



solothurner
spitäler so H

“Bei der Migration zu Ninja haben wir festgestellt, dass einige der 425 Server seit Monaten nicht gepatcht worden sind“

Yanick Häuptli, *System Engineer*

STANDORT

Schweiz

BRANCHE

Gesundheit

ENDPUNKTE

430

PRODUKTE

NinjaOne Core

HERAUSFORDERUNG

Die Solothurner Spitäler AG ist seit 2006 in Händen einer gemeinnützigen Aktiengesellschaft und betreibt die öffentlich-rechtlichen Spitäler im Schweizer Kanton Solothurn. Trotz der Herausforderungen der Pandemie und des sich zuspitzenden Fachkräftemangels gelingt es dieser Traditionseinrichtung, deren Anfänge bis ins 15. Jahrhundert zurückgehen, mit ihren über 4200 Mitarbeitern die Gesundheitsversorgung der solothurner Bevölkerung auf höchstem Niveau zu sichern.

Gerade vor dem Hintergrund der im Gesundheitssektor in vielen europäischen Ländern vermehrt auftretenden Ransomware-Attacken kommt dem sicheren Betrieb der IT-Infrastruktur der Spitäler eine besonders kritische Bedeutung zu. Ein fundamentaler Bestandteil davon ist das Patch-Management der 430 Server. Dafür maßgeblich verantwortlich sind Michel Schmid und Yanick Häuptli.

→ „Dank der intuitiven Benutzeroberfläche von NinjaOne und dem robusten Windows-Server-Patching konnten wir unseren Arbeitsaufwand um 22% senken“

WARUM DIE VORHERIGE PATCH MANAGEMENT LÖSUNG FÜR DIE SOLOTHURNER SPITÄLER NICHT MEHR TRAGBAR WAR

Ursprünglich wurde in den Spitälern ausschließlich mit WSUS gearbeitet. In den Jahren 2017 und 2018 wurde für das Patch-Management schließlich eine kommerzielle On-Premise-Lösung für das Patching eingeführt. Ein neuer IT Manager war hier die treibende Kraft. Er brachte aus einer vorherigen Tätigkeit eine Reihe von Powershell-Skripten mit, die für den Betrieb dieser Lösung in ihrer Systemlandschaft unerlässlich waren. Diese Skripte mussten in regelmäßigen Abständen angepasst und aktualisiert werden, was von den heute Verantwortlichen als problematisch angesehen wurde. Im Grunde wurden alle Patching-Jobs durch diese Skripte gesteuert.

Dann gab es ein Update, wonach die besagten Powershell-Skripte nicht mehr funktionierten. Der Support der vorherigen Lösung hatte ihnen mitgeteilt, dass sie nur noch die Möglichkeit hätten, alles über die Rest API laufen zu lassen. Dies hätten sie technisch umsetzen können. Allerdings wäre die Dokumentation für Kollegen, welche nur am Rande mit Patching zu tun haben, viel zu kompliziert geworden. Schließlich wurde im Team die Entscheidung getroffen, sich auf dem Markt nach einer einfach zu bedienenden Cloud-Lösung umzuschauen.

WODURCH KONNTE NINJAONE ÜBERZEUGEN?

Das Server-Patching wird bei den Solothurner Spitälern in Gruppen durchgeführt.

Dementsprechend gibt es gemäß der internen SLAs eine Bronze-, eine Silber-, und eine Goldgruppe, wobei in der Goldgruppe die kritischsten Server sind und in den anderen beiden Gruppen die weniger kritischen. Das Ausrollen der Patches wird in der zweiten, dritten und vierten Woche des Monats durchgeführt. Die Patches werden bei den weniger kritischen Gruppen zuerst getestet und erst nach diesen Tests auf den kritischsten Servern installiert.

„Neben der nicht zufriedenstellenden Benutzerfreundlichkeit bei der On-Premise-Lösung gab es noch einen weiteren Störfaktor: Die Patch-Scans und die Patch-Installation sind nicht sauber getrennt.“

Das wird insbesondere problematisch, wenn Microsoft Patches außerhalb des klassischen Patch-Tuesday herausbringt. In der vorherigen Lösung wird vor der geplanten Patch-Installation automatisch ein weiterer Scan durchgeführt. Das bedeutet, dass Patches ungewollt und ungetestet in die kritische Servergruppe reinrutschen können. Um das zu vermeiden, muss man entweder das Monitoring des Patching verstärken und mehr händisch arbeiten oder mit dem unguten Gefühl leben, dass ungetestete Patches auf den kritischsten Servern der Infrastruktur installiert werden, was wiederum zu Störungen oder sogar Unterbrechungen beim Betrieb führen kann. Diese klare Trennung zwischen

Patch-Scan und Patch-Installation war eine zentrale Anforderung bei der Auswahl eines Tools und ist in NinjaOne gegeben.

„Dank der intuitiven Benutzeroberfläche von NinjaOne und dem robusten Windows-Server-Patching konnten wir unseren Arbeitsaufwand um 22% senken“, stellt Michel Schmid, der schon seit 20 Jahren für die Solothurner Spitälern in der IT tätig ist, nach ein paar Berechnungen fest.

Eine intuitive Bedienung und die Trennung von Scan und Deployment sind wichtig. Aber auch die weiteren Anforderungen konnte NinjaOne im Verhältnis zur Konkurrenz, wie z. B. Topia Vicarius und PatchManager Plus, am besten erfüllen. Dazu hatten Michel und Yanick noch eine mögliche Anbindung an einen WSUS-Server, eine granulare Patch-Klassifizierung, eine mögliche Deaktivierung bestimmter Software-Updates und eine gute Abbildung des Patch-Managements in Gruppen im Policy-Management gezählt. In dem Punktesystem ihrer Entscheidungsmatrix sind sie bei NinjaOne zu einem Ergebnis von 96,3% gekommen.

„Bei der Migration zu Ninja haben wir festgestellt, dass einige der 430 Server seit Monaten nicht gepatcht worden sind“, erinnert sich Yanick.

In unter einem Monat konnten sie die Implementierung mit der Hilfe des Supports von NinjaOne umsetzen. Auch nach einem Jahr sind die IT-Verantwortlichen davon überzeugt, dass sie die richtige Entscheidung getroffen haben.

NinjaOne ist eine führende Unified-IT-Management-Plattform, welche die Arbeit von IT-Teams vereinfacht. Mit NinjaOne können MSPs und IT-Abteilungen ihre Aufgaben im Endpunktmanagement verwalten, automatisieren und alle Probleme auf einer schnellen, modernen und intuitiven Plattform lösen. Dadurch werden die Effizienz der Techniker und die Zufriedenheit der Endnutzer verbessert.

Starten Sie noch heute Ihr kostenfreies 14-tägiges Testkonto

