Simple administration, easy operation, and cost savings

SIEM at B+S Card Service: Splunk instead of ArcSight

photo: fotolia

Interview with Jan Gierhan, B+S Card Service GmbH, Team leader IT Operations Server Systems

Consist Connect: Mr. Gierhan, B+S Card Service GmbH, one of the largest service providers in Germany for non-cash payment solutions, decided in Summer 2013 to replace their existing SIEM solution of HP ArcSight with Splunk. How long had HP ArcSight been in use before that time?

Jan Gierhan: We had been using HP ArcSight for two and a half years.

Consist Connect: What brought B+S to undertake the change?

Jan Gierhan: ArcSight is a very powerful tool, which in principle can cover all the functions we need. But the tool is very difficult to operate. The user interface is complicated and very comprehensive. Despite an introductory phase with a lot of support from external consultants, who set up the system for us according to our requirements, and despite trained staff in-house, we couldn't access all the functionality. In the daily doing of things, it just wasn't possible to get familiar with the system. The previous tool required truly large amounts of time for maintenance. On top of this, there were also cost factors.

Consist Connect: Mr. Pistol, the Department Head of IT Operations at B+S Card Service, will of course be going into more detail at our Comply & Secure event in June about the management decision in favor of Splunk. Can you briefly explain to our readers what system environment is in use at B+S Card Service?

Jan Gierhan: We have a very multifaceted and complex system environment of Windows and Linux servers, a few HPUX systems, and network components from other manufacturers. As far as firewalls, load balancing, and switches are concerned, we use a dual-vendor strategy distributed over a total of three computer centers and four locations. The SIEM system will be mainly fed by two syslog servers, as well as special solutions for the Windows area, databases and filers. We reach a total of about 85 million events per day. That corresponds to about 40 GB of data.

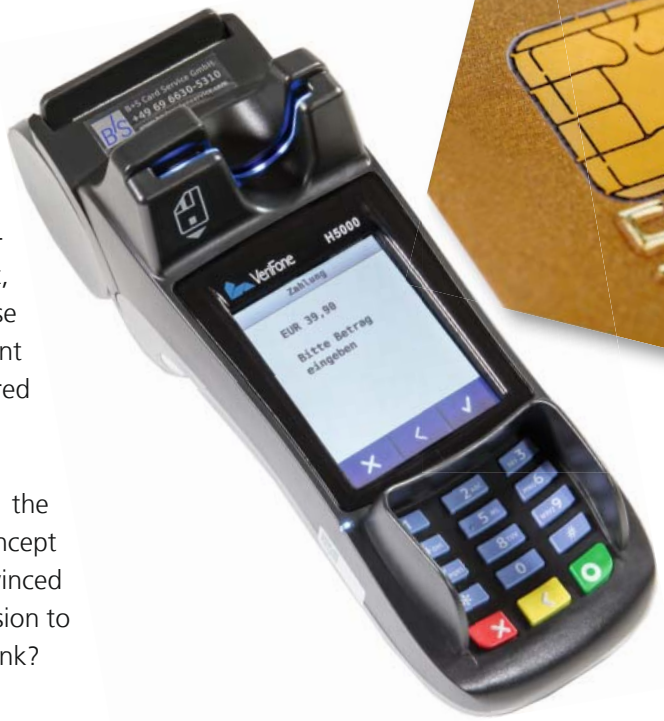
Consist Connect: What expectations did you have for Splunk?

Jan Gierhan: In addition to the reduced costs, of course, we especially expected to get a tool that we could administer relatively easily and that could be operated intuitively.

We have to assume that more and more systems will be added in the future, that multiple servers will be set up and that someday we will also use a new operating system or network components with an entirely different log format.

The disadvantage of the existing solution was that we had to build a connector for each individual log for-

photo: fotolia



Awarded as top product: The Terminal H5000 from B&S Card Service

photo: B&S Card Service

mat. To do that, we had to hire an external consultant. In that respect, Splunk is much easier to use because the most important fields can simply be filtered out.

Consist Connect: In the context of the proof of concept with Consist, what convinced you to make the final decision to replace ArcSight with Splunk?

Jan Gierhan: We saw that we would run into significant difficulties and thought about how to fix that. The result was that we found it best to start from scratch and to rebuild the concept. The question was whether we really wanted to do that with the existing tool or whether we wanted to put our money into a new tool we could work better with and that is more future-oriented. With ArcSight, we would have ended up with a really expensive license extension. Some of our staff already knew Splunk and were using it privately. The actual decision for Splunk was made relatively quickly – three months after the question first came up.

Consist Connect: Please describe the implementation and the support you got from Consist.

Jan Gierhan: First, we created a rough concept of how to integrate Splunk and initially we ran it in parallel. With Splunk, we decided on a single-server solution because it is entirely sufficient for our environment. Consist provided us with the Splunk license and supported us in setting up and installing the server.

Then we put our heads together with Consist at a one-week workshop and training sessions in the last week of September, 2013, and implemented example reports for all the larger system groups – Linux, Windows, and important network components. We learned how Splunk worked, how the log file has to be handled, and got a feeling for operation of the user interface. We covered about 80 percent of the system. All other reports were then implemented independently by B+S staff.

Over the next two months, we worked hard to roll out Splunk on all systems, that is, brought in all the servers and built groups. 90 percent of all systems had been migrated to Splunk by December 1, 2013. During the Splunk introduction, we also corrected a few conceptual weaknesses from the old project.

Consist Connect: B+S concluded a highly flexible Managed Services agreement with Consist. In what situations can you fall back on the specialists at Consist?

