Die unterschiedlichen Ausprägungen von Greenbone Networks' Technologie

Greenbone Security Manager und Greenbone Community Edition

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2020-03-20

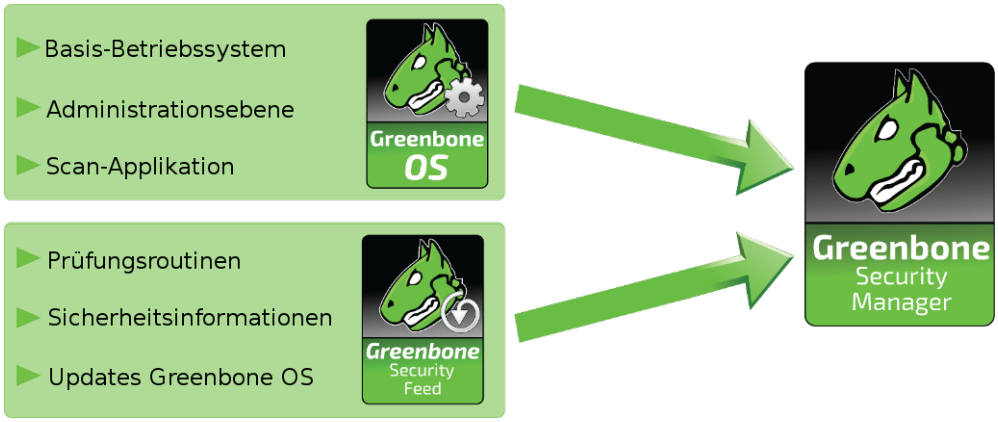
Inhalt

1. Offen, Transparent, Professionell

Open-Source-IT-Sicherheit liefert nicht nur ein hohes Level an Transparenz der Lösung selbst, sondern ist auch ein Beitrag zur IT-Sicherheitsgemeinschaft im Allgemeinen. Wir sind mit dieser Idee verbunden und ihr verpflichtet. Dieses Whitepaper soll unseren Kunden und Nutzern dabei helfen, die Unterschiede zwischen den verschiedenen Lösungen zu verstehen.

2. Einleitung

Unsere Greenbone-Networks-Technologie unterteilt sich in zwei Hauptkomponenten: Greenbone Operating System (GOS) und Greenbone Security Feed (GSF). Sie ist in zwei verschiedenen Versionen verfügbar.



Der **Greenbone Security Manager (GSM)** ist eine funktionsreiche Unternehmenslösung, die das nötige Potential für die Integration in eine übergreifende Sicherheitsarchitektur liefert, selbst für Hochsicherheitsnetzwerke, die einen Airgap-Ansatz erfordern. Er ist für den professionellen Gebrauch in Unternehmen und Administrationen konstruiert und wird als schlüsselfertige Appliance geliefert. Er stellt unseren Unternehmenskunden vollständige Möglichkeiten und Funktionen auf einfache Weise zur Verfügung, während nur einer für die Funktionstüchtigkeit der Schwachstellen-Mangement-Lösung verantwortlich ist: Greenbone Networks.

Die **Greenbone Community Edition (GCE)** für den sicherheitsbewussten Nutzer in SOHO-Umgebungen (Small Office, Home Office) wird als virtuelle Maschine oder in Form von Source-Paketen geliefert. Die Installation der Hardware, des Betriebssystems und zusätzlicher Komponenten, selbst die Kompilation (im Falle von Source-Paketen), liegt in der Verantwortung des SOHO-Nutzers. Die GCE ist eine schwächere Version des kommerziellen Produkts für die professionelle Nutzung (GSM). Die GCE ist für den unabhängigen Betrieb in kleinen Umgebungen konzipiert.

Die Projektanforderungen machen den Unterschied. Die folgenden Kapitel zeigen detailliert die Unterschiede zwischen den Ausprägungen von Greenbone Networks’ Technologie, zusammengefasst für die Hauptaspekte der Lösung:

- Feed
- Lösungsbereitstellung, -einsatz und -support
- Funktionen

3. Feed

Der Feed für beide Versionen unterscheidet sich in vier Hauptbereichen: Inhalt, Umfang, Qualität und Verfügbarkeit.

