Lösungsbroschüre

SOPHOS

SOPHOS ADVISORY SERVICES

Web Application Security Assessment

Ausnutzbare Schwachstellen finden und unbekannte Risiken ermitteln, bevor Angreifer zuschlagen

Schützen Sie Ihre externen und internen Webanwendungen, indem Sie Sicherheitslücken und verborgene Risiken aufdecken. Das stärkt Ihre Cyberabwehr, schützt Ihre sensiblen Daten und weist nach, wie ernst Sie die Compliance nehmen.

Das gute Gefühl, dass Ihre Webanwendungen sicher sind

Webanwendungen sind geschäftskritische Tools, die wertvolle Daten verarbeiten, übertragen und speichern. Sie helfen Ihrem Unternehmen, seine operativen Ziele zu erreichen, und spielen auch eine wichtige Rolle, wenn es darum geht, Ihre Reputation zu schützen. Es ist daher für eine gute Security Posture unerlässlich, Ihre Webanwendungen zu schützen. Der proaktive erste Schritt, um die Resilienz Ihres Unternehmens zu steigern: die Sicherheit der Webanwendungen von erfahrenen Testern überprüfen lassen, um Schwachstellen aufzudecken.

Sophos Web Application Security Assessment Service

Der Sophos Web Application Security Service findet Schwachstellen wie unzureichende Access Controls, Fehlkonfigurationen bei Sicherheitseinstellungen oder Probleme im Anwendungsdesign. Mit unserem umfassenden Wissen über die globale Bedrohungslandschaft und die Taktiken, Techniken und Prozesse von Angreifern prüfen wir, wie angreifbar Sie sind und wie Sie Ihre Webanwendungen noch sicherer machen können.

Bei Sophos Web Application Security Assessments werden hauptsächlich zwei Bereiche betrachtet:

- **Externe Anwendungen:** Ihre Webanwendungen sind Ihre Verbindung ins Internet und zu Ihren (potenziellen) Kunden, Partner und Lieferanten. Sie spielen eine große Rolle für das Kundenbewusstsein, Ihren Umsatz und den Vertrieb und sind deshalb ein attraktives Angriffsziel. Beim Testen externer Anwendungen simulieren wir anonyme Angreifer oder Angreifer, die sich für authentifizierten Zugriff registrieren oder ein Abo abschließen.
- **Interne Anwendungen:** Angreifer nehmen auch Anwendungen ins Visier, die über Ihr internes Netzwerk erreichbar sind. Diese Applikationen sind wichtig für Ihre Geschäftsprozesse und verarbeiten sensible Informationen wie geistiges Eigentum, Kundendaten, Mitarbeiterinformationen und Vertriebsdaten. Beim Testen interner Anwendungen simulieren wir verärgerte Mitarbeiter oder Angreifer mit gestohlenen Zugangsdaten, die sie sich über ein Datenleck oder einen Phishing-Angriff beschafft haben.

Sophos passt jede Sicherheitsprüfung individuell an das jeweilige Unternehmen an. Die branchenweit besten Sicherheitstester gehen nach unserer zielorientierten Methodik vor und nutzen dabei unsere selbstentwickelten Taktiken sowie die Bedrohungsdaten des Sophos-X-Ops-Threat-Intelligence-Teams. Dieses Team umfasst u. a. die Counter Threat Unit (CTU), die für ihre Expertise im Bereich Advanced Persistent Threats (APTs) und staatlich initiierte Cyberangriffe bekannt ist.

Vorteile

- Webanwendungen werden sicherer
- Praktische Empfehlungen zur Verbesserung der Sicherheit
- Weniger Risiko, mehr betriebliche Effizienz
- Vertrauen Ihrer Kunden, Mitarbeiter und Geschäftspartner wird gewahrt
- Compliance-Vorgaben werden eingehalten (z. B. PCI-DSS).

Webanwendungen testen lassen, um das Sicherheitsrisiko zu minimieren

Die Sophos-Tester prüfen Ihre Webanwendungen mit einer Kombination aus automatisierten und manuellen Testtechniken, um Schwachstellen zu finden, bevor Angreifer sie ausnutzen. Sie agieren dabei wie externe Angreifer und böswillige Nutzer, indem sie die Anwendung sowohl anonym als auch authentifiziert angreifen. Auf diese Weise decken wir eine große Bandbreite ab, von breitangelegten Kampagnen bis hin zu ausgefeilten Anwendungslogik-Angriffen auf geschützte Ressourcen.

Nach dem Test stellt Sophos detaillierte Hinweise zur Behebung bereit, mit denen Sie die ermittelten Konfigurationsfehler, bekannte und potenzielle Schwachstellen, Access-Control-Probleme und andere ausnutzbare Defizite korrigieren können.

Das finden Sie in Ihrem Report

Kurzfassung: Für Stakeholder ohne technisches Know-how – Führungskräfte, Prüfer, Vorstand und andere wichtige Personen.

Detaillierte Ergebnisse: Die Findings im Detail mit zugehörigen Empfehlungen für Ihre technische Teams.

Eingesetzte Methodik: Informationen zum Umfang des Einsatzes und zu den durchgeführten Tests.

Empfehlungen: Detaillierte Ergebnisse, Links zu Webseiten mit weiteren Informationen und Empfehlungen zur Behebung oder Risikominderung. Die Tester stellen gegebenenfalls Nachweise zu ihren Ergebnissen und, wenn möglich, ausreichende Informationen bereit, um die Ergebnisse anhand öffentlich zugänglicher Tools zu replizieren.

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

- Prüfung von Webanwendungen zum Ermitteln von Schwachstellen
- Verbesserung der Security Posture mit Hinweisen und Empfehlungen von Experten
- Unter anderem Test auf die 10 kritischsten OWASP-Anwendungssicherheitslücken
- Unterstützung für praktisch alle Web-Development-Frameworks, -Plattformen und -Infrastrukturen
- Gründliche Prüfung nicht nur der Anwendung, sondern auch, ob Angreifer auf das Netzwerk oder die Daten dahinter zugreifen könnten

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