Einfache Administration, leichte Bedienung und Kostenersparnis

SIEM bei B+S Card Service: Splunk statt ArcSight

Foto: fotolia

Interview mit Jan Gierhan, B+S Card Service GmbH, Teamleiter IT-Betrieb-Serversysteme

Consist Connect: Herr Gierhan, die B+S Card Service GmbH, einer der größten Dienstleister in Deutschland für bargeldlose Bezahllösungen, hat sich im Sommer 2013 entschieden, die bestehende SIEM-Lösung von HP ArcSight durch Splunk zu ersetzen. Wie lange war HP ArcSight zuvor im Einsatz gewesen?

Jan Gierhan: Wir hatten HP ArcSight seit zweieinhalb Jahren im Einsatz.

Consist Connect: Was hat B+S veranlasst, diesen Wechsel vorzunehmen?

Jan Gierhan: ArcSight ist ein sehr mächtiges Tool, das im Prinzip alle Funktionen abdeckt, die wir brauchen. Das Tool lässt sich aber schlecht bedienen. Die Benutzeroberfläche ist kompliziert und sehr umfassend. Trotz einer Einführungsphase mit starker Unterstützung durch externe Consultants, die uns das System eingestellt und unsere Wünsche umgesetzt haben, und trotz geschultem Personal bei uns konnten wir nicht die gesamten Funktionen abgreifen. Im täglichen Doing war es nicht möglich, sich gut einzuarbeiten. Das vorherige Tool braucht zur Pflege einen wirklich hohen Zeitaufwand. Hinzu kamen noch Kostengründe.

Consist Connect: Herr Pistol, der Abteilungsleiter IT-Betrieb bei B+S Card Service wird ja bei unserer Veranstaltung Comply & Secure im Juni auch noch näher auf die Management-Entscheidung zugunsten von Splunk eingehen. Können Sie unseren Lesern kurz erklären, welche Systemumgebung bei B+S Card Service vorliegt?

Jan Gierhan: Wir haben eine ziemlich vielfältige und komplexe Systemumgebung aus Windows- und Linux-Servern, einigen HPUX-Systemen und Netzwerkkomponenten unterschiedlicher Hersteller. Was Firewalls, Loadbalancing und Switche angeht, fahren wir eine Dual-Vendor-Strategie, verteilt auf insgesamt drei Rechenzentren und vier Standorte. Das SIEM-System wird größtenteils von zwei Syslogservern gefüttert, hinzu kommen noch Sonderlösungen für den Windowsbereich, Datenbanken und Filer. Wir kommen auf eine Zahl von ca. 85 Millionen Events pro Tag. Das sind umgerechnet etwa 40 GB an Daten.

Consist Connect: Welche Erwartungen hatten Sie an Splunk?

Jan Gierhan: Neben den verringerten Kosten hatten wir natürlich vor allem die Erwartung, dass wir ein Tool bekommen, das wir relativ einfach administrieren können und das sich intuitiv bedienen lässt.

Wir müssen davon ausgehen, dass in Zukunft immer mehr Systeme hinzukommen, dass mehrere Server neu aufgesetzt werden und dass wir auch mal ein neues Betriebssystem oder Netzwerkkomponenten anwenden, die ein ganz anderes Log-Format haben werden.

Foto: fotolia

Ausgezeichnet als Top-Produkt: Das Terminal H5000 von B&S Card Service

Foto: B&S Card Service

Nachteil bei der bestehenden Lösung war, dass man für jedes der einzelnen Log-Formate einen Connector bauen musste. Dafür mussten wir immer einen externen Berater dazu holen. In dieser Hinsicht ist Splunk viel leichter zu bedienen, weil man sich die wichtigsten Felder einfach herausfiltern kann.

Consist Connect: Was hat Sie im Rahmen des Proofs of Concept mit Consist überzeugt, die Entscheidung der ArcSight-Ablösung durch Splunk endgültig zu fällen?

Jan Gierhan: Wir haben gesehen, dass wir in erhebliche Schwierigkeiten laufen werden und haben überlegt, wie man das beheben kann. Dabei kam heraus, dass es am besten ist, bei null anzufangen und das Konzept neu aufzuziehen. Die Frage war, ob wir das wirklich mit dem bisherigen Tool machen wollen oder ob man das Geld in ein neues Tool steckt, mit dem man besser umgehen kann und das zukunftsorientierter ist. Bei ArcSight hätte eine recht teure Lizenzerweiterung angestanden. Manche Mitarbeiter kannten Splunk schon, setzten es im privaten Bereich ein. Die Entscheidung bewusst für Splunk ist relativ schnell gefallen – drei Monate, nachdem das Thema das erste Mal aufkam.

Consist Connect: Bitte beschreiben Sie die Umsetzung und die Unterstützung durch Consist.

Jan Gierhan: Zuerst haben wir ein grobes Konzept erstellt, wie Splunk eingebunden werden soll und hatten zunächst einen Parallelbetrieb. Wir haben uns bei Splunk für eine Single-Server-Lösung entschieden, weil sie völlig ausreichend für unsere Umgebung ist. Consist hat uns die Splunk-Lizenz bereitgestellt und uns beim Aufsetzen und der Installation des Servers unterstützt.

