Herausforderungen bei der Patch-Verwaltung

Umfrageergebnisse und Einblicke bei der Umstellung von Unternehmen auf den „Everywhere Workplace“

Einführung

Heutige Arbeitsumgebungen sind nicht mehr auf einen geschlossenen Raum beschränkt, in dem IT-gesteuerte PC-Arbeitsplätze das Zentrum der Produktivität sind. Unternehmen sind heute verteilter als je zuvor, was zu größeren Angriffsflächen führt. Am „Everywhere Workplace“ greifen Mitarbeiter mit verschiedenen Geräten auf Unternehmensnetzwerke, -daten und -dienste zu, während sie von neuen und anderen Standorten aus arbeiten und zusammenarbeiten, so dass das Patchen noch nie eine größere Herausforderung war.

In der Zwischenzeit haben IT- und Sicherheitsteams Mühe, die sich ständig erweiternde Landschaft der Remote-Arbeit unter Kontrolle zu halten. Es ist notwendig, den neuen Online-Arbeitsplatz sicher und mit den neuesten Sicherheitspatches auf dem aktuellen Stand zu halten, aber es wird immer schwieriger.

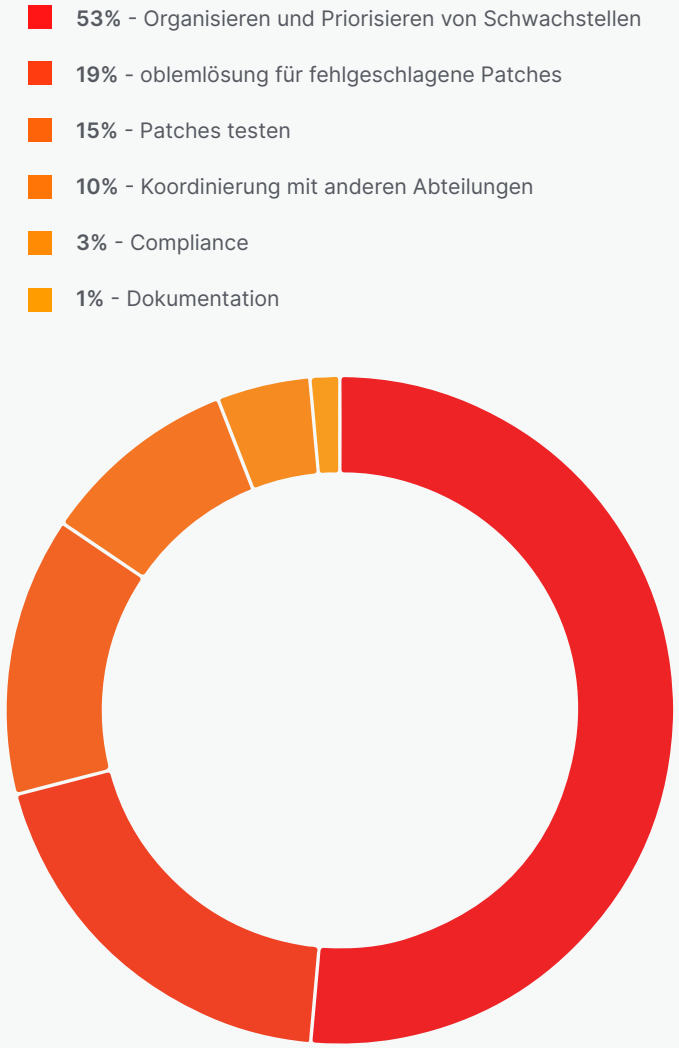
Die Herausforderungen

Eine neue Studie von Ivanti ergab, dass 71 % der IT- und Sicherheitsexperten das Patchen als zu komplex und zeitaufwändig empfinden. Da Angreifer ihre Taktiken weiterentwickeln und Schwachstellen als Waffe einsetzen, insbesondere solche mit Remote-Code-Ausführung, müssen sich Unternehmen mit dem Risiko von Angriffsflächen und Möglichkeiten zur Beschleunigung von Patch- und Abhilfemaßnahmen auseinandersetzen.

