Lösungsbroschüre

SOPHOS

SOPHOS ADVISORY SERVICES

Penetrationstests für drahtlose Netzwerke

Identifizieren Sie Schwachstellen in Ihrem drahtlosen Netzwerk und prüfen Sie, wie Angreifer sie ausnutzen könnten

Über drahtlose Netzwerke können sich Mitarbeiter und Gäste an einem physischen Standort bewegen und in Verbindung bleiben. Wireless-Technologien bergen jedoch auch Risiken für Ihr Unternehmen. Falsch konfigurierte Infrastrukturen, nicht autorisierte Access Points und Wireless-Clients können zu unvorhergesehenen Sicherheitsrisiken führen. Penetrationstests für drahtlose Netzwerke bewerten proaktiv die WLAN-Infrastruktur Ihres Unternehmens und ermitteln, wie Angreifer Schwachstellen nutzen könnten, um in Ihr Netzwerk einzudringen.

Stärken Sie die Security Posture Ihres drahtlosen Netzwerks

MAC-Filterung, WEP-Verschlüsselung und Pre-Shared Keys sind keine wirksamen Schutzmaßnahmen mehr, um die Informationen und Clients zu schützen, die Ihr Wireless-Netzwerk verwenden. Angreifer können die meisten dieser Maßnahmen innerhalb von Minuten umgehen oder durchbrechen und so Ihre interne Infrastruktur offenlegen.

Proaktive Tests zur Identifizierung von Geräten, die auf Ihr Netzwerk zugreifen, und zur Bewertung der Sicherheit Ihrer WLAN-Infrastruktur sind unerlässlich, um zu erkennen, wie ein Angreifer in Ihre Umgebung eindringen könnte, bevor Schwachstellen ausgenutzt werden.

Sophos Wireless-Netzwerkpenetrationstests

Der Service „Sophos Wireless-Netzwerkpenetrationstests" bewertet die Sicherheit Ihrer drahtlosen Netzwerke und die Einhaltung der entsprechenden Vorschriften durch Konfigurationsüberprüfungen, technische Tests und das Scannen nach nicht autorisierten Access Points. Die hochqualifizierten Security-Tester von Sophos versuchen, Schwachstellen in der Verschlüsselung, Authentifizierung und Access Control auszunutzen. Dabei gehen sie sowohl „passiv" als auch „aktiv" vor:

- **Passive Prüfung:** Beinhaltet die Überwachung des drahtlosen Traffic, um nicht autorisierte Geräte, unbekannte Access Points und Fehlkonfigurationen zu identifizieren, ohne aktiv eine Verbindung herzustellen.
- **Aktive Prüfung:** Simuliert einen Angreifer, der versucht, Schwachstellen im drahtlosen Netzwerk auszunutzen, indem er die Verschlüsselung knackt, die Authentifizierung umgeht und sich unbefugt Zugriff verschafft.

Leistungen

- Verschaffen Sie sich die Gewissheit, dass sensible Daten, die über Ihre drahtlosen Netzwerke übertragen werden, vor unbefugtem Zugriff und Interception geschützt sind.
- Finden Sie heraus, wie Ihre drahtlosen Verbindungen interne Netzwerke offenlegen.
- Identifizieren Sie Möglichkeiten, wie ein Angreifer in Ihr drahtloses Netzwerk eindringen könnte.
- Stellen Sie sicher, dass nur autorisierte Benutzer auf das Netzwerk zugreifen können.
- Profitieren Sie von umsetzbaren Anleitungen zur Bereinigung.
- Geht über eine Compliance-Bewertung hinaus.

Warum sollten Sie Ihr drahtloses Netzwerk testen?

Indem Sie in regelmäßigen Abständen proaktive Tests durchführen, können Sie die Bedrohung durch Angreifer verringern, die ihre Techniken kontinuierlich anpassen und neue Schwachstellen ausnutzen, um auf vertrauliche Daten zuzugreifen, die über Ihre drahtlosen Netzwerke übertragen werden. Regelmäßige Tests helfen auch dabei, Schwachstellen zu identifizieren, die durch Änderungen in der WLAN-Infrastruktur Ihres Unternehmens entstanden sind, und vermitteln ein realistisches Verständnis Ihres Risikos.

- Identifizieren nicht autorisierte Wireless Access Points und Fehlkonfigurationen
- Stellen sicher, dass Richtlinien zur WLAN-Sicherheit den Best Practices entsprechen
- Reduzieren das Risiko von Datenpannen durch WLAN-Sicherheitslücken
- Bewerten sowohl passive als auch aktive Risiken
- Dienen dazu, nachzuvollziehen, wie Ihre Geräte auf einen böswilligen nicht autorisierten Access Point reagieren

Das finden Sie in Ihrem Report

Kurzfassung: Eine Zusammenfassung der Bewertung, der wichtigsten Ergebnisse und der allgemeinen Empfehlungen.

Prüfmethodik: Beschreibt den Umfang des Einsatzes im Detail und gibt an, welche Tests durchgeführt wurden.

Konzept: Beschreibt die detaillierte Abfolge von Maßnahmen, die die Tester ergriffen haben, um die Bewertungsziele zu erreichen.

Erkenntnisse und Empfehlungen: Einzelheiten zu den wichtigsten Ergebnissen, die während der Bewertung ermittelt wurden, werden nach Schweregrad mit einem Bereinigungsplan und gegebenenfalls zusätzlichen Informationen als Referenz bereitgestellt.

Andere Cybersecurity-Test-Services

Keine einzelne, eigenständige Analyse oder Technik bietet einen umfassenden Überblick über die Security Posture einer Organisation. Für jeden Angriffstest werden die Ziele und annehmbaren Risiken individuell festgelegt. Gemeinsam mit Ihnen kann Sophos ermitteln, welche Kombination aus Analysen und Techniken Sie zur Bewertung Ihrer Security Posture und Kontrollen nutzen sollten, um Schwachstellen zu erkennen.

Leistungen

- Passive Überwachung Ihres drahtlosen Netzwerks, um Schwachstellen in der Sicherheitsarchitektur und in Verschlüsselungsschlüsseln, Konfigurationsfehler und Abwehrmaßnahmen zu ermitteln.
- Hochqualifizierte Tester versuchen, sich Zugang zu verschaffen, indem sie Verschlüsselungsschlüssel knacken und sich als Access Points ausgeben, um Benutzerzugangsdaten zu stehlen.
- Umfassende Berichte liefern detaillierte Ergebnisse und Empfehlungen aus der Bewertung.
- Die Regeln für den Einsatz werden im Voraus während der Einführungssitzungen festgelegt, damit Sie Sicherheit haben.
- Wählen Sie den Serviceumfang, der Ihren Anforderungen entspricht, um einen oder mehrere physische Standorte abzudecken.
- Remote-Tests – die die gleiche Qualität wie ein Vor-Ort-Test liefern – bieten Flexibilität bei der Planung und ermöglichen Tests an Orten, die normalerweise aus Sicherheitsgründen oder wegen eingeschränktem Zugang nicht zugänglich sind.
- Optionale Vor-Ort-Tests verfügbar – ideal für große oder verteilte Standorte.

Mehr erfahren:
sophos.de/advisory-services

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2025-06-05 BRDE (MP)

SOPHOS