Dann haben wir uns mit Consist in einem einwöchigen Workshop in der letzten Septemberwoche 2013 samt Training zusammengesetzt, haben Beispielreports für alle größeren Systemgruppen – Linux, Windows und wichtige Netzwerkkomponenten – umgesetzt. So haben wir gelernt, wie Splunk funktioniert, was man bei dem Logfile beachten muss und ein Gefühl für die Bedienung der Oberfläche bekommen. Damit hatten wir 80 Prozent der Systemtypen abgedeckt. Alle weiteren Reports haben B+S-Mitarbeiter danach selbstständig umgesetzt.

In den nächsten zwei Monaten haben wir in Fleißarbeit Splunk auf alle Systeme ausgerollt, also alle Server dazu geholt und Gruppen gebildet. 90 Prozent aller Systeme waren am 1. Dezember 2013 auf Splunk migriert. Bei der Splunk-Einführung haben wir auch gleich einige konzeptionelle Schwächen aus dem Altprojekt beseitigt.

Consist Connect: B+S hat einen hochflexiblen Managed-Services-Vertrag mit Consist abgeschlossen. In welchen Situationen greifen Sie auf die Spezialisten von Consist zurück?

Jan Gierhan: Das Standard-Reporting, Log-Auswertungen und all das, was die PCI-Compliance von uns fordert, können wir mit Splunk selbstständig erfüllen. Wir wollten mit der Umstellung auf Splunk ja auch die externe Unterstützung deutlich zurückfahren. Das ist uns gelungen.

Den Support-Vertrag mit Consist haben wir explizit dafür abgeschlossen, ein Back-up-System zu haben für den Fall, dass wir mal ein Problem mit Splunk nicht selbst innerhalb einer bestimmten Zeit lösen können. Das hat in dem einen Mal, bei dem

wir diesen Vertrag bislang genutzt haben, wunderbar funktioniert. Wir haben mit Consist einen Experten für den Notfall im Hintergrund.

Consist Connect: Wie zufrieden sind Sie insgesamt mit der Zusammenarbeit mit Consist?

Jan Gierhan: Aus meiner Sicht klappt das wirklich gut. In dem einen Fall, in dem wir alleine nicht weiterwussten, hat uns Consist innerhalb von 24 Stunden komplett geholfen. Wenn ich Kontakt zu Consist suche, erhalte ich auch sofort und regelmäßig eine Antwort. Wir sind der Consist sehr positiv gegenüber gestimmt.

Consist Connect: Wie viele und welche Personen nutzen Splunk in Ihrem Unternehmen?

Jan Gierhan: Im Wesentlichen wird Splunk bei uns vom IT-Betrieb genutzt, der aus drei Teams besteht. Team 1 ist die Netzwerkadministration. Diese Kollegen bekommen eine große Anzahl verschiedener Reports, weil sie relativ viele verschiedene Hersteller für Switches, Loadbalance und andere im Einsatz haben. Team 2 ist für die Applikationssysteme zuständig, Team 3 für den Backofficebereich und in der Windowswelt unterwegs. Insgesamt sind das 35 Mitarbeiter, von denen pro Tag drei zuständig sind, die Reports zu lesen und auszuwerten. Es gibt bei B+S außerdem noch ein paar andere Teams, die Splunk-Reports nutzen.

Consist Connect: Wie ist die Benutzerakzeptanz von Splunk?

Jan Gierhan: Vor allem bei der Netzwerkadministration und auf der Applikationsseite kommt Splunk sehr gut an. Die Kollegen sind froh, mit diesem Tool jetzt einen vernünftigen Report zu bekommen, mit dem sie arbeiten können. Und der Netzwerkbereich freut sich, dass er mit Splunk auch über das normale Reporting hinaus vieles analysieren kann, z. B. über die 100 wichtigsten Angreifer des letzten Tages auf unserer Internet-Firewall. Ein bunter Graph wird dafür einmal am Tag am Dashboard generiert. Die graphische Aufbereitung ist auch für das Management interessant.

Consist Connect: Wird Splunk bei B+S Card Service für weitere Analysen über das tägliche Reporting hinaus eingesetzt?

Jan Gierhan: Ja, wir nutzen mittlerweile Splunk auch in anderen Bereichen. Zum Beispiel werten wir die Systemlogs der Firewall aus. Wenn wir eine Kommunikationsmatrix erstellen sollen über die Kommunikation zwischen zwei Netzbereichen, kann ich in Splunk innerhalb von fünf Minuten eine Abfrage generieren.

Consist Connect: Welchen Mehrwert hat B + S Card Service durch die Umstellung auf Splunk gewonnen?

Jan Gierhan: Der Mehrwert ist eindeutig die Administrierbarkeit. Wir können die Anforderungen, die PCI an uns stellt, erfüllen, und zwar selbstständig. Wir können Splunk administrieren, bedienen, umkonfigurieren. Wir können damit täglich arbeiten und nutzen es auch tatsächlich. Das ist ein Mehrwert, den wir bei vorher nicht hatten.