IT- und Sicherheitsexperten können einfach nicht schnell genug reagieren. 53 % der Befragten gaben an, dass die Organisation und Priorisierung von Schwachstellen den größten Teil ihrer Zeit in Anspruch nimmt. Dies ist besorgniserregend, denn je länger die Schwachstellen nicht behoben werden, desto größer ist das Risiko eines Angriffs oder von Ransomware für ein Unternehmen. Kein Unternehmen kann jedoch alle Schwachstellen ausbessern, und eine risikobasierte Priorisierung muss schnell vorgenommen werden, um automatisierten Angriffen der Gegner einen Schritt voraus zu sein. Ungepatchte Sicherheitslücken sind nach wie vor einer der häufigsten Einfallstore für Ransomware-Angriffe, die immer häufiger auftreten und Unternehmen jeder Größe betreffen.

IT- und Sicherheitsteams verbringen auch viel Zeit damit, Lösungen für fehlgeschlagene Patches zu finden (19 %), Patches zu testen (15 %) und sich mit anderen Abteilungen abzustimmen (10 %). Die unzähligen Herausforderungen, mit denen IT- und Sicherheitsteams beim Patching konfrontiert sind, könnten der Grund dafür sein, dass 49 % der Befragten der Meinung sind, dass die aktuellen Patch-Management-Protokolle ihres Unternehmens nicht ausreichen, um die Risiken wirksam zu mindern.

IT- und Sicherheitsexperten gaben an, dass sie jeden Monat die meiste Zeit für die folgenden Aktivitäten aufwenden:



Die Ursachen

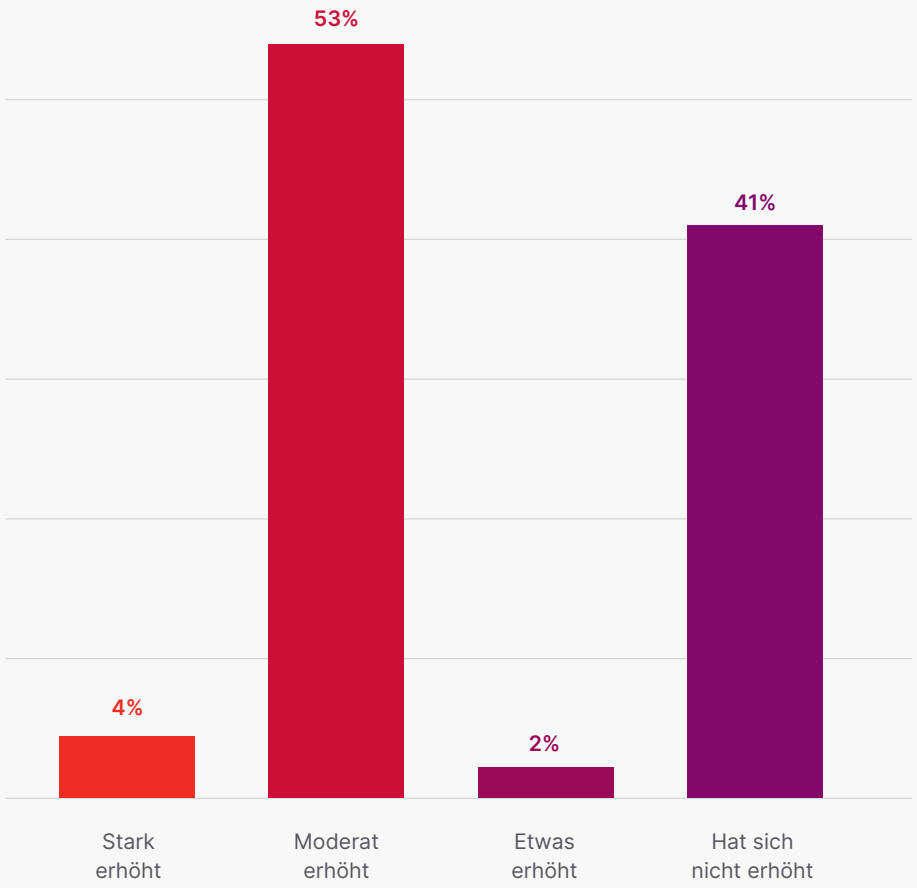
Eine Mehrheit (57 %) der Befragten ist der Meinung, dass der globale Übergang zu einem dezentralisierten Arbeitsumfeld die Verwaltung von Patches komplexer gemacht hat. Der Umfang der Patch-Verwaltung hat sich mit den vielen verschiedenen Endgeräten, die den Benutzern zur Verfügung stehen, und den geschäftskritischen Systemen, die sie unterstützen, ebenfalls vergrößer – von Windows über macOS, Linux bis hin zu Windows-Servern und mehr.

