

Zentrales Log-Management „tacLOG“...

...sorgt beim Kanton Aargau für noch mehr Sicherheit.

Der Kanton Aargau vertraut schon seit 2002 auf terreActive als Partner für externe Sicherheit und lässt sich von den Spezialisten für IT-Sicherheit in Sachen Strategie und Architektur beraten. In verschiedenen Schritten wurde seither eine redundant ausgelegte Sicherheitsinfrastruktur aufgebaut. Das neueste Projekt, welches für die Abteilung Informatik realisiert wurde, umfasst das zentrale Log-Management mit tacLOG.

Als Teil der Abteilung Informatik fungiert die aus sieben Personen zusammengesetzte Gruppe Telekommunikation für die Verwaltung des Kantons Aargau und den Grossteil der Gemeinden als Netzwerk- und Internetprovider. An diesem Netz hängen alle kantonalen Stellen – von der Polizei und den Gerichten über Schulen und Spitäler bis zur Sozialversicherung und der Pensionskasse sowie die meisten der 230 Gemeinden. Das Netz erstreckt sich über das ganze Kantonsgebiet und erschliesst rund 450 bis 500 Standorte.

Um die Sicherheit dieses Netzes, über welches beispielsweise auch der gesamte E-Mail-Verkehr oder die E-Government-Plattform abgewickelt wird, kümmert sich die Gruppe Telekommunikation. Andreas Hüppi erklärt: „Wir verantworten den reibungslosen Betrieb von Internet und Telefonie und sorgen dafür, dass die angeschlossenen Institutionen jederzeit Zugriff haben.“ Rund 70 Unix-Systeme, die auf Solaris laufen, stellen die benötigten Services im Netzwerk und Sicherheits-Bereich sicher.

„Seit wir tacLOG bei uns im Einsatz haben, kann ich mir nicht mehr vorstellen, jemals wieder darauf zu verzichten. Das zentrale Log-Management von terreActive entspricht genau unseren Bedürfnissen und erleichtert unsere Aufgabe enorm.“



Andreas Hüppi
 Network-Security
 Kanton Aargau

Die wichtigsten Vorteile auf einen Blick

- Zentrale Verwaltung von Logdateien
- Senkung des Aufwands für die Systemadministration
- Erhöhung der Netzwerksicherheit
- Optimale Konfigurationsmöglichkeiten
- Frühzeitige Erkennung von Störungen

Auf der Suche nach einem effizienten Log-Management

In diesem Zusammenhang suchte die Gruppe Telekommunikation nach einer Lösung für das zentrale Log-Management. „Früher haben wir die Logdateien unserer Unix-Systeme manuell ausgewertet – das war allerdings alles andere als effizient und sehr zeitraubend“, erläutert Andreas Hüppi. In der Tat: Die Praxis zeigt, dass schon in mittelgrossen Netzwerken die Anwendungen täglich grosse Mengen an Logdateien erzeugen. Um diese auf allfällige Hinweise hinsichtlich Unregelmässigkeiten oder Problemen hin zu untersuchen, fehlt meist die Zeit. Zusätzlich zur Menge, die eine sinnvolle Planung der Auswertung zur Herausforderung macht, kommt hinzu, dass die Dateien vielfach auf den einzelnen Systemen verteilt sind und dass die Interpretation der Logfiles alles andere als trivial ist.

Bei der Evaluation einer geeigneten Lösung wurden verschiedene Tools – darunter auch tacLOG – unter die Lupe genommen; mit einigen wurde eine Testinstallation durchgeführt, um die Funktionalitäten zu prüfen. terreActive hat das Rennen gemacht.

Andreas Hüppi begründet die Wahl: „tacLOG hat uns durch seine Zweckmässigkeit überzeugt und entsprach genau unseren Bedürfnissen. Die Lösung ist sehr ausgereift und kommt einfach daher. Unsere Anforderungen konnten mit geringem Aufwand erfüllt werden, ohne dass noch zusätzliche Komponenten benötigt wurden. Weitere Punkte beim Entscheid zu Gunsten von terreActive waren das ausgezeichnete Preis-Leistungs-Verhältnis, die Flexibilität der Lösung sowie die geografische Nähe von terreActive.“



