ivanti

Der ultimative Leitfaden für risikobasiertes Patch-Management

Eine Arbeitsreferenz für IT-Betrieb und Sicherheit für moderne Patch-Programm-Implementierungen

Executive Summary

Angesichts von mehr als 187.000 Schwachstellen, die derzeit in der National Vulnerability Database (NVD)(1) registriert sind – und täglich kommen durchschnittlich 61 neue Schwachstellen hinzu[(2)]– **können Unternehmen realistischerweise nicht alle potenziellen Bedrohungen gegen ihre Systeme beseitigen.**

Darüber hinaus zeigen umfassende Betrachtungen aller verfügbaren Daten, dass es insgesamt mehr als 236.000 Schwachstellen gibt, wobei der Prozentsatz der tatsächlichen Bedrohung bei etwa 12,4 % liegt, die von Cyberkriminellen als Waffe eingesetzt werden.[(3)]

Herkömmliche Patch-Management-Strukturen bieten keinen derartigen Überblick über die gesamte Schwachstellenlandschaft, was zu kritischen Lücken in Ihrer Cybersicherheitsabdeckung führt.

Aber selbst, wenn Sie über alle möglichen Schwachstellen Bescheid wüssten, wie entscheiden Sie, welche dieser CVEs zuerst gepatcht werden sollten? Wann sollten Sie Ihren normalen Wartungszyklus für die Einführung von Patches mit höchster Priorität unterbrechen?

Die Lösung: risikobasiertes Patch-Management.

Als einer der effektivsten Ansätze zur Risikominderung geht das risikobasierte Patch-Management über die grundlegenden CVSS-Scores (Common Vulnerability Scoring System) und Scanner hinaus, um die spezifischen Schwachstellen zu identifizieren und zu qualifizieren, die das größte Risiko für die Geräte, Daten und Endbenutzer eines Unternehmens darstellen.

> “Unternehmen können realistischerweise nicht alle potenziellen Bedrohungen gegen ihre Systeme beseitigen.”

Diese Erweiterung des risikobasierten Schwachstellenmanagements bringt einen realen Risikokontext in den Patch-Management-Prozess ein, indem Updates mit bekannten, ausgenutzten Schwachstellen integriert werden, die für die Sicherheitslage eines Unternehmens am wichtigsten sind.

Dieser Ansatz stellt Schwachstellen in einen Kontext, der es Patch-Administratoren ermöglicht, kritische Abhilfemaßnahmen zu priorisieren, und der es den Betriebsteams erlaubt, die Dringlichkeit ihrer Aktivitäten durch dieselbe reale Risikobetrachtung wie die Sicherheitsteams zu verstehen.

Das risikobasierte Patch-Management erfordert zusätzliche Ressourcen, die über die herkömmliche lineare Struktur der Patch-Priorisierung hinausgehen, darunter:

- **Mehrere Datenquellen –** sowohl externe als auch interne –, die dynamisch aktualisiert und schnell zusammengeführt werden können, um die Informationen zu erhalten, die erforderlich sind, um die einzigartigen Risiken eines Unternehmens zu identifizieren und mit bekannten Schwachstellen und Patches zu vergleichen.
- **Ein Priorisierungsschema,** das kritische Schwachstellen für das Unternehmen nach ihrem Schadenspotenzial, bekannten Ransomware-Aktivitäten, der Einfachheit der Behebung und mehr ordnet.
- **Genügend Bandbreite –** entweder menschliche Teammitglieder oder zunehmend automatisierte Funktionen – um kritische Schwachstellen zu erkennen, zu melden und zu beheben, sobald sie auftreten.

Inhaltsverzeichnis

Kritische Stunden: Zu viele Schwachstellen, zu wenig Zeit

Die National Vulnerability Database (Nationale Datenbank für Schwachstellen) listet über 187.000 Schwachstellen mit unterschiedlichen Schweregraden auf, die spezifische Risiken für einzelne Organisationen verdeutlichen.[4]

Für Unternehmen, die in der Lage sind, ihre Überwachungskapazitäten zu erweitern, um alle möglichen Datenquellen abzudecken – einschließlich der NVD- und CISA-Datenbanken, Industriescanner, Bug Bounties, Penetrationstests und verschiedener Branchenforschungen zu Bedrohungstrends - liegt die tatsächliche Zahl der potenziellen Schwachstellen im Juni 2022 bei über 236.000.[5]

Von diesen haben 12,4 % bekannte Schwachstellen für Ransomware und Cyberkriminelle.[6]

Allein die schiere Menge erfordert einen proaktiven, priorisierten Ansatz für das Patch-Management, wenn Unternehmen eine konsistente Sicherheit gewährleisten wollen.

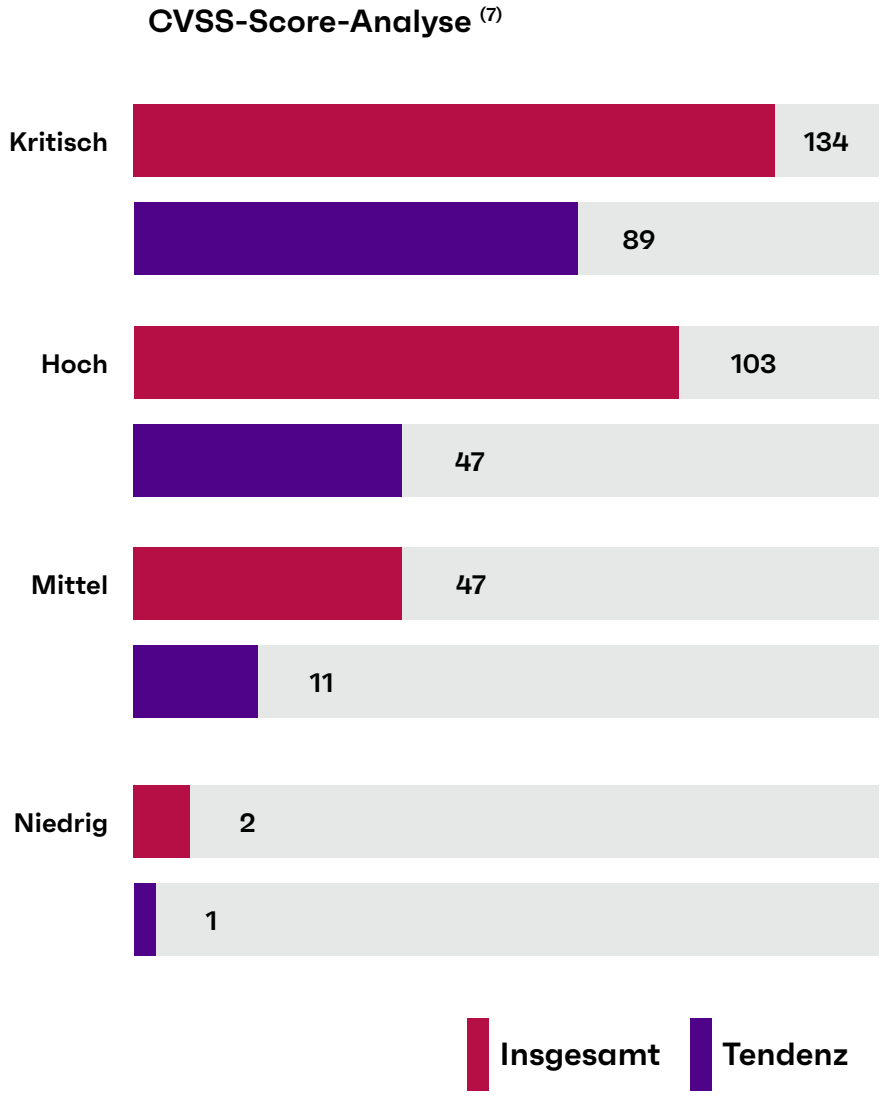
Es gibt über 236.000 bekannte Schwachenstellen.

12,4 % dieser Schwachstellen werden aktiv ausgenutzt oder sind anderweitig mit Ransomware verbunden.

Leider bieten die Einstufungen der Anbieter und der CVSS keinen ausreichenden Kontext, um internen Sicherheitsteams zu helfen, zu priorisieren, auf welche Schwachstellen sie sich zuerst konzentrieren sollten.

Der neueste Ransomware-Bericht von Ivanti[8] zeigt dies:

- Unternehmen, die nur als kritisch eingestufte CVEs patchen, verpassen fast 40 % der aktuellen Schwachstellen, die heute von Ransomware-Banden und anderen Cyberkriminellen aktiv genutzt werden.
- 91 % aller aktiven Schwachstellen im Zusammenhang mit Ransomware sind mehr als ein Jahr alt.



Ohne eine Zuordnung von Schwachstellen zu realen Ransomware-Bedrohungen sowie zu Exploits, die für Remote-Code-Ausführung (RCE) und Privilegienerweiterung (PE) anfällig sind, ist es für ein Unternehmen schwierig, die Prioritäten für Abhilfemaßnahmen effektiv zu setzen und gleichzeitig Sicherheit und Produktivität zu gewährleisten.

Schließlich müssen Sicherheitsteams jede relevante Schwachstelle patchen, um die Sicherheit ihrer Organisation – Geräte, Daten und Endbenutzer – zu gewährleisten.

Cyber-Kriminelle müssen nur einmal Glück haben.

Auswirkungen in der realen Welt:

Microsoft[9]

Im Jahr 2021 hat Microsoft 23 Zero-Day-Schwachstellen behoben.

15 davon wurden nur als wichtig – nicht als kritisch – eingestuft (Patch-Prioritäten).

100 % aller 2021 Zero-Day Microsoft-Schwachstellen wurden aktiv von Cyberkriminellen und Ransomware ausgenutzt.

