Unsere Lösungen im Vergleich

Greenbone Source Edition, Greenbone Professional Edition und Greenbone Cloud Services

WhitePaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2020-10-29

Inhalt

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.

1 Einleitung

Das **Greenbone Vulnerability Management** (GVM) ist ein Framework, welches ursprünglich als Community-Projekt unter dem Namen „OpenVAS“ entstanden ist und seit vielen Jahren maßgeblich von Greenbone Networks entwickelt und vorangetrieben wird.
Es besteht aus dem **Greenbone Vulnerability Manager Daemon** (gvmd), dem **Greenbone Security Assistant** (GSA) mit dem **Greenbone Security Assistant Daemon** (gsad) und der ausführbaren Scanner-Anwendung, die Schwachstellen-Tests (engl. Vulnerability Tests, VT) gegen Ziele durchführt.

Das GVM-Framework wird regelmäßig unter Open-Source-Lizenzen unter dem Namen **Greenbone Source Edition** (GSE) veröffentlicht. Damit können Linux-Distributionen GVM in Form von Installationspaketen erstellen und bereitstellen. Auch Privatpersonen können GVM so installieren und nutzen.

Der GSA ist die Web-Oberfläche, über die der Nutzer Scans steuern und Schwachstellen-Informationen abrufen kann. Die Kommunikation findet über das **Greenbone Management Protocol** (GMP) statt, mit welchem der Nutzer mithilfe verschiedener Tools auch direkt kommunizieren kann.

Die **Greenbone Professional Edition** (GPE) ist die kommerzielle Produktlinie und als virtuelle oder physische Appliance verfügbar. Sie basiert auf dem **Greenbone Security Manager** (GSM), der das Framework GVM sowie das **Greenbone Operating System** (GOS), das weitere Funktionalitäten bereitstellt, enthält.

Die Schwachstellen-Tests zum Scannen erhält der GSM über den **Greenbone Security Feed** (GSF). Der **Greenbone Security Manager TRIAL** (GSM TRIAL) ist eine virtuelle Maschine und dient als kostenlose Probeversion. Er nutzt standardmäßig den weniger umfangreichen **Greenbone Community Feed** (GCF) anstelle des GSF.

Die **Greenbone Scan Services** (GSC) sind eine SaaS-Lösung. Scananfragen werden über die Cloud an den **Greenbone Scan Cluster** (GSC) weitergeleitet. Vom GSC aus werden Scans für externe Ziele oder Ziele ausgeführt. Zum Scannen werden der GVM-Scanner genutzt und die Schwachstellen-Tests ebenfalls über den GSF bezogen.

2 Feed

Der Greenbone Security Feed (GSF) und der Greenbone Community Feed (GCF) unterscheiden sich in vier Hauptbereichen: Inhalt, Umfang, Qualität und Verfügbarkeit.

Funktionen	GSF	GCF
Enthaltene VTs	Alle VTs	Nur Basis-VTs
Qualitätssicherung	Einheitlich	Variabel
Verfügbarkeit	Verbindlich geregelt mit SLA	Unverbindlich
Korrekturen/Verbesserungen	Verbindlich geregelt mit SLA	Unverbindlich
Support	Verbindlich geregelt mit SLA	Über Community auf freiwilliger Basis
Updates	Konstant/täglich	Konstant/täglich, aber ohne Unternehmensfunktionen
Übertragung	Verschlüsselt	Unverschlüsselt
VT-Signaturen	SLA für Qualitätssicherung/ Korrekturen	Transfer-Integrität

Greenbone Networks bezieht alle selbstentwickelten Schwachstellen-Tests (engl.: Vulnerability Tests, VT) in den professionellen Greenbone Security Feed (GSF) ein, allerdings nicht in den Greenbone Community Feed (GCF).

Die VTs können wie in der folgenden Tabelle gezeigt gruppiert werden:

Gruppe	GSF	GCF
Aktuell wichtige VTs	Ja	Ja
VTs für Heimanwenderprodukte	Ja	Ja
“IT-Grundschutz”	Ja	Ja
VTs für Unternehmensprodukte	Ja	Nein
Compliance (z. B. PCI, ISO27001)	Ja	Nein
Betriebstechnologie (ICS/SCADA)	Ja	Nein
Signierte VTs	Ja	Nein

Die folgende Liste zeigt einige Beispiele für Produkte und Anwendungen, für die keine Schwachstellen-Tests im Greenbone Community 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)
- HCL Notes
- Bezahlte VMware-Produkte

Alles in allem umfasst der Community Feed etwa 30 % weniger VTs als der professionelle Feed.

