

FAQ

Inhalt

- [1. Wer ist Greenbone?](#)
- [2. Was ist unser Ansatz?](#)
- [3. Was sind unsere Produkte?](#)
- [4. Wie kann man unsere Produkte kaufen?](#)
- [5. Was sind die Unterschiede zwischen Greenbone Security Feed und OpenVAS NVT Feed?](#)
- [6. Was sind die Unterschiede zwischen Greenbone Security Manager und einer eigenen OpenVAS-Installation?](#)
- [7. Verstoßen die Greenbone Lösungen gegen den "Hacker-Paragraph" 202c StGB?](#)

Einleitung

1. Wer ist Greenbone?

Greenbone Networks liefert eine Schwachstellen-Management-Lösung zur Vorsorge gegen Netzwerk-Einbrüche - ergänzt durch Sicherheits-Berichte mit Change-Management.

Das Unternehmen wurde im Jahr 2008 von führenden Experten aus den Bereichen Netzwerksicherheit und Freie Software gegründet. Unser Ziel ist die Entwicklung von Produkten und Konzepten, die es erlauben die aktuellen und zukünftigen Herausforderungen zur Vermeidung erfolgreicher Angriffe auf Ihre Netzwerk-Infrastruktur zu meistern. Wir legen besonderen Wert auf eine transparente White-Box um den Kunden eine überprüfbare Lösung für den Betrieb in kritischer Fortune-500 IT-Umgebung zu bieten sowie eine umfangreiche kostengünstige schlüsselfertige Lösung für kleine und mittlere Unternehmen.

2. Was ist unser Ansatz?

Bei Greenbone setzen wir auf einen ganzheitlichen Ansatz für Minimierung und Management von Risiken die aus Schwachstellen der Systeme resultieren.

Greenbone ist der erste Anbieter in diesem Bereich der eine 100%ige Open Source Lösung anbietet. Diese White-Box Lösung gestattet den Kunden die Risiken zu vermeiden die entstehen wenn man ein proprietäres Schwachstellenanalyse-System in seinen kritischen IT Infrastrukturen einsetzt.

Greenbone engagiert sich in den globalen und multi-kulturellen Open Source Gemeinschaften in kooperativer Weise. Wir verstehen das Konzept von Nehmen und Geben sowie von gemeinsamen Entwicklungsprozessen bei Freier Software.

3. Was sind unsere Produkte?

Der Greenbone Security Manager ist eine schlüsselfertige Lösung für Netzwerksicherheits-Scanning: Er kombiniert den Greenbone Security Feed, eine Scan Engine und eine web-basierte administration.

Der Greenbone Security Feed ist unser Basisprodukt. Es handelt sich dabei um einen permanenten Strom kleiner Prozeduren zu Erkennung bekannter und potentieller Sicherheitsprobleme in allen aktiven Elementen Ihrer IT Infrastruktur: Desktop PCs, Server, Appliances und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Andere Hersteller können den Greenbone Security Feed auch als OEM-Lizenz integrieren.

4. Wie kann man unsere Produkte kaufen?

Sie finden das Vorgehen zum Kauf unserer Produkte auf der Seite [Bezugspartner](#).

5. Was sind die Unterschiede zwischen Greenbone Security Feed und OpenVAS NVT Feed?

Zentrale Unterschiede zwischen der kostenpflichtigen Subscription des Greenbone Security Feed (in Verbindung mit einer GSM-kompatiblen Scan-Engine) und dem kostenfreien OpenVAS NVT Feed (eine Kopplung dieses Feed mit dem Greenbone Security Manager wird nicht unterstützt) sind (Stand März 2010):

	Greenbone Security Feed	OpenVAS NVT Feed
Qualitätssicherung (QS)	Einheitlich	Unterschiedlich
Verfügbarkeit	Zugesagt mit SLA	Keine Zusage
Korrekturen	Zugesagt mit SLA	Keine Zusage
Support	Zugesagt mit SLA	Durch Community auf freiwilliger Basis
Kompatibilität	OpenVAS 3.0, 3.1 und 4	OpenVAS 2.0, 3.0, 3.1 und 4
Aktualisierung	Regelmäßig	Unregelmäßig
Übertragung	Verschlüsselt	Unverschlüsselt
NVT Signaturen	SLA für QS/Korrekturen	Transfer-Integrität

Umfang/Abdeckung: Greenbone und ihre Partner stellen ihre Entwicklungen als Freie Software der OpenVAS Gemeinschaft zur Verfügung. Aufgrund von z.B. Versions- oder Schnittstellen-Konflikten kann es dabei zu Verzögerungen kommen. NVTs welche in den freien OpenVAS NVT Feed integriert sind, aber nicht im Greenbone Security Feed enthalten sind, haben unsere strengen Qualitätssicherungs-Kriterien nicht bestanden.

6. Was sind die Unterschiede zwischen Greenbone Security Manager und einer eigenen OpenVAS-Installation?

Zentrale Unterschiede zwischen der Appliance Greenbone Security Manager (ausschließlich in Verbindung mit dem Greenbone Security Feed erhältlich) und einer selbst eingerichteten OpenVAS-Installation (mit Greenbone Security Feed oder OpenVAS NVT Feed verwendbar, Stand Mai 2010):

Greenbone Security Manager

Eigene OpenVAS-Installation

Inbetriebnahme	Turn-key (ca. 10 Minuten)	Auswahl Betriebssystem und Hardware, dann Eigenbau oder Installation von fertig herunterladbaren Community-Paketen; ggf. auch Verwendung einer Community-VM
Umfang	Aufeinander abgestimmt: Alle OpenVAS Module mit diversen Scan-Tools	Selbst zu definieren und aufeinander abzustimmen oder Community-Voreinstellungen übernehmen
Feed-Kompatibilität	Zugesagt mit SLA	Selbst sicherzustellen, bei Verwendung des GSF Unterstützung durch Greenbone möglich
Performanz	Für Hardware optimiert	Selbst sicherzustellen
Backup/Recovery	Integriert	Separat zu lösen
Korrekturen	Zugesagt mit SLA	Selbst ausführen, ggf. einspielen von Community-Fixes
Support	Zugesagt mit SLA	Durch Community auf freiwilliger Basis
Aktualisierung	Regelmäßig und nahtlos	Nach eigenem Ermessen und Verfahren

7. Verstoßen die Greenbone Lösungen gegen den "Hacker-Paragraph" 202c StGB?

Die Herstellung und Verbreitung von Sicherheitssoftware ist kein strafbares Verhalten nach § 202c des Strafgesetzbuches ("Hacker-Paragraph"). Dieses hat das Bundesverfassungsgericht mit Beschluss vom 18.05.2009 (2 BvR 2233/07) ausdrücklich klargestellt. Nach Auffassung des Bundesverfassungsgerichts ist strafbar nur die Herstellung und Verbreitung von Computerprogrammen, deren Zweck das Ausspähen oder Abfangen von Daten nach §§ 202a und 202b des Strafgesetzbuches ist. Dieses erfordert, dass die Software in der Absicht der Begehung dieser Straftaten entwickelt wurde. Es reicht nicht aus, dass ein Programm für die Begehung der Computerstraftaten auch geeignet sein kann. Da unsere Software für Sicherheitszwecke entwickelt und genutzt wird, wird der Tatbestand des § 202c StGB nicht tangiert.