

Security Event Management verbessert die Sicherheitsinfrastruktur bei der Basler Kantonalbank

Sicherheit wird bei der Basler Kantonalbank (BKB) gross geschrieben. Die gesamte IT-Infrastruktur muss diesbezüglich höchsten Anforderungen gerecht werden. Beim Redesign ihrer DMZ-Infrastruktur hat sich die BKB zur Einführung einer umfassenden Security Event Management (SEM)-Lösung von terreActive auf der Basis von tacLOG entschieden.

Die BKB ist darauf angewiesen, dass ihre IT-Infrastruktur rund um die Uhr reibungslos funktioniert. Potenzielle Störfaktoren und Schwachstellen im Netzwerk sollen deshalb möglichst frühzeitig identifiziert und eliminiert werden. Zu diesem Zweck wird die bestehende Infrastruktur regelmässig auf ihre Funktionstüchtigkeit und Sicherheit geprüft.

Security Audit zur Aufdeckung von Schwachstellen

terreActive wurde von der BKB mit einem umfassenden Security Audit der DMZ (Demilitarized Zone; Netzwerk mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server) beauftragt. Die Spezialisten von terreActive verschafften sich einen externen Überblick über die involvierten Komponenten. Dabei kamen vor allem Tools und Methoden zum Einsatz, wie sie teilweise auch von böswilligen Angreifern aus dem Internet angewendet werden. Dadurch lässt sich ein Angriff simulieren und die eingebauten Schutzmechanismen können auf ihre Wirksamkeit getestet werden.

Redesign der DMZ-Infrastruktur

Die im Audit gesammelten Informationen wurden anschliessend analysiert, bewertet und in einem ausführlichen Bericht festgehalten. Dieser Bericht diente zur Einschätzung des Sicherheitsniveaus bei der BKB und brachte einige Schwachstellen zu Tage. Auf dieser Grundlage haben die BKB und terreActive Massnahmen erarbeitet, um diese Sicherheitslücken zu beheben und die DMZ-Infrastruktur den aktuellen Bedürfnissen anzupassen.

SEM wider die Komplexität

Zur gleichen Zeit wurde bei der BKB auch SEM zu einem Thema. SEM wirkt der steigenden Komplexität der Sicherheitsinfrastruktur – hervorgerufen durch den stetigen Strom von neuen

Die wichtigsten Vorteile auf einen Blick

- Die SEM-Lösung reduziert die Komplexität in der DMZ
- Transparenz im gesamten E-Mail-Verkehr
- Spam-Reporting durch passives Monitoring sichergestellt
- Relevante Informationen jederzeit auf Abruf verfügbar
- SEM kann problemlos auf weitere DMZ-Komponenten ausgeweitet werden

Abwehrsystemen aufgrund neuer Bedrohungen – entgegen und hilft den Überblick zu behalten, indem die SEM-Lösung permanent das Verhalten der IT-Infrastruktur analysiert. Bei terreActive kommt hierzu eine Kombination von passivem Monitoring mit tacLOG und aktivem Monitoring durch tacMON zum Einsatz. Diese Kombination ermöglicht dem Kunden eine einmalige Übersicht über den Zustand seiner gesamten IT-Infrastruktur.

Langjährige Partnerschaft

Für das neue DMZ-Design sowie die Sicherung des gesamten E-Mail-Verkehrs hat die BKB auf die langjährige Partnerschaft mit terreActive gesetzt. „Wir haben in der Vergangenheit sehr gute Erfahrungen mit terreActive gemacht“, sagt dazu Gilles Rapp, der bei der BKB für das ganze Projekt verantwortlich war. „Für uns war es deshalb schon sehr schnell einmal klar, dass wir auch bei der Implementierung einer SEM-Lösung auf die Erfahrungen und Kompetenzen dieses Partners zurückgreifen wollten.“

„Alleine schon die Sammlung und Auszählung der Logdaten durch tacLOG sowie die Möglichkeiten der grafischen Darstellung gibt uns einen hervorragenden Überblick und zeigt sehr schön Ausnahmesituationen auf, die dann direkt anhand der Logfiles überprüft werden können.“



Gilles Rapp
 Mitglied Kader
 Basler Kantonalbank

Reporting mit neuen Möglichkeiten

Bei der alten DMZ-Infrastruktur kam für das Reporting eine Eigenentwicklung zum Einsatz. Die BKB hat sich beim Redesign dazu entschlossen, dieses System abzulösen. Zur Absicherung des E-Mail-Verkehrs hat terreActive eine auf die spezifischen Bedürfnisse der BKB zugeschnittene Lösung entwickelt, die tacLOG mit bewährten Open Source-Produkten verbindet. „Die gemeinsam mit terreActive entworfene Lösung ist massgeschneidert auf unsere Anforderungen ausgerichtet und erfüllt unsere Ansprüche optimal“, erläutert Gilles Rapp.

