Warum Greenbone?

Greenbone
Sustainable Resilience

WARUM CYBER-RESILIENZ?

Unter Cyber-Resilience versteht man die Fähigkeit eines Unternehmens, seine Geschäftsprozesse trotz widriger Cyber-Umstände aufrechtzuerhalten. Das können Cyber-Angriffe, aber auch unbeabsichtigte Hindernisse wie fehlgeschlagene Software-Updates oder menschliches Versagen sein. Cyber Resilience ist ein umfassendes Konzept, das über IT-Sicherheit hinausgeht. Um einen Zustand der Cyber Resilience zu erreichen, ist es wichtig, Schwachstellen frühzeitig zu erkennen, sie wirtschaftlich zu priorisieren und zu beseitigen.

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 eines Angreifers. Dabei ist es das Ziel, Schwachstellen, die von potenziellen Angreifern 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 Professional Edition

- Keine Begrenzung bei der Anzahl der Zielsysteme
- Leistungsstarkes Appliance-Betriebssystem Greenbone OS
- Integrierter Greenbone Security Feed (GSF) 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 Services

- Geringe Betriebskosten, da kein Fachpersonal sowie keine Hard- und Software benötigt wird
- Integrierter Greenbone Security Feed (GSF) mit täglicher, automatischer Aktualisierung
- Monatliche Gebühr in Form eines Abonnements
- Individuelle Anpassung der Kosten an den Umfang der Scanziele
- 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 SECURITY FEED

- Tausende 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 unsere Greenbone Cloud Services (GCS) werden 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

Greenbone Networks GmbH • Neumarkt 12 • 49074 Osnabrück • www.greenbone.net