splunk>

CASE STUDY

Swisslos steigert Verfügbarkeit, verbessert Kundenerfahrung und Sicherheit

SWISSLOS

Kurzfassung

Die 1937 gegründete Swisslos Interkantonale Landeslotterie (Swisslos) ist eine Genossenschaft aus 20 Kantonen. Swisslos bietet verschiedene nationale und transnationale Lotterien (Swiss Lotto, Euro Millions), Sportwetten, Bingo und viele andere Lose an. Swisslos musste alte Technologie ersetzen und suchte eine langfristige, skalierbare Analyselösung, die aussagekräftige Echtzeitinformationen über die Daten liefert. Seit der Einführung von Splunk Enterprise zeichnen sich für Swisslos deutliche Verbesserungen ab, wie etwa:

- Verbesserte Kundenerfahrung
- Erkennung und Abwehr komplexer Betrugsversuche
- Verbesserte Compliance-Prozesse

Warum Splunk?

Swisslos zahlt pro Jahr über 600 Millionen Schweizer Franken an Lottogewinner aus und gibt 354 Millionen Schweizer Franken an die kantonalen Lotteriefonds und verschiedene Sportfonds weiter. Mit dem Reingewinn werden jedes Jahr mehr als 12000 Projekte unterstützt, und seit seiner Gründung hat Swisslos über fünf Milliarden Schweizer Franken an karitative und gemeinnützige Projekte gespendet.

Die Herausforderung für Swisslos besteht darin, laufend neue Gewinnspiele in die Plattform integrieren zu müssen. Es ist daher ein hohes Maß an Skalierbarkeit notwendig, damit das System- und Netzwerk-Management wirkungsvoll eingesetzt werden kann. Bisher verwendete Swisslos eine IBM Tivoli-Konsole für das System- und Netzwerk-Management, die jedoch ersetzt werden musste, da sie das Ende ihrer Lebensdauer erreicht hatte. Außerdem wollte das Unternehmen seine Online-Spielplattform (http://www.swisslos.ch) innerhalb des eigenen Rechenzentrums hosten und benötigte deshalb eine dynamischere Infrastruktur für seine 500000 Benutzer. Swisslos wollte in Echtzeit Erkenntnisse aus seinen Daten gewinnen und die Performance und Stabilität der Website beurteilen können.

Swisslos entschied sich für Splunk Enterprise. Gründe waren seine Flexibilität, seine Erweiterbarkeit und die Möglichkeit, die bestehende, heterogene IT von Swisslos zu integrieren. LC Systems, ein Schweizer Splunk-Partner, führte bewährte Verfahren ein und übernahm die Beratung hinsichtlich Typ und Volumen der täglich zu indizierenden Daten. Nach der erfolgreichen Bereitstellung der Splunk-Plattform konnte die IBM Tivoli-Konsole in nur sechs Tagen ersetzt werden.

Branchen

- Medien und Unterhaltung

Splunk Use Cases

- Anwendungsbereitstellung
- IT Operations
- Business Analytics
- Sicherheit und Betrugsbekämpfung

Herausforderungen

- Ersetzen der alten IBM-Konsole
- Dynamischere Plattform für Benutzer
- Aussagekräftige Echtzeiteinblicke in Daten

Auswirkungen für das Unternehmen

- Sofortüberblick über Stabilität und Performance der Website
- Schnellere Reaktion auf Sicherheitsbedrohungen
- Integrierte Sicht auf IT-Abläufe innerhalb der Infrastruktur
- Verbesserte Kundenerfahrung auf mehreren Spielplattformen
- Deutliche Kosteneinsparungen gegenüber alten Lösungen und Vorgängerdatenbank
- Deutliche Zeitersparnis für das IT-Team

Datenquellen

- Anwendungslogs: JREE2-Anwendungsserver, Webserver-Logs, Nagios, Chat-Server, CMS, Back Office-Systeme, Datenbanken
- Netzwerkdaten: Firewall-Logs, Router/Switch-Logs, Cisco NAM-Logs und Benachrichtigungen
- Spieldaten: Online-Verkaufsaktivität
- Sicherheitsdaten: Firewall-Logs, VPN-Gateways, Firewall-Logs von Webanwendungen, Unix/Linux Shell-Auditlogs, AAA-Systeme

Splunk-Produkte

- Splunk Enterprise
- Google Maps Add-on for Splunk Enterprise
- Splunk Add-on for OSSEC
- AfterGlow Visualization
- Splunk on Splunk (S.oS)

Mehr Compliance und Sicherheit für Swisslos

Da Swisslos von der World Lottery Association zertifiziert wird, muss die Genossenschaft sehr schnell auf jeglichen Systemmissbrauch oder auf Sicherheitsbedrohungen reagieren. Die Systemverwaltungsabteilung von Swisslos nutzt jetzt Splunk-Software, um die Spielsysteme zu überwachen und unter anderem die Netzwerkstabilität und -sicherheit zu messen. Ungewöhnliche Vorkommnisse, wie beispielsweise eine falsche Benutzeranmeldung oder ein Verstoß gegen Compliance-Richtlinien, werden ebenfalls registriert.

