IBM implementiert Tivoli Endpoint Manager für seine internen Prozesse

Deutlicher Rückgang bei den Sicherheitsproblemen bei Endpunkten

Überblick

Anforderung

Durch die wachsende Anzahl an nicht standardisierten Endpunkten und immer komplexere Sicherheitsbedrohungen benötigte IBM einen neuen Lösungsansatz, um auch bei diesen veränderten Bedingungen den Schutz der internen Infrastruktur weiterhin zu gewährleisten.

Lösung

Mit Tivoli Endpoint Manager konnte IBM mehr Echtzeittransparenz bei den Endpunkten schaffen und Probleme bei über 500.000 Endpunkten automatisch beheben. Zudem konnten dadurch zahlreiche Richtlinien auf Basis von Mitarbeiterrollen und Datenzugriffsberechtigungen unterstützt werden.

Vorteile

Reduzierung der Sicherheitsprobleme bei Endpunkten um 78 Prozent im ersten Quartal nach der Lösungsimplementierung, Senkung der Supportkosten um deutlich über 10 Millionen US-Dollar, Unterstützung von über 500.000 Endpunkten durch nur drei Vollzeitkräfte (FTEs).

Laut Aussage des IBM Chief Information Security Office (CISO) ist ein Anstieg bei den Sicherheitsrisiken festzustellen, die die IBM interne Infrastruktur betreffen. Durch das Wachstum im Unternehmen in Folge von Firmenübernahmen und gemeinsamen Entwicklungsprojekten mit IBM Business Partnern stieg auch der Prozentsatz der Mitarbeiter, die in einer ungeschützten Infrastruktur arbeiteten oder über eine solche Infrastruktur Verbindungen zum internen IBM Netzwerk herstellten. Hinzu kam außerdem ein Anstieg bei den Windows-fremden Endpunkten. Da sich gleichzeitig Anzahl, Typ und Aggressivität der Sicherheitsbedrohungen in der Branche ebenfalls erhöht haben, sind die Unternehmen deutlich höheren Risiken als bisher ausgesetzt.

Für das CISO-Team stellte sich daher die folgende Frage: Wie können wir unsere Endpunkte unter diesen veränderten Bedingungen effektiv verwalten und schützen? Für David Merrill, im CISO-Team für strategische Aufgaben zuständig, kam nur ein neues Sicherheitsmodell in Frage.

„Das alte Modell war nicht mehr in der Lage, den veränderten Anforderungen gerecht zu werden“, erklärt Merrill. „Bisher verfolgten wir beim Endpunktmanagement einen reaktiven Korrekturansatz. Die Mitarbeiter erhielten entsprechende Workstationberichte. Wenn sie einen Patch nicht installiert hatten oder ihre Virenschutzdefinitionen nicht mehr aktuell waren, schickten wir ihnen Links zu Informationen, wie sie dieses Problem lösen konnten. Um unsere Infrastruktur besser schützen zu können, mussten wir auf ein Modell umstellen, mit dem wir eine kontinuierliche Compliance mit internen Sicherheitsrichtlinien gewährleisten konnten, sodass auftretende Probleme automatisch behoben wurden“.

„Nach der Implementierung von Tivoli Endpoint Manager konnten wir einen Rückgang bei den Endpunktsicherheits-problemen um 78 Prozent im ersten Quartal der weltweiten Nutzung der Lösung feststellen, was deutlich über unseren Schätzungen aus der Pilotphase lag. Dadurch konnte man davon ausgehen, dass die Einsparungen wesentlich über den ursprünglich geschätzten 10 Millionen US-Dollar liegen würden – und ich bin überzeugt, dass wir noch höhere Einsparungen erzielen werden, sobald die Implementierung auf allen 750.000 Endpunkten abgeschlossen ist“.