Der traditionelle Patch-Management-Prozess

In der Vergangenheit folgte das Patch-Management einem linearen, wasserfallartigen Ansatz:

1. **Der Schwachstellen-Scanner oder die Datenbank des Sicherheitsteams** entdeckt eine neue Schwachstelle in der Umgebung und veranlasst eine CVSS-Kritikalitätsbewertung für hoch bewertete Schwachstellen, um eine Triage der Abhilfemaßnahmen durchzuführen.
2. **In der Zwischenzeit bewerten die Patch-Administratoren** die Umgebung, um Software zu finden, die im Rahmen des regulären Wartungszyklus aktualisiert werden muss, und beurteilen den Schweregrad kritischer Anbieter als Teil ihrer Prioritäten für die Abhilfemaßnahmen – unabhängig von der Bewertung des Sicherheitsteams.
3. **Sicherheitsteams und Patch-Administratoren** diskutieren über die Priorisierung von Patches, um eine abgestimmte Liste kritischer Patches für die Korrektur zu erstellen.
   - Im Allgemeinen haben die Empfehlungen der Sicherheitsbehörden Vorrang vor den Empfehlungen der Patch-Administration und der IT-Abteilung, die von den Herstellern stammen.
4. **Patch-Administratoren finden die relevanten Patches** zur Behebung der priorisierten Liste von Schwachstellen – sofern vorhanden – und testen sie idealerweise in einer Sandbox-Umgebung, bevor sie die Korrektur für das gesamte Unternehmen bereitstellen.
   - Administratoren sind mit der Tatsache konfrontiert, dass Testumgebungen nur selten alle Nuancen des lebendigen Unternehmensnetzwerks abbilden.
5. **Der Patch wird ausgerollt und verursacht** möglicherweise Abschaltungen oder Abstürze, da der Patch die Funktionalität oder die Interkonnektivität mit anderen Anwendungen beeinträchtigt – selbst wenn der Patch in der Sandbox-Testrunde als unbedenklich eingestuft wurde und keine Auswirkungen zu erwarten waren.
6. **Der wiederholte Säuberungszyklus beginnt,** während Patch-Administratoren und Sicherheitsteams gleichermaßen die Ergebnisse des Rollouts überprüfen und Rechner identifizieren, die nicht aktualisiert wurden – oder die bei dem Prozess völlig übersehen wurden.

Herausforderungen beim traditionellen Patch-Management

Jeder, der sich mit Patch-Management beschäftigt hat, kann die Mängel des traditionellen linearen Ansatzes aufzeigen. So können Ransomware-Banden beispielsweise Schwachstellen innerhalb weniger Tage ausnutzen, nachdem sie in zentralen Datenbanken identifiziert wurden, was das Zeitfenster verkürzt, in dem Patch-Administratoren die Schwachstellen vor einem Angriff identifizieren und beheben können.

Mehrere große Schwachstellen des letzten Jahres – wie bei QNAP, Sonic Wall, Kaseya und Apache Log4j – wurden ausgenutzt, bevor sie den NVD erreichten.[11]

der Exploits treten innerhalb von 14 bis 28 Tagen nach der Verfügbarkeit von Patches auf(12), wobei Cyberkriminelle im Durchschnitt nur 22 Tage benötigen, um funktionierende Exploits zu entwickeln.[13]

Auswirkungen in der realen Welt: BlueKeep[10]

14. Mai 2019
CVE-2019-0708 mit Patch veröffentlicht.

15. Mai 2019
Die Proof-of-Concept-Forschung beginnt.

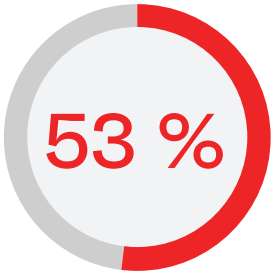
20. Mai 2019
BSOD-Exploit von Forschungsunternehmen bestätigt.

28. Mai 2019
Sechs unabhängige Forschungsunternehmen erreichten RCE, wobei weitere Exploits durch Cyberkriminelle bestätigt wurden.

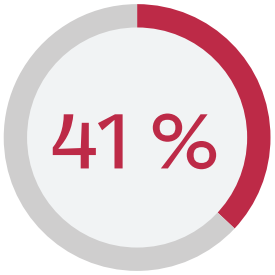
Nur 14 Tage von der Veröffentlichung bis zu aktiven Angriffen durch Cyberkriminelle

Ohne zusätzliche Bandbreite, Ressourcen und Mitarbeiter sind

Patch-Administratoren und Sicherheitsteams gezwungen, sich ausschließlich auf die Schweregradeinstufungen und CVSS-Scores der Hersteller zu verlassen, ohne weiteren Kontext für ihre individuelle Risikoumgebung.



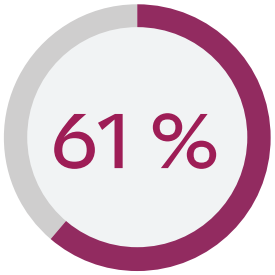
53 % der befragten IT-Ops- und Sicherheitsteams geben an, dass sie die meiste Zeit damit verbringen, Schwachstellen zu organisieren und nach Prioritäten zu ordnen, anstatt sie aktiv zu beheben![14]



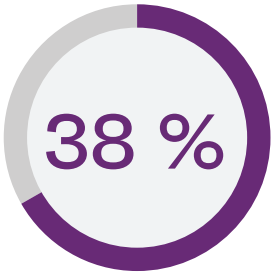
Eine kürzlich durchgeführte internationale Umfrage ergab, dass 41 % der befragten Unternehmen aufgrund der hohen Arbeitsbelastung auf dem hart umkämpften Arbeitsmarkt IT-Ops-Mitarbeiter verloren haben.[15]

Ein Missverhältnis zwischen Sicherheits- und IT-Ops-Zielen

führt häufig zu fehlgeschlagenen Patches und Produktivitätsverlusten.

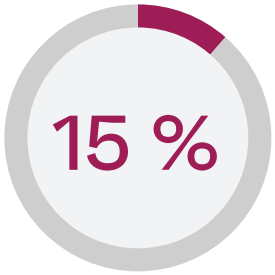


61 % der befragten IT und Sicherheitsexperten erhalten einmal pro Quartal – 28 % sogar jeden Monat – die Aufforderung, Wartungsfenster zu verschieben, wodurch Unternehmen für vermeintliche „Produktivitätsgewinne“ anfällig für Cyberangriffe werden.[16]



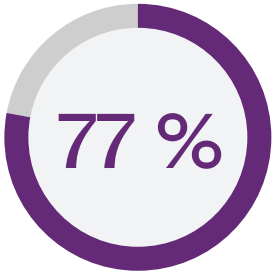
Wenn Unternehmen von Cyberangriffen betroffen sind – wie es bei 63 % der befragten Unternehmen im Jahr 2021 der Fall war –, haben 38 % der Opfer die Produktivität des gesamten Unternehmens um eine Woche verringert; 24 % der Unternehmen haben einen ganzen Monat lang nicht gearbeitet.[17]

Die meisten Abteilungen haben keine Zeit, Updates zu testen oder sich mit anderen Abteilungen abzustimmen, bevor sie Patches bereitstellen.



Nur 15 % der IT-Ops- und Sicherheitsteams geben an, dass sie die meiste Zeit mit dem Testen von Patches verbringen, während nur 10 % angaben, dass sie die meiste Zeit mit der Koordination mit anderen Abteilungen verbringen.[18]

Scanner und Datenbanken können nicht alle ausnutzbaren Schwachstellen aufspüren und publizieren.



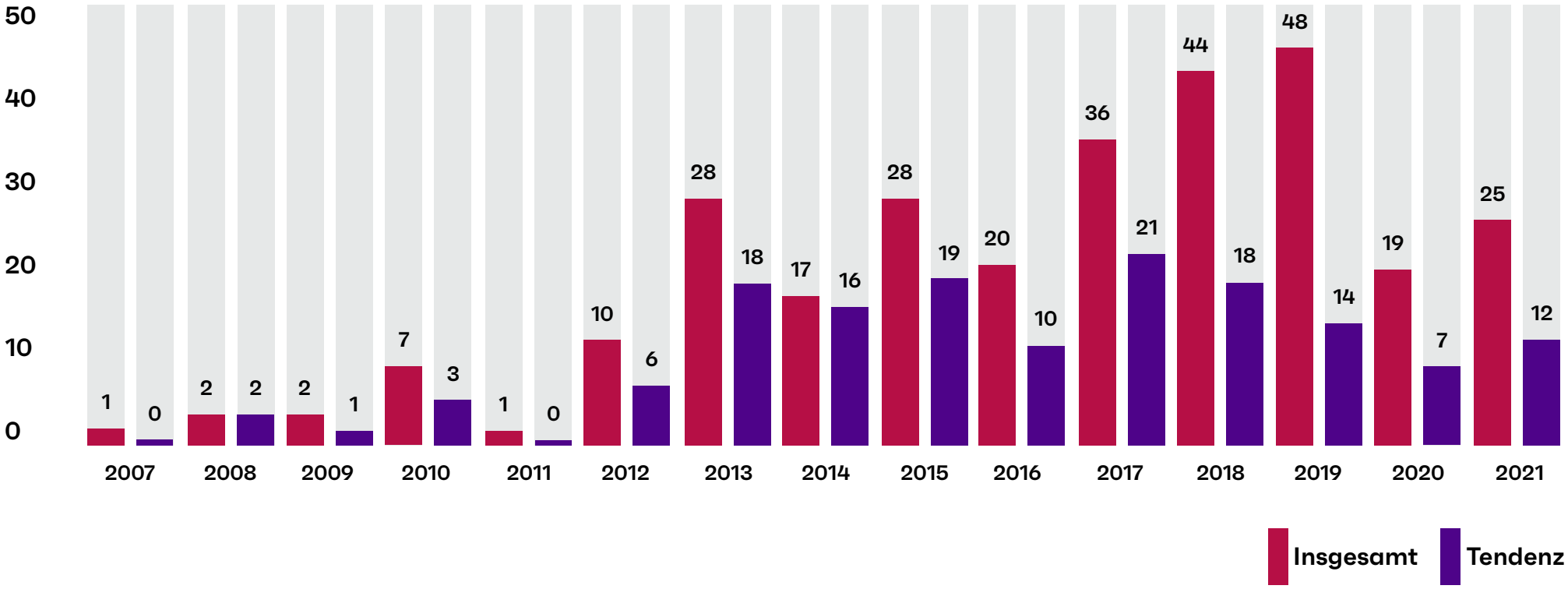
Drei der bekanntesten Schwachstellen-Scanner – Nessus, Qualys und Nexpose – entdeckten im vergangenen Jahr nur 77 % aller ausnutzbaren Schwachstellen.[19]

