

GESIS

Die globale Stahlproduktion rund um die Uhr gestattet keine Ausfallzeiten. Der Salzgitter-Konzern nutzt daher für den Betrieb seiner geschäftskritischen Anwendungen SUSE Linux Enterprise Live Patching. Systemadministratoren des IT-Dienstleisters GESIS können damit Security-Patches für den Linux-Kernel installieren, ohne die Systeme offline nehmen zu müssen. Heute muss GESIS Unternehmensleiter nicht mehr davon überzeugen, unerwünschte Ausfallzeiten zu planen, sondern kann Systeme alle sechs bis acht Wochen nahtlos patchen, ohne dass es zu Störungen kommt.

Überblick

Der IT-Service-Anbieter GESIS (Gesellschaft für Informationssysteme mit beschränkter Haftung) stellt für den Stahlkonzern Salzgitter Netzwerk-, Data Center-, eBusiness-, Business Intelligence-, Dokumentenverwaltungs- und SAP-Anwendungsservices bereit. Das Unternehmen mit Sitz in Salzgitter, Deutschland, beschäftigt 200 Mitarbeiter.

„Mit SUSE Linux Enterprise Live Patching können wir das Sicherheitspatching schnell während der Geschäftszeiten durchführen. Dank der Anwendung von Linux-Kernel-Fixes ohne Beeinträchtigung geschäftskritischer SAP-Anwendungen, die auf dem System ausgeführt werden, müssen wir keine Ausfallzeiten planen. Wir können Systeme praktisch patchen, wann immer wir möchten.“

THOMAS LOWIN

Server Operations Lead
GESIS

Mit mehr als 30 Jahren Erfahrung bietet GESIS Lösungen und Services an, die von Infrastruktur und Betrieb über Fertigung, Materiallogistik und Produktionssicherung bis hin zu Finanzen und Controlling, Marketing und Vertrieb sowie Personalwesen reichen.

GESIS gehört zum Salzgitter-Konzern, einem der größten Stahlproduzenten Europas mit etwa 25.000 Mitarbeitern und einem Jahresumsatz von 9 Milliarden Euro. Der Konzern besteht aus mehr als 150 Tochtergesellschaften weltweit, für die GESIS IT-Services bereitstellt.

Herausforderung

WELTWEIT BOOMENDES BUSINESS LÄSST WENIG RAUM FÜR WARTUNGSFENSTER

Der globale Markt für Stahlprodukte wächst ungebrochen – getrieben vor allem durch die Entwicklung in vielen Schwellenländern. Für die boomende Industrie, zunehmende Urbanisierung und ehrgeizigen Infrastrukturprojekte in Ländern wie Brasilien und Russland werden Stahlprodukte benötigt – der Salzgitter-Konzern will von dieser Nachfrage profitieren.



Foto: Salzgitter AG



GESIS auf einen Blick:

GESIS (Gesellschaft für Informationssysteme mit beschränkter Haftung) ist der zentrale IT-Service-Anbieter des Salzgitter-Konzern, zu dem Stahl- und Technologieunternehmen mit etwa 25.000 Mitarbeitern und einem Jahresumsatz von 9 Milliarden Euro gehören.

■ Branche und Standort

Verarbeitende Industrie, Salzgitter, Deutschland

■ Produkte und Services

SUSE Linux Enterprise Live Patching
SUSE Linux Enterprise Server for SAP Applications
SUSE Manager

■ Ergebnisse

- + Vermeidet bis zu 125 Stunden kumulierte Downtime – bei jedem einzelnen Patch
- + Reduziert die Koordinierungskosten zwischen der IT-Abteilung und den Unternehmensabteilungen für das Patching, wodurch die Teams 50 % an Kommunikations- und Administrationsaufwand einsparen
- + Erhöht die Sicherheit, indem gewährleistet wird, dass die Systeme mit aktuellen Linux-Kernel-Patches auf dem neuesten Stand sind
- + Maximiert die Verfügbarkeit von Diensten, da Systeme für das Patching nicht offline genommen werden müssen

Um das aktuelle Wirtschaftsklima optimal zu nutzen, hat sich Salzgitter Wachstum und Innovation auf allen Märkten zum Ziel gesetzt. Im Rahmen seiner zukunftsorientierten Geschäftsstrategie strebt der Konzern im Zeitraum von 2017 bis 2021 ein organisches Wachstum von mehr als 250 Mio. EUR pro Jahr an.