– David Merrill, Strategist, Chief Information Security Office, IBM

Kontinuierliche Compliance mit internen Sicherheitsrichtlinien

Das CISO-Team konzentrierte sich auf zwei grundlegende Anforderungen. Erstens wollte das Team Patches schneller bereitstellen. Bei den im Unternehmen vorhandenen Tools mussten die Mitarbeiter Sicherheitspakete für die Implementierung neu verpacken. Dies verzögerte die Patchverfügbarkeit häufig um bis zu 14 Tage.

„Jede Verzögerung bei der Patchbereitstellung kann auch das Zeitfenster für Anfälligkeiten vergrößern“, erklärt Merrill. „Wir mussten also das Neuverpacken von Patches vermeiden, da es ineffizient und kostspielig war“.

Zweitens musste das CISO-Team, wie Merril es formulierte, die „kontinuierliche Compliance mit internen Sicherheitsrichtlinien“ gewährleisten.

„Unser bisheriges Modell bot bei der Ausführung der Tools nur eine punktuelle Sicht zum Status eines Endpunkts“, sagt Merrill. „Es gab also durchaus auch Zeitfenster, in denen der Status eines Endpunkts nicht bekannt war. Mit Tivoli Endpoint Manager können wir den Status von Endpunkten nun transparent und in Echtzeit abrufen und damit belegen, dass unsere Infrastruktur durchgängig unseren internen Sicherheitsrichtlinien entspricht“.

Ein Pilotprojekt als Business Case

Eine Veränderung, die über eine halbe Million Mitarbeiter und Partner unterstützen kann, setzt eine umfassende Kosten-Nutzen-Analyse voraus. Folglich setzte das Team einen POC-Prozess (Proof of Concept) mit IBM Tivoli Endpoint Manager in Gang.

„Und dieser POC-Prozess bestärkte mich in meiner Einschätzung, dass dies der richtige Weg für uns war“, beschreibt Merrill. „Wir testeten die Lösung umfassend, um ganz sicher zu sein, dass sie auch hielt, was sie versprach – und wurden nicht enttäuscht. Im nächsten Schritt brachten wir ein größeres Pilotprojekt auf den Weg, zunächst mit ein paar tausend Endpunkten, später dann mit ca. 18.000 Endpunkten, um die Skalierbarkeit zu überprüfen“.

Durch dieses Pilotprojekt hatte unser Team zudem die konkreten Daten zur Hand, die es brauchte, um das Management zu überzeugen.

Lösungskomponenten

Software

- IBM Tivoli Endpoint Manager, built on Bigfix Technology.

Server

- IBM System x

„Dies war eine der größten und schnellsten internen Kunden-implementierungen in der Geschichte der IBM.“

– David Merrill

„Die über das Pilotprojekt ermittelten Daten waren der Wendepunkt“, sagt Merrill. „Basierend auf den Ergebnissen des Pilotprojekts kamen wir beim Support für Sicherheitsprobleme bei Endpunkten auf geschätzte Einsparungen von 50 Prozent. Jeder, der diese Ergebnisse sah, kam sofort zu dem Schluss, dass diese Lösung 'so schnell wie möglich implementiert werden sollte'. Im Dezember 2010 nahmen wir das Projekt in Angriff und schon sechs Monate später hatten wir Tivoli Endpoint Manager auf mehr als 550.000 Endpunkten weltweit implementiert. Dies war eine der größten und schnellsten internen Kundenimplementierungen in der Geschichte der IBM.“

Die Implementierung bei IBM wurde in drei geografische Gruppierungen unterteilt und organisiert: Nordamerika, Europa und Asien/Pazifik. Jeder geografische Bereich wird von einem dedizierten physischen Tivoli Endpoint Manager-Management-Server unterstützt – einem IBM System x Server mit redundanten Speicherplattenarrays (RAIDs). „Die IBM System x-Plattform bietet hohe Leistung und ausreichend optische Speicherkapazität und ermöglicht dadurch hohe Transaktionsraten und das zentrale Management von ca. 250.000 Endpunkten für jeden geografischen Bereich“, erklärt Merrill.