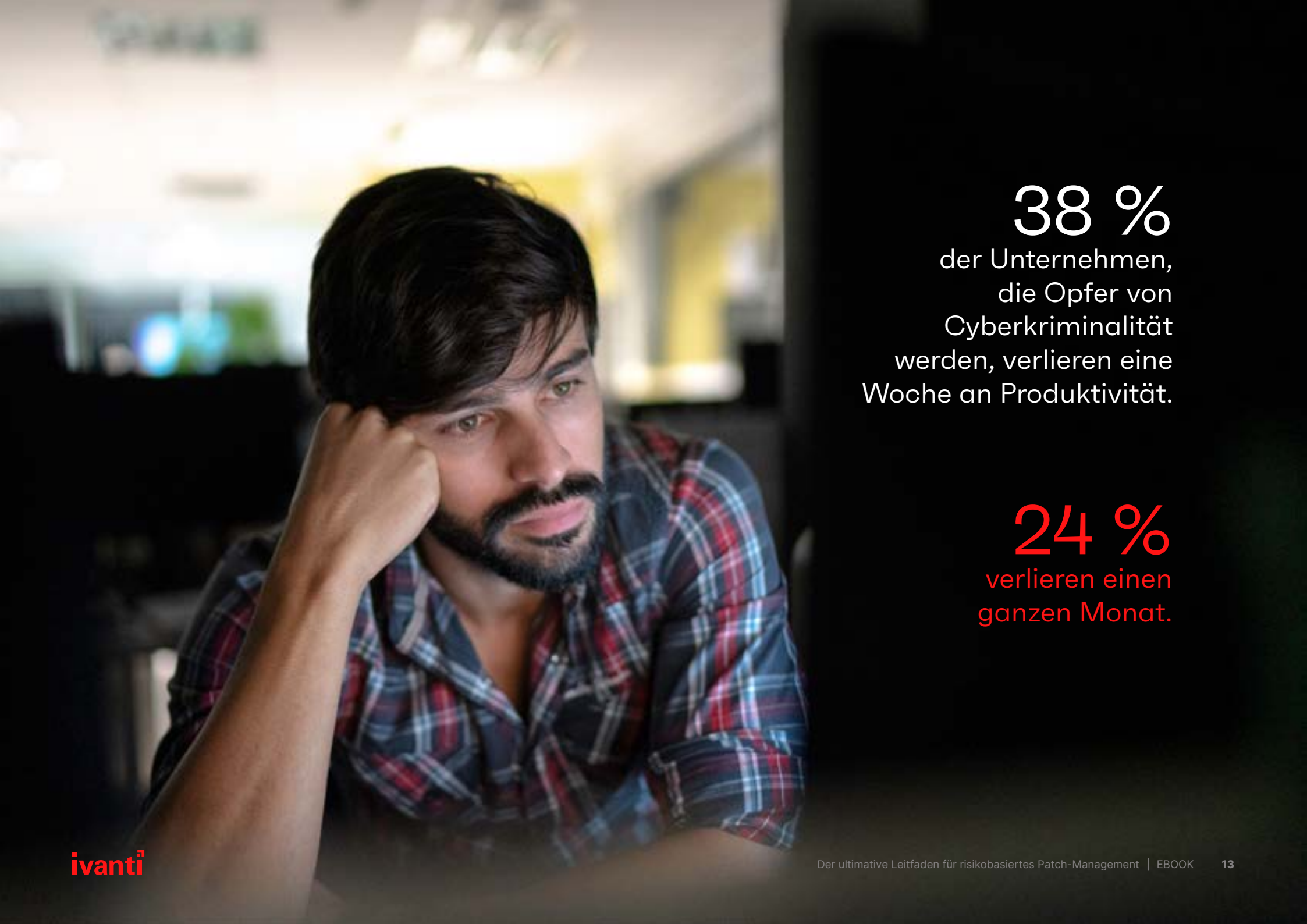
ivanti

Cyberkriminelle und Ransomware-Banden können immer noch unkritische oder ältere Schwachstellen für ihre Angriffe nutzen.

- Unternehmen, die nur die als kritisch eingestuften CVEs gemäß CVSS patchen, würden 53 % aller ausnutzbaren Schwachstellen im Zusammenhang mit Ransomware übersehen.[20]
- 92 % aller aktiven Schwachstellen wurden vor 2021 öffentlich bekannt gegeben – zwei der jüngsten Schwachstellen wurden sogar schon 2008 bekannt gegeben![21]
- Nach Untersuchungen der Rand Consulting Group werden Schwachstellen noch bis zu sieben Jahre nach ihrer ersten Veröffentlichung aktiv von Cyberkriminellen ausgenutzt.[22]

Schwachstellen im Zusammenhang mit Ransomware und Tendenzen nach Jahr der NVD-Veröffentlichung[23]





38 %

der Unternehmen, die Opfer von Cyberkriminalität werden, verlieren eine Woche an Produktivität.

24 %

verlieren einen ganzen Monat.

Ungepatchte Schwachstellen sind nach wie vor der Hauptangriffsvektor für Ransomware-Gruppen. Wenn nicht sofort reagiert wird, kann die Sicherheitsumgebung eines Unternehmens schnell gefährdet werden, was die Produktivität und Rentabilität erheblich beeinträchtigt.

Und da die durchschnittlichen Gesamtkosten eines Ransomware-Verstoßes auf 4,62 Millionen US-Dollar geschätzt werden[24], ist eine effektive Strategie zur Behebung von Schwachstellen für Sicherheits- und IT-Ops-Teams von entscheidender Bedeutung, um diese Schlupflöcher und Schwachstellen zu schließen.

Aber das Patchen aller Schwachstellen ist einfach keine praktikable Lösung für jedes IT-Ops- oder Sicherheitsteam, ganz zu schweigen von überlasteten und unterbesetzten Abteilungen.

Patch-Administratoren benötigen einen strategischen Angriffsplan, der die oft begrenzten Ressourcen wie Zeit, Personal und interne Bandbreite optimal nutzt und gleichzeitig Cyberkriminellen und anderen Bedrohungsakteuren einen Schritt voraus ist.

Hier kommt das risikobasierte Patch-Management (RBPM) ins Spiel.

Ein durchschnittlicher Ransomware-Angriff kostet schätzungsweise

4,62 Millionen US-Dollar.

Risikobasiertes Patch-Management im Überblick

Eine risikobasierte Patch-Management-Strategie verfolgt einen differenzierten Ansatz für das Patching, anstatt zu versuchen, das einzigartige Risikoprofil eines Unternehmens in den traditionell verwendeten linearen Patching-Ansatz zu pressen, der nur eine Größe zulässt.

Zunächst sammeln Admins Informationen aus externen Quellen: Netzwerkscanner, Datenbanken wie NVD und CISA sowie Schwachstellenfeststellungen aus manuellen Untersuchungen und Penetrationstests.

Sie sammeln auch interne Daten, um das genaue Risikoprofil des gesamten IT-Bereichs des Unternehmens zu ermitteln.

Dieser Datensatz umfasst:

- Eine Liste der im Einsatz befindlichen Geräte und Betriebssysteme, die von den IT- und Ops-Teams des Unternehmens unterstützt werden.
- Alle Anwendungen und Software, die derzeit von den Endbenutzern der Organisation verwendet werden – einschließlich offiziell installierter Software und vom Benutzer selbst erstellter Anwendungen, die entweder heruntergeladen oder cloudbasiert sind.
- Ein Verständnis dafür, wie Daten abgerufen werden – sowohl firmeneigene Daten als auch Kundendaten – sowie dafür, wo sie gespeichert sind und wie sie verwendet werden.

Durch den Abgleich von externen Schwachstellen- und Bedrohungsinformationen mit der unternehmensinternen Sicherheitsumgebung können Patch-Administratoren Bedrohungsinformationen in den richtigen Kontext setzen und Prioritäten für die Patches setzen, die für das Unternehmen am wichtigsten sind, anstatt die Bedrohungswahrnehmung einer externen Quelle zu berücksichtigen.

Mit RBPM kann ein kleines Team eine ständig wachsende Zahl von Schwachstellen bewältigen und das Unternehmen, seine Endbenutzer und Kunden schützen, ohne die bereits überlasteten IT-Ops- und Sicherheitsteams zu überfordern.

