

Warum Greenbone?



WARUM SCHWACHSTELLEN-MANAGEMENT?

999 von 1.000 erfolgreich ausgenutzten Schwachstellen sind seit mehr als einem Jahr bekannt. Das bedeutet, dass diese Angriffsfläche schnell und einfach verkleinert werden kann.

Schwachstellenmanagement ist ein Prozess, um Schwachstellen in einer IT-Infrastruktur zu finden, ihren Schweregrad einzustufen und zusätzlich eine Auflistung der zu ergreifenden Maßnahmen zum Beseitigen der Schwachstellen zu liefern.

Ziel ist es, Schwachstellen zu eliminieren, bevor sie von Angreifenden ausgenutzt werden können.



SCHWACHSTELLEN-MANAGEMENT VS. FIREWALLS & CO.

Ziel von Firewalls und ähnlichen Systemen ist es, tatsächlich stattfindende Angriffe abzuwehren. Sie greifen deshalb oft erst ein, wenn der Angriff schon passiert ist.

Im Gegensatz dazu betrachtet das Schwachstellenmanagement die IT-Infrastruktur aus dem Blickwinkel einer angreifenden Person. Dabei ist es das Ziel, Schwachstellen, die von potenziellen Angreifenden ausgenutzt werden könnten, zu schließen, sodass es gar nicht erst zu einem Angriff kommt. Eine Kombination aus beiden Lösungen ist die beste Wahl.



VORTEILE UNSERER LÖSUNGEN

Greenbone Enterprise Appliances

- Keine Begrenzung bei der Anzahl der Zielsysteme
- Leistungsstarkes Appliance-Betriebssystem Greenbone OS
- Integrierter Greenbone Enterprise Feed mit täglicher, automatischer Aktualisierung
- Steuerung über grafische Web-Oberfläche
- Zahlreiche Berichtformate
- Scan-Automatisierung durch Zeitpläne und Benachrichtigungen
- Scannen von Hochsicherheitszonen durch Master-Sensor-Setup und Airgap

Greenbone Cloud Service

- Geringe Betriebskosten, da kein Fachpersonal sowie keine Hard- und Software benötigt wird
- Integrierter Greenbone Enterprise Feed mit täglicher, automatischer Aktualisierung
- Monatliche Gebühr in Form eines Abonnements
- Anpassung der Anzahl der Scanziele monatlich möglich
- Zahlreiche Berichtformate
- Scan-Automatisierung durch Zeitpläne und Benachrichtigungen
- Deutscher Serverstandort, damit Erfüllung der DSGVO



TRANSPARENZ

- Erster und einziger Anbieter einer 100%igen Open Source Schwachstellenmanagement-Lösung
- Quellcode jederzeit in unserem GitHub einsehbar: <https://github.com/greenbone/>
- Whitebox- statt Blackbox-Lösung
- Keine Risiken, die aus dem Einsatz eines proprietären Schwachstellenanalyse-Systems in kritischen IT-Infrastrukturen entstehen



GREENBONE ENTERPRISE FEED

- Über 100.000 Schwachstellentests sowie Security Policies
- Verschlüsselte und signierte Übertragung
- Tägliche Aktualisierung
- Zugang über Greenbone-Subscription
- Enthält Schwachstellentests für:
 - Aktuell wichtige Schwachstellen
 - Heimanwenderprodukte
 - BSI IT-Grundschutz
 - Unternehmensprodukte
 - Betriebstechnologie (ICS/SCADA)



MADE IN GERMANY

Aus einer Kooperation entstanden, steht unsere Entwicklung noch heute in enger und stetiger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Mit Produktion, Entwicklung und Support in Deutschland garantieren wir eine vollwertige Übereinstimmung mit der DSGVO.

Auch unser Greenbone Cloud Service wird ausschließlich in deutschen Rechenzentren betrieben, sodass die Einhaltung der DSGVO gewährleistet ist.



SUPPORT & PROFESSIONAL SERVICES

- Deutsch- und englischsprachiger Support
- Volle Herstellergarantie für Hardware
- Feed-Updates und Software-Upgrades
- Austausch defekter Hardware
- Laufzeiten nach Bedarf: 1, 3 oder 5 Jahr(e)
- Umfassende Schulungen und Webinare
- Unterstützung bei Sizing und anderen technischen Fragen
- Proof-of-Concept-Installationen
- Vorbereitung und – auf Wunsch – Übernahme der Einrichtung