Über so genannte Tivoli Endpoint Manager-Relays kommuniziert die Software mit Endpunkten, die nicht regelmäßig mit dem Netzwerk verbunden sind, wie z. B. Supportsysteme, die von Mitarbeitern für die Unterstützung von IBM Kunden verwendet werden.

„Wir wollen alle Bereiche abdecken, vom Server bis zu Smartphones“, sagt Merrill. „Schwerpunktmäßig konzentrierten wir uns zunächst auf Workstations. Wir begannen mit Windows-basierten Endpunkten und wenden uns nun Mac- und Linux-Systemen zu. Außerdem binden wir Tivoli Endpoint Manager in den Standardbuild für jede neue IBM Maschine ein“.

Reduzierung der Sicherheitsprobleme bei Endpunkten um 78 Prozent

Durch den Einsatz von Tivoli Endpoint Manager konnte das Team den Zeit- und Kostenaufwand für die Überwachung von Endpunkten reduzieren, Patches effizienter anwenden und neue Konfigurations-einstellungen und Sicherheitssoftware wie Firewalls und Virenschutz-lösungen schneller implementieren. Bei der Implementierung ermittelte Tivoli Endpoint Manager, welche Patches für jeden einzelnen Endpunkt fehlten, und wandte die erforderlichen Patches automatisch an. Zudem ist Tivoli Endpoint Manager in der Lage, spezielle Aktionen für eine bestimmte Endpunktkonfiguration oder einen bestimmten Benutzertyp festzulegen.

„Obwohl bei uns das Thema Sicherheit immer im Mittelpunkt steht, ist ein weiterer großer Vorteil auch die höhere Effizienz und die Fähigkeit, unsere Endpunkte mit nur drei Vollzeitkräften verwalten zu können.“

– David Merrill

Hinzu kommt, dass Tivoli Endpoint Manager automatisch ca. 90 Prozent der Windows-Anforderungen selbst korrigiert, die bisher über Workstationberichte und manuelle Korrekturmaßnahmen durch die Mitarbeiter aufwendig erfüllt werden mussten. Tivoli Endpoint Manager-Administratoren verfügen nun über ausreichend Echtzeittransparenz, um den Status jedes Endpunkts zuverlässig überprüfen zu können.

Patches stehen jetzt innerhalb von 24 Stunden zur Verfügung (bisher konnte dies durchaus bis zu 14 Tage dauern). So konnte das Unternehmen seine Patchzykluszeiten um 60 Prozent reduzieren und die Patch-Compliancerate deutlich erhöhen (98 Prozent der angewandten erforderlichen Patches). Obwohl die Patches innerhalb von 24 Stunden verfügbar sind, versäumt es Merrill nicht, herauszuheben, dass das Team die Verteilung neuer Patches erst innerhalb eines Zeitraums von 48 Stunden vornimmt, um das Risiko fehlerhafter Patches so gering wie möglich zu halten.

„Wir könnten durchaus 98 Prozent der Patches innerhalb von 24 Stunden verteilen. Wir haben diesen Prozess aber ganz bewusst verlangsamt, um sicherzustellen, dass keine Probleme mit den Patches auftreten oder möglicherweise 'unsaubere' Patches verwendet werden“, verdeutlicht Merrill. „Durch eine zu schnelle Aktualisierung einer halben Million Systeme würden wir zum Testzentrum für Softwareanbieter werden. Und diesem Risiko wollen wir uns bewusst nicht aussetzen“.

Einsparungen in Millionenhöhe

Bei der Implementierung waren die beim Pilotprojekt ermittelten Einsparungen als eher konservativ zu bezeichnen.