Vier wirtschaftliche Vorteile eines risikobasierten Patch-Management-Ansatzes

- RBPM spiegelt den pragmatischen Mittelweg zwischen „alles patchen“ und „warum sich überhaupt die Mühe machen“ wider.
- RBPM bietet eine „realitätsbasierte“ Priorisierung für Schwachstellen, die auf Ihr Unternehmen zugeschnitten ist und mit realen Angriffsinformationen kontextualisiert wird. So können Sie feststellen, was wirklich wichtig ist.
- RBPM kann schneller sein als ein herkömmlicher Patch-Management-Ansatz.
- RBPM bildet eine abteilungsübergreifende Brücke für Sicherheits- und IT-Ops-Teams

1. RBPM fördert einen pragmatischen – nicht idealisierten – Ansatz für das Patching.

Die risikobasierte Methode des Patch-Managements trägt der Realität Rechnung, in der alle Administratoren arbeiten: Es gibt einfach zu viele Schwachstellen und zu wenig Ressourcen, um mit allem Schritt zu halten.

Im Jahr 2021 stieg die Zahl der mit Ransomware verbundenen Schwachstellen um 29 % gegenüber dem Vorjahr.

Andererseits ist es auch keine Option, nichts zu tun: Ungepatchte Schwachstellen sind die wichtigsten Angriffsvektoren, die von Ransomware-Gruppen und Bedrohungsakteuren ausgenutzt werden. Im vergangenen Jahr stieg die Zahl der Schwachstellen im Zusammenhang mit Ransomware um unglaubliche 29 % gegenüber dem Vorjahr.[25]

RBPM ist der optimale Mittelweg zwischen „alles patchen“ und „warum sich überhaupt die Mühe machen“.

Ein proaktives, risikobasiertes Schwachstellenprogramm kann die Zahl der Datenschutzverletzungen in einem Unternehmen um 80 % reduzieren.

Je eher Unternehmen begreifen, dass es kein realistisches Ziel mehr ist, wahllos alles zu patchen – auch nicht jedes „kritische“ CVE mit CVSS-Einstufung oder Hersteller-Einstufung –, desto schneller können sie zu einer proaktiven, aktualisierten Patch-Management-Strategie übergehen, die ihre Benutzer, Systeme und Assets besser schützt.

Und laut Gartner Research kann ein umfassendes risikobasiertes Schwachstellenmanagementprogramm, das RBPM einschließt, die Zahl der Datenschutzverletzungen in einem Unternehmen um 80 % reduzieren, selbst wenn ein Unternehmen nicht alle Patches einsetzt.[26]

Das ist eine bemerkenswerte wirtschaftliche Verbesserung für eine relativ kleine weltanschauliche Veränderung.

2. RBPM ist ein „realitätsbasierter“ Priorisierungsprozess, der die Risiken nach dem organisatorischen Kontext einstuft.

Durch die Einstufung von Problemen auf der Grundlage des Verhaltens von Ransomware-Banden und der von ihnen ausgenutzten Schwachstellen – neben anderen Prioritäten, einschließlich RCE- und PE-Potenzial – können die Patch-Administratoren von Unternehmen die möglichen Auswirkungen einer Schwachstelle realistischer einschätzen.

Bei diesen Bewertungen werden Schwachstellen nicht nur als isolierte Bedrohung betrachtet, sondern auch in Kombinationen mehrerer Schwachstellen, die durch „Schwachstellenverkettung“ gemeinsam ausgenutzt werden.”

Schwachstellenverkettung liegt vor, wenn Ransomware mehrere Schwachstellen auf einmal ausnutzt – oft Schwachstellen mit unterschiedlichen Schweregraden und Altersstufen – um einen umfassenden Angriff auf ein Unternehmen durchzuführen.

Die LockFile-Ransomware-Angriffe von 2021(27) verknüpften zum Beispiel insgesamt vier Schwachstellen von Microsoft Exchange und Windows OS:

Die „ProxyShell“-Schwachstellen

ermöglichen es Cyberkriminellen, in das Netzwerk eines Unternehmens einzudringen und Remote-Code auszulösen, der weitere Exploits ermöglicht, sowie Hintertüren für einen späteren Zugriff zu installieren.[28]

Die „PetitPotam“-Schwachstelle

ermöglicht es Angreifern, noch tiefer in die Systeme eines Unternehmens einzudringen, um sich Zugang zu wertvollen und unternehmenskritischen Systemen zu verschaffen

Unternehmen, die nur einen traditionellen, linearen Patch-Management-Prozess befolgten, hätten nicht alle Schwachstellen gepatcht, die bei diesem und ähnlichen Angriffen auftraten.

Von den vier Schwachstellen in der LockFile-Ransomware wurde nur eine als kritische Schwachstelle eingestuft, die gepatcht werden muss – zwei wurden lediglich als „mittel“ eingestuft.[30]

Die LockFile-Schwachstellen

Schwachstelle	CVSS-Score	CVSS-Schweregrad	Produkt
CVE-2021-31207	7.2	Hoch	Microsoft Exchange Server
CVE-2021-34473	9.8	Kritisch	Microsoft Exchange Server
CVE-2021-34523	9.8	Mittel	Microsoft Exchange Server
CVE-2021-36942	5.3	Mittel	Microsoft Windows Windows Server 2008, 2012, 2016 und 2019

Und obwohl die LockFile-Ransomware-Angriffe erst im Jahr 2021 stattfanden, gibt es laut Forschungsberichten immer noch mehr als 34.000 ProxyShell-Schwachstellen im Internet[29] – und warten auf eine neue Gruppe von bösen Akteuren, die die Schwachstellen ausnutzen.

3. RBPM verkürzt die Zeit bis zur Behebung von Schwachstellen.

Je länger eine kritische Schwachstelle ungepatcht bleibt, desto größer ist das Risiko einer Datenschutzverletzung oder eines Ransomware-Angriffs für ein Unternehmen.

Im Jahr 2021 erließ das US-Ministerium für Innere Sicherheit über die Agentur für Cybersicherheit und Infrastruktursicherheit (CISA) die verbindliche operationelle Richtlinie 22-01.

Diese neuen Anforderungen für öffentliche Organisationen verkürzten die Patching-Zeit für kritische Schwachstellen auf zwei Wochen und schlugen zusätzliche angepasste Fristen im Falle eines „ernsten Risikos“ für die Infrastruktur einer Organisation vor.[32]

Übrigens enthält diese CISA-Liste der erforderlichen Schwachtstellen-Patches 20 % aller CVEs, die derzeit von Ransomware-Familien aktiv ausgenutzt werden.[33]

Selbst für Sicherheitsteams, die ein System zur Priorisierung von Schwachstellen nutzen, um die wichtigsten Patches zu bestimmen, gibt es immer unzählige Schwachstellen, die gepatcht werden müssen, und nicht viel Zeit, um sie zu patchen.

Bei herkömmlichen Patch-Management-Methoden verbringen Administratoren oft Stunden damit, zu recherchieren und herauszufinden, welche Maßnahmen zu ergreifen sind, wenn sie einen Schwachstellenbericht erhalten.

Die CISA-Liste der erforderlichen Patches deckt nur 20 % aller aktiv ausgenutzten Schwachstellen ab.

Im Gegensatz dazu können einige moderne Patch-Management-Systeme Informationen über Schwachstellen automatisch mit Patch-Daten und dem organisatorischen Kontext abgleichen. Diese Abgleiche erhöhen den Einblick in unternehmensspezifische Risiken, beschleunigen den gesamten Abhilfeprozess und reduzieren die verbleibende Bereinigung nach jedem Wartungszyklus.

Darüber hinaus ist ein umfassender risikobasierter Ansatz für die Patch-Verwaltung auch am ehesten geeignet, die Auswirkungen von Zero-Day-Schwachstellen zu bekämpfen oder zu begrenzen:

- Es genügt zu wissen, dass die Schwachstelle existiert, damit ein Patch – sobald er verfügbar ist - vorrangig freigegeben und auf den Systemen des Unternehmens installiert werden kann.
- Entwicklung von Ad-hoc-Strategien, die die Auswirkungen auf potenziell gefährdete Systeme abmildern, ohne den laufenden Betrieb zu behindern.
- Einrichtung eines internen Warnsystems, um sofort zu wissen, wenn ein Cyberkrimineller diese Schwachstelle ausnutzt.

Durch die Erkennung und Priorisierung von Updates zum Schutz der anfälligsten Systeme innerhalb des Unternehmens nutzen Patch-Administratoren ihre Ressourcen optimal und schützen die Systeme vor externen Cyberkriminellen und Ransomware-Banden.

Was ist eine Zero-Day-Schwachstelle?

Eine Zero-Day-Schwachstelle ist eine Schwachstelle, die folgende Eigenschaften aufweist:

- Vom Anbieter identifiziert – oft nach einem Exploit-Angriff.
- Wird von Cyberkriminellen aktiv ausgenutzt..
- Kann nicht gepatcht werden (oder es ist kein Patch verfügbar).

4. RBPM reduziert die natürliche Reibung zwischen IT-Ops- und Sicherheitsteams.

Risikobasiertes Patch-Management schafft Raum für Empathie:

Das IT-Ops-Team

versteht die Prioritäten des Sicherheitsteams und die Gründe für wirklich wichtige Patches für kritische Schwachstellen besser.

Das Sicherheitsteam

kann besser einschätzen, wie sich ein fehlerhafter Patch auf das Unternehmen auswirkt, kritische Anwendungen beschädigt und eine Flut von Benutzertickets verursacht.

Wenn das IT-Ops-Team darauf vertraut, dass das Sicherheitsteam die Patches richtig priorisiert – damit es nicht seine Zeit oder die der Endbenutzer mit jeder möglichen Schwachstelle vergeudet –, ist es wahrscheinlicher, dass das IT-Ops-Team kooperiert und proaktiv Zeit für die wichtigsten Sicherheitsrisiken findet.

