Checkliste zur Schwachstellen-Behebung

Ihre Endpunkte werden immer zahlreicher (Laptops, Server, VMs, Mobilgeräte), und Ihre Benutzer:innen sind überall. Dies geht mit großen Risiken einher, die minimiert werden müssen. Während das Patch-Management Endpunkte auf dem neuesten Stand hält und dazu beiträgt, die Endpunktsicherheit zu erhöhen, sollte die Beschleunigung des Patchings, insbesondere bei kritischen Patches, eine Priorität sein. Die Ausstattung von Patch-Management-Teams mit dynamischem Zugriff auf Schwachstellendaten hilft IT-Teams, Schwachstellen proaktiv zu identifizieren, zu priorisieren und zu beheben, die Reaktionszeit zu verkürzen, die Widerstandsfähigkeit zu erhöhen und die Compliance zu gewährleisten.

34 %
Zunahme der ausgenutzten Schwachstellen

60 %
der Sicherheitsverletzungen betreffen Schwachstellen, für die Patches verfügbar waren, aber nicht angewendet wurden.

24 Tage
durchschnittliche Zeit bis zur Entdeckung einer Sicherheitsverletzung

Quelle: 2025 Verizon Data Breach

Automatisierter Import von Schwachstellendaten
Dynamischer und kontinuierlicher Zugriff auf Schwachstellendaten, verbesserte Transparenz für die datengestützte Priorisierung von Patches und beschleunigtes Patching, insbesondere bei kritischen Schwachstellen.

Risikobasiertes Patching
Setzen Sie Prioritäten bei CVEs und CVSS-Informationen, um die kritischsten Patches zuerst anzuwenden.

KI-gesteuerte Patch-Sentiment-Analyse
Verwenden Sie KI-gesteuerte Patch-Sentiment-Analyse, um die Stabilität von Windows KB-Updates zu bewerten. Dadurch wird sichergestellt, dass Patches auf Basis von fundierten Entscheidungen bereitgestellt und dass bekannte fehlerhafte Patches nicht verteilt werden.

Intuitives Patching-Dashboard
Ermöglichen Sie es Techniker:innen, Schwachstellen zu identifizieren und Patches auf alle Endpunkte zu verteilen, um Ihre Angriffsfläche zu verringern.

Sofortige Warnmeldungen und Benachrichtigungen
Erhalten Sie sofortige Benachrichtigungen per E-Mail, Slack, SMS oder andere Kanäle über Schwachstellen mit hoher Priorität und fehlgeschlagene Patches für eine garantierte Behebung.

Zentralisierter Überblick dank einer einheitlichen Konsole
Verbessern Sie die Genauigkeit und steigern Sie die Effizienz mit einem Überblick über Endpunkte, Patches und den Patch-Status. Stellen Sie sicher, dass fehlgeschlagene oder abgelehnte Patches schnell behoben werden, insbesondere bei kritischen Schwachstellen.

Gewährleistung der Compliance
Sorgen Sie für die Einhaltung von HIPAA, DSGVO, NIST, PCI DSS und anderen Sicherheitsstandards.

Integrierte Fehlerbehebungs-Tools
Integrierte Tools wie Remote-Terminal, Registrierungs-Editor und Remote-Zugriff erleichtern das effektive Patching von Workflows.

Mehr Informationen unter www.ninjaone.com/de/schwachstellen-management/

Kostenlos testen