Jan Gierhan: We can handle standard reporting, log evaluations and everything that requires PCI compliance from us independently with Splunk. After all, after moving to Splunk we wanted to cut back significantly on external support. And we succeeded with that.

We explicitly decided on the support agreement with Consist in order to have a backup system for the case that we couldn't solve a problem with Splunk ourselves within a given time. On the one occasion we've used the agreement so far, that worked wonderfully. With Consist, we always have an expert in the background for emergencies.

Consist Connect: Overall, how satisfied are you with your collaboration with Consist?

Jan Gierhan: From my point of view, it works really well. In the one case when we couldn't get further on our own, Consist completely helped us out within 24 hours. When I need to get in touch with Consist, I get a response immediately and regularly. We have a very positive attitude towards Consist.

Consist Connect: How many people and who uses Splunk in your company?

Jan Gierhan: Primarily, Splunk is used by us in IT operations, consisting of three teams. Team 1 is network administration. They get a large number of different reports because we have a relatively large number of different manufacturers for switches, load balancers and other components. Team 2 is responsible for application systems, and Team 3 for the back office and the world of Windows. In all, that's 35 people, of which three are responsible every day for reading and evaluating reports. There are also a few other teams that use Splunk reports at B+S.

Consist Connect: How is the user acceptance of Splunk?

Jan Gierhan: Especially in network administration and on the application side, Splunk is really helpful. Our colleagues are happy to get a reasonable report from the tool that they can work with. And the network team is happy that they can also use Splunk to do a lot of analysis beyond the normal reporting, for example, to see the 100 largest attackers against our Internet firewall in the last day. A colorful graph is generated once a day on the dashboard for that. The graphical preparation is also interesting for management.

Consist Connect: Is Splunk used at B+S Card Service for additional analysis beyond daily reporting?

Jan Gierhan: Yes, we now use Splunk in other areas, too. For example, we evaluate the system logs of the firewall. When we create a communications matrix, about the communication between two network domains, I can generate a query in Splunk in five minutes.

Consist Connect: What added value has B+S Card Service gained by converting to Splunk?

Jan Gierhan: The added value is clearly the manageability. We can meet all the requirements of PCI, on our own. We can administer, use, and reconfigure Splunk. We can work with it every day and actually use it. That's an added value we simply didn't have before.

We've also taken advantage of the Splunk conversion to optimize our SIEM concept.

One great advantage is of course the significantly improved reporting. Here's an example: Instead of the previous 21 e-mails with a total of 747 pages to evaluate, in Splunk we get three e-mails a day for the Windows, Linux, and HPMX servers with a total of 34 pages. They include a summary and details. Only when something strange appears in the summary do you really have to look at the pages with the details. In each team, there is always one person every day responsible for analyzing the reports. Per team, we save half an hour a day with Splunk.

Consist Connect: What percentage of costs have you gained in licensing, maintenance, setup and operating costs and in usage by switching to Splunk?

Jan Gierhan: The ongoing licensing costs for Splunk are about 75% of the costs for ArcSight. We have a relatively large Splunk license for 150 gigabytes which we're not even fully using yet. We could move three times as many systems to Splunk and analyze three times as many log files as we're doing right now. With ArcSight, we would have had to have expanded the license to do that.

With respect to maintenance, with the old solution we had to count on 20 person-days per year of external support. We've definitely come down from that figure. With Consist we have a support agreement of three hours per month, which is about four to five person-days in a year. There may be some extensions added, where we'll need the experts at Consist. So we've maybe cut maintenance costs by half.

We haven't looked at the savings in usage in terms of money. The previous tool wasn't accepted in the company. We still ran the reports for compliance, but we didn't really use the tool. Splunk is fortunately being used a lot more.

Consist Connect: If you take a short look into the future: What extensions in Splunk and what additional usage scenarios are you planning?

Jan Gierhan: We are coming up with more and more wishes. The people who know Splunk now know what the tool can do. The next big extension will be replacing the Nagios dashboard with a Splunk dashboard. And now that we have the system log files in Splunk we'll also be moving the application log files into Splunk, for example the mail server. That will be a lot of additional gigabytes of data that we've never looked at before. Marketing has also asked us whether we can set up a dashboard for Web analytics. For that kind of case, we'll surely turn to Consist again. Consist has supported us very well so far.

Consist Connect: Mr. Gierhan, thank you very much for the informative interview.

Isabel Braun conducted the interview.

For further information:

Asmus Hammer
Phone: +49 (0)431/3993-637
E-Mail: hammer@consist.de

About B+S Card Service

B+S Card Service is one of the leading service providers for card acceptance. B+S Card Service provides companies who want to offer their customers non-cash payment options with the required infrastructure they need and all important services.

B+S is a subsidiary of the Deutscher Sparkassenverlag (German savings bank's publishing house) and belongs to the Sparkassenfinanzgruppe (Saving Banks Finance Group). The company employs over 470 people, 320 of whom are at the headquarters in Frankfurt am Main.

With 25 years of experience and over 227,000 customers, B+S Card Server is one of the most experienced and largest service providers in Germany for non-cash payment solutions at the Point of Sale (POS), POI, and in the Internet and mail order trade. In thirteen other European countries, numerous customers also rely on the services of B+S Card Service.

B+S customers also include smaller and medium-sized companies as well as large groups. They come from a wide variety of industries. These include: commerce, gastronomy, travel and entertainment, petroleum, public transport, craft, clinics, government offices, and service providers of all kinds.

www.bs-card-service.com