Allgemeiner ausgedrückt kann ein risikobasierter Schwachstellenmanagementprozess diese Teams auch darüber aufklären, was sie riskieren, wenn eine bestimmte Schwachstelle nicht gepatcht wird.(34)

Plötzlich behebt der angeforderte Patch nicht mehr nur eine von vielen Schwachstellen, sondern das Risiko wird in Bezug auf die Abteilung und die Geschäftsergebnisse kontextualisiert, wobei die Erfahrung der Endbenutzer und der Umsatz durch einen möglichen Verstoß beeinträchtigt werden, wenn er nicht behoben wird.

Die unmittelbare, kurzfristige Unannehmlichkeit, ein paar Stunden Zeit für die Aktualisierung zu finden, wird durch das längerfristige Risiko eines Zeitverlusts von einer Woche oder mehr aufgrund eines Ransomware-Angriffs aufgewogen.

Ein durchschnittlicher Ransomware-Angriff kostete im Jahr 2021 4,62 Millionen Dollar.(34)

Wenn die Sicherheitsbehörden nicht versuchen, alle offenen Fragen auf einmal zu klären, sondern nur die wichtigsten, können sie flexibler mit ihren Partnern in der IT-Abteilung zusammenarbeiten, um Patches nicht während kritischer Zeiten abzustimmen, den Wartungszyklus zu verkürzen und Systemabstürze durch ungeplante Updates zu vermeiden.

Darüber hinaus zentralisiert eine moderne RBPM-Plattform die Datenanalyse und Priorisierung an einem einzigen zugänglichen Ort oder in einem Dashboard, was mehrere Vorteile mit sich bringt:

IT-Ops-Teams

müssen nicht mehr darauf warten, dass die Sicherheitsabteilung Schwachstellenberichte herausgeben. Sie können über das Dashboard sehen, was für ihr Unternehmen am wichtigsten ist, und sofort mit dem Testen von Updates in einer sauberen Umgebung beginnen, um die Reaktionszeit zu verbessern, einschließlich der Zuordnung relevanter CVEs zu internen Umgebungen.

Die Sicherheitsabteilung

sieht auf einen Blick den Status der Patch-Einführung, mögliche Engpässe und Patches, die noch im Rückstand sind und in einem zukünftigen Sprint oder Wartungszyklus bearbeitet werden müssen.

Bei RBPM wird der Prozess zu einem Prozess der gegenseitigen Abstimmung - ohne ständige Unterbrechung.

ivanti

Können Sie ein risikobasiertes Patch-Management-Programm manuell durchführen?

Risikobasiertes Patch-Management ist die natürliche Alternative zu dem Versuch, alles zu patchen, aber es ist alles andere als ein einfacher Prozess.

(Wäre es nämlich einfach zu implementieren, wäre dieser Leitfaden überflüssig.)

Die Festlegung risikobasierter Prioritäten und die Verfolgung von Schwachstellenveränderungen in Echtzeit – ganz zu schweigen von ordnungsgemäßen Tests und der Bereitstellung von Patches – überfordert unvorbereitete Teams, die versuchen, RBPM manuell und nicht mithilfe expliziter Tools oder automatisierter Prozesse zu bewältigen.

Nehmen wir zum Beispiel an, ein Unternehmen möchte eine RBPM-Strategie umsetzen. Um zu vermeiden, dass sie von zu vielen Datenquellen überwältigt werden, haben sie sich entschieden, sich nur auf den NVD zu konzentrieren, bei dem im vergangenen Jahr jeden Tag durchschnittlich 61 neue Schwachstellen hinzukamen.[35]

Als Teil ihrer RBPM-Philosophie – die verlangt, dass neue Schwachstellen intern mit der möglichen Angriffsfläche in Zusammenhang gebracht werden und nicht einfach auf eine externe Bewertung der Kritikalität gestützt werden – muss das Team täglich alle 61 neuen NVD-Schwachstellen manuell überprüfen, um 61 separate Prioritäten zu setzen.

(Der Rückstand am Montag wäre in diesem Team schrecklich.)

Und unser hypothetisches Unternehmen bezieht sich nur auf eine einzige, wenn auch umfassende, Datenquelle.

Ganz zu schweigen von der Flut an Informationen über Schwachstellen, die ihnen aus anderen Datenbanken, Untersuchungen und Berichten zur Verfügung stehen könnten.

Auswirkungen in der realen Welt:

Schwachstellen- und Patch-Abgleich

In Gesprächen mit Ivanti-Experten berichten IT-Betriebs- und Sicherheitsteams in Unternehmen auf der ganzen Welt anekdotisch, dass ihre traditionellen Schwachstellen- und Patch-Abgleichsberichte mindestens 8 Stunden benötigen, um sie von Hand auszufüllen. Die Fachleute, die an diesen manuellen Berichten arbeiteten, gaben zu, dass sie wussten, dass das endgültige Dokument – obwohl kritisch! – nicht zu 100 % zutreffend sein würde.

Nehmen wir jedoch an, dass unser Unternehmen über genügend Sicherheits- und IT-Mitarbeiter verfügt, um große Anbieter wie Microsoft, Apple, Linux und andere App-Anbieter regelmäßig direkt zu überwachen, um Schwachstellen und Exploits zu finden, sobald sie bekannt werden.

Es gibt sogar Stellen im Internet – wie PatchMangement.org, Reddit und das Ivanti Patch Tuesday Webinar – die besonders relevante Schwachstellen sammeln. Diese und andere Branchen-Websites sind sicherlich großartige Ressourcen, um Teams bei der Navigation durch diesen Teil des RBPM-Prozesses zu helfen – und das kostenlos!

Die Überwachung ist jedoch nur eine von vielen Aufgaben, die vor dem Ende des Patching-Zyklus erledigt werden müssen.

Als Teil des RBPM-Prozesses müssen die Sicherheits- und IT-Betriebsteams unserer hypothetischen Organisation noch immer die gleichen Aufgaben erfüllen:

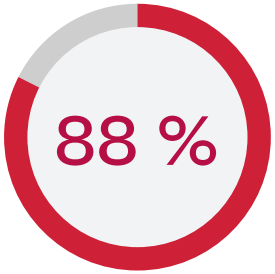
- Identifizieren Sie alle internen Geräte und Anwendungen – von der IT genehmigte und vom Benutzer installierte.
- Bestimmen Sie, welche Endbenutzer und Anwendungsfälle zuerst Patches erhalten.
- Testen Sie den Patch in allen Variationen und Variablen – oder in so vielen, wie es für die jeweilige Schwachstelle sinnvoll ist.
- Planen Sie den Patch-Rollout und führen Sie ihn durch.

Vor allem bei hybriden oder vollständig dezentralen Arbeitsplätzen können diese Verfahren zu endlosen Prozessen eskalieren, die nicht mit der Geschwindigkeit der Realität mithalten können.

Und nicht zuletzt verwenden viele manuelle Systeme kalkulationsähnliche Dokumentationen und Datenbankabgleiche.

Wenn man sich jedoch auf Tabellenkalkulationen verlässt, sind Fehler vorprogrammiert. Je mehr Personen häufig denselben Bericht anpassen, desto wahrscheinlicher ist es, dass sich Fehler einschleichen, die zu kostspieligen Verzögerungen und Korrekturen führen.

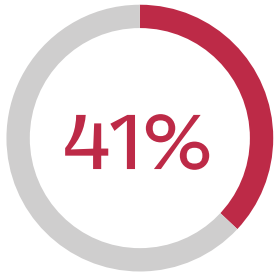
Tatsächlich hat eine Studie ergeben, dass 88 % aller Tabellenkalkulationen „signifikante“ Fehler aufweisen – die meisten davon werden von den Personen verursacht, die sie bearbeiten![36]



aller Tabellenkalkulationen weisen „erhebliche“, vom Menschen verursachte Fehler auf.

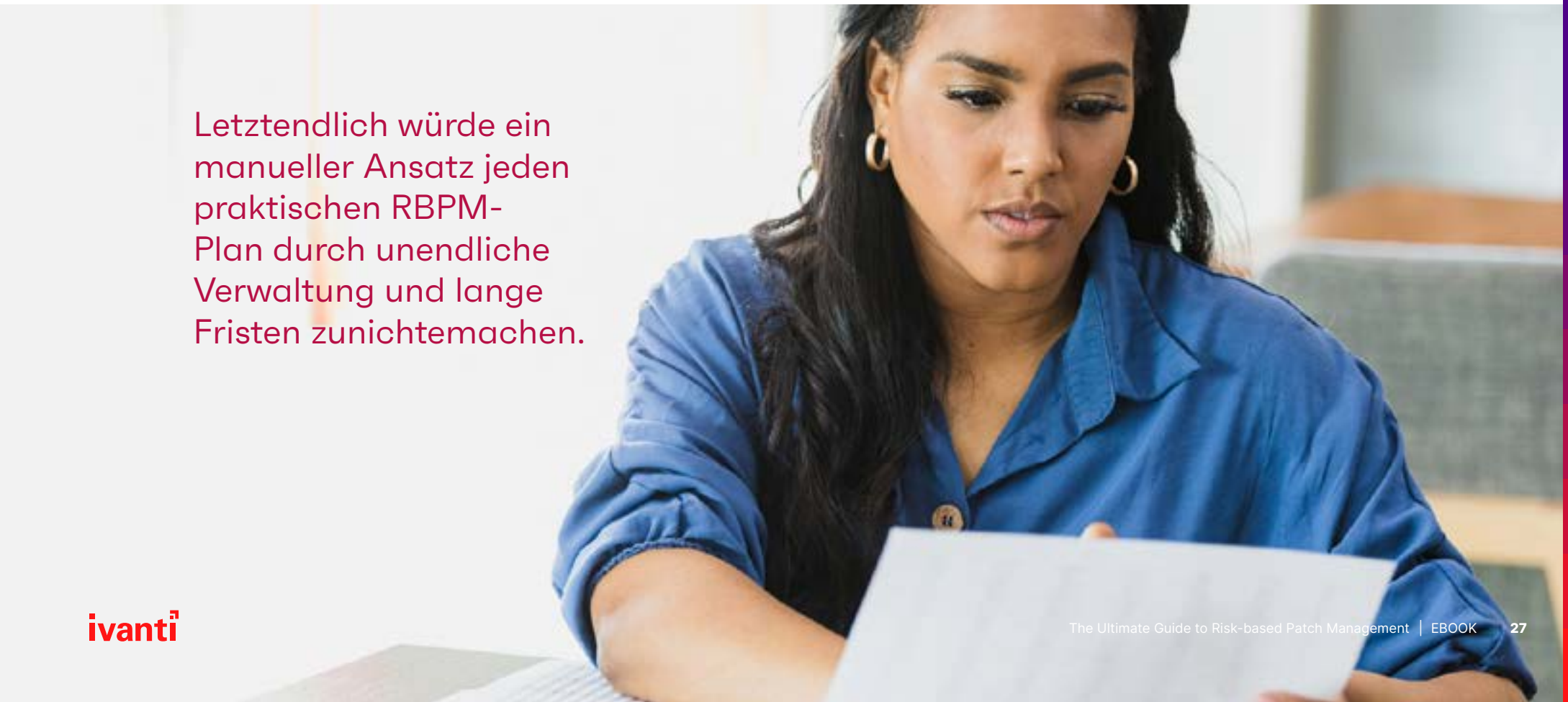
Die manuelle Ausführung einer risikobasierten Patch-Management-Strategie ist zwar durchaus möglich – vor allem zu Beginn, um ein Gefühl für den Ansatz zu bekommen und bevor spezielle Tools angeschafft werden –, wäre aber nicht die optimale Konfiguration für Teams, die sich die RBPM-Philosophie wirklich zu eigen machen wollen.

