Schwachstellenmanagement der nächsten Generation

Schwachstellen im Unternehmensnetzwerk müssen erkannt, kategorisiert und behoben werden. Die umfassende Insight-Plattform von Rapid7 stärkt das Vulnerability and Risk Management markant – heute und in Zukunft.

Moderne Unternehmensnetzwerke sind enormen Gefahren und Risiken ausgesetzt. Die Anzahl der Cyberattacken nimmt stetig zu und die Angriffsmethoden werden raffinierter. Zudem beschränkt sich das Netzwerk nicht mehr auf Server und Workstations. Vielmehr prägen virtuelle Infrastrukturen, Containertechnologien und Cloud-Services die IT-Landschaft.

Um den vielfältigen Gefahren zu begegnen, setzen grössere Unternehmen durchschnittlich 75 Sicherheitsprodukte ein. Diese generieren unendlich viele proprietäre Statusmeldungen, Alarme und Berichte – eine Datenflut, die kaum noch zu bewältigen ist. Hier setzen Vulnerability-Risk-Management-Lösungen (VRM) ein. Sie gewährleisten eine Übersicht über die vorhandenen Schwachstellen und Risiken. Doch manche Tools dieser Kategorie bieten kaum mehr als ellenlange Listen und statische Dashboards. Und sie kategorisieren die Schwachstellen ausschliesslich nach der relativ groben 10-stufigen CVSS-Schweregradskala.

Vulnerability Management durchgängig im Griff

Rapid7 geht mit InsightVM einen bedeutenden Schritt weiter. Die Lösung bietet eine umfassende Sichtbarkeit sämtlicher Schwachstellen über das gesamte Unternehmensnetzwerk hinweg – vom einzelnen PC über die Server im Datacenter bis zu den genutzten Cloud-Diensten wie Microsoft Azure oder Amazon Web Services. Auch Schwachstellen in virtualisierten Infrastrukturen (VMware) und Container-Repositories (Docker) werden erfasst. Dazu sammelt InsightVM kontinuierlich sämtliche sicherheitsrelevanten Daten mithilfe des schlanken «Insight Agent», der auf den Servern, Endpunkten und weiteren Systemen installiert wird: Statt einzelne «Silos» zu überwachen, liefert InsightVM laufend aktualisierte, unternehmensweit umfassende Sicherheitsinformationen.

Anders als vergleichbare VRM-Produkte analysiert und priorisiert InsightVM die Schwachstellen fein granuliert in Stufen von 1 bis 1000. Rapid7 nennt dies «Real Risk Score» und berücksichtigt dabei nicht nur wie der CVSS-Score das unveränderliche Basisrisiko einer Schwachstelle, sondern auch deren Alter, die aktuelle Existenz von Exploit-Kits und Malware sowie den konkreten Einfluss auf das Unternehmen. So kann eine ältere, eigentlich weniger bedeutende Schwachstelle einen höheren Score aufweisen, weil bereits Malware zu deren Ausnutzung existiert. Und eine Schwachstelle auf Server X kann für den Geschäftsgang ein wesentlich höheres Risiko darstellen als die gleiche Schwachstelle auf Server Y.

Schwachstellen erkennen und adäquat handeln

InsightVM greift für die unternehmensspezifische Priorisierung der Schwachstellen auf die jahrelange Erfahrung von Rapid7 mit den Methoden und dem Mindset der Hacker zurück: Die VRM-Lösung erkennt und beurteilt die Schwachpunkte im Netz aus der Sicht eines Angreifers und liefert den Sicherheitsteams präzise Erkenntnisse, die sich unmittelbar umsetzen lassen.

Sind die dringendsten Schwachstellen ans Licht gebracht, geht es darum, die geeigneten Massnahmen zu deren Behebung zu planen und den zuständigen Spezialisten zuzuteilen. InsightVM arbeitet dazu mit IT-Ticketing-Plattformen wie Atlassian Jira und ServiceNow, mit Patch-Management-Lösungen sowie mit der eigenen Security-Orchestration-and-Automation-Lösung InsightConnect zusammen. So entsteht im Sinn von SecOps eine solide, einheitliche Grundlage für alle involvierten Personen – vom Sysadmin über die IT-Sicherheitsteams bis zum CISO und CIO – um die Schwachstellen bedarfsgerecht zu beheben und das Gesamtrisiko zu minimieren.

Übersicht für alle Beteiligten

InsightVM sammelt laufend Vulnerability-Daten und ist damit in der Lage, ständig aktualisierte Resultate in Echtzeit auf interaktiven «Liveboards» zu präsentieren. Diese dynamischen Dashboards lassen sich mithilfe einer einfachen Abfragesprache unkompliziert individuell für einzelne Mitarbeitende und Team-Funktionen konfigurieren.

Attacken zuverlässig identifizieren

Das Angebot von Rapid7 geht weit über die VRM-Lösung InsightVM hinaus: Rapid7 offeriert eine umfassende, cloudbasierte Plattform, die alle Aspekte des Vulnerability Management abdeckt – Sichtbarkeit, Analyse und Automation.

Eine wichtige Komponente der Insight-Plattform ist die Incident-Detection-and-Response-Lösung InsightIDR, die InsightVM optimal ergänzt. InsightIDR kombiniert Funktionen von SIEM (Security Information and Event Management), UBA (User Behavior Analytics) und EDR (Endpoint Detection and Response) und ermöglicht eine verhaltensbasierte, durch Machine Learning unterstützte Analyse, die auch bisher unbekannte Attacken zuverlässig identifiziert.

