



# Lücken und Risiken im Griff

## Umfassende Transparenz mit Vulnerability Risk Management für Netzwerk und Web-Apps

Rapid7 befasst sich mit der Erkennung, Priorisierung und Behebung von Schwachstellen und Cyberattacken. Das Unternehmen mit Hauptsitz in Boston beschäftigt über 1400 Mitarbeitende, darunter 200 Sicherheitsforschende, und kann als Eigner des Penetration-Test-Tools Metasploit auf die Erkenntnisse einer weltweiten Community von 200 000 «White Hat»-Hackern zurückgreifen.

Unternehmen sind vermehrt Gefahren und Risiken durch Cyberattacken ausgesetzt. Zudem beschränkt sich das Netzwerk nicht mehr auf Server und Workstations. Vielmehr prägen virtuelle Infrastrukturen, Containertechnologien, Web-Applikationen und Cloud Services die IT-Landschaft. Die umfassende Insight-Plattform vereint das Wissen und die Technologie von Rapid7, um Unternehmen vor bekannten wie auch neuen Cyberattacken erfolgreich zu schützen. Das Wissen basiert auf der Schwachstellenforschung von Nexpose, den Exploit-Daten von Metasploit, dem weltweiten Angreiferverhalten, internetweiten Scan-Daten und Bedrohungsanalysen und liefert über anschauliche Dashboards direkt umsetzbare, priorisierte Erkenntnisse zur Sicherheitslage im Unternehmen. Mit InsightVM und InsightAppSec bietet Rapid7 Vulnerability-Risk-Management-Lösungen an, um eine umfassende Transparenz im Unternehmensnetzwerk und bei Web-Applikationen zu erhalten. Denn nur wenn man die eigenen Schwachstellen kennt, kann man gezielt Massnahmen definieren, die schliesslich die Angriffsfläche und somit das Risiko verringern.

Mehr Informationen über  
die Rapid7-Produkte



## InsightVM/InsightAppSec: Next Generation Vulnerability Management

### Neue Dimension für das Schwachstellenmanagement

Mit InsightVM ermöglicht Rapid7 in Echtzeit umfassende Sichtbarkeit aller Schwachstellen im gesamten Unternehmensnetzwerk inklusive virtualisierter Infrastrukturen, Container-Repositoryn und Cloud-Diensten. Die Lösung priorisiert die Sicherheitsprobleme mit dem sogenannten «Real Risk Score» in Stufen von 1 bis 1000 – im Gegensatz zum branchenüblichen CVSS Score mit einer Einteilung von 0 bis 10. Darüber hinaus berücksichtigt InsightVM neben dem unveränderlichen Grundrisiko einer Schwachstelle auch deren Alter, das Vorhandensein von Exploit Kits sowie den konkreten Einfluss auf das individuelle Unternehmen und ermöglicht so eine realistische Einschätzung der Tragweite des Problems.

### Rapid7 Insight VM: die Highlights

- Priorisierung der Scan-Ergebnisse (Real Risk Score)
- Analyse von Containern sowie virtueller und Cloud-Infrastruktur
- Festlegung von Remediation-Projekten
- Automation-Integration in Service Now, Jira und weitere Drittanbieter
- Offene RESTful-API
- Erhältlich als Cloud Service

### InsightConnect/SOAR

Unternehmen müssen erkannte Lücken in ihrer IT-Landschaft rasch beseitigen und Angriffe abwehren. Zunehmend fehlen jedoch IT-Professionals, die solche Aufgaben wahrnehmen können. Aus diesem Grund ist SOAR (Security Orchestration, Automation and Remediation) ein aktuelles Thema. Mit InsightConnect von Rapid7 können InsightVM und InsightAppSec automatisch Prozesse in anderen Security Tools anstossen, um die erkannten Lücken rasch und mit wenig manuellem Aufwand zu schliessen.

### Umfassende Sicherheit für Web-Applikationen

Web-Applikationen gehören zu den Schlüsselanwendungen für die Interaktion zwischen Unternehmen, Kunden und Mitarbeitenden. Viele Web-Applikationen sind von aussen erreichbar und somit für Cyberattacken exponiert. Mit InsightAppSec können Unternehmen ihre Web-Apps bereits während deren Entwicklung sowie in der produktiven Umgebung laufend auf Sicherheitslücken überprüfen. Ein übersichtliches Reporting zeigt auf, welche Lücken welche Risiken aufweisen und wie diese geschlossen werden können, um so die Prioritäten für deren Beseitigung richtig definieren zu können. Um bestehende wie auch künftige Frameworks und Technologien für Web-Applikationen auf deren Lücken zu prüfen, setzt Rapid7 auf den Universal Translator.

### Rapid7 InsightAppSec: die Highlights

- Dynamic Application Security Testing (DAST)
- Universal Translator
- Unterstützt einfache und komplexe Authentifizierungsmethoden
- Über 95 Arten von simulierten Angriffen
- Aufzeichnung und Abspielen von Angriffen
- Erhältlich als Cloud Service

