Computerworld Magazin Sonderausgabe "Security" Erscheinungstermin 19.5.2017

Professionelle Angriffe erfordern Überwachung und Abwehr durch Spezialisten-Team

Einsatzzentrale gegen Cybercrime

Von Urs Rufer, CEO terreActive AG
Die Angreifer sind drei Schritte weiter als die meisten Unternehmen: Sie teilen sich ihre kriminellen Aktivitäten in spezialisierten Teams. Ihre Angriffe sind schnell und präzise. Die Schäden enorm. Davor schützt man sich am besten mit einem spezialisierten Einsatzteam.

Schutzzäune sind nutzlos, wenn niemand erkennt, dass sie durchlässig geworden sind. Firmen müssen überwachen, was ihnen wertvoll ist: Einkommen, Wissen, Reputation. Schutzmassnahmen alleine genügen nicht mehr.

Studie: Jede zweite Firma ohne organisierte Abwehr
Eine Studie von EY zeigt, dass bei vielen Firmen die Überwachung fehlt. 44 Prozent der Befragten gaben an, über kein Security Operations Center zu verfügen, welches Bedrohungslagen untersucht, Angriffe erkennen und die Abwehrmassnahmen koordinieren kann.

Genau dies wird aber wichtiger: Denn Cyberkriminelle gehen professionell vor. Oft handeln keine Individuen, sondern Organisationen. Die Spezialisten teilen sich die Aufgaben: Das Aufspüren von Schwachstellen etwa oder das Programmieren von Schadsoftware.

Einsatz bei terreActive in Aarau: SOC mit Incident & Response Center

Trend: Die Einsatzteams spezialisieren sich
Sein eigenes Einsatzteam zu professionalisieren ist die beste Methode, um die Firma vor solchen Angriffen zu schützen. Die Cyber Security macht hier grosse Entwicklungsschritte: Aus einzelnen Managed Security Services formierten sich die Security Operations Center. Sie können Angriffe nicht nur erkennen, sondern auch die Abwehr koordinieren.

Planen Sie Ihre Abwehr auszubauen? terreActive hilft, den Bedarf zu beurteilen und Massnahmen zu definieren.
www.securityMonitoring.ch

Um neuen Anforderungen begegnen zu können entstehen jetzt innerhalb des SOCs hoch spezialisierte Teams, welche aktiv nach Gefahren oder Hinweise auf Attacken suchen (Threat Hunting und Anomaly Detection). Ihr Vorteil: Sie reagieren schneller, weil für jede Aufgabe spezifisch geschulte Fachkräfte zum Einsatz kommen. Wer im Outsourcing auf solche Teams zugreift, erhält alle notwendigen Rollen auf einmal. Denn für eigene spezialisierte Einsatzzentralen gegen Cybercrime, fehlen vielen Firmen die Ressourcen.

Ausbau: terreActive trennt die Aufgaben
Der Schweizer IT-Security-Anbieter terreActive hat sein Einsatzteam und das Security Operations Center deshalb stark ausgebaut. Die Aufgaben des Betriebs wie System Monitoring, Support und Maintenance erhalten ihr eigenes Operations Control Center (OCC). Ein weiteres Security-Kompetenzteam ist neu im Incident & Response Center (IRC) eigenständig organisiert. Die Spezialisten konzentrieren sich vollumfänglich auf die Überwachung, die aktive Suche nach Bedrohungen und die Koordination der Abwehr. So halten sie mit den Angreifern Schritt.