Greenbone Security Manager: Aktualität und Qualität durch Open Innovation

Für Stefan Schwarz, Leiter des Rechenzentrums der Universität der Bundeswehr München liegt der Fall ganz klar: Freie Software und kommerzielle Appliance-Lösungen haben beide ihre Daseinsberechtigung. Entscheidend sind die jeweiligen Rahmenbedingungen und Anforderungen. Das gilt für ihn auch beim Einsatz von Vulnerability Management Lösungen, also der Analyse von Schwachstellen im Unternehmensnetz. Er setzt für diese Aufgabe den Security Manager GSM 500 von Greenbone ein – nicht zuletzt weil das Unternehmen auch die Entwicklung einer Open Source Variante unterstützt.

der Bundeswehr Universität München

Der Kunde:
Universität der Bundeswehr München

3.000 Studierende erhalten hier das nötige Wissen in verschiedenen Disziplinen von Bauingenieurswesen bis zu Psychologie und Pädagogik. Grundlagenforschung, anwendungsbezogene Forschungs- und Entwicklungsvorhaben erfolgen auf internationaler Ebene und in Kooperation mit wissenschaftlichen Einrichtungen, öffentlichen Institutionen und der Wirtschaft.

Die im Jahr 1973 gegründete Universität der Bundeswehr München dient der wissenschaftlichen Ausbildung von Offizieren und Offiziersanwärtern. Aber auch zivile Studenten findet man hier zunehmend. Denn der Campus-Charakter der Universität mit kurzen Wegen und individueller Betreuung macht ein konzentriertes und schnelles Studium möglich. Die Universität betreibt ein weitverzweigtes Datennetzwerk und eine Vielzahl von Systemen, die nicht nur performant, sondern vor allem auch sicher arbeiten müssen.

„Durch OpenVAS bin ich erst auf den GSM 500 gestoßen. Ich finde es absolut bemerkenswert, dass Greenbone die Entwicklung der freien Software unterstützt und sich aktiv in der Community einbringt."

Stefan Schwarz ist als Leiter des Rechenzentrums verantwortlich für ein Heer von Clients und Servern, verteilt auf eine Vielzahl von Netzen und Subnetzen - und damit vor allem auch für deren Sicherheit.

Die größte Herausforderung dabei: Die wachsende Dynamik durch virtuelle Systeme oder wechselnde Zuständigkeiten in der Betreuung der IT aber auch aufgrund der universitären IT-Souveränität der Anwender in etwa durch die Nutzung von Social Media und Web 2.0-Diensten. „Auch wenn alle Sicherheitsmaßnahmen greifen, passiert es doch immer wieder, dass jemand vergisst, seine Joomla Content Management Software zu aktualisieren oder bei der Erstellung einer Webseite mit Typo3 ein Passwort einzurichten", weiß Stefan Schwarz.

Alltagsfehler automatisch erkennen
Diese scheinbar kleinen, dafür aber potentiell umso gefährlicheren Flüchtigkeitsfehler manuell zu finden, würde ihn und sein Team täglich etwa drei Stunden Zeit kosten - ein teures und ineffizientes Unterfangen. Mit dem Greenbone Security Manager 500 kann der Rechenzentrumsleiter diese Aufgabe automatisieren und seine Systeme in bestimmten und frei definierbaren Zeitabständen nach Sicherheitsschwachstellen scannen. Bei einem Scan großer Systemlandschaften wäre die Analyse des gesamten Scans noch viel zeitraubender. „Mir kommt es darauf an, Veränderungen und Unterschiede zu erkennen. Sie zeigen mir, wo Gefahr drohen könnte. Das Wertvolle an der Greenbone-Lösung ist die Zuverlässigkeit, Regelmäßigkeit und damit die Vergleichbarkeit der Scans", erläutert Schwarz.

Zweigleisig
Neben dem Greenbone Security Manager nutzt der IT-Leiter auch die Open Source Software OpenVAS. „Durch OpenVAS bin ich erst auf den Greenbone Security Manager gestoßen", berichtet er. „Ich suchte nach einer Lösung, die sich schnell und flexibel an neue Anforderungen anpasst. Die große, sehr aktive und responsive Community von OpenVAS, in der sich auch die Entwickler einbringen, war aus meiner Sicht das entscheidende Kaufargument. Denn alles, was hier erarbeitet wird, fließt in die Greenbone-Lösung ein." So sind die Produkte von Greenbone stets eine optimale Kombination aus Aktualität, Stabilität und Qualität, denn sie enthalten von den neuen Funktionen nur jene, die auf Herz und Nieren geprüft wurden, stabil und sicher laufen und auch beim Einsatz zuverlässige Aussagen liefern.

