IT-Sicherheit
Vorteile von Threat Hunting

[10.5.2019] Der Threat-Hunting-Ansatz geht davon aus, dass Bedrohungen in IT-Systemen gefunden werden können, indem sie proaktiv aufgespürt werden. Entscheidend sind Tools, welche die gesamte Behörde im Blick haben.

In der heutigen Cyber-Welt ist es gefährlich anzunehmen, dass Behörden nur die richtigen Tools installieren müssten, um Angriffe auf ihre Systeme zu verhindern. Die Frage sollte eher lauten: Was tun, wenn Angreifer im Behördennetzwerk sind? Bundesbehörden haben es mit finanziell gut ausgestatteten Angreifern aus dem Ausland zu tun, die sich neuartiger Methoden und Technologien bedienen, denen die zu ihrer Abwehr eingesetzten Tools nur mit Mühe begegnen können. Diese Angriffe sind deutlich schwerer vorherzusagen, was die Fähigkeit einschränkt, den damit verbundenen Bedrohungen entgegenzuwirken.
An dieser Stelle kommt das Threat Hunting ins Spiel, eine Sicherheitsstrategie, in deren Mittelpunkt das proaktive Aufspüren von Bedrohungen steht und deren Grundlage die Kenntnisse der Organisation und das Wissen um deren Widersacher sind. Jede Threat-Hunting-Jagd beginnt mit einer Anomalie, auf die eine Hypothese folgt, die auf menschlicher Intelligenz beruht. Anschließend gilt es, auf Grundlage der vorhandenen Daten die richtigen Fragen zu stellen, um Beweise für die Theorie zu finden oder sie zu verwerfen.

Proaktiv suchen statt reaktiv alarmieren

Threat Hunting ist das Gegenteil von reaktivem Alarmieren. Natürlich sind Alarme sinnvoll, aber zuviele davon können dazu führen, das Sicherheitsteams Tag für Tag denselben Alarm sehen. Dies kann Frust verursachen, selbst wenn das Ereignis den Alarm rechtfertigt. Um von dieser Alarmkultur wegzukommen, ist ein profunder Einstellungswandel gefragt. Der Threat-Hunting-Ansatz geht davon aus, dass Bedrohungen in den Systemen existieren und dass man diese finden kann, indem man sie proaktiv aufspürt. Das setzt voraus, dass Behörden in der Lage sind, ihre IT-Logs, Firewalls, Datenbanken, Intranets und Clouds zu durchsuchen. Die Notwendigkeit, Daten in einer Vielzahl unterschiedlicher Formate, strukturiert und unstrukturiert, in all diesen Orten zu sieben, macht das Durchsuchen komplex. Moderne Such-Tools sind jedoch in der Lage, die unterschiedlichen Datentypen zu knacken, damit sie indexiert, analysiert und so aufbereitet werden können, dass sie die Einblicke liefern, welche die IT-Verantwortlichen in den

Behörden benötigen, um mit der Suche beginnen zu können. Dank ihres Wissens über die verwundbaren Stellen ihrer Behörde, die wahrscheinlichen Gegner und deren mögliche Absichten können IT- und Sicherheitsteams Daten aus jeder Ecke ihrer Infrastruktur abfragen, Hypothesen prüfen und ungewöhnliche Aktivitäten identifizieren – und das innerhalb von Sekunden.

Geschwindigkeit ist alles

Die Jagd auf Cyber-Bedrohungen wird erfolgreicher, je mehr Daten vorliegen. Nicht jede Hypothese fördert eine Bedrohung zutage. Die meisten erweisen sich sogar als falsch. Deshalb braucht es Tools, die Hypothesen schnell prüfen und gegebenenfalls auch schnell verwerfen, damit sofort die nächste Hypothese auf den Prüfstand gestellt werden kann. Diese Anforderung bedingt in der Regel eine Modernisierung der Systeme.
Enterprise-Search-Tools haben ihren Ursprung in den Zeiten der Mainframes, aber die Suchanforderungen von Behörden sind heute deutlich komplexer. Moderne verteilte Systeme benötigen Suchfunktionen, die in Echtzeit tief in riesige Datenmengen eintauchen können und in der Lage sind, Indizes kontinuierlich zu aktualisieren, während immer mehr Daten hinzukommen. Suchen müssen so schnell Einblicke ermöglichen, dass Behörden ohne Verzögerung missionskritische Entscheidungen treffen können.

Keine Jagd in Silos

Einige Bundesbehörden in den USA nutzen bereits Threat Hunting, allerdings häufig in Silos. IT- und Sicherheitsverantwortliche, die mit Firewalls, Erkennungsplattformen, Endpunkt-Agents und anderen Diensten zu tun haben, können Hypothesen nur innerhalb bestimmter Systeme prüfen. So gibt es beispielsweise Punktlösungen, mit denen sich hervorragend Endpunktdaten evaluieren lassen, aber nichts anderes. Das ist besser als ohne Threat Hunting zu agieren, für ein echtes Threat Hunting braucht es jedoch Tools, welche die gesamte Behörde im Blick haben – nur so können Anomalien entdeckt werden, die Grenzen und Silos durchbrechen.
Hinzu kommt, dass eine Beschränkung der Suche nach Bedrohungen auf Einzelsysteme den Weg für neue Angriffsvektoren freimachen könnte. Angreifer, welche die Untersuchungstaktiken einer Behörde auswerten, haben die Möglichkeit, ihre Strategien flexibel anzupassen und sich auf die Bereiche zu konzentrieren, die gerade nicht im Fokus stehen.

Stark in Gemeinschaft

Mittlerweile gibt es in der Sicherheits-Community eine Reihe von Zusammenschlüssen, deren Ziel es ist, Best Practices auszutauschen, sich vor neuen Bedrohungen zu warnen und gemeinsam an Lösungen zu arbeiten. Um ein umfassendes Bild der Cyber-Anforderungen und -Strategien zu erhalten, ist es sehr wichtig, dass in diesen Communities Experten von Regierung, Vertragsunternehmen und Herstellern von Sicherheitslösungen vertreten sind.
Der Mensch ist nicht nur das schwächste Glied in der Sicherheitsstrategie von Unternehmen und Behörden, sondern auch der wichtigste Faktor, wenn es um die Entwicklung und erfolgreiche Umsetzung einer Threat-Hunting-Strategie geht.

Kevin Keeney ist Cyber Security Advocate bei Elastic.

https://www.elastic.co

Stichwörter: Threat Hunting, IT-Sicherheit, IT Security, Cyber-Sicherheit

---

Quelle: www.move-online.de