Mit seinem globalen Produktions- und Servicenetz hat der Salzgitter-Konzern deutliche Vorteile gegenüber seinen Wettbewerbern. Der Konzern verfügt über Produktionsstätten auf der ganzen Welt, unter anderem in Deutschland, den USA, Mexiko, Brasilien, Indien und China. Diese Betriebe arbeiten rund um die Uhr und an 365 Tagen im Jahr. Um die Fertigungsstraßen in Betrieb zu halten und Produkte ohne Verzögerung auf den Weg zum Kunden zu bringen, nutzt das Unternehmen leistungsfähige IT-Systeme. In dieser hoch automatisierten und eng miteinander verbundenen Produktions- und Logistikumgebung sind geschäftskritische SAP-Unternehmensanwendungen besonders wichtig, um einen zuverlässigen Ablauf zu gewährleisten – Tag für Tag.

Thomas Lowin, Server Operations Lead bei GESIS, erklärt: „Während andere Unternehmen einfach ihre Fertigungsstraßen stoppen können, besteht diese Möglichkeit bei einem integrierten Stahlwerk nicht. Zur Unterstützung der Produktion rund um die Uhr ist der Salzgitter-Konzern auf die ununterbrochene Verfügbarkeit und Zuverlässigkeit seiner IT-Systeme angewiesen. Jede Minute einer außerplanmäßigen Ausfallzeit würde Tausende von Euro kosten und komplexe Produktionspläne verschiedenster Stahlerzeugnisse gefährden.“

BALANCE VON VERFÜGBARKEIT UND SICHERHEIT

Aufgrund der kontinuierlichen Fertigungsprozesse des Salzgitter-Konzerns war es schwierig, bei Systemwartungen, Betriebssystem-Upgrades und vor allem

beim Sicherheitspatching auf dem neuesten Stand zu bleiben.

Nicolas Otten, System Analyst and Engineer bei GESIS, erläutert: „Früher mussten wir Ausfallzeiten einplanen, um einzelne IT-Systeme zu patchen und zu aktualisieren. Da diese Systeme aber unternehmenskritische Workloads unterstützen und der Fertigungsbetrieb rund um die Uhr läuft, fährt der Salzgitter-Konzern sie nur äußerst ungern herunter. Sogar eine kurze Ausfallzeit führt zu erheblichen Störungen. Daher war es immer eine Herausforderung, Geschäftsführer davon zu überzeugen, Systeme offline zu nehmen.“

„Um ein Software-Update bereitzustellen oder ein Sicherheitspatch anzuwenden, mussten wir jedes System für 30 Minuten offline nehmen. Das klingt vielleicht nicht nach einem langen Zeitraum, aber jede Unterbrechung des Produktionsbetriebs stellt ein echtes Problem dar. Wenn wir schließlich die Erlaubnis zum Patchen der Systeme vom Salzgitter-Konzern erhielten, kostete es immer noch viel Zeit und Mühe, die Ausfallzeiten zu planen. Wir mussten viele verschiedene Ansprechpartner kontaktieren, z. B. das SAP-Verwaltungsteam, Anwendungsmanager usw. Es gab viel Hin und Her. Schätzungsweise dauerte es ungefähr eine Stunde, nur ein Wartungsfenster zu vereinbaren.“

REAKTION AUF AUFKOMMENDE SICHERHEITSBEDROHUNGEN

Um die Erwartungen des Salzgitter-Konzerns hinsichtlich eines rund um die Uhr verfügbaren Services zu erfüllen, hat GESIS die Systeme nur dann offline genommen, wenn dies für eine erweiterte Wartung unbedingt erforderlich war, in der Regel etwa einmal pro Jahr.

Thomas Lowin bestätigt: „Da wir Systeme selten offline nehmen konnten, war ein häufiges Patchen einiger Systeme nicht möglich. Bei den wichtigsten Anwendungen

konnten wir nur eine Ausfallzeit pro Jahr einplanen, sodass manche bekannten Probleme für längere Zeiträume nicht behoben wurden. Angesichts der zunehmenden Cyberkriminalität in den letzten Jahren ist es aber wichtiger denn je, Software regelmäßig mit Patches zu aktualisieren, um maximalen Schutz vor externen Bedrohungen zu bieten.“

Für die Gewährleistung der System-sicherheit plante GESIS, häufiger Patches zu installieren. Aber wie sollte dies bei gleichzeitig minimalen Ausfallzeiten möglich sein?