Wir haben die Umstellung auf Splunk auch genutzt, um das SIEM-Konzept zu optimieren.

Ein großer Vorteil ist natürlich auch das deutlich verbesserte Reporting. Ein Beispiel: Statt 21 E-Mails mit insgesamt 747 Seiten zur Auswertung wie früher, bekommen wir in Splunk drei E-Mails pro Tag für die Windows-, Linux- und HPMX-Server mit insgesamt 34 Seiten. Sie enthalten eine Zusammenfassung und Details. Erst wenn einem in der Zusammenfassung etwas Merkwürdiges auffällt, muss man sich die Seiten mit den Details ansehen. In jedem Team gibt es immer einen Verantwortlichen pro Tag, der die Reports analysiert. Pro Team sparen wir pro Tag eine halbe Stunde Zeit durch Splunk.

Consist Connect: Wieviel Prozent der Kosten haben Sie bei der Lizenz, der Wartung, den Einrichtungs- und Betriebskosten und in der Benutzung durch den Wechsel auf Splunk gewonnen?

Jan Gierhan: Die laufenden Lizenzkosten liegen mit Splunk bei etwa 75% der Kosten mit ArcSight. Wir haben eine relativ große Splunk-Lizenz für 150 Gigabyte, die wir noch gar nicht voll ausnutzen. Wir können noch dreimal so viele Systeme auf Splunk ziehen und dreimal so viele Logfiles analysieren, wie wir es zurzeit machen. Bei ArcSight hätten wir hierfür die Lizenz noch erweitern müssen.

Bezüglich der Wartung hatten wie bei der alten Lösung mit 20 Manntagen pro Jahr externem Support gerechnet. Von der Zahl sind wir deutlich heruntergekommen. Wir haben mit Consist einen Support-Vertrag von drei Stunden pro Monat, das sind vier bis fünf Manntage im Jahr. Es kommen vielleicht noch ein paar Erweiterungen hinzu, bei denen wir auf die Experten von Consist zurückgreifen. Also haben wir die Wartungskosten locker halbiert.

Die Ersparnis der Benutzung haben wir noch nicht monetarisiert. Das vorige Tool hat keine Akzeptanz im Haus gefunden. Man hat zwar die Reports für die Compliance erstellt, aber richtig genutzt hat man das Tool nicht. Splunk wird erfreulicherweise viel mehr eingesetzt.

Consist Connect: Wenn Sie einen kurzen Ausblick in die Zukunft vornehmen: Welche Erweiterungen in Splunk und welche zusätzlichen Einsatzszenarien planen Sie?

Jan Gierhan: Es wachsen immer mehr Begehrlichkeiten. Die Leute, die Splunk kennen, wissen mittlerweile, was das Tool alles kann. Die nächste größere Erweiterung wird die Ablösung des Nagios-Dashboards durch ein Splunk-Dashboard sein. Und wir werden jetzt, nachdem wir die System-Logfiles in Splunk haben, auch die Applikations-Logfiles, zum Beispiel vom Mailserver, in Splunk hineinziehen. Das werden viele zusätzliche Gigabyte an Daten sein, die wir bislang noch gar nicht betrachtet haben. Auch hat das Marketing hat bei uns angefragt, ob wir uns ein Dashboard für die Webanalyse vorstellen können. Für solche Fälle werden wir sicher nochmal auf die Consist zukommen. Consist hat uns bis jetzt sehr gut unterstützt.

Consist Connect: Herr Gierhan, ich danke Ihnen herzlich für das informative Interview.

Das Interview führte Isabel Braun.

Weitere Informationen:

Asmus Hammer
Telefon: 0431/3993-637
E-Mail: hammer@consist.de

Über B+S Card Service

B+S Card Service ist einer der führenden Dienstleister für die Kartenakzeptanz. Von B+S Card Service erhalten Unternehmen, die ihren Kunden bargeldloses Bezahlen anbieten möchten, die nötige Infrastruktur und alle wichtigen Serviceleistungen.

B+S ist ein Beteiligungsunternehmen des Deutschen Sparkassenverlags und gehört zur Sparkassen-Finanzgruppe. Es beschäftigt mehr als 470 Mitarbeiter, davon ca. 320 am Hauptsitz in Frankfurt am Main.

Mit 25 Jahren Erfahrung und mehr als 227.000 Kunden ist B + S Card Service in Deutschland einer der erfahrensten und größten Dienstleister für bargeldlose Bezahllösungen am Point of Sale (POS), POI sowie im Internet- und Versandhandel. In dreizehn weiteren europäischen Ländern setzen ebenfalls zahlreiche Kunden auf die Leistungen von B+S Card Service.

Zu den Kunden von B+S gehören sowohl kleinere und mittlere Unternehmen als auch große Konzerne. Sie kommen aus den unterschiedlichsten Branchen. Dazu zählen unter anderem: Handel, Gastronomie, Travel & Entertainment, Mineralöl, ÖPNV, Handwerk, Kliniken, Behörden und Dienstleister aller Art.

www.bs-card-service.com