CIO

Link: https://www.cio.de/a/mehr-intelligenz-statt-hoehere-mauern,3102319

Tipps für den Aufbau eines Security Operations Center (SOC)

Mehr Intelligenz statt höhere Mauern

Datum: 22.01.2015
Autor(en): Markus Müssig

Spätestens durch die NSA-Affäre ist klar: Die klassischen IT-Security-Maßnahmen reichen nicht aus, um die Sicherheit von sensiblen Daten zu gewährleisten. Statt die virtuellen Mauern höher zu bauen, empfiehlt sich der gezielte Einsatz intelligenter Analyse- und Abwehrmaßnahmen, angesiedelt in einem Security Operations Center (SOC).

SOCs sind derzeit angesagt. Ohne eine differenzierte Betrachtung des Begriffes SOC gehen derzeit 70 bis 80 Prozent der Unternehmen davon aus, dass sie bereits ein solches Center für IT-Security betreiben, so die Einschätzungen von HP. Doch bei genauerer Betrachtung sinkt diese Zahl auf unter 10 Prozent. Denn in vielen Fällen wird unter einem SOC der Betrieb klassischer IT-Security-Tools wie Firewalls und Antiviren-Software verstanden.

Markus Müssig ist Security Consultant bei HP Enterprise Security Services
Foto: HP Deutschland

In den vergangenen Jahren haben Unternehmen immer mehr in solche Werkzeuge investiert, haben die virtuellen Mauern um sich herum immer höher gezogen, um sich und ihre unternehmenskritischen Daten dahinter zu verschanzen. Doch die Sicherheit, in der sie sich wiegen, ist trügerisch: Die meisten Organisationen sind heute Ziel von Angriffen - merken es aber oft nicht einmal.

Laut dem 2013 Threat Report von Mandiant vergehen aktuell im Mittel 243 Tage, bevor Organisationen Angreifer in ihren Netzwerken entdecken. Das heißt, Angreifer haben alle Zeit der Welt, um Daten und Informationen abzugreifen. Dies liegt, nach der Meinung von HP, zu einem wesentlichen Anteil an den nicht erkannten Mehrwerten der Auswertung von Logdaten.

Statt des Aufbaus noch höherer Mauern um das gesamte Unternehmen empfiehlt es sich daher, mit intelligenten Methoden herauszufinden, wo sich potenzielle Schlupflöcher in der Mauer befinden, welche Hinweise es auf potenzielle Angreifer gibt - und aufgrund dieser Daten die für das Unternehmen wesentlichen Daten und Anwendungen zu schützen. Dies muss die Aufgabe eines SOC sein.

Eigenständigkeit der Organisation auf C-Level

SOCs sind dabei nicht nur ein Thema für große, bekannte Unternehmen. Als Faustformel lässt sich festhalten: Ein SOC empfiehlt sich für jedes Unternehmen, das über Informationen verfügt, die in seinen Märkten wegweisend und damit interessant für Außenstehende sind. Das kann zum Beispiel auch der Fall sein, wenn ein kleines Unternehmen einen neuen Geschäftsbereich mit großem Potenzial am Weltmarkt etabliert.

Welche Faktoren gilt es beim Aufbau eines SOC zu beachten? Wichtig ist zunächst das SOC als eigenständige Organisation außerhalb der Linie und Produktion zu begreifen - am besten auf CIO- beziehungsweise CISO-Ebene. Denn nur durch die operationelle Unabhängigkeit vom Kerngeschäft kann ein SOC echten Mehrwert für genieren, indem es die wirklich unternehmenskritischen Informationen schützt.

Welche dies sind, das gilt es im ersten Schritt zu identifizieren. Je nach Unternehmen kann dies sehr unterschiedlich sein: Bei einem produzierenden Unternehmen können dies Entwicklungsdaten sein, bei einem Telekommunikationsunternehmen die Kundendatenbanken, bei einem E-Commerce-Anbieter die Kreditkarteninformationen seiner Kunden.

Risiken identifizieren und Maßnahmen daraus ableiten

Unabhängig davon, um welche Informationen es sich handelt: Ein Unternehmen muss für sich individuell die größten Risiken festlegen - und welche IT-Systeme und Anwendungen damit verbunden sind. In vielen Fällen wird es als Konsequenz darum gehen, beispielsweise ein ERP-System, bestimmte Webserver oder auch Datenbanken gezielt abzusichern. Die Zusammenhänge und Abhängigkeiten zwischen kritischen Geschäftsprozessen und den darunter liegenden IT-Systemen lassen sich am besten über eine Configuration Management Data Base, kurz CMDB, erfassen. Sie ermöglicht einem SOC beispielweise, effizient darüber zu entscheiden, ob auffällige Vorkommnisse im Netzwerk oder Angriffe von außen als geschäftskritisch einzustufen sind. Denn genau darum geht es in einem SOC - auf Basis einer Vielzahl von Informationen und auch trotz einer Flut von Daten, einen kühlen Kopf zu bewahren, wichtiges herauszufiltern und die kritischen Assets im Unternehmen zu schützen.

