

# Nessus im Blick: Schwachstellen entlarven und sichern

Category: Online-Marketing

geschrieben von Tobias Hager | 7. Februar 2026



# Nessus im Blick: Schwachstellen entlarven und sichern

Du hast Firewalls, du hast VPNs, du hast vielleicht sogar einen übernächtigen ITler im Keller sitzen – und trotzdem ist dein Netzwerk ein Schweizer Käse? Willkommen in der Realität der IT-Sicherheit 2024. Nessus ist nicht nur ein weiteres Tool im unübersichtlichen Security-Zoo – es ist die Lupe, das Skalpell und der fiese Bohrer, mit dem du deine Infrastruktur

wirklich durchleuchten kannst. Aber nur, wenn du weißt, wie. Dieser Artikel zeigt dir, warum Nessus kein Gadget, sondern Pflichtprogramm ist – und wie du es richtig einsetzt, bevor es jemand anderes tut.

- Was Nessus ist – und warum es in keiner Security-Strategie fehlen darf
- Wie Nessus Schwachstellen erkennt, bewertet und priorisiert
- Die wichtigsten Funktionen von Nessus – von Netzwerk-Scan bis Compliance-Check
- Anleitung: So richtest du Nessus richtig ein und startest deinen ersten Scan
- Best Practices für den produktiven Einsatz in Unternehmen
- Was Nessus kann – und was du besser mit anderen Tools abdeckst
- Typische Fehler bei der Nutzung – und wie du sie vermeidest
- Sicherheitslücken verstehen, bevor Angreifer sie ausnutzen
- Warum ein ungenutzter Nessus-Scan schlimmer ist als keiner

# Was ist Nessus? Der Platzhirsch unter den Schwachstellenscannern

Nessus ist ein kommerzieller Schwachstellenscanner von Tenable, der seit über zwei Jahrzehnten im Spiel ist – lange bevor die meisten „Cybersecurity-Startups“ überhaupt wussten, wie man TCP/IP buchstabiert. Ursprünglich als Open-Source-Projekt gestartet, hat sich Nessus zu einem der zuverlässigsten und umfassendsten Tools für die Schwachstellenanalyse entwickelt. Heute ist es ein de-facto-Standard in der IT-Sicherheitsbranche.

Im Kern durchsucht Nessus Systeme, Netzwerke und Geräte nach bekannten Schwachstellen. Das umfasst CVEs (Common Vulnerabilities and Exposures), Fehlkonfigurationen, veraltete Softwareversionen, offene Ports, unsichere Dienste und vieles mehr. Der Fokus liegt dabei nicht nur auf der reinen Erkennung, sondern auch auf der Bewertung des Risikos – inklusive CVSS-Score, Exploit-Verfügbarkeit und möglichen Auswirkungen.

Nessus funktioniert agentenlos – das heißt, du musst keine Software auf den Zielsystemen installieren. Stattdessen greift Nessus über Netzwerkprotokolle wie SSH, SMB oder SNMP auf Systeme zu, um Informationen zu sammeln und zu analysieren. Damit eignet es sich besonders gut für große, heterogene Netzwerke, in denen zentralisierte Kontrolle gefragt ist.

Die Datenbasis von Nessus ist beeindruckend: Über 160.000 Plugins sorgen dafür, dass Schwachstellen in Windows, Linux, macOS, Netzwerkhardware, Webservern, Datenbanken und Anwendungen zuverlässig erkannt werden. Diese Plugins werden kontinuierlich aktualisiert – oft innerhalb von Stunden nach der Entdeckung neuer Sicherheitslücken.

Kurz gesagt: Nessus ist kein nettes Tool für Pentest-Spielereien – es ist ein ernstzunehmendes, professionelles Werkzeug für IT-Security-Teams, das täglich

Leben retten kann. Digital gesehen jedenfalls.