3 Lösungsbereitstellung, -einsatz und -support

Die Greenbone Professional Edition (GPE) kann im Vergleich zu einer eigenen GSE-Softwareinstallation, bei der der Kunde sich um die zugrundeliegende Hardware, das Betriebssystem und das Datenbanksystem kümmern muss, mit viel weniger Aufwand hinsichtlich Setup und Betrieb gehandhabt werden.

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

Die Greenbone Cloud Services (GCS) werden als Cloud-Lösung geliefert, was ebenfalls einen geringen Aufwand bei der Einrichtung bedeutet. Gateway-Komponenten ermöglichen das Scannen interner IP-Adressen.

Alle Elemente der GPE und der GCS werden vom professionellen Support durch Greenbone Networks abgedeckt.

Die Tabelle unten listet einige weitere unterschiedliche Elemente bezüglich Lösungsbereitstellung, -einsatz und -support auf:

Kriterien	GSE	GPE	GCS
Einrichtung	Eigenverantwortliche Wahl des Betriebssystems und der Hardware Eigenverantwortlich zu bauen oder Community-Pakete installieren	Schlüsselfertig (ungefähr 10 min)	Schlüsselfertig (ungefähr 10 min)
Feedkompatibilität	Eigenverantwortlich herzustellen	Zugesichert mit SLA	Zugesichert mit SLA
Leistung	Eigenverantwortlich zu optimieren	Für Hardware optimiert	Variabel je nach Anforderung
Backup/Wiederherstellung	Individuell gelöst	Integriert	Integriert
Fehlerbeseitigung/ Verbesserungen	Eigenverantwortlich zu verwalten	Zugesichert mit SLA	Zugesichert mit SLA
Support	Über (externe) Community auf freiwilliger Basis	Zugesichert mit SLA	Zugesichert mit SLA
Softwareupdates	Manuelle Updates des Source-Builds und manuelle Migration der Daten	Regelmäßig und nahtlos	Kontinuierlich

4 Funktionen

Das GVM-Framework 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.

Darüber hinaus bieten GPE und GCS eine Vielzahl von Funktionen, die auf die jeweilige Umgebung zugeschnitten sind:

Kriterien	GSE	GPE	GCS
Möglichkeiten für Updates & Feed	Nur Greenbone Community Feed	Täglich automatisch Möglich über pro GSM konfigurierbare Synchronisationsports, redundante Proxy-Server, USB- oder FTP-Airgap oder GSM-Master	Täglich automatisch Keine Compliance-Tests
Systemupdate	Abhängig von Distribution oder eigenverantwortlich	Enthält Sicherheitsupdates Update von jeder Version auf neuesten Release möglich Übergangszeitraum für EoL und LTS Migration von Daten und Konfigurationen zwischen Appliances und Versionen	Automatisch Kontinuierliche Sicherheits- und Plattformupdates
Protokolle	Eigenverantwortlich zu konfigurieren und einzurichten	NTP, GMP, OSP, HTTPS, SSH, SNMPv2, SNMP, Syslog, IPv6, LDAP, RADIUS und mehr	NTP, GMP, HTTPS, SSH, SNMPv2, SNMP, Syslog, LDAP, RADIUS und mehr
Integrationen und Konnektoren	Nicht verfügbar	Unterschiedliche Anbieter wie PaloAlto, Fortinet, Cisco FireSight, NAGIOS, Splunk, Verinice und mehr	RestFull API für alle Funktionalitäten
Backup/ Wiederher-stellung	Individuell gelöst	Backup für Benutzerdaten, Systemdaten über LVM, Transfer über SCP oder USB	Automatische(s) Backup/Wiederherstellung
Benachrichti-gungen/ Zeitpläne	Eigenverantwortlich über Betriebssystem zu konfigurieren	Über E-Mail, HTTP, SMS, Konnektor zu einem SIEM oder Ticketsystem und mehr Komplette Terminplanung möglich	Über E-Mail, Slack oder Microsoft Teams
Scanarchitektur	Nicht verfügbar	Master/Sensor, Airgap innerhalb von Hochsicherheitszonen	Cloud-Scanner, Gateway-Komponente für interne Scans