Außerdem sind einige IT-Systeme schwer zu flicken, weil sie Ausfälle verursachen. Beängstigende 61 % der IT- und Sicherheitsexperten gaben an, dass sie einmal pro Quartal von den Inhabern der Geschäftsbereiche aufgefordert werden, Wartungsfenster zu verschieben. Weitere 28 % gaben an, dass sie einmal im Monat eine solche Anfrage erhalten.

Gleichzeitig werden Schwachstellen immer schneller zu Waffen umfunktioniert, insbesondere solche, die eine Remotecodeausführung (Remote Code Execution = RCE) ermöglichen. Es ist der perfekte Sturm aus mangelnder Sichtbarkeit aufgrund der jüngsten Umstellung auf ortsunabhängiges Arbeiten und der Zunahme von Angreifern, die Schwachstellen immer schneller finden und ausnutzen.

Darüber hinaus fehlt es vielen Unternehmen an Sicherheitsexpertise oder Zeit, um ihre Ressourcen in die Lage zu versetzen, Bedrohungsdaten zu sammeln und aktive Bedrohungen mit den offenen Schwachstellen in ihrem Unternehmen abzugleichen, um einen risikobasierten Bedrohungskontext zu schaffen. Aufgrund des Mangels an IT-Personal sind viele Unternehmen nicht mehr in der Lage, Sicherheitsprobleme umgehend zu beheben. Und für Organisationen wie diese haben sich Cyberangriffe, insbesondere Ransomware, als besonders verheerend erwiesen.

Inwieweit hat Remote-Arbeit die Komplexität und den Umfang des Patch-Managements in Ihrem Unternehmen erhöht?



Die Bedrohungslandschaft

Da IT-Teams mit einer größeren Angriffsfläche zu kämpfen haben, entwickeln Hacker ihre Taktiken weiter und beobachten, wo Unternehmen Schwachstellen aufweisen. Sie kombinieren Hartnäckigkeit und Geduld mit einem ausgeklügelten Einsatz von Exploits, Tools und neuen Technologien. Ihr Hauptziel ist es, Unternehmen zu stören, zu stehlen und durch die Ausbeutung von Unternehmen finanzielle Gewinne zu erzielen.

Eine weitere Umfrage von Ivanti ergab, dass 63 % der Befragten angaben, dass ihr Unternehmen im vergangenen Jahr von einem Ransomware-Angriff betroffen war. Und 89 % der Befragten bezeichneten Laptops, Desktops und mobile Geräte als die am stärksten betroffenen Geräte.

Hacker sind ständig auf der Suche nach Schwachstellen, und IT- und Sicherheitsteams haben Schwierigkeiten, bei der Patch-Verwaltung Prioritäten zu setzen, um das Risiko von Schwachstellen schnell zu beseitigen.

Der WannaCry-Ransomware-Angriff, bei dem schätzungsweise 200.000 Computer in 150 Ländern verschlüsselt wurden, ist auch nach vier Jahren noch ein Paradebeispiel für die schwerwiegenden Folgen, die auftreten können, wenn Patches nicht rechtzeitig angewendet werden. Ein Patch für die ausgenutzte Sicherheitslücke existierte bereits mehrere Monate vor dem ersten Angriff, wurde aber von vielen Unternehmen nicht implementiert. Und selbst heute haben zwei Drittel der Unternehmen ihre Systeme noch nicht gepatcht. Dennoch sind Organisationen auf der ganzen Welt immer noch Ziel von WannaCry-Ransomware-Angriffen; die Zahl der von WannaCry-Ransomware betroffenen Organisationen ist von Januar bis März 2021 um 53% gestiegen.

Vertrauensbildung – Kontext für Sicherheit und Risikomanagement

Die Erweiterung der Arbeitslandschaft und der digitale Wandel werden sich fortsetzen. Es muss jedoch ein Weg gefunden werden, den Vertrauenskontext für Sicherheit und Risikomanagement zu erweitern.