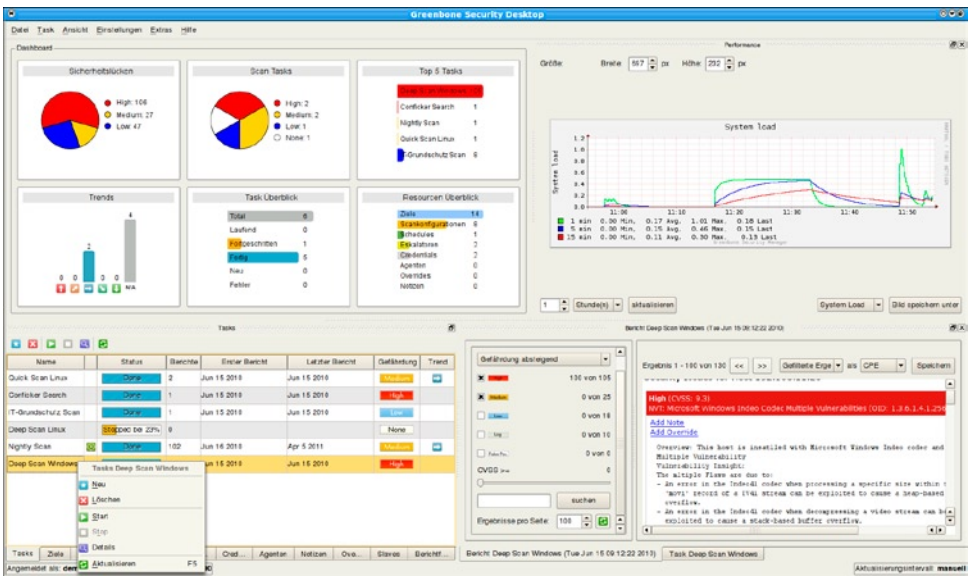
Die OpenVAS Community wird von Greenbone explizit unterstützt. Gemeinsam mit den engagierten Nutzern sind Verbesserungen und Anpassungen an der Software zügig verfügbar, oder auch seltene Security-Fragen schnell gelöst. Und natürlich kann jeder der möchte, die freie Software kostenlos zur Schwachstellenanalyse nutzen.

Fallstudie Vulnerability Management
Universität der Bundeswehr München

„Wer den Vulnerability Scan in einer produktiven Umgebung einsetzen will und eine entsprechende Verfügbarkeit garantieren muss, hat zur Greenbone-Lösung eigentlich keine Alternative.“

Stefan Schwarz, Leiter des Rechenzentrums der Universität der Bundeswehr München

Prioritäten für Produktivumgebung
„Betriebswirtschaftlich macht der Einsatz der freien Software im Vergleich zur Greenbone-Appliance aber für ein Unternehmen wenig Sinn“, weiß Schwarz. „Die freie Software zeichnet sich durch Aktualität und Vielseitigkeit aus. Sie ist aber auch anfällig für Entwicklerfehler und man benötigt sehr solide Programmier- und Netzwerkkenntnisse, um sie zielführend einzusetzen. Oder anders gesagt: Man muss sein eigener Qualitätsmanager sein“, mahnt Schwarz. „Wer den Vulnerability Scan in einer produktiven Umgebung einsetzen will und eine entsprechende Verfügbarkeit garantieren muss, hat zur Greenbone-Lösung eigentlich keine Alternative. Bei uns läuft sie ohne jegliche Ausfälle stabil und zuverlässig und macht genau das, was ich brauche.“



„Mir kommt es darauf an, Veränderungen und Unterschiede zu erkennen. Sie zeigen mir, wo Gefahr drohen könnte.“

Einfache Bedienung spart Zeit
Der Experte schätzt, dass auch ein Laie das Boxsystem von Greenbone problemlos in kurzer Zeit nutzen kann. Die Open Source Variante benötigt dagegen einige Vorkenntnisse und nimmt mindestens einen Tag oder mehr und aufgrund der ständigen Aktualisierungen auch kontinuierlich Zeit in Anspruch. Sie ist aber für Stefan Schwarz eine wichtige Ergänzung zum System, mit der er experimentieren, sich mit zukünftigen Anforderungen beschäftigen und mit der Community austauschen kann. So wünscht er sich zum Beispiel, dass künftige Versionen auch verstärkt Applikationen nach Schwachstellen prüfen können.

Engagement für Offenheit
Neben den Vorteilen in Bezug auf Verfügbarkeit, Stabilität und Qualität betrachtet er den Einsatz der kommerziellen Lösung auch als Anerkennung für die offene Arbeitsweise des Herstellers. „Ich finde es absolut bemerkenswert, dass Greenbone die Entwicklung der freien Software unterstützt und sich aktiv in der Community einbringt. Ich habe selten einen solch engagierten, zugänglichen und kooperativen Hersteller erlebt. Das unterstütze ich auch gerne mit dem Kauf der Lösung.“

Greenbone Security Manager

GSM 500

Einsatzfelder

- Mittlere bis große Unternehmens-IT
- Größere Zweigstellen
- Steuerung von bis zu 10 Scan-Sensoren
- 500 - 5000 IPs

Funktionen

- Schlüsselfertige Lösung: Inbetriebnahme innerhalb von 10 Minuten
- Leistungsstarkes Betriebssystem Greenbone OS mit speziell angepasster Kommandozeilen-orientierter Administration
- Integrierter Greenbone Security Feed mit über 25.000 Netzwerk Schwachstellen-Tests mit täglicher, automatischer Aktualisierung
- Integriertes Backup, Restore, Snapshot und Update
- Integriert Greenbone Security Assistant als zentrale Web-Schnittstelle
- Keine Begrenzung bezüglich Anzahl der Zielsysteme bzw. IPs (die maximal erreichbare Zahl hängt vom Scan-Muster und den Scan-Zielen ab)
- Bezug umfasst sowohl den Austausch defekter Hardware als auch Zugang zum Greenbone Security Feed, Feature-Updates und Support

Greenbone Networks GmbH
Neuer Graben 17,49074 Osnabrück, Germany
Telefon: +49-541-335084-0
Fax: +49-541-335084-99
Email: info@greenbone.net