Lösung

VERWALTEN EINER GROSSEN IT-UMGEBUNG

GESIS wandte sich an SUSE, einen seiner wichtigsten Technologiepartner. Nach Erörterung der Ziele und technischen Anforderungen führte das SUSE Team SUSE Linux Enterprise Live Patching bei GESIS ein. Diese hochmoderne Technologie ermöglicht Systemadministratoren, Linux-Kernel-Korrekturen bei laufenden Systemen anzuwenden, ohne den Dienst zu unterbrechen.

Hierzu Thomas Lowin: „Wir nutzen SUSE Linux Enterprise Server seit einigen Jahren zur Unterstützung des IT-Betriebs. Unsere SUSE Linux Enterprise Server-Umgebung ist ausgesprochen stabil, zuverlässig und produktiv und erleichtert uns die Erfüllung der Unternehmensanforderungen. Als wir herausfanden, dass SUSE eine ergänzende Live-Patching-Lösung entwickelt hatte, wollten wir diese unbedingt testen.“

GESIS hostet alle geschäftskritischen Systeme des Salzgitter-Konzerns, einschließlich SAP-ERP-Anwendungen und zunehmend auch SAP-HANA-Datenbanken, die auf SUSE Linux Enterprise Server for SAP Applications ausgeführt werden, sowie allgemeine Infrastrukturdienste auf Microsoft Windows Server. Die Infrastruktur ist

auf 40 physischen Servern mit VMware vSphere vollständig virtualisiert.

Insgesamt betreibt GESIS etwa 500 virtuelle Maschinen, von denen etwa 225 SAP-Software mit SUSE Linux Enterprise Server for SAP Applications und zusätzliche allgemeine Unternehmenssoftware hosten. Für spezielle Workloads, bei denen sich eine Virtualisierung nicht empfiehlt, betreibt GESIS zudem circa 25 dedizierte physische Server mit SUSE Linux Enterprise Server.

INFORMATIONEN ZU SUSE LIVE PATCHING

Mit der SUSE Live Patching-Lösung können Systemadministratoren Linux-Kernel-Fixes ohne Dienstunterbrechung und Neustart von Systemen installieren. So werden geschäftskritische Anwendungen auch bei kritischen Kernel-Sicherheitsupdates weiter ausgeführt.

SUSE Linux Enterprise Live Patching basiert auf der kGraft Linux-Kernel-Technologie von SUSE. SUSE entwickelte kGraft zusammen mit der Linux-Community, um den Schutz von Linux-Systemen ohne Unterbrechung zu verbessern. Durch die zunehmende Verbreitung von In-Memory-Datenbanken wie SAP HANA werden die Auswirkungen von Neustarts sogar noch größer, da es bei diesen normalerweise großen Workloads länger dauert, bis sie vollständig hochgefahren sind. SUSE Linux Enterprise Live Patching nutzt Standard-Kernel-Funktionen und kombiniert diese, um laufende Systeme zu patchen. Die Lösung nutzt das integrierte Debugging- und Analyse-Werkzeug von Ftrace, um zu überwachen, welche Kernel-Funktionen aufgerufen werden. Die SUSE Linux Enterprise Live Patching-Technologie leitet dann Aufrufe von Kernel-Funktionen dynamisch auf eine neue, gepatchte Version dieser Funktion um. Dieser Ansatz stellt sicher, dass keine laufende Software angehalten werden muss, da der Upgrade-Prozess für Benutzerbereichsprozesse (z. B. Unternehmensanwendungen), die außerhalb des Linux-Kernels ausgeführt werden, vollständig im Hintergrund abläuft.

REIBUNGSLOSE UND EINFACHE BEREITSTELLUNG

GESIS erörterte und bewertete SUSE Linux Enterprise Live Patching in Zusammenarbeit mit einem Team von SUSE. Die nahtlose Integration mit der bestehenden SUSE Manager-Lösung des Unternehmens sorgte für eine reibungslose Bereitstellung auf allen Produktionssystemen.

