Externe Bedrohungen aus dem Darknet erkennen und vorwegnehmen

Der für Schwachstellenmanagement bekannte Hersteller Rapid7 hat das Softwareunternehmen IntSights übernommen. Was es damit auf sich hat und wie Rapid7 in der Cybersecurity-Landschaft dasteht, schildert Luca Forcellini, Product Manager Rapid7 bei BOLL, im Interview.

Das Cybersecurity-Angebot präsentiert sich ausgesprochen heterogen und wird immer komplexer. Ginge es nicht auch einfacher?
Bei unseren Kunden und Partnern spüren wir vermehrt, dass sie lieber möglichst viele Aspekte der Cybersicherheit mit Lösungen aus einer Hand abdecken als für alle Themenbereiche unterschiedliche Tools einzusetzen. So sollte nicht bei jeder Neuerung oder Erweiterung der Security-Landschaft eine weitere Geschäftsbeziehung mit einem zusätzlichen Hersteller erforderlich und das Security-Team gezwungen sein, sich auf zusätzliche Technologien und Philosophien einzustellen. Diesen Trend haben viele Hersteller erkannt und gehen als Folge dessen daran, ihr Produktportfolio zu erweitern und zu konsolidieren.

Wie sieht es in dieser Hinsicht bei Rapid7 aus?
Rapid7 ist primär bekannt für die führende Rolle im Bereich Vulnerability Management. Doch der Hersteller offeriert mit Insight schon länger eine umfangreiche Cybersecurity-Plattform, die laufend ausgebaut wird und eine zentrale Sichtweise ermöglicht. Insight umfasst neben dem Schwachstellenmanagement für On-Premises- und Cloud-IT-Infrastrukturen auch Lösungen für die Überwachung und Schutz von Multi-Cloud-Umgebungen, Web-Applikationen und Kubernetes. Dazu kommen Detection and Response (XDR), SIEM und Automatisierung (SOAR). Alles in allem ein rundes Angebot, das für Kunden und Partner gleichermassen interessant ist.

Jetzt hat Rapid7 IntSights gekauft. Was zeichnet dessen Software aus?
Cybersecurity-Lösungen kümmern sich üblicherweise um das, was im Firmennetzwerk geschieht und was von aussen, zum Beispiel in Form von Phishingattacken und Malware, ins Unternehmen kommt. Die Lösung von IntSights überprüft, was im Namen des Unternehmens extern geschieht – wir reden von Missbrauch des Brands für Phishingkampagnen, von gefälschten Social-Media-Profilen, Websites und Onlineshops sowie von vertraulichen Informationen, die im Darknet zum Kauf angeboten werden. All dies kann einer Organisation massiven Schaden zufügen.

Luca Forcellini, Product Manager, BOLL

Und was bedeutet diese Übernahme für Rapid7?
Mit IntSights ergänzt Rapid7 sein Angebot mit External Threat Intelligence. Es ist ein weiterer Baustein für die bestehende Insight-Plattform, der den Kunden den Blick auf externe Cyberrisiken öffnet und es ermöglicht, das Clear-, Deep- und Darknet zu überwachen und passende Gegenmassnahmen zu ergreifen, bevor ein Schaden entsteht, beziehungsweise diesen zu unterbinden, bevor er zu gross wird.

Für wen eignet sich External Threat Intelligence?
Primär für international tätige Unternehmen oder Firmen mit starken Brands, die ihre Marke schützen wollen und eventuell bereits komplexe Attacken erlitten haben. Die Lösung ist also nicht nur aus Sicht der IT-Sicherheit interessant, sondern auch für andere Unternehmensbereiche wie etwa die Rechtsabteilung oder das Marketing. Auch im Namen von Behörden wird vermehrt Missbrauch betrieben – External Threat Intelligence ist für die öffentliche Hand ebenfalls relevant.

Welche weiteren Vorteile bietet die IntSights-Lösung?
Als reine Cloud-Lösung ist sie sehr rasch einsetzbar und nicht mit der Unternehmens-IT verbunden. Es werden keinerlei Unternehmensdaten abgegriffen. Denn External Threat Intelligence sammelt ausschliesslich Daten aus dem Internet, die dort ohnehin zu finden sind, und erstellt daraus eine Risikoanalyse. Davon profitieren insbesondere Branchen mit hohen Ansprüchen an die Vertraulichkeit – wie beispielsweise der Finanzsektor.

Erfolgt die Analyse der gefundenen Informationen automatisiert?
Zu einem gewissen Teil. Die Intelligenz der Software wird ergänzt durch das Know-how der Spezialisten von Rapid7. Denn nicht alle bedenklichen Vorkommnisse lassen sich automatisiert erkennen. In komplexeren Fällen braucht es menschliches Wissen, um die Situation zu bewältigen. Diese Erfolg bringende Kombination innovativer Software mit der Erfahrung von Experten ist ein generelles Merkmal der Gesamtlösung von Rapid7.

→ **www.boll.ch/rapid7**

BOLL
IT Security Distribution

BOLL Engineering AG
Jurastrasse 58
CH-5430 Wettingen

Telefon +41 56 437 60 60
info@boll.ch
www.boll.ch