Dass dafür IT-Security-Systeme zum Einsatz kommen, ist selbstverständlich. Dabei können vorhandene Systeme durchaus einbezogen werden. Doch ein SOC muss weit mehr als dies leisten: Diese Organisation braucht entsprechendes Personal mit dem nötigen Know-how und der entsprechenden Kompetenz im Unternehmen, um proaktiv Zusammenhänge zwischen Daten herstellen und um daraus gegebenenfalls schnell Notfallpläne umsetzen zu können.

Welche Aufgaben ein SOC konkret erfüllen sollte, ist im zweiten Schritt zu definieren. Bei der Definition des SOC-Service-Portfolios spielen interne organisatorische Gegebenheiten - sollen Aufgaben vorhandener IT-Security Fachbereiche übernommen werden, welche Überschneidungen mit anderen Bereichen wie CERTs gibt es - ebenso eine Rolle wie die personelle Ausstattung eines SOC. Nach Erfahrungen von HP ist der schrittweise Auf- und Ausbau eines SOC ratsam.

SIEM korreliert Log-Daten intelligent

Zu den Services, die ein SOC dem Business auf alle Fälle anbieten sollte, gehören Security-Information- und Event-Management (SIEM)- sowie Vulnerability-Management-basierte Dienste.

Mithilfe von SIEM lassen sich Log-Daten im Unternehmen zentral sammeln und intelligent auswerten, indem sie miteinander in Beziehung gesetzt und mittels zusätzlicher Informationsquellen angereichert werden. Firewalls registrieren, dass es eine Kommunikation zwischen Mitarbeitern im Unternehmen und externen Partnern gibt. Doch sie geben keinerlei Hinweis darauf, ob diese Kommunikation erwünscht, ob sie in der registrierten Häufigkeit üblich ist oder ob es Zusammenhänge zu anderen, nicht erlaubten oder gewünschten Kommunikationsformen gibt.

So kann ein SIEM-System intelligente Verbindungen herstellen zwischen den bei einem kritisch eingestuften Webserver registrieren Log-Daten und dem E-Mail-Verkehr besonders wichtiger Personen im Unternehmen. Dazu könnten der Entwicklungsleiter oder aber der Leiter Kundenservice gehören. Damit können die Mitarbeiter im SOC proaktiv Bedrohungsszenarien erkennen. Vorausgesetzt, es ist vorab festgelegt: Wo liegen die größten Risiken für das Unternehmen? Welche Situationen werden als kritisch eingestuft? Und welche Informationen aus der IT-Infrastruktur müssen dafür gesammelt werden?

Vulnerability Management spürt Schatten-IT auf

Ziel des Vulnerability Management ist es, diejenigen Schwachstellen in der IT-Infrastruktur aufzudecken und zu schließen, die für das Unternehmen geschäftskritisch sind. Bei einer Überprüfung finden sich oft überraschende Schlupflöcher, mit denen die Verantwortlichen nicht gerechnet haben: Schlecht gepatchte Systeme, falsch installierte, konfigurierte oder schlecht programmierte Software; oder auch Systeme, die eigentlich nicht installiert sein dürften. Aufgabe eines SOC muss es sein, kritische Schwachstellen entweder ganz zu eliminieren oder zumindest zu entschärfen.

Im Verbund mit dem Vulnerabiliy Management spielt SIEM schließlich seine Vorteile aus: Die identifizierten Schwachstellen lassen sich im Hinblick auf ihre Kritikalität für das Business so beobachten und überwachen, dass das SOC ein Risikobild in Echtzeit zeichnen kann. Auf dieser Basis ist das SOC jederzeit handlungsfähig - und kann für das Business außerdem regelmäßig Reports über den Bedrohungszustand liefern.

Zusätzlich zu SIEM und dem Vulnerability Management kann ein SOC weitere Services erbringen: Diese beginnen bei klassischen CERT-Diensten, um auf vorhandene Bedrohungen möglichst schnell und effizient zu reagieren, und gehen über Forensik und Penetration-Tests bis hin zu Research-Services, welche die Bedrohungslage außerhalb des Unternehmens genau erfassen, und Awareness-Schulungen für die Mitarbeiter im Unternehmen.

SOC ist alles andere als Plug & Play

Dies alles zeigt: Ein SOC kann sich weder Tools bedienen, die einfach per Plug and Play einsatzfähig sind, noch lässt sich eine solche Organisation in einem Adhoc-Projekt aufsetzen. Unternehmen, die ein professionelles SOC betreiben wollen, müssen - je nach Voraussetzungen - mindestens ein Jahr Aufbauarbeit betreiben, bis Know-how, Prozesse und Tools den Anforderungen genau entsprechen. Und auch danach handelt es sich aufgrund der hohen Komplexität des Themas um einen fortlaufenden Optimierungsprozess, man befindet sich daher immer mehr oder weniger auf der "Road to SOC".

Der Autor: Markus Müssig ist Security Consultant bei HP Enterprise Security Services

---