Das Netzwerksicherheitsteam von Swisslos setzt bei Second- und Third-Level-Support ebenfalls auf Splunk und kann so auch Sicherheitsprobleme und Angriffe aufspüren und verhindern. Zudem können komplexe betrügerische Angriffe erkannt und abgewehrt werden.

Verbesserte Kundenerfahrung durch Auswertung „kryptischer“ Daten

Swisslos profitiert enorm von der breit angelegten Implementierung von Splunk Enterprise. Einer der größten Vorteile besteht darin, dass Splunk Daten korreliert und Visualisierungen auf Netzwerkebene bereitstellt, die einen umfassenden Überblick bieten. Informationen aus zahlreichen Systemen werden in Splunk erfasst und ausgewertet, sodass Swisslos eine lückenlose, integrierte Sicht auf sämtliche IT-Abläufe erhält. Die Performance-Diagramme sind besonders informativ. Sie können mit nur drei Mausklicks erstellt werden und verwandeln kryptische Logs in aussagekräftige Erkenntnisse.

Die schnellen Response- und Echtzeitanalysemöglichkeiten der Splunk-Software haben Swisslos deutliche Vorteile verschafft und das Nutzungserlebnis der zahlreichen Benutzer der Online-Plattform deutlich verbessert. Bei einem Anwendungsausfall im Online Gaming-Portal könnten die Benutzer nicht spielen, was Umsatzeinbußen für Swisslos bedeuten würde. Durch die Monitoring- und Benachrichtigungsfunktionen von Splunk kann

„Splunk schließt die Lücke zwischen Mensch und Daten. Big Data-Analysen lassen sich mit Splunk ganz einfach durchführen, und wir profitieren in Sekundenschnelle von aussagekräftigen Informationen. Auch die komplexeren Visualisierungsfunktionen möchten wir auf keinen Fall missen.“

Joris Vuffray, Leiter des Teams für Netzwerk- und Systemmanagement
Swisslos

dieses Worst-Case-Szenario schnell behoben oder sogar proaktiv verhindert werden, indem die zuständigen Teams bei jeglichen Anomalien oder dem Erreichen von Schwellenwerten informiert werden. „Die Zufriedenheit unserer Benutzer ist ausschlaggebend für unseren Erfolg. Wir sind daher höchst erfreut, dass wir die Verfügbarkeit unserer Gaming-Plattform so deutlich verbessern und damit natürlich auch die Benutzererfahrung mit der Website optimieren konnten“, erklärt Joris Vuffray, Leiter des Teams für Netzwerk- und Systemmanagement bei Swisslos.

Mehr Effizienz im gesamten Unternehmen

Durch die Bereitstellung verschiedener Anwendungen aus dem Splunk-Ökosystem baut Swisslos die Nutzung der Splunk-Lösung noch weiter aus. Google Maps for Splunk lokalisiert und visualisiert Angriffe auf das Swisslos Gaming-Portal. Splunk Add-On for OSSEC prüft den Sicherheitszustand der aktuellen Betriebssysteme, und AfterGlow Visualization stellt ungewöhnliche, interne IP-Aktivitäten grafisch dar. Die App Splunk on Splunk (S.oS) analysiert und überwacht die Nutzung von Splunk Enterprise.

Die Splunk-Plattform hat die Kundenerfahrung verbessert, die Compliance erleichtert und die Kosten für Swisslos gesenkt. Außerdem hat sie die Effizienz des Swisslos IT-Teams gesteigert, wodurch der Zeitaufwand für Schulungen sowie die Zahl der Mannstunden für die Datenauswertung deutlich gesenkt werden konnten. Kosteneinsparungen sind im gesamten Unternehmen zu verzeichnen, da bei Swisslos keine hohen Lizenz- und Wartungskosten mehr für den Unterhalt einer großen Datenbank anfallen.

splunk> SplunkCe@Splunk.com www.splunk.com

CS-Splunk-Swisslos-A4-102_DE