InsightIDR sucht nach auffälligem User-Verhalten. Dazu gehört der sehr häufige Missbrauch von User-Logins – verdächtig ist etwa, wenn sich der gleiche Nutzer innert Sekunden von weit voneinander entfernten Orten anmeldet oder wenn in kurzer Zeit zahlreiche Login-Versuche erfolgen. InsightIDR erkennt zudem Angriffe, die sich über verschiedene Systeme hinwegbewegen und stellt den Angreifern Fallen in Form von «Lockvögeln» wie Honeypots, Honey Credentials oder Honey Users – so werden potenzielle Angreifer sofort erkannt, wenn sie das Unternehmensnetz auskundschaften – also noch bevor sie zum eigentlichen Angriff übergehen können.

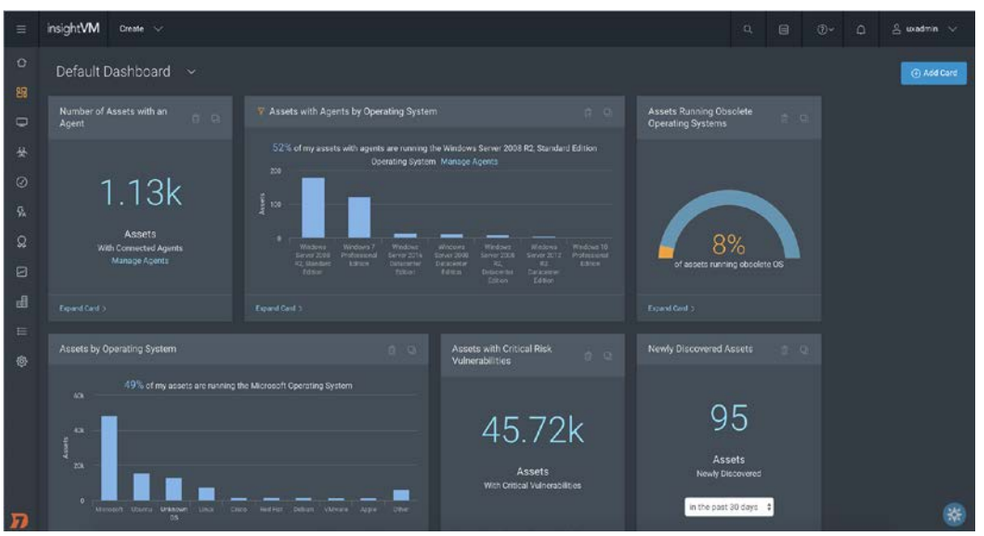
Wie InsightVM bietet auch InsightIDR Dashboards mit priorisierten Erkenntnissen und detaillierten Informationen. So lassen sich zum Beispiel verdächtige Prozesse anzeigen, die nur auf einem einzigen System laufen.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch



Die umfassende Insight-Plattform von Rapid7 stärkt das «Vulnerability and Risk Management» nachhaltig (links). Anschaulich präsentierte Echtzeitinformationen schaffen eine solide Entscheidungsgrundlage für den Umgang mit Schwachstellen (rechts).

Leader in der «Forrester Vulnerability and Risk Management Wave 2018»

Rapid7, gegründet im Jahr 2000 in Boston, Massachusetts, beschäftigt heute über 1400 Mitarbeitende. Es bietet eine umfassende Plattform zur Erkennung, Priorisierung und Behebung von Schwachstellen und unbekannten Attacken. Das Unternehmen ist dafür bestens aufgestellt: Das Research-Team mit mehr als 200 Spezialisten ist seit 2016 Mitglied der CVE Numbering Authority, die für den CVSS-Score verantwortlich zeichnet.

Als Eigner des Penetration-Testing-Tools Metasploit kann Rapid7 zudem auf die Erkenntnisse einer weltweiten Community von 200 000 «White Hats» zurückgreifen. Darüber hinaus führt das Unternehmen eigene Penetration-Tests durch, unterhält 300 Honeypots bei den grössten Cloud-Anbietern und ist Mitglied der anbieterübergreifenden Cyber Threat Alliance.

Mit diesem soliden Hintergrund ist Rapid7 in der Lage, Angreifer und ihre Methoden bis ins Detail zu verstehen. Kein Wunder, dass Rapid7 in der «Forrester Vulnerability and Risk Management Wave» von 2018 als Leader qualifiziert wird. Rapid7 zählt weltweit über 7000 Organisationen zu seinen Kunden, darunter mehrere namhafte Unternehmen aus der Schweiz.

InsightVM: die Highlights

- Umfassende Sichtbarkeit aller Schwachstellen
- Kontinuierliches, agentenbasiertes Monitoring
- Interaktive Live-Dashboards, laufend aktualisierte Echtzeitinformationen
- Fein granulierte Schwachstellenbewertung
- Berücksichtigt auch virtualisierte Infrastrukturen, Container-Repositories und Cloud-Services

InsightIDR: die Highlights

- Ermittelt Eindringlinge zuverlässig
- Erkennt Missbrauch von Anmeldedaten, verdächtige Prozesse und Log-Manipulationen
- Präsentiert Informationen zu Assets, Usern und deren Verhalten in einheitlicher Sicht
- Arbeitet mit Behavior Analytics und Machine Learning
- Lockt Angreifer mit Fallen an (Honeypots, Honey Users etc.)
- Vereint Funktionen von SIEM, UBA und EDR