# Wie Nessus Schwachstellen scannt und bewertet

Der Scan-Prozess von Nessus ist nicht einfach nur ein Port-Scan mit etwas CVE-Datenbank obendrauf. Vielmehr ist es ein mehrstufiger, adaptiver Prozess, der sich an die Zielumgebung anpasst und Kontextinformationen berücksichtigt. Nessus analysiert zunächst grundlegende Netzwerkdaten: IP-Adressen, offene Ports, laufende Dienste. Auf dieser Basis identifiziert es potenzielle Angriffspunkte.

Im nächsten Schritt versucht Nessus, sich authentifiziert auf den Zielsystemen einzuloggen – sofern Zugangsdaten bereitgestellt wurden. Authentifizierte Scans liefern eine deutlich höhere Qualität, da Nessus dann direkt auf Konfigurationsdateien, installierte Softwarepakete und Registry-Einträge zugreifen kann. Ohne Authentifizierung bleibt vieles im Dunkeln.

Jede gefundene Schwachstelle wird mit einem CVSS-Score versehen – dem Common Vulnerability Scoring System. Dieser Score bewertet das Risiko anhand von Faktoren wie Komplexität des Angriffs, Auswirkungen auf Verfügbarkeit, Integrität und Vertraulichkeit sowie der Frage, ob ein Exploit öffentlich verfügbar ist.

Nessus ist außerdem in der Lage, Schwachstellen kontextualisiert zu priorisieren. Das bedeutet: Kritische Lücken auf einem öffentlich erreichbaren Webserver wiegen schwerer als dieselben Lücken auf einem isolierten Testsystem. Diese Priorisierung ist Gold wert für überlastete IT-Abteilungen, die nicht jede Warnung sofort abarbeiten können.

Ein weiterer Pluspunkt: Nessus erkennt nicht nur Schwachstellen – es liefert auch konkrete Handlungsempfehlungen, inklusive Links zu Patch-Quellen, Workarounds und Best Practices. Damit wird der Scanner zum aktiven Teil des Remediation-Prozesses, nicht nur zum Alarmsystem.

## Nessus einrichten und nutzen: Schritt für Schritt

Ein Schwachstellenscanner nützt dir nichts, wenn er nicht richtig konfiguriert ist. Zu viele Unternehmen installieren Nessus, lassen einen Default-Scan laufen und betrachten sich dann als sicher. Spoiler: Das ist ungefähr so sinnvoll wie ein Rauchmelder ohne Batterie. Hier die Essentials für eine sinnvolle Einrichtung:

- 1. Installation: Lade Nessus von der Tenable-Website herunter. Es gibt Versionen für Windows, Linux und macOS. Die Installation ist in wenigen Minuten erledigt – allerdings solltest du das System danach ordentlich

absichern.

- 2. Lizenz aktivieren: Nessus Essentials ist kostenlos, aber eingeschränkt. Für professionelle Nutzung brauchst du Nessus Professional – und dazu eine gültige Lizenz.
- 3. Plugin-Updates: Nach der Installation lädt Nessus automatisch die neuesten Plugins herunter. Ohne aktuelle Plugins ist dein Scan so nützlich wie ein Virenschanner von 2002.
- 4. Scan-Ziele definieren: Trage IP-Ranges, Subnetze oder einzelne Hosts ein. Vermeide es, produktive Systeme zu scannen, ohne mit dem Betrieb abgestimmt zu haben – manche Scans können Systeme belasten.
- 5. Credentials einrichten: Für authentifizierte Scans hinterlege SSH-, SMB- oder SNMP-Zugangsdaten. Ohne diese siehst du nur die Oberfläche – wie ein Autokäufer, der nie unter die Haube schaut.
- 6. Scan-Policy konfigurieren: Wähle aus vordefinierten Templates oder erstelle eigene Policies. Du kannst z. B. nur nach bestimmten CVEs, Schwachstellenklassen oder Konfigurationen suchen.
- 7. Scan starten: Los geht's. Je nach Umfang und Tiefe kann ein Scan von wenigen Minuten bis zu mehreren Stunden dauern.
- 8. Ergebnisse analysieren: Nessus liefert Reports mit Schwachstellen, Scores und Maßnahmen. Arbeite die Liste nicht blind ab – priorisiere nach Risiko und Machbarkeit.