Mehr manuelle Arbeit in einer Zeit, in der 41 % der befragten Unternehmen angeben, dass sie aufgrund der hohen Arbeitsbelastung IT-Personal abbauen, erscheint ebenfalls unklug.[37]



der befragten Unternehmen berichten, dass sie aufgrund der hohen Arbeitsbelastung wichtige IT-Mitarbeiter verlieren.

Letztendlich würde ein manueller Ansatz jeden praktischen RBPM-Plan durch unendliche Verwaltung und lange Fristen zunichtemachen.



Fünf bewährte Verfahren für Ihr risikobasiertes Patch-Management-Programm

1. Sie können nicht patchen, wovon Sie nichts wissen.
2. Sorgen Sie dafür, dass die IT-Ops-und die Sicherheits-Abteilung auf demselben Stand sind.
3. Arbeiten Sie mittels eines internen SLA parallel.
4. Bilden Sie Pilotgruppen.
5. Nutzen Sie Automatisierung!

ivanti

1. Finden Sie heraus, was Sie derzeit haben und wie Sie es nutzen.

Man kann nicht etwas schützen oder patchen, von dem man nicht weiß, dass es existiert. Daher spielt die Asset-Erkennung – herauszufinden, was Sie mit welchen Endbenutzerprofilen haben – eine entscheidende Rolle in jeder Initiative zum Schwachstellenmanagement.

Asset-Management für RBPM

Moderne Asset-Management-Tools können Unternehmen dabei helfen, ihren aktuellen Technologiebestand zu verstehen und zu verfolgen. Es beginnt mit der Identifizierung aller Geräte – Laptops, Desktops, Telefone, Tablets, Server und Netzwerkgeräte – und Software, die im Unternehmen eingesetzt werden.

Genau wie beim allgemeinen Patch-Management-Programm stammen die Informationen über Ihre Assets aus verschiedenen Quellen, wie z. B.:[38]

- ☐ Microsoft Endpoint Configuration Manager (SCCM) und Microsoft Intune
- ☐ CSV-Dateien oder Tabellenkalkulationen
- ☐ Microsoft Active Directory
- ☐ Arbeitsbereich Eins (AirWatch)
- ☐ Ivanti Neurons for Discovery

Nachdem Sie alle Assets aufgelistet haben, müssen Sie Duplikate beseitigen und sicherstellen, dass alle Daten in der Datenbank konsistent sind.

Nicht zuletzt organisieren die Asset Manager in IT-Ops-Teams die Datensätze, sodass die Patch-Administratoren die kritischsten Terminals und alle potenziellen Schwachstellen finden können – Informationen, die bei der Priorisierung Ihrer Patches helfen.

Service-Zuordnung für RBPM

Als Erweiterung des Discovery-Prozesses kann das Service Mapping Ihnen dabei helfen, die Systeme zu finden, die verwaltet und gesichert werden müssen, und aufzeigen, wie sie – und die von ihnen verwendeten Daten – miteinander verbunden sind und auf sie zugegriffen wird.

Servicekarten können enthalten:

- Die Infrastruktur und das Hardware-Inventar.
- Anwendungen, Konfigurationsdokumentation und eine Software-Bibliothek, die die neuesten Versionen der verwendeten Software auflistet.
- Einstellungen und Netzwerkdiagramme, die den Informationsfluss und die Verbindung der Geräte im gesamten Unternehmen verdeutlichen.
- Endbenutzer, Benutzerprofile und risikoreiche Terminals sowie das Ausmaß der Auswirkungen, die jeder von ihnen auf das kritische System des Unternehmens haben kann, wenn es kompromittiert wird.

Sicherheitsteams können dann den Weg abbilden, den ein Angreifer über eine Schwachstelle nehmen könnte, um ein kritisches System über die angeschlossenen Benutzersysteme oder Anwendungen erreichen.

Gleichzeitig erhält das IT-Ops-Team einen Überblick darüber, wie viele Systeme mit einer geschäftskritischen Anwendung verbunden sein können, und erhält so wichtige Informationen darüber, wie Patch-Tests am besten konfiguriert und implementiert werden können.

2. Stellen Sie sicher, dass jeder auf dieselben Informationen zugreifen kann.

Die Effizienz des risikobasierten Patch-Managements hängt davon ab, wie gut Ihre IT-Ops- und Sicherheitsteams zusammenarbeiten, um ihre Eingriffe zu synchronisieren. Dazu benötigen sie wahrscheinlich Hilfe bei der funktionsübergreifenden Abstimmung, um alle ihre Ziele zu erreichen.

Theoretisch sollten alle Teams auf das gleiche Ziel hinarbeiten: eine sichere Organisation, die ihre Arbeit ohne Unterbrechung durch Cyberangriffe erledigen kann.

In der Praxis scheinen ihre Ziele diametral entgegengesetzt zu sein: Die Sicherheitsabteilung versucht, das Risiko zu minimieren, während die IT-Ops-Abteilung die Leistung und die Erfahrung der Endbenutzer optimieren möchte.

Das Sicherheitsteam

behandelte früher alles als Risiko, oft ohne praktische Möglichkeit, die relevanten Bedrohungen für das Unternehmen zu identifizieren, und mit wenig Bewusstsein dafür, wie sich Patch-Rollouts auf die tägliche Arbeit auswirken. .

Das IT-Ops-Team

muss die Service-Level-Vereinbarungen (SLAs) mit den Endbenutzern abstimmen, um die reguläre Arbeit wie geplant fortzusetzen, und die theoretische Bedrohung durch potenzielle Ransomware, die nie nachzulassen scheint.

Ein hervorragendes RBPM-System wird versuchen, diesen natürlichen Reibungspunkt durch gemeinsame Informationen und eine gegenseitig verständliche Risikoanalyse zu verringern:

Die Sicherheitsabteilung

wird nur die Schwachstellen priorisieren, die für die Cybersicherheitslage des Unternehmens wirklich wichtig sind.

Das IT-Ops-Team

kann sich selbst ein Bild davon machen, wie sich die Schwachstellen in Echtzeit auf die Endbenutzer auswirken könnten, und ist daher eher bereit, sich Zeit für die Einführung zu nehmen.

3. Arbeiten Sie parallel, um die Zeit bis zum Patch durch ein RBPM SLA zu verkürzen.

Im günstigsten Fall macht eine risikobasierte Patch-Management-Lösung alle Beteiligten auf Schwachstellen aufmerksam und zeigt ihnen, wie sie diese in Echtzeit beseitigen können.

IT-Ops- und Sicherheitsteams würden dieselbe Methodik verwenden und verstehen, um Risiken zu priorisieren, sodass sie parallel arbeiten und sich an mehreren Punkten während des Abhilfeprozesses abstimmen können, um sicherzustellen, dass sie sich darüber einig sind, was gelöst werden muss.

Mit diesem Ansatz kann der Wartungszyklus von Wochen auf Tage oder Stunden verkürzt werden, je nachdem, wie kritisch die Schwachstellen sind – und wie gut die einzelnen Teams mit ihren abteilungsübergreifenden Partnern zusammenarbeiten.

Die IT-Ops- und Sicherheitsteams müssen interne bewährte Verfahren einführen und sich gemeinsam auf Wartungsfenster einigen, die sowohl die Ziele der einzelnen Teams als auch die allgemeinen Unternehmensziele berücksichtigen.

Zu diesem Zweck sollten Sie eine Service-Level-Vereinbarung für das Patch-Management zwischen den IT-Ops- und Sicherheitsteams treffen.

Erstellen Sie Ihr SLA

In diesem SLA sollten die Erwartungen an die Zusammenarbeit und der Zeitrahmen für jeden Schritt festgelegt werden, damit jeder weiß, was wann und durch wem umgesetzt wird.

