

Rapid7 ermöglicht Avira ein skalierbares Schwachstellen-Management über jegliche Assets – auch auf Cloud-Plattformen

Avira	Herausforderung	Ergebnis
Branche: Software	Handarbeit im Schwachstellen-Management ablösen	Verbesserte Sicherheit des Unternehmens durch effizientes Schwachstellen-Management
Größe: 500+ Mitarbeiter	Scans über verschiedene Distributionen und Cloud-basierte Dienste	Zuverlässige Absicherung von Cloud-Diensten
Produkte: InsightVM	Integration mit internen Aufgabenmanagement-Tools	Reports und nahtlose Transparenz über Abteilungen hinweg

Als Pionier des Freemium-Geschäftsmodells bietet Avira qualitativ hochwertige, selbst entwickelte Sicherheitssoftware, wie beispielsweise Avira Antivirus und den Password Manager, sowohl für den professionellen als auch für den privaten Einsatz an. 1986 gegründet, zählt das multinationale Unternehmen heute mit rund 100 Millionen Kunden und 500 Mitarbeitern zu den weltweit führenden Anbietern in diesem Segment.

Das Thema ‚Sicherheit‘ spielt für Avira eine sehr wichtige Rolle, zumal man sich in einem hochsensiblen Bereich bewegt. Dazu erklärt uns Herr Marian Alexander Schneider, Teamleiter des Information Security Teams bei Avira Operations GmbH & Co. KG: „Wir selbst haben es uns zur Aufgabe gemacht Millionen von Kunden zu schützen, was im Umkehrschluss bedeutet, dass wir uns selbst auch absichern müssen, um für unsere Kunden den bestmöglichen Mehrwert zu erzielen. Außerdem leben wir in einer Zeit, in der täglich Hacker-Angriffe passieren, weshalb wir darauf achten müssen, dass unser Geschäftswert gut geschützt ist.“

Seit der Übernahme des noch jungen Teams, welches sich bei Avira um die Themen Application Security, Infrastructure Security sowie Gouvernance und Compliance kümmert, legt Marian Schneider und sein Team ein besonderes Augenmerk auf das Schwachstellen-Management. „Vulnerability Management in Firmen muss eines der Kernpunkte in der Security-Strategie sein. Wer heutzutage eine Security Strategie entwickelt und das Schwachstellen-Management außen vorlässt, egal, ob auf Applikationsebene oder in der Infrastruktur, der hat einfach einen sehr großen Blind Spot, den man nicht vernachlässigen darf“, so Schneider.

Top User-Experience: Einsatzfähig in nur vier Stunden

Bis dato hatte man viel manuellen Aufwand ins Schwachstellen-Management reingesteckt. Diesen galt es abzulösen und gleichzeitig einen neuen Qualitätsstandard, mit einer sich noch skalierbaren, zuverlässigeren Lösung, zu setzen.

Innerhalb von zwei Wochen seit der ersten Kontaktaufnahme lief bei Avira bereits der Rapid7 Proof-of-Concept. Zudem hat die gute User-Experience mit InsightVM das Team bei Avira begeistert, wie uns Herr Schneider bestätigt: „Von der Bereitstellung der Lizenz und der Infrastruktur bei uns im Rechenzentrum bis zum ersten Scan haben wir knapp vier Stunden gebraucht. Und nach insgesamt neun Stunden hatten wir bereits die ersten Patches eingespielt.“

Immens an Übersicht gewonnen

Die Komplexität der IT-Umgebung bei Avira ist beachtlich. Von über 2.500 lizenzierten Assets erwartet man nach Durchführung aller Scans am Ende auf 3.500 bis 4.500 Assets zu kommen – wohlgemerkt nur auf der Server-Infrastruktur. Dabei handelt es sich um verschiedenste Distributionen, von Solaris 9 bis Ubuntu 18.04. Die Assets sind verteilt auf Rechenzentren in mehreren Standorten und zwei Cloud-Anbietern, Azure und Amazon.