Monitoring zeigt Abweichungen auf

Zurzeit werden mit der neuen SEM-Lösung die Logfiles des E-Mail-Verkehrs gesammelt und ausgewertet. Dabei laufen die Logfiles permanent auf einem Monitor und werden von den Mitarbeitern der IT-Abteilung überwacht. Dazu Gilles Rapp: „Mit der SEM-Lösung sind wir in der Lage, Abweichungen vom Normalbetrieb schon früh zu erkennen, zu analysieren und gegebenenfalls notwendige Massnahmen einzuleiten.“ Die Logdaten dienen dazu, Statistiken über die Anzahl der E-Mails, der Anteil an Spam, das Aufkommen von Viren sowie den Prozentsatz von blockierten E-Mails zu erstellen. Hierzu erhält die Geschäftsleitung der BKB jeden Monat eine Zusammenfassung mit allen relevanten Informationen.



**Basler
Kantonalbank**
fair banking

Über die Basler Kantonalbank

Die Basler Kantonalbank nahm am 1. Oktober 1899 ihre Geschäftstätigkeit auf. Ihr Angebot umfasste neben der Kreditvergabe und der Annahme von Spargeldern auch Börsengeschäfte. Heute ist die Basler Kantonalbank in Basel und der Region als Universalbank tätig. Sie ist ein Institut mit Staatsgarantie. Das Privat-, das Anlage- und das Kommerzkundengeschäft zählen zu den Kernsegmenten der Basler Kantonalbank. Die Dienstleistungen werden über ein dichtes Filialnetz (19 Standorte) für die Bevölkerung und die Unternehmen der Region Nordwestschweiz erbracht. Darüber hinaus ist die Basler Kantonalbank durch Private-Banking-Aktivitäten in Zürich und Olten vertreten, und betreibt das Geschäft mit grossen Firmenkunden, Institutionellen sowie Banken in der ganzen Schweiz.

„Mit der Einführung der SEM-Lösung von terreActive hat die BKB die entscheidende Grundlage gelegt, um eine umfassende Übersicht über den Zustand der gesamten IT-Infrastruktur zu erhalten und so insbesondere die Sicherheit der Systeme jederzeit zu gewährleisten.“



Urs Rufer
Leiter Consulting & Projects
terreActive AG

Stufenweiser Ausbau in Planung

Zusätzlich zum E-Mail-Verkehr sammelt tacLOG auch systematisch die Firewall-Logs, deren Auswertung ist in einem weiteren Schritt vorgesehen. Und das ist noch nicht alles. Die BKB baut die Lösung in Zusammenarbeit mit terreActive kontinuierlich aus. Das Ziel dabei ist die Ausdehnung von SEM auf die Überwachung der kompletten DMZ-Infrastruktur – wie beispielsweise Logfiles der Windows-Server, Netzwerkkomponenten oder auch Internet-Verkehr. Mit SEM hat die BKB einen weiteren grossen Schritt zur Erhöhung der Sicherheit der IT-Infrastruktur gemacht.

SEM in Kürze

Der SEM-Markt ist noch relativ jung und die genaue Bezeichnung nicht ganz eindeutig. Man spricht von Security Event Management (SEM) und seit Gartner den Markt analysiert auch von SIEM, wobei das I für Information steht. Mit Information sind Themen wie Reporting (Compliance) gemeint, wohingegen der Event für operative Themen wie das laufende Erkennen von Vorfällen steht. Da viele Lösungen beide Themen zu vereinen versuchen, spricht Gartner vom SIEM-Markt. Eine SEM-Lösung analysiert permanent das Verhalten der IT-Infrastruktur und verfügt dazu über die folgenden Grundfunktionen:

- Monitoring von allen relevanten Objekten
- Normalisierung und zentralisierte Eventdaten-Speicherung
- Zentrale Archivierung der Daten
- Manuelle Analyse und Berichterstellung
- Datenkorrelation und automatisierte Event-Generierung
- Reports für Compliance, Audits und Management

terreActive AG Kasinostrasse 30 CH-5001 Aarau
www.terreactive.ch

Wir sichern Ihren Erfolg.

terreActive
terreActive
terreActive
terreActive