Nicolas Otten erinnert sich: „Wir waren angenehm überrascht, wie schnell und einfach Live-Kernel-Patching für SUSE Linux Enterprise Server implementiert werden konnte. Innerhalb weniger Stunden konnten wir alles in Betrieb nehmen. Die Unterstützung durch SUSE war wie immer hervorragend. Sie standen jederzeit zur Verfügung, um alle Fragen zu beantworten, die wir hatten, und gaben uns während der Implementierung verschiedene hilfreiche Tipps. Auch die Detailgenauigkeit der Lösungsdokumentation hat uns sehr beeindruckt.“

Und Thomas Lowin fügt hinzu: „Die Tatsache, dass wir die Live Patching-Technologie problemlos in SUSE Manager integrieren können, ist für uns ein großer Vorteil. Alles ging sehr schnell, es war so einfach wie das Hinzufügen eines neuen Update-Kanals in SUSE Manager, und wir konnten sofort mit dem Live-Patching beginnen.“

Dank SUSE Linux Enterprise Server Live Patching laufen Anwendungen jetzt während Updates weiter, da das Patching aus Sicht der auf dem Linux-System ausgeführten Anwendung im Hintergrund ausgeführt wird. Dadurch bietet sich GESIS eine enorme Flexibilität, die es Systemadministratoren ermöglicht, erste Schwachstellen schnell und ohne Beeinträchtigung der Verfügbarkeit von Diensten zu beheben. Mit Live-Kernel-Patching für SUSE Linux Enterprise Server kann GESIS Sicherheits- und Zuverlässigkeitspatches auf physischen und virtuellen Servern bereitstellen, ohne dass Systeme offline genommen werden müssen.

Ergebnisse

ERHÖHUNG DER SYSTEMSICHERHEIT

Mit SUSE Linux Enterprise Live Patching konnte GESIS Systemausfallzeiten nahezu eliminieren. Heute kann das Unternehmen Software-Updates und Sicherheitspatches bei Bedarf ohne Dienstunterbrechung bereitstellen. Dies bedeutet, dass GESIS durch den Wegfall zusätzlicher Wartungsfenster in allen SAP-Anwendungen für alle wichtigen Sicherheitspatches potenziell etwa 125 Stunden Ausfallzeit vermeiden kann.

Thomas Lowin merkt an: „Mit SUSE Linux Enterprise Live Patching können wir das Sicherheitspatching schnell während der Geschäftszeiten durchführen. Dank der Anwendung von Linux-Kernel-Fixes ohne Beeinträchtigung geschäftskritischer SAP-Anwendungen, die auf dem System ausgeführt werden, müssen wir keine Ausfallzeiten planen. Wir können Systeme praktisch patchen, wann immer wir möchten. Wir verwenden SUSE Linux Enterprise Live Patching jetzt seit einiger Zeit, und Endbenutzer haben nie eine Auswirkung auf ihre Unternehmensanwendungen festgestellt. Durch die Flexibilität, Systeme im laufenden Betrieb zu patchen, wird die System- und Dienstverfügbarkeit maximiert. So können wir sicherstellen, dass Geschäftsabläufe, die eng in die Fertigungsprozesse integriert sind, ununterbrochen laufen und uns gleichzeitig erheblicher Koordinierungsaufwand und Ärger erspart bleibt.“

Die Möglichkeit eines schnelleren Patchings erleichtert auch zukünftige Zertifizierungen, beispielsweise die Einhaltung der internationalen Norm für Informationssicherheit ISO 27001.

HÖHERE EFFIZIENZ UND VERFÜGBARKEIT VON DIENSTEN

Mit SUSE Linux Enterprise Live Patching konnte GESIS die Anzahl der erforderlichen Systemneustarts reduzieren. Das Unternehmen plant nur einmal im Jahr ein einzelnes Ausfallzeitfenster, um wichtige Wartungsarbeiten und Service Pack-Updates durchzuführen.

„Wir waren angenehm überrascht, wie schnell und einfach Live-Kernel-Patches für SUSE Linux Enterprise Server implementiert werden konnten. Innerhalb weniger Stunden konnten wir alles in Betrieb nehmen. Die Unterstützung durch SUSE war wie immer hervorragend.“

NICOLAS OTTEN

Systems Analyst and Engineer
GESIS

Kontakt:
www.suse.com

Dank Live-Kernel-Patching für SUSE Linux Enterprise Server konnten GESIS und der Salzgitter-Konzern die Koordinierungskosten zwischen den IT- und Unternehmensabteilungen für jede Linux-Kernel-Patch-Bereitstellung senken, wodurch die Teams 50 % an Kommunikations- und Administrationsaufwand einsparen.

