Lösungsbroschüre

SOPHOS

SOPHOS ADVISORY SERVICES

Penetrationstests

Praxisnahe Tests Ihrer Sicherheitsmaßnahmen

Ermitteln Sie Schwachstellen und testen Sie Ihre Sicherheitsmaßnahmen mit unabhängiger Expertise, Erfahrung und angepassten Strategien. So verbessern Sie Ihre Security Posture, reduzieren Risiken, erleichtern die Compliance und steigern Ihre betriebliche Effizienz.

Proaktives Stärken von Abwehr und Sicherheits-Status

Unbefugter Zugriff auf Unternehmensressourcen, die Ausbeutung bestehender und neuer Sicherheitslücken und die Ausnutzung von Fehlkonfigurationen und mangelhaften Sicherheitsrichtlinien – all das sind ernsthafte Sicherheitsrisiken. Diese müssen beseitigt werden, bevor Angreifer sie ausnutzen können. Dafür müssen Sie wiederum umfassend prüfen können, ob Anwendungen, Netzwerke und Systeme einem Sicherheitsrisiko ausgesetzt sind. Zwar bilden Schwachstellen-Scans und -Analysen eine gute „Vorstufe" der Auswertung, um Lücken und Schwachstellen in Ihrem Netzwerk zu ermitteln. Es sind jedoch tiefergehende Tests erforderlich, um dahinterzukommen, wie ein Angreifer Zugriff auf Ihre Umgebung erhalten und diese Systeme als Basis für Angriffe nehmen würde, um tief in die Weiten des Netzwerks einzutauchen.

Penetrationstest-Services von Sophos

Mit Penetrationstests – oder „Pentests" – ermitteln und weisen Sie Cybersecurity-Schwachstellen nach und beantworten die Frage: „Könnte ein Angreifer in mein Netzwerk eindringen?" Die Tests 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:

- **Externe Penetrationstests:** Der Schwerpunkt liegt auf Systemen, auf die über das Internet zugegriffen werden kann, z. B. Websites, VPNs und öffentlich zugängliche Dienste. 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.

Sophos geht jeden Penetrationstest individuell für die jeweilige Organisation an. Die branchenweit besten Sicherheitstester gehen nach unserer zielorientierten Methodik vor und nutzen dabei unsere selbst entwickelten Taktiken sowie die Bedrohungsdaten des Sophos-X-Ops-Threat-Intelligence-Teams. Dieses Team umfasst u. a. die Counter Threat Unit (CTU), die für ihre Bedrohungsdaten und ihre Forschung zu Advanced Persistent Threats (APTs) und staatlich initiierten Cyberangriffen bekannt ist.

Leistungen

- Anhand von Tests Ihrer internen und externen Sicherheitskontrollen, u. a. der Schutzmaßnahmen für wichtige Systeme und Ressourcen, erhöhen Sie die Sicherheit.
- Und über ein Bedrohungsmodell und Kontext, die beide auf Ihre individuelle Umgebung abgestimmt sind, werden spezifische Testziele erreicht.
- Sie erhalten Empfehlungen zu den besten Maßnahmen für die Risikominderung.
- Sie halten unterschiedliche Vorschriften und Normen ein, darunter PCI DSS, HIPAA, GDPR, NIS, ISO 27001, SOC 2.
- Sie erhalten Insights aus aktuellen Bedrohungsdaten des Sophos-X-Ops-Threat-Intelligence-Teams.
- Sie können Ihre Risiken für den Praxisbetrieb ermitteln.

Simulation komplexer Angriffe und Tests von Sicherheitsmaßnahmen

Organisationen setzen auf regelmäßige Penetrationstests – und das nicht nur, um Branchenvorschriften einzuhalten, sondern auch, um in der immer komplexeren und sich weiterentwickelnden Bedrohungslandschaft einen Schritt voraus zu sein. Wenn Penetrationstests regelmäßig durchgeführt werden, können Organisationen mit Angreifern Schritt halten, die ihre Techniken stets anpassen, um neue Schwachstellen auszunutzen. Durch regelmäßige Tests können auch Schwachstellen ermittelt werden, die im Rahmen von Änderungen an der Infrastruktur, Anwendungen oder Drittanbieter-Integrationen eingeführt wurden. Darüber hinaus erhalten Organisationen durch Penetrationstests einen realistischen Einblick in riskante Schwachstellen und konkrete Strategien zur Bereinigung. Außerdem können sie Sicherheitsverbesserungen im Laufe der Zeit aussagekräftig nachverfolgen und messen.