# Typische Fehler und Missverständnisse im Umgang mit Nessus

Viele IT-Teams nutzen Nessus – aber nur wenige nutzen es richtig. Der häufigste Fehler: einmal installiert, nie wieder angefasst. Sicherheitslücken entstehen kontinuierlich. Ein wöchentlicher oder mindestens monatlicher Scan ist Pflicht. Alles andere ist fahrlässig.

Ein weiterer Klassiker: fehlende Authentifizierung. Ohne Zugang zu den Systemen bleibt Nessus blind für viele interne Konfigurationen. Wer glaubt, ein externer Scan reicht aus, sollte sich besser gleich vom Gedanken an Sicherheitsniveau verabschieden.

Auch falsch gesetzte Scan-Policies sind ein Problem. Entweder zu breit (und damit zu ungenau) oder zu eingeschränkt (und relevante Probleme werden übersehen). Policies müssen zur Zielumgebung passen – und regelmäßig überprüft werden.

Nicht zu vergessen: Die Ergebnisse werden oft falsch interpretiert. Ein hoher CVSS-Score heißt nicht automatisch, dass ein Exploit auch realistisch ist. Ebenso sind manche „Low“-Schwachstellen in sensiblen Systemen extrem kritisch. Kontext ist alles.

Und schließlich: Kein Follow-up. Nessus zeigt dir ein Problem – aber lösen musst du es selbst. Ohne Patch-Management, Change-Prozesse und

Verantwortlichkeiten bleiben die Reports PDFs mit rotem Text. Schön fürs Archiv, aber nutzlos für die Sicherheit.

# Best Practices für den Einsatz von Nessus in Unternehmen

Wer Nessus produktiv und effizient nutzen will, braucht mehr als nur einen installierten Scanner. Es braucht Prozesse, Verantwortlichkeiten und ein Mindestmaß an Automatisierung. Hier ein kompakter Fahrplan für den professionellen Einsatz:

- Regelmäßige Scans planen: Automatisiere monatliche Scans für alle produktiven Systeme. Kritische Systeme kannst du wöchentlich prüfen.
- Scan-Ergebnisse versionieren: Vergleiche Ergebnisse über Zeit, um Regressionen oder neue Risiken zu erkennen.
- Integration in ITSM: Binde Nessus in dein Ticket-System ein, damit Schwachstellen automatisch als Aufgaben verteilt werden.
- Berichtsformate anpassen: Erstelle unterschiedliche Reports für Technik (vollständig) und Management (aggregiert, mit Risikoübersicht).
- Compliance-Checks nutzen: Nessus kann auch auf CIS Benchmarks, PCI DSS oder HIPAA prüfen – und das automatisiert. Nutze diese Funktion für Audits und Zertifizierungen.

## Fazit: Nessus als unverzichtbares Werkzeug in der Cyberabwehr

Wer heute ernsthaft IT-Sicherheit betreibt, kommt an Nessus nicht vorbei. Es ist mehr als ein Scanner – es ist ein Frühwarnsystem, das dir zeigt, wo dein digitaler Zaun Löcher hat, bevor die Angreifer sie finden. In einer Welt, in der neue CVEs im Stundentakt auftauchen und Ransomware-Gruppen operieren wie mittelständische Unternehmen, ist ein proaktiver Ansatz überlebenswichtig.

Nessus liefert dir die Daten, die du brauchst – aber handeln musst du selbst. Wer dieses Tool nur installiert, aber nicht lebt, wird Opfer der eigenen Nachlässigkeit. Wer es aber klug einsetzt, verschafft sich einen echten Sicherheitsvorsprung. Nicht perfekt, aber verdammt nah dran.