Nicolas Otten sagt: „Keine Kernsysteme für 20.000 Benutzer herunterfahren zu müssen, um kleine, aber dennoch sehr wichtige Sicherheits-Patches und Korrekturen zu implementieren, ist für uns eine enorme Erleichterung. Auf diese Weise vermeiden wir den Stress und die Unannehmlichkeiten bei der Planung unerwünschter Ausfallzeiten im Unternehmen. Außerdem müssen wir und unsere Kollegen nicht mehr am Wochenende arbeiten, um Patches zu installieren – ein großer Vorteil für unsere Work-Life-Balance.

Entscheidend ist, dass wir Systeme viel häufiger patchen können als bisher, um sicherzustellen, dass sie sicher sind. Normalerweise patchen wir jetzt sämtliche Systeme alle sechs bis acht Wochen. Es ist auch beruhigend zu wissen, dass wir eine Sicherheitslücke sofort beheben können, wenn sie auftritt. Anstatt also Linux-Kernel-Patches, wie es in der Vergangenheit häufig der Fall war, bis zum nächsten geplanten Ausfallzeitfenster zu verschieben, können wir sie jetzt ohne Auswirkungen auf

den Betrieb anwenden. So werden Risiken minimiert und die Sicherheit erhöht, und wir können die Systeme vor internen und externen Bedrohungen schützen.“

Neben SUSE Linux Enterprise Live Patching hat die Verwendung von SUSE Manager den manuellen Arbeitsaufwand für GESIS erheblich reduziert.

Thomas Lowin erklärt: „Vor der Implementierung von SUSE Manager waren wir gezwungen, erforderliche Patches auf jedem Server einzeln zu installieren. Mit SUSE Manager verfügen wir jetzt über eine benutzerfreundliche Schnittstelle, über die uns angezeigt wird, welche Server am dringendsten Patches erfordern. Dies hat für uns vieles sehr vereinfacht, und auch die Aktualisierung der Server wurde um 75 Prozent beschleunigt. Dank der engen Integration mit SUSE Linux Enterprise Live Patching können wir Sicherheits-Patches auch direkt über SUSE Manager verfolgen, planen und bereitstellen. Einfacher könnte der Schutz unserer Systeme nicht sein.“

ETABLIEREN EINES NEUEN STANDARDS

SUSE Linux Enterprise Live Patching ist bei GESIS schnell zur Standardkonfigurationsoption geworden. Das Unternehmen muss eine höchstmögliche Verfügbarkeit für die Kernanwendungen des Salzgitter-Konzerns sicherstellen, und Live-Kernel-Patching für Linux Enterprise Server hilft GESIS, dieses Ziel zu erreichen.

Nicolas Otten sagt: „Der Salzgitter-Konzern ist für den globalen Betrieb darauf angewiesen, dass alle IT-Systeme rund um die Uhr reibungslos funktionieren. Mit SUSE Linux Enterprise Live Patching müssen geschäftskritische SAP-Unternehmensanwendungen nicht mehr offline geschaltet werden, um Patches anzuwenden. Diese Anwendungen werden nicht nur zur Unterstützung der Finanz- und Back-Office-Verwaltung, sondern auch für die Verwaltung von HR-Self-Service-Funktionen verwendet und mit Stahlproduktionsbetrieben an Standorten auf der ganzen Welt, die rund um die Uhr arbeiten, verbunden. Mit SUSE Linux Enterprise Live Patching können wir Verzögerungen bei grundlegenden Prozessen wie Urlaubsanträgen für 20.000 Mitarbeiter vermeiden und gleichzeitig den nahtlosen Betrieb der integrierten Fertigungsstraßen gewährleisten.“

Thomas Lowin schließt: „Wir verwenden SUSE Linux Enterprise Live Patching jetzt seit einigen Jahren und sind sehr zufrieden. Die Lösung ist für GESIS besonders wertvoll, da wir damit Sicherheit und Verfügbarkeit von Diensten ohne zusätzlichen Verwaltungsaufwand verbessern können. Dies hilft uns dabei, die Fertigungsstraßen des Salzgitter-Konzerns am Laufen zu halten.“