Vorteile von Penetrationstests:

- **Proaktive Reduzierung von Risiken:** Bei Organisationen, die regelmäßig Penetrationstests durchführen, kommt es 50 % seltener zu Sicherheitsvorfällen. Zudem werden die Gesamtkosten für die Bearbeitung von Sicherheitsvorfällen um 30 % reduziert.[1]
- **Unterstützung bei der Compliance:** Vorschriften und Normen wie PCI DSS, HIPAA und ISO 27001 setzen Penetrationstests oft voraus. Tatsächlich geben 73 % der Organisationen Compliance als Treiber für Penetrationstests an.[2]
- **Kosteneinsparungen:** Die durchschnittlichen Kosten einer Datenpanne belaufen sich auf 4,45 Millionen $.[3] Durch Penetrationstests können Schwachstellen allerdings für nur einen Bruchteil dieser Kosten behoben werden.
- **Kundenvertrauen:** 65 % der Kunden geben an, dass sie eher einem Unternehmen vertrauen würden, das starke Cybersecurity-Maßnahmen nachweisen kann.[4]

Stellen Sie Ihre Mitarbeiter auf die Probe

Durch künstliche Intelligenz erreicht die Authentizität von Phishing-Angriffen neue Höhen, da nun sehr raffinierte und überzeugende Nachrichten möglich sind, die sich auf den ersten Blick nur schwer als Angriff erkennen lassen. Im Gegensatz zu traditionellen Phishing-E-Mails voller Rechtschreibfehler und generischen Inhalten können beim KI-basierten Phishing personalisierte, kontextrelevante Nachrichten generiert werden, die auf bestimmte Personen oder Organisationen abzielen. Infolgedessen sehen sich sowohl Sicherheitsteams als auch Benutzer mit neuen Herausforderungen konfrontiert, wenn es darum geht, Phishing-Angriffe zu erkennen und ihre Organisation davor zu schützen. Deswegen sind kontinuierliche Schulungen unerlässlich.

Unser Penetrationstest-Programm kann mit simulierten Phishing-Angriffen kombiniert werden, um zu prüfen, wie gut Ihre Mitarbeiter Phishing-Versuche erkennen und darauf reagieren können.

Leistungen

- Angepasste Regeln zu Anforderungen und Leistungen, u. a. Prüfung der Zielsysteme für geschäftskritische Daten
- Abschlussberichte mit detaillierten Ergebnissen und einer Kurzfassung
- Optionen für lokale und Remote-Tests
- Auswahl zwischen externen Penetrationstests, internen Penetrationstests und Simulationstraining zu Phishing-Angriffen, um ein Szenario mit gemischten Bedrohungen für Ihren spezifischen Anwendungsfall zu schaffen
- Testergesteuerter, manueller Prozess, bei dem von Bedrohungsakteuren angewandte Taktiken zum Einsatz kommen
- Zielorientierte Methodik, durch die sichergestellt wird, dass Systeme im breiteren Kontext ihrer Umgebung getestet werden

Das ist in Ihrem Report enthalten

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

Detaillierte Ergebnisse: Für technische Teams, um detaillierte Ergebnisse und Empfehlungen bereitzustellen.

Eingesetzte Methodik: Definiert den Umfang des Einsatzes und gibt an, welche Tests durchgeführt wurden.

Konzept: Beschreibt die Abfolge von Aktionen der Tester, um die Ziele des Einsatzes zu erreichen und beim Verständnis gemischter Bedrohungen und/oder abhängiger Phasen zu helfen.

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

Phishing-Ergebnisse (falls vorhanden): Gibt die angewendeten Phishing-Angriffe und deren Erfolgsrate an.

Andere Cybersecurity-Test-Services

Keine einzelne, eigenständige Analyse oder Technik bietet einen umfassenden Überblick über die Security Posture 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

[1]Ponemon Institute [2]SANS Institute [3]IBM [4]PwC

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

© Copyright 2025. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

2025-06-05 BRDE (MP)

SOPHOS