Schnelle Implementierung, einfache Konfiguration

Die Implementierung und Konfiguration von tacLOG gestaltete sich problemlos und erfolgte innert kürzester Zeit. Seither werden die Logdaten nicht mehr dezentral auf den einzelnen Systemen gehalten, sondern an einen zentralen Loghost geschickt. Ein Kernelement der automatischen Sichtung der Logfiles bilden die vordefinierten Regeln zur Erzeugung von Events und Alerts. Dabei werden jedoch nicht ausschliesslich sicherheitsrelevante Vorkommnisse einbezogen. Vielmehr wird zusätzlich auch auf das Erkennen von Konfigurations- und Nutzerproblemen grossen Wert gelegt. Das hat den Vorzug, dass viele potenziell gefährliche Situationen, die oft nur mit grossem Zeit- und Kosteneinsatz wieder in den Griff zu bekommen sind, gar nicht erst eintreten. Durch eine kontinuierliche Optimierung der angewandten Regeln mittels Feineinstellung wird das System laufend verbessert.



Über die Abteilung Organisation und Informatik

Die Abteilung Informatik ist der zentrale IT-Dienstleister der gesamten kantonalen Verwaltung und in einzelnen Belangen auch für Gemeinden, Körperschaften des öffentlichen Rechts und Dienststellen anderer Kantone. Sie gehört zum Departement Finanzen und Ressourcen, welches mit seinen rund 600 Mitarbeiterinnen und Mitarbeitern finanzielle, personelle, wirtschaftliche und natürliche Ressourcen für die Erfüllung der Aufgaben des Kantons Aargau erschliesst und betreut. Ihre Dienstleistung erstreckt sich von der Beratung bezüglich IT-Anwendungen, IT-Infrastrukturaufgaben, Telefonie, Helpdesk und IT-Ausbildung über die Realisierung von IT-Projekten, Internet- beziehungsweise Intranetvorgaben und der laufenden Betreuung zentraler Querschnittsapplikationen bis zum Betrieb des Netzwerkes und des Rechenzentrums. Zu den Aufgaben zählen unter anderem die Serverbetreuung, die Datensicherung, der gesamte Zugriffsschutz oder die Nachbearbeitung des Massenausdrucks.

„Mit der Implementierung einer zentralen Log-Management-Lösung hat der Kanton Aargau einen wichtigen Schritt gemacht, seine Logdateien effizient und systematisch in sein IT-Sicherheitskonzept zu integrieren und das Frühwarnsystem zu optimieren.“



Urs Rufer

Leiter Consulting & Projekts
terreActive AG

Für den einwandfreien Betrieb der Log-Management-Lösung sorgt terreActive. „Das hat für uns den Vorteil, dass wir unsere knappen Ressourcen anderweitig einsetzen können und uns nicht erst eigenes Know-how aneignen müssen“, sagt Andreas Hüppi. „Dieses Konzept hat sich bislang sehr bewährt. Bei Bedarf bieten wir einfach die Experten von terreActive auf.“

Partnerschaft hat sich einmal mehr bewährt

Durch die Einführung der zentralen Log-Verwaltung ist die tägliche Arbeit der Gruppe Telekommunikation erheblich einfacher geworden, weil die manuelle Sichtung der Logfiles der Vergangenheit angehört. Potenzielle Vorfälle können dank tacLOG mit geringem Aufwand schon frühzeitig erkannt und Gegenmassnahmen in die Wege geleitet werden, bevor die Endanwender überhaupt etwas davon merken. Und weil die Lösung aufgrund ihrer modularen Architektur sehr gut skalierbar ist und sich in der Praxis bestens bewährt hat, interessieren sich mittlerweile auch andere Abteilungen innerhalb der Verwaltung dafür.

Das Fazit von Andreas Hüppi fällt entsprechend positiv aus: „Wir haben schon in der Vergangenheit sehr gute Erfahrungen in der Zusammenarbeit mit terreActive gemacht und das hat sich auch bei diesem Projekt wieder bestätigt. Wir haben in sehr kurzer Zeit eine schlanke Lösung erhalten, die unsere Ansprüche ohne aufwändige Schulung ideal erfüllt und bereits zu einem unverzichtbaren Hilfsmittel geworden ist. Zudem gibt es einem einfach ein gutes Gefühl, wenn man in Sachen IT-Sicherheit mit einem Partner zusammenarbeitet, der kompetent ist und auf den man sich jederzeit verlassen kann.“