Lösungsbroschüre

SOPHOS

Sophos Advisory Services

Proaktive Reduzierung von Risiken und Resilienz angesichts sich ständig weiterentwickelnder Cyber-Bedrohungen

Maßgeschneiderte, von Experten durchgeführte Security Assessments

Die digitale Transformation setzt stetig neue Anforderungen, KI wird immer präsenter und Cyber-Bedrohungen entwickeln sich ständig weiter. Deswegen sehen zukunftsorientierte Unternehmen Cybersecurity nicht nur als eine Liste wichtiger Technologien an, die es zu implementieren gilt, sondern auch als strategische Priorität. Fortgeschrittene Angreifer, behördliche Kontrollen und die Erwartungen von Stakeholdern erfordern einen proaktiven und umfassenden Ansatz zum Schutz digitaler Assets. Die Sophos Advisory Services bieten unabhängiges Fachwissen, Erfahrung und maßgeschneiderte Strategien, um systemische Schwachstellen zu identifizieren, Abwehrmechanismen zu stärken und die Widerstandsfähigkeit Ihres Unternehmens zu verbessern.

Mithilfe realer, von Bedrohungsakteuren verwendeter Taktiken, Techniken und Prozesse (TTPs) testen unsere hochqualifizierten Sicherheitsexperten Ihre Netzwerke, Systeme und Mitarbeiter, um Ihr Unternehmen in unterschiedlichen Bereichen zu unterstützen:

- Identifizierung von Schwachstellen, bevor Angreifer sie ausnutzen können
- Stärkung Ihrer Abwehrmaßnahmen gegen komplexe Bedrohungen
- Einhaltung gesetzlicher Vorschriften
- Bewertung, wie gut Sie im Ernstfall auf Vorfälle reagieren können
- Aufbau von Vertrauen bei Kunden, Partnern und Stakeholdern

Proaktives Stärken von Abwehr und Security Posture

Penetrationstest (Pentests)

Penetrationstests simulieren Cyberangriffe aus der Praxis, um Schwachstellen in Systemen, Netzwerken und Anwendungen zu erkennen. Erfahrene Tester (ethische Hacker) versuchen, Schwachstellen auszunutzen, um zu zeigen, was für einen Angreifer möglich wäre.

Es gibt zwei wesentliche Typen von Penetrationstests: Bei externen Penetrationstests liegt der Schwerpunkt auf Systemen, auf die über das Internet zugegriffen werden kann, z. B. Websites, VPNs und öffentlich zugängliche Services. Bei diesen Tests wird simuliert, wie ein Angreifer Ihren Perimeter von außerhalb durchbrechen möchte. Interne Penetrationstests simulieren eine interne Bedrohung oder einen Angreifer, der den Perimeter bereits durchbrochen hat. Der Schwerpunkt liegt auf Systemen, Anwendungen und Daten im internen Netzwerk.

Warum sie wichtig sind:

- Identifizieren versteckte Schwachstellen, die bei Routine-Scans möglicherweise übersehen werden
- Liefern konkrete Empfehlungen zur Stärkung der Abwehrmaßnahmen
- Halten unterschiedliche Vorschriften und Normen ein (z. B. PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2)
- Weisen das Engagement für proaktives Risikomanagement nach
- Bieten umfassende Abdeckung sowohl für Perimeter- als auch für interne Sicherheitsrisiken

Wichtige Fragen, die damit beantwortet werden können:

- Wo befinden sich die kritischsten Schwachstellen in unserer Infrastruktur?
- Wie leicht könnte ein Angreifer unsere Abwehrmaßnahmen von außen überwinden?
- Welche Risiken bestehen innerhalb unseres Netzwerks, wenn ein Angreifer Zugriff erhält?
- Was sind die möglichen Folgen eines erfolgreichen Angriffs?
- Welche Maßnahmen können wir ergreifen, um die festgestellten Schwachstellen zu beheben?

Penetrationstests für drahtlose Netzwerke

Bei Penetrationstests für drahtlose Netzwerke wird die Sicherheit der WLAN-Netzwerke und -Infrastruktur eines Unternehmens bewertet und die Einhaltung der entsprechenden Vorschriften überprüft. Tester versuchen, Schwachstellen in der Verschlüsselung, Authentifizierung und Access Control auszunutzen.