Funktionen	Greenbone Security Feed	Greenbone Community Feed
Enthaltene NVTs	Alle NVTs	Nur Basis-NVTs
Qualitätssicherung	Durchgängig	Variabel
Verfügbarkeit	Zugesichert mit SLA	Keine Zusicherung
Fehlerbeseitigung/ Verbesserungen	Zugesichert mit SLA	Keine Zusicherung
Support	Zugesichert mit SLA	Über Community auf freiwilliger Basis
Updates	Konstant/täglich	Konstant/täglich, aber ohne Unternehmensfunktionen
Transfer	Verschlüsselt	Unverschlüsselt
NVT-Signaturen	SLA für Qualitätssicherung/ Fehlerbeseitigung	Transfer-Integrität

Greenbone Networks bezieht alle selbstentwickelten Network Vulnerability Tests (NVT) in den professionellen Greenbone Security Feed (GSF) ein, allerdings nicht in den Greenbone Community Feed (GCF).

Diese NVTs können wie in der folgenden Tabelle gezeigt gruppiert werden:

Gruppe	Greenbone Security Feed	Greenbone Community Feed
Aktuell wichtige NVTs	Ja	Ja
NVTs für Heimanwenderprodukte	Ja	Ja
“IT-Grundschutz”	Ja	Ja
NVTs für Unternehmensprodukte	Ja	Nein
Compliance (z. B. PCI, ISO27001)	Ja	Nein
Betriebstechnologie (ICS/SCADA)	Ja	Nein
Signierte NVTs	Ja	Nein

Die folgende Liste zeigt einige Beispiele dieser professionellen Produkte der Unternehmensklasse, die nur im Greenbone Security Feed enthalten sind:

- Grundsätzlich alle Produkte der Unternehmensklasse und der Betriebstechnologie (d. h. ICS/SCADA)
- Microsoft-Windows-Server und Microsoft-Innendienst-Lösungen (z. B. SharePoint, SQL-Server)
- Produkte von Palo Alto Networks, Cisco, Juniper Networks und Fortinet
- Oracle-Solaris-IBM-WebSphere-Produkte (z. B. IBM WebSphere Application Server)
- Lotus-Notes- oder SAP-Produkte
- Bezahlte VMware-Produkte

Alles in allem umfasst der Community Feed etwa 30 % weniger NVTs als unser professioneller Feed.

4. Lösungsbereitstellung, -einsatz und -support

Eine Appliance kann normalerweise im Vergleich zu einer Softwareinstallation, bei der der Kunde sich um die zugrundeliegende Hardware, das Betriebssystem und das Datenbanksystem kümmern muss, mit weniger Aufwand hinsichtlich Setup und Betrieb gehandhabt werden. Aus diesem Grund wird der Greenbone Security Manager immer als Appliance geliefert, bei der alle Elemente der Lösung vom professionellen Support durch Greenbone Networks abgedeckt sind.

Master-Sensor-Einsätze, um landesweite Unternehmen mit mehreren Standorten oder sogar globale Netzwerke von Zweigstellen abzudecken, sind mit der professionellen Lösung möglich.

Die Greenbone Community Edition wird für Studien-/Testzwecke genutzt und ist an kleine Umgebungen angepasst. Die Tabelle unten listet einige weitere unterschiedliche Elemente bezüglich Lösungsbereitstellung, -einsatz und -support auf:

