OPSWAT.

IT Sector Case Study

Critical Infrastructure Protection

ROHDE&SCHWARZ

Viele Scanner schützen besser: Rohde & Schwarz setzt auf den Anti-Malware Multiscanner MetaDefender™ Core von OPSWAT™

Beim Code Signing und in der IT-Forensik legt der international aufgestellte Technologiekonzern höchste Maßstäbe an.

Weltweit führend: Mit rund 12.000 Mitarbeitern in mehr als 70 Ländern ist Rohde & Schwarz ein international aufgestellter, erfolgreicher Technologiekonzern. Das bereits in den 1930er Jahren gegründete Unternehmen beliefert mit Produkten aus den Geschäftsfeldern Messtechnik, Broadcast- & Medientechnik, Aerospace/ Verteidigung/Sicherheit sowie Netzwerke und Cybersicherheit Kunden aus der Industrie und dem hoheitlichen Sektor. Inzwischen hat sich Rohde & Schwarz mit Hauptsitz in München gleichzeitig auch zu einem der wichtigsten deutschen Anbieter von IT-Sicherheitsprodukten entwickelt.

Bei Softwareprodukten steht die Reputation des Unternehmens auf dem Spiel

Dieser Anspruch und die über Jahrzehnte gewachsene Reputation verpflichten den Konzern dazu, in allen Bereichen auf die Einhaltung höchster Qualitäts- und Sicherheits-Standards zu achten. Ein Beispiel dafür ist das Code Signing bei Software: Von Rohde & Schwarz erstellte Lösungen durchlaufen vor der unter Umständen weltweiten Freigabe für interne und externe Kunden nicht nur umfangreiche Prüfungen, sondern werden auch digital signiert. So wird unter anderem belegt, dass das jeweilige Softwareprodukt auch tatsächlich von Rohde & Schwarz stammt.

2021.01.07 CS-NA (RSZ)

ProSoft
MANAGE | SECURE | OPTIMISE IT

Da der derart signierte Code selbstverständlich frei von jeglichen Viren oder sonstiger Malware sein muss, durchlaufen Installationspakete oder ausführbare Dateien vor der Verteilung grundsätzlich entsprechende Scan-Prozesse. Hier sah der Technologiekonzern allerdings klaren Optimierungsbedarf, wie Alexander Gehrig, Information-Security Operations bei der Rohde & Schwarz GmbH & Co. KG, berichtet.

„Es gab früher zwei größere Probleme. Zum einen kam für die Prüfung der Dateien in der Entwicklung in der Regel nur der im Haus ohnehin eingesetzte Standard-Scanner zum Einsatz. Man war On-Premises also von den Ergebnissen einer einzigen Lösung abhängig und es ließ sich dadurch nicht gänzlich ausschließen, dass hier im Einzelfall doch einmal Malware durchrutscht und signiert wird. Zum anderen hatte es sich parallel dazu eingebürgert, Dateien über kostenfreie, öffentliche Anti-Virus-Online-Plattformen prüfen zu lassen. Vielen Anwendern war hier allerdings schlicht und ergreifend nicht bewusst, dass durch ein Hochladen bei solchen Diensten unter Umständen vertrauliche Daten für Dritte verfügbar werden – mit allen damit verbundenen Konsequenzen."

Zielsetzung: Ein On-Premises betriebener Anti-Malware Multiscanner

Eine Ausgangslage, durch die bei Rohde & Schwarz der Wunsch nach einer komplett On-Premises betriebenen Multi-Scanning-Lösung aufkam. Damit sollte die Vertrauenswürdigkeit der Rohde & Schwarz Produkte noch weiter gesteigert und gleichzeitig das Hochladen von Daten auf externe Plattformen aus Sicherheitsgründen deutlich eingeschränkt werden.

Bei einer Sichtung am Markt erhältlicher Optionen zog der weltweit agierende Technologiekonzern auch Open-Source-Lösungen in Betracht. Aufgrund des fehlenden Supports und der teilweise ungenügenden Reife der Produkte in diesem Segment wurde das jedoch ebenso verworfen wie eine Eigenentwicklung, da sich intern ein klarer Fokus auf Konsolidierung und Standardisierung abzeichnete.

Auf der weiteren Suche stieß Rohde & Schwarz auch auf MetaDefender Core von OPWSAT. Die ehemals unter dem Namen Metascan bekannte Lösung ist konsequent als Anti-Malware Multiscanner ausgelegt. Mehr als 30 Anti-Malware Engines lassen sich dabei innerhalb eines übergreifenden Produkts betreiben. Die Verwaltung erfolgt über eine einheitliche, zentrale Oberfläche, was den Aufwand sowohl für die Administration als auch die Pflege von Software-Lizenzen drastisch reduziert. Denn die einzelnen Virenscanner müssen nicht separat und jeder für sich lizenziert werden, sondern sind bereits im Komplettpreis von MetaDefender Core enthalten. Durch ein optimiertes Zusammenspiel der jeweiligen Schutztechnologien und Heuristiken der unterschiedlichen Hersteller werden höchste Erkennungsraten gewährleistet. Dies liegt unter anderem auch daran, dass Tools zur Malware-Erkennung aus unterschiedlichen internationalen Regionen zum Einsatz kommen, etwa US-amerikanische ebenso wie europäische. Auf diese Weise können auch zunächst regional auftretende, neue Bedrohungen schnellstmöglich erkannt werden.