Die SLA sollte Folgendes enthalten:

- **Alle Definitionen –** selbst für so etwas Grundlegendes wie die Bedeutung von „Schwachstelle“!
- **Erforderliche Spezifikationen** und eingesetzte Technologiepakete für jede Stufe.
- **Kriterien für die Priorisierung von Schwachstellen.**
- **Kommunikationsfrequenz** während des Patching-Zyklus.
- **Explizite Ausnahmen** für den Fall, dass Schwachstellen out-of-band und/oder außerhalb des regulären Wartungszyklus behoben Wartungszyklus behoben Wartungszyklus behoben werden müssen.

Besonderes Augenmerk sollte auf die Festlegung erreichbarer und realistischer Leistungsindikatoren (Key Performance Indicators, KPIs) für alle beteiligten Abteilungen gelegt werden, wobei nach Möglichkeit gemeinsame KPIs verwendet werden sollten.

Auswirkungen in der realen Welt:

SLAs für Patches und Schwachstellen

Ein großer globaler Hersteller mit über 100.000 Geräten berichtete Ivanti von der Implementierung eines SLAs für Schwachstellen zwischen seinen IT-Ops- und Sicherheitsteams.

Das Unternehmen hat seitdem eine Konformitätsrate von 95 % bei der Behebung von Schwachstellen innerhalb des von der SLA vorgegebenen Zeitrahmens von 2 Wochen erreicht.

4. Richten Sie Pilotgruppen mit den wichtigsten Stakeholder für die Festlegung von Patch-Prioritäten und das Testen ein.

Pilotgruppen sind vorher festgelegte (und geschulte) Gruppen von repräsentativen Benutzerrollen und Gerätekonfigurationen, die Schwachstellen-Patches in einer Live-Umgebung testen können, bevor sie im gesamten Unternehmen eingeführt werden.

Denn wenn ein Patch geschäftskritische Software zum Absturz bringt, dann ist es besser, das auf einigen wenigen Rechnern festzustellen, als das gesamte Unternehmen lahmzulegen.

Pilotgruppen ergänzen kontrollierte Testlaborumgebungen, um besser vorhersagen zu können, wie sich Patches auf die Geschäftsaktivitäten auswirken können.

Da Testsysteme nur selten die Auswirkungen auf die nachgelagerten Bereiche bestimmen, ist die Einrichtung einer oder mehrerer Pilotgruppen für die Einführung eines Patches entscheidend, um das Potenzial für negative betriebliche Auswirkungen zu verringern.

“Denn wenn ein Patch geschäftskritische Software zum Absturz bringt, dann ist es besser, das auf einigen wenigen Rechnern festzustellen, als das gesamte Unternehmen lahmzulegen.”

Die Zustimmung für Pilotgruppen gewinnen

Diese Best Practice setzt voraus, dass die Patch-Administratoren von der gesamten Organisation unterstützt werden – nicht nur vom IT-Ops-Team, denn zu den relevanten Pilotgruppen sollten alle wichtigen Anwendungsgruppen oder Abteilungen gehören, in denen geschäftskritische Systeme eingesetzt werden.

Zu diesem Zweck sollten Sie über die Service-Map der IT hinausgehen und die Zielbenutzergruppen direkt fragen, wie ihre Geräte und Daten miteinander interagieren und wie sich jede Aktualisierung auf ihre üblichen Prozesse auswirken könnte.

Sie gewinnen Reputationspunkte, wenn Sie nachfragen, bevor wieder ein Patch versehentlich die Anwendungen während der Geschäftszeiten lahmlegt. Außerdem bilden die von Ihnen geknüpften Kontakte die Grundlage für künftige Pilotgruppen, zu denen auch engagierte Stakeholder gehören, die Ihnen proaktiv Hilfe und Einblicke bieten, die Sie sonst nicht hätten.

Erstellen Ihrer Patch-Pilotgruppen

Pilotgruppen sollten:

- Mindestens in eine erste „primäre“ Pilotgruppe eingeteilt werden – um sicherzustellen, dass nichts Wesentliches kaputt ist – mit erweiterten Pilotgruppen, um seltenere oder anwendungsspezifische Probleme zu ermitteln.
- Die Ziele des Unternehmens berücksichtigen sowie die spezifischen Ziele, die alle beteiligten Abteilungen – d. h. IT-Ops- und Sicherheitsabteilung – verfolgen.
- Jederzeit Feedback geben.
- Alle im Unternehmen verwendeten Geräte darstellen um Probleme mit der Patch-Kompatibilität ermitteln.
- Alle Benutzerprofile (auch bekannt als „User Personas“) in der Umgebung des Unternehmens berücksichtigen.

Mitarbeiter und Stakeholder – unabhängig von ihrer Teilnahme an Pilotgruppen – müssen verstehen, warum das Patchen von Schwachstellen entscheidend für die Verringerung des Risikos von Ransomware und anderen Cyberangriffen ist.

Die Botschaft sollte klar sein: Tests sind unerlässlich, um die Sicherheit des Unternehmens und Ihrer Arbeit zu gewährleisten. Wenn Sie als Testperson einer Pilotgruppe ein paar Unannehmlichkeiten auf dem Ihnen zugewiesenen Gerät in Kauf nehmen, haben Sie die gesamte Abteilung vor einem kritischen Ausfall bewahrt.

Auswirkungen in der realen Welt:

PrintNightmare[39]

Im Juni 2021 entdeckte ein Forscher eine RCE-Schwachstelle im Windows-Druckspooler.

- Als Windows im Juni dieses Jahres ein Patch für die Schwachstelle im Druckspooler veröffentlichte, dachte der Forscher, dass seine spezielle Schwachstelle behoben sei, und veröffentlichte seine Ergebnisse ... nur um festzustellen, dass Windows ein Patch für eine andere Schwachstelle veröffentlicht hatte.
- Cyberkriminelle machten sich diese Erkenntnisse schnell zunutze und nutzten aktive Exploits, die es Bedrohungsakteuren ermöglichten, ein Opfersystem aus der Ferne mit Administratorrechten zu übernehmen.
- Der erste PrintNightmare-Exploit wurde am 1. Juli 2021 gepatcht, und am 16. Juli 2021 wurde eine neue Version veröffentlicht.
- Seitdem wurden mehrere weitere Patches für den Druckspooler veröffentlicht - im Mai 2022 waren es vier weitere.

Many organizations now prioritize these patches for remediation and pilot group testing, due to excessive operational impact.

Im Juni 2021
entdeckte ein Forscher eine RCE-Schwachstelle im Windows-Druckspooler.

Juli 2021
Windows veröffentlicht erste PrintNightmare-Patches

Juni 2021
Windows patcht verschiedene Schwachstellen; Forscher veröffentlichen Ergebnisse

Mai 2021
4 weitere Patches für den Druckspooler werden veröffentlicht

5. Nutzen Sie die Automatisierung – vor allem bei der Einführung von neuen Produkten.

Die Automatisierung bietet einen großen Vorteil für risikobasierte Patch-Management-Programme, insbesondere wenn es um die Sammlung, Kontextualisierung und Priorisierung von externen Schwachstellenberichten geht.

Wie wir bereits erwähnt haben, wäre der Versuch, ein RBPM-Programm manuell durchzuführen, gelinde gesagt schwer zu bewerkstelligen – ganz zu schweigen von den negativen Auswirkungen auf Ihre Mitarbeiterbindungskennzahlen.

Die Automatisierung kann jedoch auch dazu beitragen, ein Patch-Rollout zu segmentieren, um sicherzustellen, dass das Projekt reibungslos abläuft, während das Patching in großem Umfang erfolgt.

Bewährte Verfahren für automatisierte Patch-Rollouts

Automatisierungsregeln und Gates können bewährte Verfahren für Testsysteme, Pilotgruppen und erweiterte Ringe von Produktionsgruppen durchsetzen, um eine Patch-Management-Erfahrung zu schaffen, die die Ausführung beschleunigt und gleichzeitig die Auswirkungen auf das Unternehmen minimiert.

Ziehen Sie in Erwägung, mit dem automatisierten Patch-Rollout mit Ihrer kleineren primären Testgruppe zu beginnen. Dann erweitern Sie auf:

1. **Eine erste Pilotgruppe** in Ihrer aktiven Umgebung.
2. **Early Adopters,** die etwa 10 % Ihrer Umgebung ausmachen.
3. **Die verbleibende Mehrheit** der Endnutzer der Organisation.

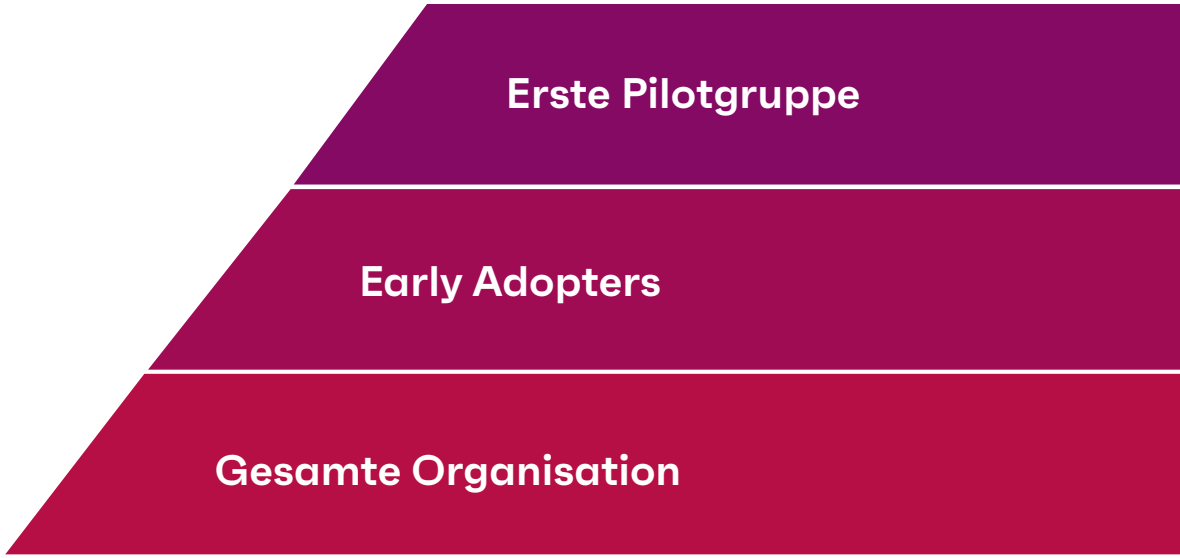
Für diesen Anwendungsfall können Patch-Administratoren Kriterien einrichten und jedem Endbenutzer eine bestimmte Rolle in jeder separaten Gruppe als Teil eines vollständigen Patch-Rollouts zuweisen. Die Automatisierung regelt dann, wer den Patch bekommt und wann dies geschieht.