„Anfänglich waren wir auf der Grundlage des Pilotprojekts von einem Rückgang bei den internen Sicherheitsproblemen von 50 Prozent ausgegangen“, sagt Merrill. „Dies würde einer Einsparung von rund 10 Millionen US-Dollar alleine bei den internen Supportkosten für Sicherheitsprobleme entsprechen. Nach der Implementierung von Tivoli Endpoint Manager konnten wir einen Rückgang bei den Endpunktsicherheitsproblemen um 78 Prozent im ersten Quartal der weltweiten Nutzung feststellen, was deutlich über unseren Schätzungen aus der Pilotphase lag. Dadurch konnte man davon ausgehen, dass die Einsparungen wesentlich über den ursprünglich geschätzten 10 Millionen US-Dollar liegen würden – und ich bin überzeugt, dass wir noch höhere Einsparungen erzielen werden, sobald die Implementierung auf allen 750.000 Endpunkten abgeschlossen ist“.

„Eines der überzeugendsten Merkmale von Tivoli Endpoint Manager ist, dass wir verschiedene Bedingungen miteinander verknüpfen und innerhalb weniger Minuten sehen können, ob Endpunkte einer neuen Sicherheits-bedrohung ausgesetzt sind.“

– David Merrill

Im heutigen Marktumfeld, in dem Unternehmen ständig nach Mitteln und Wegen suchen, um die Mitarbeiterproduktivität zu erhöhen, fällt bei dieser Lösung auf, dass für die Verwaltung von über 500.000 Endpunkten nur drei Vollzeitkräfte benötigt werden.

„Obwohl bei uns das Thema Sicherheit immer im Mittelpunkt steht, ist ein weiterer großer Vorteil auch die höhere Effizienz und die Fähigkeit, unsere Endpunkte mit nur drei Vollzeitkräften verwalten zu können“, sagt Merrill.

Erweiterte Untersuchungsprozesse für die heutigen anspruchsvollen Herausforderungen bei der Sicherheit

Bei Projektbeginn war das Patch-Management das zentrale Element. Mittlerweile nutzt das CISO-Team die Tivoli Endpoint Manager-Software auch für andere Zwecke und untersucht damit ganz spezielle Sicherheitsprobleme. Erst kürzlich trug das Team Informationen zu einem Sicherheitsrisiko zusammen, bei dem eine Kombination aus Änderungen an DLL-Dateien und Registryeinträgen festzustellen war. DLL-Dateien enthalten Code, der von Programmen aufgerufen wird, um eine bestimmte Funktion (z. B. Drucken von Dokumenten) auszuführen. Registryeinträge sind Systemeinstellungen, die für die Stabilität des Computerbetriebssystems wichtig sind. Änderungen an diesen Dateien können hohe Risiken für Unternehmen in Bezug auf Sicherheitsverletzungen und sicherheitsrelevante Ausfälle nach sich ziehen. Daher ist es besondes wichtig, dass das CISO-Team innerhalb kürzester Zeit sicherstellen kann, dass die IBM Systeme davon nicht betroffen sind.

„Eines der überzeugendsten Merkmale von Tivoli Endpoint Manager ist, dass wir verschiedene Bedingungen miteinander verknüpfen und innerhalb weniger Minuten sehen können, ob Endpunkte einer neuen Sicherheitsbedrohung ausgesetzt sind“, sagt Merrill. „Wir müssen nun nicht mehr nach jeder Bedingung einzeln suchen und die Ergebnisse dann manuell konsolidieren. Außerdem müssen wir bei der Behebung eines Problems die physische Maschine nicht mehr erst zeit- und kostenintensiv suchen, weil die Systeme in der Regel auf verschiedene Standorte in verschiedenen Ländern verteilt sind. Tivoli Endpoint Manager ist flexibel genug, sodass wir Technologien für nahezu jedes Problem bereitstellen oder entsprechend steuern können“.

Weitere Informationen

Wenn Sie mehr über IBM Endpoint Management-Lösungen erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/tivoli/endpoint

Nutzen Sie Tivoli Software noch effizienter, indem Sie an einer der weltweiten unabhängigen Tivoli User Groups teilnehmen. Weitere Informationen hierzu erhalten Sie unter www.tivoli-ug.org

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

TIC14204-DEDE-00