MetaDefender Core von OPSWAT überzeugte in der Evaluierung

Rohde & Schwarz prüfte MetaDefender Core zunächst in einer Evaluierungsphase über mehrere Monate auf Herz und Nieren. Nachdem sich der positive Eindruck nachhaltig bestätigte, fiel 2016 die Entscheidung, den Anti-Malware Multiscanner über den deutschen OPSWAT-Partner ProSoft zu implementieren.

Die komplett inhouse betriebene Lösung wird nun beispielsweise genutzt, um Installationsfiles oder ausführbare Dateien im Rahmen des Code Signings zu scannen. Die Anbindung war durch diverse, von OPSWAT mitgelieferte Schnittstellen sehr einfach. Hier steht bei Rohde & Schwarz letztlich auf operativer Seite eine Schnittstelle zur Verfügung, über die Benutzer zugreifen können. Ob es sich bei der Lösung, von der eine zu prüfende Datei eingereicht wird, um ein Standardprodukt handelt oder um eine spezielle Eigenentwicklung von Rohde & Schwarz, spielt für den Betrieb von MetaDefender Core dabei keine Rolle.

Verschiebung von Cloud zu On-Premises

Die Nutzung von Online-Scan-Plattformen wurde im Zuge der Einführung des Anti-Malware Multiscanners gleichzeitig deutlich eingeschränkt. Hierbei kam Rohde & Schwarz auch zugute, dass das Thema Informationsklassifizierung innerhalb des Konzerns schon länger eine wichtige Rolle spielt. Dabei wurde beispielsweise die notwendige Awareness dafür aufgebaut, welche Schutzmechanismen für welche Arten von Informationen erforderlich sind oder welchen Verteilerkreisen diese zugänglich gemacht werden dürfen. Online-Scanner werden nun nur noch von Experten aus der IT-Security genutzt, die um mögliche Risiken wissen. Hochgeladen werden darüber hinaus ausschließlich Daten, die ohnehin als öffentlich gekennzeichnet sind und somit keiner besonderen Vertraulichkeit unterliegen.

Handling von False Positives als weiterer Mehrwert

Ein wichtiger Punkt beim Einsatz des Anti-Malware Multiscanners ist für Rohde & Schwarz der Umgang mit False Positives. Da der Einsatz mehrerer Scanner die Trefferquote erhöht, führt dies naturgemäß immer wieder zu fälschlicherweise positiven Ergebnissen, also dem Erkennen vermeintlicher Malware. Ist die Erkennung tatsächlich fehlerhaft, kann bereits vor der Auslieferung einer Software proaktiv der Kontakt mit den jeweiligen Anti-Virus-Herstellern aufgenommen werden, um rechtzeitig bis zum geplanten Release entsprechende Korrekturen anzustoßen.

Mittlerweile nutzt Rohde & Schwarz MetaDefender Core in einer deutlich größeren Ausbaustufe mit zusätzlichen variablen Scannern. Als sehr positiv hat sich im Nachgang die Tatsache herausgestellt, dass der Multiscanner von OPSWAT auch in die vorhandene Forensik-Lösung integriert werden konnte.

„Wir nutzen dies zum Beispiel, um Vor- und Zwischenvalidierungen von Dateien durchzuführen. MetaDefender Core fungiert hier als Teil der Gesamt-Forensiklösung. Sehr positiv ist uns dabei die Zusammenarbeit der beiden Hersteller aufgefallen, die beide sehr daran interessiert waren, eine unseren Anforderungen entsprechende Lösung zu realisieren.“ sagt Alexander Gehrig.

Ebenfalls positiv fällt auch das Gesamtfazit aus, das die IT-Verantwortlichen von Rohde & Schwarz aufgrund ihrer bisherigen Erfahrung mit MetaDefender Core ziehen. *„Der geringe Wartungsaufwand und der stabile Betrieb sind klare Vorteile für uns“*, resümiert Gehrig. *„Neben der deutlich erhöhten Sicherheit beim Code Signing ist es uns zudem gelungen, die Nutzer von einer tendenziell unsicheren, öffentlichen Portallösung zu einem On-Premises-System zu bewegen, über das wir die volle Kontrolle haben. Das ist in der Gesamtschau wohl einer der wichtigsten Vorteile im Vergleich zur früheren Vorgehensweise.“*

Mehr Informationen zu OPSWAT-Lösungen finden Sie beim deutschen Partner ProSoft GmbH.

ProSoft
MANAGE | SECURE | OPTIMISE IT

2021.01.07 CS-NA [RSZ]