Bei Penetrationstests für drahtlose Netzwerke unterscheiden wir zwischen zwei verschiedenen Prüfmethoden. Bei der passiven Prüfung wird der drahtlose Traffic überwacht, um nicht autorisierte Geräte, unbekannte Access Points und Fehlkonfigurationen zu identifizieren, ohne aktiv eine Verbindung herzustellen. Die aktive Prüfung simuliert einen Angreifer, der versucht, Schwachstellen im drahtlosen Netzwerk auszunutzen, indem er die Verschlüsselung knackt, die Authentifizierung umgeht und sich unbefugten Zugriff verschafft.

Warum sie wichtig sind:

- Schützen sensible Daten, die über drahtlose Netzwerke übertragen werden
- Identifizieren unberechtigte 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

Wichtige Fragen, die damit beantwortet werden können:

- Können unbefugte Benutzer auf unsere drahtlosen Netzwerke zugreifen?
- Verwenden wir starke Verschlüsselung und sichere Authentifizierungsmethoden?
- Sind nicht autorisierte Geräte mit unserem Netzwerk verbunden?
- Kann ein Angreifer unsere WLAN-Sicherheitsvorkehrungen umgehen?
- Welche Maßnahmen können wir ergreifen, um die Sicherheit von drahtlosen Netzwerken zu verbessern?

Web Application Security Assessments

Webanwendungen verarbeiten häufig wichtige Geschäfts- und Kundendaten und sind daher ein bevorzugtes Ziel für Angreifer. Web Application Security Assessments bieten Ihnen die Gewissheit, dass Ihre Webanwendungen sicher sind, indem sie sich auf häufige Schwachstellen wie SQL-Injection, Cross-Site-Scripting (XSS) und fehlerhafte Authentifizierung konzentrieren.

Diese Prüfungen können Black-Box-Tests umfassen, bei denen der Tester einen externen Angreifer ohne Vorkenntnisse über die inneren Abläufe der Anwendung simuliert, oder White-Box-Tests, bei denen der Tester vollen Zugriff auf den Quellcode und die Architektur hat, was eine tiefere Analyse potenzieller Schwachstellen ermöglicht.

Warum sie wichtig sind:

- Schützen Kunden- und Unternehmensdaten, die von Webanwendungen verarbeitet werden
- Identifizieren Programmierungs- und Konfigurationsfehler, die das Risiko erhöhen
- Unterstützen die Einhaltung von Standards wie OWASP Top 10 und PCI DSS
- Reduzieren das Risiko von Websitemanipulationen, Datenschutzverstößen und Reputationsschäden
- Bieten sowohl eine Außenperspektive als auch eine eingehende Analyse der Anwendungssicherheit

Wichtige Fragen, die damit beantwortet werden können:

- Sind unsere Webanwendungen anfällig für gängige Angriffsmethoden?
- Sind sensible Daten aufgrund von Programmierfehlern oder Fehlkonfigurationen gefährdet?
- Können externe Angreifer Schwachstellen ausnutzen oder gibt es tiefere Probleme im Code?
- Wie können wir die Benutzerauthentifizierung und die Sitzungsverwaltung sicherstellen?
- Welche Abhilfemaßnahmen sind erforderlich, um Schwachstellen in Webanwendungen zu beheben?

Zusammenfassung der Security Assessment Services

Prüfungstyp	Schwerpunkt	Beantwortet die folgenden wichtigen Fragen	Beispielszenarios
Penetrationstest (Pentests)	Infrastruktur, Systeme und Netzwerke	Wo liegen die Schwachstellen? Wie kann ein Angreifer unsere Abwehrmaßnahmen überwinden?	Extern: Testen von öffentlich zugänglichen Websites und Services; Intern: Testen interner Access Controls und Rechteausweitung
Penetrationstests für drahtlose Netzwerke	WLAN-Sicherheit, Verschlüsselung, Access Controls	Ist unser WLAN sicher? Gibt es nicht autorisierte Geräte?	Testen der WLAN-Sicherheit im Büro; Identifizieren von unberechtigten Access Points; Versuch der Herstellung von unbefugten Verbindungen
Web Application Security Assessment	Webanwendungen, Programmierfehler, Authentifizierung	Sind unsere Apps sicher? Sind sensible Daten gefährdet? Wie können wir Schwachstellen beheben?	Testen von Kundenportalen, E-Commerce-Websites und internen Webanwendungen; Identifizieren von SQL-Injection, XSS oder Authentifizierungsfehlern

Weitere Cybersecurity Testing Services

Keine einzelne, eigenständige Analyse oder Technik bietet einen umfassenden Überblick über die Sicherheit einer Organisation. Jeder Angriffstest hat eigene Ziele und annehmbare Risiken. 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.

Mehr erfahren:
sophos.de/advisory-services

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

2025-05-30 BRDE (MP)

SOPHOS