Patch-Administratoren können den automatisierten Prozess so programmieren, dass er mit komplexen Regeln und Akzeptanzkriterien arbeitet, z. B. dass eine bestimmte Erfolgsquote oder ein direktes Benutzerfeedback erforderlich ist, um eine neue Rollout-Stufe auszulösen.

Vorteile der automatisierten Wartung

Die Automatisierung kann die regelmäßige Wartung übernehmen, sodass die Mitarbeiter aller Abteilungen mehr Zeit haben, die Zusammenarbeit zu verbessern, einen einheitlichen Abstimmungsprozess zu unterstützen und sich mit außergewöhnlichen Bedrohungen zu befassen, wenn sie auftreten.

IT-Ops- und Sicherheitsteams können sogar gemeinsam automatisierte Sicherheitskontrollen entwickeln und konfigurieren, sodass das Sicherheitsteam kleinere Eindämmungsmaßnahmen durchführen und überwachen kann, die bei bestimmten Auslösern aktiviert werden, ohne dass das IT-Ops-Team für jede Aufgabe zuständig ist.

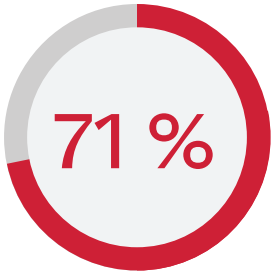


Auswahl eines Anbieters für risikobasiertes Patch-Management

71 % der IT- und Sicherheitsexperten halten das Patchen für zu komplex und zeitaufwändig(40), was in erster Linie darauf zurückzuführen ist, dass es an geeigneten Tools zur Unterstützung ihrer Patch-Management-Strategie fehlt.

Bevor Sie einen risikobasierten Ansatz implementieren, sollten Sie Ihre derzeitigen Prozesse zur Verwaltung von Schwachstellen und Patches bewerten. Sicherheits- und IT-Ops-Teams müssen sich über die Ziele des Projekts und die zu verwendenden Messgrößen einig sein.

Insbesondere müssen sich beide Teams darauf einigen, denselben risikobasierten Ansatz und dasselbe Ranking-System zu verwenden, bei dem nicht nur der Schweregrad und die CVSS-Scores des Anbieters zur Priorisierung von Updates herangezogen werden.



71 % der befragten IT- und Sicherheitsexperten halten das Patchen für kompliziert und zeitaufwändig.(41)

Ihre nächste risikobasierte Patch-Management-Plattform sollte Folgendes umfassen:

- ☐ **Daten** von Netzwerkscannern, Endpunkten, Datenbanken, manuellen Erkenntnissen, IoT-Geräten und anderen unabhängigen Quellen, um einen tiefen Einblick zu erhalten.
- ☐ **Heterogene Unterstützung,** die alle intern unterstützten Betriebssysteme abdeckt.
- ☐ **Erkenntnisse darüber,** welche Schwachstellen mit Ransomware in Verbindung stehen oder als RCE oder PE ausnutzbar sind, die sowohl aus von Menschen erstellten Quellen als auch aus anderen Bedrohungsdaten stammen.
- ☐ **Ein klares Risikobewertungssystem** – entweder automatisch oder bei der Einrichtung anpassbar –, das die Eigenschaften der Schwachstelle und den realen Bedrohungskontext berücksichtigt, um Genauigkeit und Relevanz zu gewährleisten.
- ☐ **Berücksichtigung einzigartiger Risikofaktoren** auf der Grundlage der Vermögenswerte Ihres Unternehmens, mehrerer Quellen für Bedrohungsdaten und externer Zugänglichkeit.
- ☐ **Automatisierungsfunktionen** – oder Integration in Automatisierungsnetze – für Abhilfemaßnahmen und Risikoüberwachung.
- ☐ Warnungen und Benachrichtigungen, die je nach Bedarf und Dringlichkeit an bestimmte Nutzerprofile gesendet werden können.
- ☐ **Vorgefertigte und/oder anpassbare Dashboards,** um die relevanten Informationen schnell an die richtigen Stakeholder weiterzugeben, ohne auf E-Mail-Weiterleitungen oder Erinnerungsketten zu warten.
- ☐ **Bedrohungsbasierte, anpassbare Filter,** die zeigen, wie sich ausgenutzte Schwachstellen in der spezifischen Umgebung eines Unternehmens manifestieren.

Referenced Sources

1. The National Vulnerability Database, abgerufen im Mai 2022
2. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
3. Über 48.285 Schwachstellen jenseits der NVD: Ein Ivanti Research Update
4. The National Vulnerability Database, abgerufen im Mai 2022
5. Über 48.285 Schwachstellen jenseits der NVD: Ein Ivanti Research Update
6. Über 48.285 Schwachstellen jenseits der NVD: Ein Ivanti Research Update
7. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
8. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
9. Das Problem der Bereitstellung eines Patches nur für kritische Schwachstellen: Eine Fallstudie zu Microsoft Zero-Day-Schwachstellen
10. Alles, was Sie über Bluekeep wissen müssen
11. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
12. 2016 Data Breach Investigations Report
13. Null Tage, Tausende von Nächten: Leben in den Zeiten von Zero-Day-Schwachstellen und ihren Exploits
14. Herausforderungen beim Patch-Management: Umfrageergebnisse und Einblicke bei der Umstellung von Unternehmen auf den Everywhere Workplace (2021)
15. Die wichtigsten IT-Trends für den Everywhere Workplace (2021)
16. Herausforderungen bei der Patch-Verwaltung: Umfrageergebnisse und Einblicke bei der Umstellung von Unternehmen auf den Everywhere Workplace (2021)
17. Sieben Ransomware-Trends, die Sie kennen sollten (2021)
18. Herausforderungen bei der Patch-Verwaltung: Umfrageergebnisse und Einblicke bei der Umstellung von Unternehmen auf den Everywhere Workplace (2021)
19. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
20. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
21. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
22. Null Tage, Tausende von Nächten: Leben in den Zeiten von Zero-Day-Schwachstellen und ihren Exploits
23. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
24. IBM Security: Cost of a Data Breach Report 2021
25. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
26. Implement a Risk-Based Approach to Vulnerability Management
27. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
28. Microsoft Exchange ProxyShell and Windows PetitPotam vulnerabilities chained in New Attack
29. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
30. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
31. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
32. Binding Operational Directive 22-01- Reducing the Significant Risk of Known Exploited Vulnerabilities
33. Der Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
34. IBM Security: Cost of a Data Breach Report 2021
35. RDer Ransomware 2022 Spotlight Report: Durch die Brille des Bedrohungs- und Schwachstellenmanagements
36. Pank, Raymond R. „What We Know About Spreadsheet Errors.“ Journal of Organizational and End User Computing (JOEUC) 10, no.2: 15-21. http://doi.org/10.4018/joeuc.1998040102
37. Die wichtigsten IT-Trends für den Everywhere Workplace (2021)
38. Warum IT-Asset-Management wie ein Puzzle ist
39. Patch-Tuesday Mai 2022
40. Herausforderungen bei der Patch-Verwaltung: Umfrageergebnisse und Einblicke bei der Umstellung von Unternehmen auf den Everywhere Workplace
41. Herausforderungen bei der Patch-Verwaltung: Umfrageergebnisse und Einblicke bei der Umstellung von Unternehmen auf den Everywhere Workplace

Über Ivanti

Ivanti macht den Everywhere Workplace möglich. Im Everywhere Workplace nutzen Mitarbeiter unzählige Geräte, um über verschiedene Netzwerke auf ITNetzwerke, Anwendungen und Daten zuzugreifen und so von überall aus produktiv arbeiten zu können. Die Ivanti-Automatisierungsplattform verbindet die branchenführenden Unified-Endpoint-Management-, Zero-Trust-Sicherheits- und Enterprise-ServiceManagement-Lösungen des Unternehmens und bietet Unternehmen eine zentrale Plattform für die Selbstheilung und Selbstsicherung von Geräten sowie für den Self-Service von Endanwendern. Mehr als 40.000 Kunden, darunter 96 der Fortune 100, haben sich für Ivanti entschieden, um ihre IT-Assets von der Cloud bis zum Edge zu erkennen, zu verwalten, zu sichern und zu warten und ihren Mitarbeitern ein hervorragendes Endbenutzererlebnis zu bieten, egal wo und wie sie arbeiten. Weitere Informationen finden Sie unter ivanti.de

Über Ivanti Neurons for Patch Management

Ivanti Neurons for Patch Management ist eine Cloud-native Patch-Management-Lösung mit verwertbaren Informationen über aktive Risiken, Patch-Zuverlässigkeit und Gerätekonformität, Gesundheit und Risiken, die Unternehmen dabei helfen, sich besser gegen Bedrohungen, einschließlich Ransomware zu schützen

ivanti

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