Kriterien	Greenbone Security Manager	GCE oder eigene Installation
Einrichtung	Schlüsselfertig (ungefähr 10 min)	Wahl des Betriebssystems und der Hardware Selbst bauen oder Community-Pakete installieren (eventuell die GCE nutzen)
Abdeckung	Abgestimmt: alle Lösungsmodule mit mehreren Scantools	Selbst wählen und ausrichten oder Community-Standards wählen
Feedkompabilität	Zugesichert mit SLA	Selbst herstellen
Leistung	Für Hardware optimiert	Selbst optimieren
Backup/ Wiederherstellung	Integriert	Individuell gelöst
Fehlerbeseitigung/ Verbesserungen	Zugesichert mit SLA	Selbst verwalten, eventuell Community-Fehlerbeseitigungen importieren
Support	Zugesichert mit SLA	Über Community auf freiwilliger Basis
Maschinenupdates	Regelmäßig und nahtlos	Neuinstallation einer neueren GCE oder manuelle Updates des Source-Builds Manuelle Migration in beiden Fällen

5. Funktionen

Die allgemeine Technologie, die vom GSM und der GCE genutzt wird, stellt bereits ein umfangreiches Set an Funktionen rund um das Schwachstellen-Scannen bereit: Scannen nach einfachen Software-Schwachstellen, Richtlinienkontrollen, Prüfungen zur Konfigurationskontrolle und Verwalten von Assets mit zusätzlichen Informationen zum Priorisieren von identifizierten Schwachstellen gemäß Asset-Kritikalität.

Es gibt Funktionen des GSM oder der GCE, die auf die Umgebung zugeschnitten sind:

Kriterien	Greenbone Security Manager	GCE oder eigene Installation
Möglichkeiten für Updates & Feed	Möglich über pro GSM konfigurierbare Synchronisationsports, redundante Proxy-Server, USB- oder FTP-Airgap oder GSM-Master	Nur Greenbone Community Feed
Systemupdate	Enthält Sicherheitsupdates Update von jeder Version auf neuesten Release möglich Übergangszeitraum für EoL und LTS Migration von Daten und Konfigurationen zwischen Appliances und Versionen	Nicht verfügbar
Protokolle	NTP, GMP, HTTPS, SSH, SNMPv2, SNMP, Syslog, IPv6, LDAP, RADIUS und mehr	HTTPS nur für Web-Oberfläche, SSH, IPv6
Integrationen und Konnektoren	Unterschiedliche Anbieter wie PaloAlto, Fortinet, Cisco FireSight, NAGIOS, Splunk, Verinice und mehr	Nicht verfügbar
Backup/ Wiederherstellung	Backup für Benutzerdaten, Systemdaten über LVM, Transfer über SCP oder USB	Nur über Umgebung (Hypervisor)
Benachrichtigungen/Zeitpläne	Über E-Mail, HTTP, SMS, Konnektor zu einem SIEM oder Ticketsystem Komplette Terminplanung möglich	Nicht verfügbar
Scanarchitektur	Master/Sensor, Airgap innerhalb von Hochsicherheitszonen	Nicht verfügbar

6. Über GCE, GVM, OpenVAS und GSM

Greenbone Networks veröffentlicht zum Zweck der Transparenz und Bewertung den Quellcode. Dies beinhaltet für diejenigen, die Erfahrung darin haben, Softwarelösungen auf Basis von Source-Paketen zusammenzustellen, die Möglichkeit, die Anwendung von Grund auf zu bauen. Die GCE ist unsere Lösung in einer fertig verfügbaren Form für unsere Community-Nutzer. Es ist eine virtuelle Appliance für die einfache Beurteilung unserer Technologie und um das Schwachstellen-Scannen und -Management in privaten und SOHO-Umgebungen durchzuführen.

Das aus mehreren Modulen bestehende Framework "Greenbone Vulnerbility Management" (GVM) ist Teil der kommerziellen Greenbone-Networks-Produkte und wird von Greenbone Networks unter einer Open-Source-Lizenz zur Verfügung gestellt. Eines der GVM-Module ist der "Open Vulnerbility Assessment Scanner" (OpenVAS). Die anderen Module befassen sich mit der Scan-Steuerung, der Web-Oberfläche und weiteren Aufgaben. Sowohl die Technologie als auch die Architektur wird kontinuierlich von Greenbone Networks weiterentwickelt.