Die Implementierung eines Zero-Trust-Frameworks ist von entscheidender Bedeutung für den Schutz sensibler Unternehmensdaten vor unbefugtem Zugriff und Cyberverletzungen durch Angriffe. Zero Trust bietet Unternehmen eine kontinuierliche Bewertung der Geräte, Endpunkte, Anlagen und Netzwerke ihrer Mitarbeiter, auf die sich das Unternehmen verlässt.

US-Präsident Biden unterzeichnete im Mai 2021 eine Executive Order, die besagt, dass Bundesbehörden Pläne zur Umsetzung einer Zero-Trust-Sicherheitsstrategie entwickeln müssen. Zero-Trust-Sicherheit hat auch für IT- und Cybersicherheitsexperten oberste Priorität: Laut einer kürzlichen Studie von Ivanti gaben 98 % der nordamerikanischen IT- und Sicherheitsexperten an, dass ihre Sicherheitspraktiken im nächsten Jahr stärker an der Zero-Trust-Strategie ausgerichtet werden sollen.

Der Vertrauenskontext befasst sich mit dem Risikoaspekt für die Geräte, Endpunkte und Anlagen, die im Everywhere Workplace verwendet werden. Es wird erwartet, dass der Wert des risikobasierten Patch-Managements zunimmt, wenn man versteht, welches Maß an Schwachstellenrisiko akzeptabel ist und welche Patches implementiert werden müssen, um die vom Unternehmen festgelegten Anforderungen an das Vertrauen zu erfüllen.

Führende Branchenexperten, Praktiker und Analystenfirmen empfehlen einen risikobasierten Ansatz, um Schwachstellen zu identifizieren und zu priorisieren und um die Wirksamkeit von Abhilfemaßnahmen zu beschleunigen. Das Weiße Haus veröffentlichte kürzlich ein Memo, in dem es Unternehmen ermutigt, eine risikobasierte Bewertungsstrategie zu verwenden, um das Patch-Management voranzutreiben und die Cybersicherheit gegen Ransomware-Angriffe zu stärken. Darüber hinaus nannte Gartner risikobasiertes Schwachstellenmanagement als eines der wichtigsten Sicherheitsprojekte, auf das sich Sicherheits- und Risikomanagementexperten im Jahr 2021 konzentrieren sollten, um den Geschäftswert zu steigern und Risiken zu reduzieren.

Schlussfolgerung

Während die Produktivität am Everywhere Workplace gestiegen ist, sind auch die Bedrohungen in die Höhe geschnellt. In diesem verstreuten Ökosystem verwenden die Mitarbeiter verschiedene Geräte, um auf Unternehmensdaten, Netzwerke und Anwendungen zuzugreifen und so jederzeit und von überall aus arbeiten zu können. Diese dezentralisierten Arbeitsplätze sind anfälliger für erhebliche Bedrohungen durch bösartige Akteure, die sich den plötzlichen Wechsel zu einem Arbeitsbereich ohne Grenzen zunutze machen, um Unternehmen zu infiltrieren.

Der Everywhere Workplace erfordert einen Ansatz für das Sicherheits- und Risikomanagement, der den aktuellen Kontext für die Schaffung von Vertrauen auf der Grundlage einer aktiven risikobasierten Analyse kontinuierlich bewertet. Mit dem Zugang zu den besten Schwachstellen- und Patch-Informationen, einschließlich aktiver Schwachstellen-Exploits in freier Wildbahn, Schwachstellen mit Verbindungen zu Ransomware und Daten zur Patch-Zuverlässigkeit, erweitert Ivanti die Tools, die IT- und Sicherheitsteams nahtlos einsetzen und die Effektivität des Sicherheits- und Risikomanagements ihrer Organisation verbessern können.

Weitere Informationen finden Sie in unserem Blog. Registrieren Sie sich außerdem gerne für die Ivanti Patch Tuesday Webinar-Reihe. Und hören Sie sich den Ivanti Insights-Podcast an: „The Next Evolution of Patch Management: Don’t Try to Patch Everything!“

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. i. Smarter with Gartner, Gartner Top 10 Security Projects for 2020-2021, February 22, 2021
2. ii. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.