terreActive
terreActive
terreActive
terreActive

Success
Story

Silos einbrechen – für eine zentrale Plattform zur Logdatensammlung

Log Management mit Archivierung, Analyse und Alarmierung als Basis für ein SIEM

Eine IT-Infrastruktur für 16 Schulen, 2 Spitäler, 26 Gemeinden, 2 Städte und einen ganzen Kanton: KSD ist das Informatikunternehmen von Kanton und Stadt Schaffhausen. Die unterschiedlichen Kundenprofile bringen unterschiedliche Bedürfnisse mit sich. terreActive implementierte eine Lösung, die alle nutzen können.

Anforderung: Silos aufbrechen

terreActive kannte die Situation bei öffentlichen Verwaltungen aus Erfahrung: Die IT-Organisation ist typischerweise in Silos aufgebaut (z. B. Team Basis-Services, Team Netzwerk etc.). Oft benutzen die Teams unterschiedliche Tools für das Monitoring. Jedes Silo ist so zwar gut aufgestellt, hat jedoch keinen Einblick in die Tools der anderen Abteilungen und sobald die Systeme untereinander mehr vernetzt werden, entstehen Abhängigkeiten, welche nicht überwacht werden.

Auch bei KSD war man sich dessen bewusst: «Wir brauchten eine zentrale Sicht auf alle relevanten Systeme, um in unserem heterogenen Umfeld schnell reagieren zu können», so Roger Speckert, Mitglied GL, Leiter Infrastructure, Client Engineering & Security, KSD.

Ziel: Zentrales Log Management als Monitoring-Basis für den sicheren Betrieb

Zukünftig sollte eine zentrale Datensammlung und -analyse die Sicherheit langfristig gewährleisten und schnelle Antworten bei Problemen liefern – wenn ein Server nicht funktioniert oder ein Teilsystem plötzlich langsamer wird. Dazu müssen die Silos aufgebrochen und Logs zentral erfasst werden. Danach kann, basierend auf den Zugriffsberechtigungen, teamübergreifend auf Daten zugegriffen werden. So erhält man den Gesamtüberblick und kann mit gezielten Auswertungen das Problem erkennen.

Hybrid-Lösung mit tacLOM und Splunk

Eingesetzt wurde tacLOM, die Monitoring-Software von terreActive. Sie bietet eine zentrale Plattform für die Archivierung, Analyse und Alarmierung von Logdaten und nutzt Synergien aus System Monitoring, Log Management und Log Analyse. Sie ermöglicht so eine Kombination aus passivem und aktivem Monitoring.

Das Lizenzmodell von tacLOM ist auf hohe Datenmengen ausgerichtet: Die Lizenzierung erfolgt pro System.

Ergänzend wurde Splunk integriert und kommt bei der automatischen Datenverdichtung zum Einsatz. Durch die Hybrid-Lösung mit der gezielten Nutzung von tacLOM *und* Splunk für unterschiedliche Aufgaben werden Ressourcen bewusst und kosteneffizient eingesetzt.

KSD

Das Informatikunternehmen von Kanton und Stadt Schaffhausen betreut mit rund 50 Mitarbeitern den Kanton, 2 Städte, 26 Gemeinden, 2 Spitäler sowie 16 Schulen. Es umfasst ca. 2’200 IT-Arbeitsplätze.

Das KSD stellt die Informatikbasis und Applikationsinfrastruktur bereit und sorgt für einen täglichen, sicheren Betrieb unter Einsatz von bewährten ICT-Technologien.

www.ksd.ch

Was bringt die zentrale Plattform

- Die zentrale Lösung unterstützt die teamübergreifende Fehleranalyse.
- Der Einbezug aller KSD-Systeme sichert schnelle und kompetente Reaktion.
- Die starke Belastung einzelner Administratoren wurde reduziert.
- Bisher verborgene Zusammenhänge wurden sichtbar. Synergien können nun genutzt werden.
- Ausfälle können im Detail nachvollzogen werden und Rückschlüsse für zukünftige Vermeidung liefern.

Im Einsatz für mehr Sicherheit:

- tacLOM Monitoring Software
- Splunk Datenanalyse
- Threat Intelligence Service
- Betriebssupport mit 7x24 Pikett durch terreActive

Die Lösung im Detail

Hohe Speicherkapazität – Erfassung in Echtzeit – verfügbar bei Ausfällen

Die neu zentral gesammelten Betriebs-Logs von verschiedenen Komponenten werden in Echtzeit erfasst und für ein Jahr gespeichert. Für Logs ist das ungewöhnlich lange – normalerweise werden sie aufgrund der Speicherkapazität rasch wieder überschrieben.

Der Vorteil: Die Speicherung über einen längeren Zeitraum lässt neben Abweichungen von der Norm auch Ausfälle im Detail nachvollziehen. Denn tacLOM speichert die Daten als Kopie, so dass alle Daten von Ausfällen zur Verfügung stehen, die Aufschluss über die Ausfallgründe und die zukünftige Vermeidung liefern können.

Rohdaten verstehen und Fehlersuche vereinfachen

Für die Analyse der Logdaten arbeitet tacLOM mit Events und Eventpacks. Aufgrund von spezifischen Logereignissen wird vom System ein Event generiert.

Bei jedem Event werden die jeweiligen auslösenden Logzeilen gespeichert. So kann man bei einer späteren Analyse schnell auf die Rohdaten zurückgreifen. Die automatische Verdichtung mittels Eventpacks vereinfacht die Fehlersuche und -behebung massiv, da so Zusammenhänge über die Teams hinweg verständlich werden.

Weniger Wartungsaufwand

Eine zentrale Eventkonsole und ein einheitliches Alarmsystem ermöglichen eine aktive Überwachung der Logdaten und der Ereignisse. Die zentrale Datensammlung und Überwachung reduziert zudem den Wartungsaufwand und die Betriebskosten.

Angepasst auf die Anwender

Wo früher nur der Administrator Zugang hatte, kann heute teamübergreifend zusammengearbeitet werden. Jeder Anwender kann die Auswertungen entsprechend seinen Bedürfnissen anpassen. Er kann seine persönliche Ansicht konfigurieren inklusive Reports und Dashboards.

Visualisierungen unterstützen die Anwender im Alltag. Auch die Zugangsberechtigungen können entsprechend den Betriebsvorgaben angepasst werden: Wichtig, denn bei KSD besonders relevant sind die hohen Datenschutzanforderungen seitens Kunden (z. B. Schutz der Daten der Bürger einer Gemeinde).

Ausblick: Bereit für die Zukunft

Mit der Einführung des zentralen Log Managements ist das KSD für die Zukunft gut aufgestellt, denn die neue Plattform bildet die ideale Ausgangslage für weitere Sicherheitsmassnahmen:

- Schrittweiser Auf- und Ausbau zu einer Security-Monitoring-Lösung (SIEM)
- Erfüllung von Compliance-Anforderungen
- Schutz vor Cyberattacken