

Bedrohungen aus dem Web, Deep Web und Darknet im Griff

Während viele Unternehmen ihr Augenmerk vermehrt auf die interne Cybersecurity legen, wissen sie oft wenig darüber, was im Namen der Firma im Internet geschieht. Threat Command von Rapid7 hilft, diese Lücke zu schliessen.

Schweizer Unternehmen mit starkem Brand sind bei der Cybersecurity auf einem hohen Stand, wenn es um die Abwehr von Bedrohungen geht, die auf das interne Netzwerk zielen. Was im Namen der Firma im Clear Web, Deep Web oder Darknet vor sich geht, ist jedoch oft nicht klar. Werden gefälschte Do-

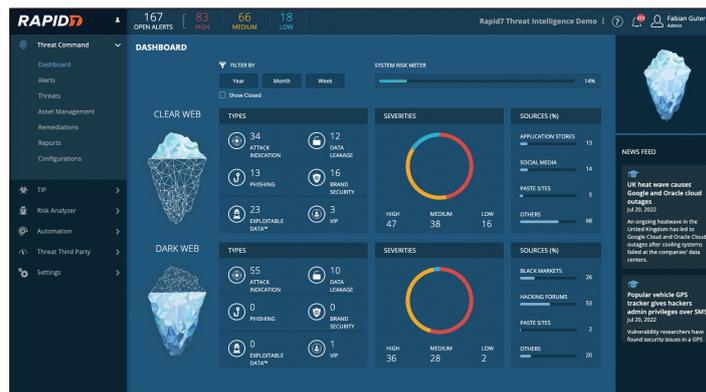
domains für Phishingkampagnen genutzt? Gibt es Fake-Social-Media-Profile, die den Ruf von Unternehmensvertretern zu nichte machen? Bieten Cyberkriminelle im Darknet geleakte Unternehmensdaten an? Solche unlauteren Aktivitäten können enormen Schaden anrichten.

External Threat Intelligence schützt Assets und Reputation

Die External-Threat-Intelligence-Lösung Threat Command von Rapid7 geht all diese Probleme an. Eine intuitiv nutzbare, cloudnative Plattform sammelt automatisiert unternehmensbezogene Informationen – auch aus den schwer zugänglichen Bereichen des Internets – und generiert eingehende Risikoanalysen. Mit einem Team von spezialisierten Analysten geht Rapid7 darüber hinaus den entscheidenden Schritt weiter: Die Experten recherchieren gezielt im Deep Web und im Darknet, decken strategisch relevante Bedrohungen auf und beseitigen, falls gewünscht, die entdeckten Bedrohungen auch gleich – von der Löschung einer Fake-Domain bis zum Kauf geleakter Daten, um sie für weitere Interessenten unzugänglich zu machen.

Einzigartige Komplettlösung

Die Kombination aus einer automatisierten Cloud-Plattform mit der Expertise spezialisierter Analysten macht Threat



Command für den Reputationsschutz einzigartig. Die Kunden erhalten nicht nur standardisierte Berichte, sondern auch massgeschneiderte, punktgenaue Reports und fachkundigen Support durch das Analytistenteam von Rapid7. Bei Anbietern, die ausschliesslich eine Softwareplattform offerieren, müssen die Kunden oder ihre Cybersecurity-Partner die Analyse und Problembeseitigung selbst übernehmen. Doch die dafür erforderlichen Spezialisten sind äusserst schwer zu finden. Das Beispiel einer Privatbank, die im Bereich Security lediglich über zwei Mitarbeitende verfügt, macht deutlich: Auch etablierte Unternehmen sind diesbezüglich auf Unterstützung angewiesen, die der bestehende IT-Partner aufgrund des Fachkräftemangels nicht liefern kann. Und Anbieter, die nur auf Experten setzen, können ihre Dienstleistung nur beschränkt skalieren.

Schnelle Resultate

Threat Command lässt sich, zum Beispiel als Proof of Concept, innert 48 Stunden einrichten und liefert auf Basis einer umfassenden External-Threat-Intelligence-Datenbank in kürzester Zeit erste Resultate. Der Kunde muss dazu nur eine Liste dessen bereitstellen, was untersucht werden soll – zum Beispiel Firmen- und Brandnamen, IP-Adressen oder Namen von Mitarbeitenden. Tiefgehende Ana-

lysen folgen innert ein bis zwei Wochen. Ein Unternehmen kann den Nutzen der Lösung somit rasch erkennen und entscheiden, ob Threat Command sich für seine Situation eignet oder nicht.

Sowohl für Kunden als auch für ihre Cybersecurity-Partner ist Threat Command attraktiv. Die Inbetriebnahme und Nutzung

der Plattform erfordert auf beiden Seiten keine technischen Ressourcen – dies entlastet die bestehenden Security-Teams. Und für die Channel-Partner bietet sie die Gelegenheit, neue Kunden zu akquirieren bzw. ihr Lösungs- und Dienstleistungsangebot abzurunden. Um die von Threat Command gelieferten Informationen in Erkenntnisse und Massnahmen zu überführen, ist jedoch Expertenwissen erforderlich – bei Threat Command inklusive!

Gefragte Lösung

Threat Command stösst in der Schweiz auf reges Interesse. Mehr als ein halbes Dutzend Banken nutzen die Lösung bereits. Am gefragtesten sind Angaben zu Phishingkampagnen im Namen des Unternehmens. Mit der Angabe eines Bereichs von Kreditkartennummern lässt sich zudem herausfinden, ob Kreditkartendaten geleakt sind. Interessant ist Threat Command aber nicht nur für das Finanzwesen, sondern auch für andere stark digitalisierte Branchen wie den Onlinehandel. Interesse zeigen auch Anwaltskanzleien.

Kontakt

BOLL Engineering AG

Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch,
www.boll.ch