

Steigerung der Mitarbeiterproduktivität

Detailliertes netzwerkübergreifendes Reporting

Überblick über den Zustand der Systeme

Reduzierung der Ausfallzeiten

Minderung von Sicherheits- und Compliance-Risiken

Features

Identifizieren Sie Schwachstellen

Erhalten Sie vollständige Transparenz in Ihrem Netzwerk, indem Sie automatisch Schwachstellen aufgrund veralteter Software erkennen.

Schneller Rollout, integriert in TeamViewer

Stellen Sie Patch Management mit nur wenigen Klicks in Ihrem gesamten Netzwerk bereit.

Automatische Patch Bereitstellung

Erkennen und verteilen Sie automatisch richtlinienbasierte Patches für veraltete, anfällige Software, Betriebssysteme und Anwendungen von Drittanbietern, um Ihre IT-Infrastruktur sicher und aktuell zu halten.

TeamViewer Patch Management Lösung

Das Patchen von Endpunkten kann Ihr gesamtes Netzwerk vor Cyber-Angreifern schützen. Aber wussten Sie, dass nur ein einziges ungepatchtes Gerät Ihre gesamte IT-Infrastruktur gefährdet?

Mit der Patch Management-Lösung von TeamViewer Remote Management werden **Schwachstellen automatisch erkannt,** so dass Sie jedes Gerät auf dem neuesten Stand halten und sicher patchen können.

Schützen Sie Ihre IT-Netzwerke mit Patch Management von TeamViewer

Behalten Sie mit der automatisierten Patch-Management-Lösung den Überblick über kritische Patches. Erkennen Sie sofort, ob Updates verfügbar sind, und stellen Sie diese von einer zentralen Plattform aus bereit.

Verwalten und verteilen Sie Windows-Updates von einem zentralen Dashboard aus und stellen Sie so sicher, dass alle Ihre Windows-Geräte auf dem neuesten Stand sind.

Reduzieren Sie Risiken, überwachen und verteilen Sie automatisch Patches für Anwendungen und Betriebssystem-Updates von Drittanbietern.

Zeigen Sie den Patch-Status Ihrer Geräte und alle verfügbaren Patches in einem einzigen Dashboard an.Dashboard an.

Definieren Sie individuelle Richtlinien für verschiedene Abteilungen oder Kunden, um Patching-Aufgaben anzupassen und zu automatisieren.

Erkennen Sie, welche Patches kritisch oder dringend sind oder verschoben werden können, indem Sie sie nach Priorität sortieren.

Verwalten und überprüfen Sie Ihre Patches aus der Ferne, von überall her. Die nahtlose Integration zwischen TeamViewer Remote Management und TeamViewer Remote Access ermöglicht es Ihnen, bei Bedarf mit nur wenigen Klicks auf Geräte zuzugreifen.

Zusammenfassung

IT-Sicherheitsfachleute wissen, dass sie ihre Unternehmen kontinuierlich vor Cyber-Kriminellen schützen müssen. Dabei sind sie sich einig das eine effiziente Patch Management Lösung ein wichtiger Bestandteil der Endgerätsicherheit ist. Lassen Sie die Hintertür zu Ihren Netzwerken nicht für Cyber-Angreifer offen. Patch Management ist wichtig und muss nicht kompliziert sein.

Die benutzerfreundlichen Funktionen von Patch Management by TeamViewer ermöglicht es Ihnen, Ihre ITSysteme proaktiv zu schützen und die Sicherheit und Integrität Ihrer Netzwerke zu erhöhen.

Weitere Infos

Fordern Sie eine kostenlose Demoversion von TeamViewer Remote Management an (einschließlich Patch Management).

Weitere Informationen finden Sie unter teamviewer.com/patchmanagement

Beginnen Sie mit einer kostenlosen Testversion von Patch Management

Verweise

1. Nationales Institut für Standards und Technologie (November 2019): Automatisierungsunterstützung für Sicherheitskontrollbewertungen: Management von Software-Sicherheitslücken, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8011-4-draft.pdf
2. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=F64FE0EE50A281C976D952B395DCD531.2_cid369?__blob=publicationFile&v=5 S.11
4. CVE-Details (2019): Aktuelle CVSS-Punkteverteilung für alle Sicherheitslücken, https://www.cvedetails.com/cvss-score-distribution.php
5. Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3 page. 43
6. CVE-Details (2019): Sicherheitslücken nach Datum, https://www.cvedetails.com/browse-by-date.php

Über TeamViewer

Als führende globale Fernverbindungsplattform ermöglicht es TeamViewer den Benutzern, jeden, alles, überall und jederzeit zu verbinden. TeamViewer bietet sicheren Fernzugriff, Support, Kontrolle und Kollaborationsmöglichkeiten für Online-Endgeräte aller Art und unterstützt Unternehmen jeder Größe dabei, ihr digitales Potenzial voll auszuschöpfen. TeamViewer wurde bereits auf rund 2 Milliarden Geräten aktiviert; bis zu 45 Millionen Geräte sind gleichzeitig online. TeamViewer wurde 2005 in Göppingen, Deutschland, gegründet und ist ein börsennotiertes Unternehmen, das an der Frankfurter Börse notiert ist und rund 800 Mitarbeiter in Niederlassungen in Europa, den USA und im asiatisch-pazifischen Raum beschäftigt.

www.teamviewer.com