terreActive
terreActive
terreActive
terreActive

Success
Story

Schaffhauser Kantonalbank stärkt Cyber Security mit Security Operations Center von terreActive

Ausbau der Cyber-Defense-Plattform erhöht Security-Maturität

Für einen Hacker spielt es keine Rolle, ob ein Unternehmen international oder lokal verankert ist, solange der erhoffte kriminell erzielte Gewinn gross genug ist. Dementsprechend braucht auch jede Bank den gleichen Schutz. Durch ein effizientes Cyber-Defense-Konzept und die Nutzung von Synergien im SOC-Betrieb konnte die Schaffhauser Kantonalbank ihr Sicherheitsdispositiv weiter ausbauen.

Ausgangslage

Die Schaffhauser Kantonalbank (SHKB) verfügte bereits über gute Sicherheitslösungen u. a. von Splunk und Vectra. Logdaten wurden gesammelt, aber noch nicht zentral ausgewertet und es fehlte die gesamtheitliche zeitnahe Sicht über alle Systeme und Appikationen. Daher suchte die Bank einen Partner für den Aufbau eines Security Operations Centers (SOC), das auf Basis einer Cyber-Defense-Plattform Vorfälle erkennen und behandeln soll. Nach dem Aufbau der Lösung im Jahr 2020 soll der neue Partner künftig auch einzelne SOC-Services erbringen, um die Personalressourcen der Bank zu entlasten. Die SHKB führte eine offizielle Ausschreibung durch, bei der terreActive aufgrund des vorgestellten, ganzheitlichen Lösungsansatzes sowie der hohen Kundenorientierung zu überzeugen vermochte.

Projektvorbereitung

Vor dem eigentlichen Projektbeginn wurde ein Proof of Concept (PoC) durchgeführt, der auch einen SOC-Workshop umfasste, in dem die ersten möglichen Use Cases (Bedrohungsszenarien) besprochen wurden. Bei einem Kick-off-Meeting planten die SHKB und terreActive Ressourcen wie auch Termine, legten die Arbeitsteilung fest und definierten die Projektmeilensteine analog dem Security Monitoring Cycle. In einem späteren Workshop wurden zusätzlich Eskalationswege, Zugriffsrechte und Verantwortungen, z. B. innerhalb des Incident-Response-Prozesses, behandelt.

Vorgehensweise

Die Cyber-Defense-Plattform (CDP) als Summe aller Sicherheitskomponenten ist entscheidend für das SOC, um Vorfälle erkennen und bearbeiten zu können. In der Planungsphase prüfte terreActive deshalb verschiedene Varianten der CDP hinsichtlich der Gegebenheiten bei der Schaffhauser Kantonalbank. «Aus vorhandenen Sicherheitskomponenten konnte terreActive schnell eine erste CDP für uns erstellen, die kontinuierlich weiterentwickelt wurde und so eine immer grössere Abdeckung von Bedrohungsszenarien erreichte,» so Andreas Glauser, Sicherheitsbeauftragter bei der Schaffhauser Kantonalbank. «Die umfangreiche Use-Case-Datenbank von terreActive wirkte sich dabei positiv auf einen zügigen Projektstart aus, denn unter Berücksichtigung der Threat Landscape unserer Bank konnten etliche Standard-Use-Cases umgehend aktiviert werden.»

«Die erfahrenen Mitarbeitenden der terreActive haben uns bei der Auswahl der effektivsten Use Cases unterstützt. Mittels regelmässiger, sehr konstruktiver Abstimmungsmeetings stellen wir die Professionalität und Weiterentwicklung der Cyber-Defense-Plattform sicher.»

Andreas Glauser, Sicherheitsbeauftragter

Schaffhauser Kantonalbank

Technische Umsetzung

«Um unseren hohen Ansprüchen an Performanz, Kapazität und Redundanz gerecht zu werden, bauten wir mit Unterstützung von terreActive die bestehende Splunk-Infrastruktur als Cyber-Defense-Plattform aus.» so Rudolf Lenz, Leiter Operations & IT bei der Schaffhauser Kantonalbank. Sicherheitsrelevante Informationssysteme wurden an die SIEM-Plattform (Security Information and Event Management) angebunden und liefern nun Logs, die zentral gespeichert und ausgewertet werden. Dabei dient Splunk Enterprise Security, dem SOC als primäres Werkzeug zur Korrelation von Logdaten sowie dem Auffinden und der Visualisierung von Bedrohungen. Desweiteren integrierte terreActive Use Cases und stimmte diese auf die SHKB ab. Für noch mehr Sicherheit wurde das Vulnerability Management von Tenable installiert und mit dem SIEM verbunden.

Schaffhauser Kantonalbank

Über die Schaffhauser Kantonalbank

Mit über 300 Mitarbeitenden und einer Bilanzsumme von 8.7 Mrd. Franken ist die Schaffhauser Kantonalbank das führende Finanzinstitut im Kanton Schaffhausen. Die moderne Universalbank mit fünf Filialen bietet Finanzdienstleistungen für Privatpersonen, Unternehmen und öffentliche Institutionen. Die Bank wurde 1883 gegründet und ist zu 100 Prozent im Besitz des Kantons.

Daily Operation und Incident Response

Der flexible Servicekatalog von terreActive ermöglicht es mittleren Unternehmen unterschiedlicher Branchen von denselben Leistungen zu profitieren wie ein Grosskonzern. Für die Schaffhauser Kantonalbank übernimmt terreActive Services wie Threat Detection und Threat Intelligence, die das Aargauer Unternehmen auch für grosse weltweit agierende Unternehmen erbringt. Von den Erfahrungen und Synergien profitieren alle Kunden gleichermassen.

Das SOC der terreActive prüft alle durch die Cyber-Defense-Plattform generierten Meldungen in erster Instanz. Im Bedarfsfall werden Vorfälle untersucht und mit der Schaffhauser Kantonalbank gemeinsam abgeklärt. Wird ein Sicherheitsvorfall (Incident) ausgelöst, so legt ein Runbook fest, wer was zu tun hat.

Das SOC der terreActive operiert von Aarau und Zürich aus und betreibt die Cyber-Defense-Plattform gemeinsam mit dem Kunden.

Nutzen für die Bank

- Die Erkennungs- und Reaktionszeit bei Sicherheitsvorfällen wurde massiv reduziert.
- Die SHKB erhält ein umfangreiches Reporting, Beurteilungsgrundlagen und Empfehlungen.
- Die firmeninternen Ressourcen werden durch den SOC-Betrieb von terreActive entlastet, die Effizienz gesteigert.
- Die Compliance-Anforderungen werden durch die zentrale und unveränderbare Logsammlung erfüllt.
- Die Cyber Defense der SHKB wird durch die enge Zusammenarbeit mit den Spezialisten von terreActive permanent verbessert.

«Monatliche Review-Meetings unterstützen uns dabei, unseren Sicherheitsstandard kontinuierlich zu überprüfen und zu optimieren.» - sagt Andreas Glauser von der Schaffhauser Kantonalbank.

Unternehmen, die jetzt vorsorgen, erarbeiten sich einen Vorsprung, wenn es darum geht, zukünftigen Angriffen von Cyberkriminellen zu begegnen.