Schutzwälle reichen nicht aus

Unternehmen müssen heute davon ausgehen, dass ihre Systeme bereits infiltriert sind oder sie Opfer einer Attacke werden. Es ist deshalb entscheidend, Infiltrationen zu erkennen, schnell darauf zu reagieren und das Sicherheitsdispositiv entsprechend zu optimieren. Und genau dazu braucht es ein Security Operation Center.

DER AUTOR

Ernesto Hartmann
Chief Security Operations Officer, Infoguard

Hackerangriffe und andere IT-Sicherheitsvorfälle sind nicht nur ärgerlich, sie können auch enorme Kosten und einen Imageschaden nach sich ziehen – und die Bedrohung durch Cyberangriffe nimmt stetig zu. Deshalb haben sich viele Unternehmen darauf fokussiert, Cyber-Risiken zu identifizieren und entsprechende (ICT-)Sicherheitsmassnahmen zu integrieren. Aber dies reicht heutzutage nicht mehr aus. Es braucht neue Ansätze bei denen die Detektion im Vordergrund steht und die Reaktion auf Angriffe ein wesentlicher Bestandteil der IT-Prozesse ist. Geschickt umgesetzt, kann so die Prävention zielgerichtet und kontinuierlich verbessert werden.

Cyber Security besteht nicht nur aus (ICT-)Sicherheitsmauern

Ein Unternehmen kann nur angemessen reagieren, wenn die administrativen Abläufe der ICT-Infrastruktur klar geregelt sind. Denn die Frage, ob der Angreifer oder Administrator den Alarm ausgelöst hat, muss schnell beantwortet werden. Deshalb braucht es zur Verteidigung technische Unterstützung in Form einer zentralen Big-Data-Plattform. Diese sammelt und verwertet Informationen über Assets und Schwachstellen sowie externe Threat-Feeds und vereint diese zu einer umfassenden Security-Intelligence-Plattform.

Eine gute Möglichkeit Angreifer nach einem erfolgreichen Angriff aufzuspüren, bieten Breach-Detection-Lösungen bei denen der Netzwerkverkehr mittels Data Science, maschinellem Lernen und Verhaltensanalysen durchsucht und ausgewertet wird. Durch diese Kombination profitieren IT-Verantwortliche nach einer Abstimmungsphase von einer sehr geringen False-Positive-Rate der Breach-Detection-Lösung. Dadurch können bei echten Alarmierungen klar definierte SLAs umgesetzt werden. Denn wenn ein Angreifer erkannt wird, muss ein Unternehmen jederzeit (auch nachts) in der Lage sein schnell zu reagieren.

Um einen Alarm effizient zu validieren und von der Netzwerkkommunikation auf den involvierten Prozess schliessen zu können, braucht es retrospektive Informationen. Mit Hilfe dieser Informationen kann sich ein Analyst schnell ein Bild von den am Angriff involvierten Prozessen machen. Nur so lässt sich die gesamte Infrastruktur im Bedarfsfall flächendeckend nach sogenannten «Indicators of Compromise» durchsuchen. Um all diese Aufgaben erfolgreich zu meistern, empfiehlt es sich mehrere Funktionen in einem dedizierten Security Operation Center (SOC) zusammenfassen. Hierzu zählt ein Team von Experten und entsprechende Tools zur Breach Detection, für das Security Information & Event Management (SIEM), aber auch für die Incident Response.

Security Operation ist nicht IT Operation

Dabei darf es nicht sein, dass sich die Mitarbeiter des SOC zusätzlich um den operativen Betrieb der IT kümmern müssen. Das SOC sollte ausschliesslich auf Sicherheitsvorfälle reagieren. Natürlich braucht es neben entsprechenden Werkzeugen zur Erkennung von Attacken oder Infiltrationen auch IT-Spezialisten. Aber noch viel wichtiger sind Cyber-Threat-Analysten und Security-Experten. Security Operation ist eine anspruchsvolle Arbeit – und bleibt leider bei vielen Unternehmen durch den Businessalltag auf der Strecke. Abhilfe schaffen da professionelle Services von spezialisierten Anbietern. Denn dort setzen sich Analysten täglich mit der aktuellen Bedrohungslage auseinander. So können Unternehmen von der grossen Erfahrung von Experten profitieren, ohne ein eigenes SOC aufbauen zu müssen.