„Uns war von vornherein wichtig, dass die richtigen Informationen zu den entsprechenden Personen in einem vollständig automatisierten Prozess und in angemessener Zeit gelangen“, so Marian Schneider. Mit InsightVM funktioniert die Kommunikation mit allen relevanten Abteilungen nahtlos und stellt die notwendige Transparenz sicher, von der IT Abteilung bis hin zum C-Level Management.

Zum einen geben die in der Lösung enthaltenen Dashboards einen Überblick über alles Wichtige. „Einigen Mitgliedern des C-Level Management sind die Dashboards sehr wichtig, um den aktuellen Status der Systemsicherheit auf einen Blick einzusehen, aber auch in der IT-Abteilung hat sich jeder schon ein eigenes gebaut. Ich selber habe mittlerweile einen Bildschirm, der nur noch ein Dashboard zeigt, damit ich jederzeit den Überblick behalte,“ erzählt uns Herr Schneider.

Zum anderen funktioniert auch die Integration mit internen Aufgabenmanagement-Tools einwandfrei und ermöglicht es den Security- und IT-Teams schnell und unkompliziert zusammenzuarbeiten. Das Potenzial von InsightVM sieht Herr Schneider noch nicht ausgereizt. Für die nahe Zukunft ist die Einführung von Automatisierungs- und Remediation-Features geplant.

„Eines der Hauptargumente für InsightVM ist in unseren Augen die sehr gute Skalierbarkeit, die uns zu einer enormen Flexibilität im Scanverhalten verhilft. Mit dem Tool kann man die Sicherheit im Unternehmen stark erhöhen. Und es vereinfacht das Leben des Security Teams massiv.“

Schutz für Assets und Anwendungen auf Cloud-Plattformen

Avira nutzt die Möglichkeiten moderner Cloud-Modelle wie Microsoft Azure und Amazon AWS, und wurde 2018 sogar zum Amazon Innovation Partner gekürt. Avira schätzt das Preis-Leistungsverhältnis sowie die hohe Verfügbarkeit und Skalierbarkeit, die Cloud-Dienste gewährleisten.

Doch mit dem Einsatz cloudbasierter Dienste entstehen neue Herausforderungen: man kann schnell den Überblick verlieren oder Konfigurationsfehler begehen. Als AWS Advanced Technology Partner ermöglicht Rapid7 mit InsightVM sowohl die Cloud-basierten Assets auf Schwachstellen als auch deren Konfigurationen in der AWS-Umgebung zu überprüfen.

Da Avira teilweise auch kritische Daten auf S3 Buckets zwischenspeichern muss, ist es für das Sicherheitsteam essentiell zu wissen, ob die Buckets verschlüsselt, von außen erreichbar oder ob sie nach den Vorgaben Aviras geschützt sind. Dies nachzuhalten ist dank InsightVM um ein Vielfaches einfacher geworden. Ein weiteres Ergebnis von InsightVM in der Cloud ist die Tatsache, dass das Bewusstsein bei den Entwicklern für das Thema Compliance geschärft werden konnte.

Bei Avira war man positiv überrascht: „Wir hatten zunächst mit einem riesigen technischen Aufwand gerechnet, und dann war die Cloud-Synchronisation innerhalb von fünf Minuten angestellt und die Amazon-Konten synchronisiert“, so Herr Schneider.

„Einfaches, hochskalierbares und hochwirksames Produkt,“ resümiert Marian Schneider

Ringsum konnte InsightVM das Team und die internen Stake-Holder bei Avira überzeugen. Marian Schneider hält fest: „Eines der Hauptargumente für InsightVM ist in unseren Augen die sehr gute Skalierbarkeit, die uns zu einer enormen Flexibilität im Scanverhalten verhilft. Mit dem Tool kann man die Sicherheit im Unternehmen stark erhöhen. Und es vereinfacht das Leben des Security Teams massiv.“

Erfahren Sie mehr über die Insight-Plattform von Rapid7 und probieren Sie die Lösungen kostenlos aus:

Besuchen Sie uns auf: www.rapid7.com/try