

Security Operations Center: Kampf den Hackern

Im Einsatz für Grossbanken, Kernkraftwerke und Rettungsdienste: Ein paar Dutzend Sicherheitsingenieure in Aarau und Zürich schützen die kritischsten Infrastrukturen der Schweiz.

Waren die Kunden von IT-Security-Anbietern lange Zeit vor allem Banken und Versicherungen, kommen sie heute aus allen möglichen Branchen. Ein gesteigertes Sicherheitsbewusstsein hat dazu geführt, dass auch Online-Shops, ein Spezialist für Flugretungen, Autohändler, Kantone und ein Kernkraftwerk auf die Dienste von «terreActive» setzen, die sich seit über zwanzig Jahren um die IT-Sicherheit von KMU und Grosskonzernen kümmern.

Security Operation Center nach Mass

Das Herz des Unternehmens ist das Security Operations Center (SOC), das nur durch eine Sicherheitsschleuse betreten werden kann. Hier sorgt man für einen reibungslosen und sicheren Betrieb von über 400 Systemen. Rund um die Uhr, an 365 Tagen im Jahr. Im Operations Control Center sind Ingenieure mit dem Betrieb und Unterhalt sämtlicher Sicherheitskomponenten beschäftigt, während nebenan



Einsatzteam in Aktion: Im Security Operations Center zeigt ein Lichtsystem an, wer beispielsweise gerade einen Angriff abwehrt.

hoch spezialisierte Fachkräfte im Incident & Response Center ständig auf der Suche nach Gefahren sind. Dabei kann jeder Kunde aus einer breiten Angebotspalette genau die Services buchen, die er braucht. Dadurch entsteht ein effizientes und schnelles SOC, das sich viele Unternehmen selber nicht leisten könnten. Dabei lohnt sich die Investition allemal.

Hacker legen Guezlifabrik lahm

Als die Erbauer einer Guezlifabrik gefragt wurden, was Hacker in ihr anrichten

könnten, schätzten sie das Schadenspotenzial auf den Verlust einer Tagesproduktion: Sie erwarteten etwas versalzenen Teig. Als eben diese Fabrik tatsächlich von Erpressern angegriffen wurde, blieb allerdings die gesamte Produktion stehen und der Teig härtete in den Transportrohren aus. Die Fabrik lief erst wieder, nachdem das gesamte Transportsystem ersetzt worden war. Dabei werden nur die wenigsten Vorfälle publik, die Betroffenen schweigen lieber. Für sie bedeutet ein erfolgreicher Angriff immer auch ein Reputationsrisiko.

Um mit solchen Angreifern Schritt zu halten, hat «terreActive» sein Einsatzteam im SOC stark ausgebaut. Mit einer immer höheren Spezialisierung der Mitarbeiter reagiert das Security-Unternehmen schnell und zuverlässig auf Vorfälle und Bedrohungen. Die Teams arbeiten mit einem bewährten Mix von eigenen Tools, Schweizer Technologien und international bekannter Software. So sorgt das Unternehmen jeden Tag von Neuem dafür, dass die Guezli in den Laden kommen, das Geld in den Bankomat und der Rettungshelikopter zur Unfallstelle. ■

Jobmöglichkeiten in der Cyber-Security

Ein SOC bietet Beschäftigungsmöglichkeiten für Ingenieure mit unterschiedlichen Hintergründen. Sie kommen aus der Berufslehre, der Fachhochschule oder der ETH. Einige sind auch Autodidakten. Zur Zeit arbeiten 50 Mitarbeiter in Aarau und in Zürich und für das SOC sucht man nach Verstärkung.

Cyber Security Engineer

Kümmert sich um den Ausbau und das Feintuning des Security Monitorings. Erweitert die Applikationen-Sicherheit und entwickelt auf Kunden zugeschnittene Use Cases.

Cyber Security Analyst (Threat Detector)

Analyse und Bewertung von Ereignissen, Erkennung von Unregelmässigkeiten und Optimierung und Verbesserung des Alarmsystems (SIEM).

Cyber Security Analyst (Threat Hunter)

Detaillierte und vertiefte Analyse von Ereignissen, Incident Management in Zusammenarbeit mit dem Kunden, Suchen und Bearbeiten von Schwachstellen.

terreActive AG, 5001 Aarau
☎ +41 (0)62 834 00 55
info@terreactive.ch, www.security.ch