Trustwave®

Managed Security Testing

PENETRATION-TESTS IN NEUER FORM

Setzen Sie auf die unvergleichlichen Penetration-Tests der Trustwave SpiderLabs für Applikationen und Netzwerke – mit dem preisgekrönten Trustwave-Portal nun exakt nach Ihrem Bedarf und in Ihrem Zeit- und Kostenrahmen!

Angriff ist die beste Verteidigung

Defensive Maßnahmen allein können Ihre Anwendungen oder Netzwerke nicht schützen. In einer klug geführten Organisation versteht man die Bedeutung proaktiver, offensiver Sicherheitstests für die Strategie zum Management der Schwachstellen, um die Abwehr effizient zu organisieren. Ein Penetration-Test für Anwendungen oder Netzwerke erfüllt diese Offensivanforderungen durch die exakte Bewertung der Gefährdung des Ziels. Offensive Tests beleuchten die Sicherheitsmängel, die Ihnen vielleicht nicht bewusst sind, um umfassenden Schutz zu gewährleisten.

Mit Trustwave Managed Security Testing (MST) bucht Ihr Security-Team die Unterstützung eines unserer Experten aus den Trustwave SpiderLabs. Sie verwalten die Penetration-Tests dabei in eigener Regie über das preisgekrönte Trustwave- Portal. So haben Sie die notwendige Kontrolle, um die Tests nach ihren zeitlichen und finanziellen Vorstellungen nachhaltig durchzuführen zu lassen.

Zeit. Sie melden Ihre Zielnetzwerke und -anwendungen an und wählen den Testzeitpunkt nach Bedarf aus.

Budget. Als Subscription Service verfügbar, können Sie ein jährliches (oder mehrjähriges) Testbudget festlegen, quartalsweise Beiträge zahlen und ihren Kontostand einsehen.

Nachhaltigkeit. Je nach gewählter Stufe besteht MST aus einem tiefgehenden, manuellen Penetration-Test für ein Netzwerk oder eine Anwendung sowie vier jährlichen Tests.

Budget- und Planungsfreundlich – Sie zahlen nur für Leistungen

Im Trustwave MST-Portal melden Sie eine Zielstufe an. Jede Stufe umfasst einen anderen Grad an Tests, die Sie risikogerecht für das Netzwerks, die Anwendung und die relevanten Daten auswählen, die gespeichert oder übertragen werden. Die Online-Auswahl der Stufen erläutert klar die zugehörigen Tests und den Preis. Die Bezahlung erfolgt automatisch.

Das Trustwave MST-Subscription-Modell verhindert unübersichtliche Kostenentwicklung. Es hilft Ihnen bei der Vorhersage ihres jährlichen Budgets und bei der effizienten Zuweisung Ihrer Mittel, ohne dass Sie immer neue Verträge aushandeln müssten.

Achtung Lücke! – Quartalsweise Maintenance

Wenn Sie ein Netzwerksegment oder eine Anwendung angemeldet haben, stellt Trustwave MST sicher, dass das Ziel regelmäßig getestet wird. Die Zeitspanne zwischen tiefgehenden Penetration-Tests kann eine günstige Gelegenheit für Cyber-Kriminelle darstellen. Quartalsweise durchgeführte Wartungstests füllen diese Lücken und warnen Sie vor Schwachstellen, die sich aus Änderungen der Netzwerkarchitektur oder Aktualisierungen im Code einer Anwendung ergeben. Trustwave MST bewertet nicht nur den Zustand eines Netzwerks oder einer Anwendung zum jeweils aktuellen Zeitpunkt, sondern führt die Tests kontinuierlich durch. Dies gewährleistet eine sichere Umgebung auch dann, wenn sich diese aufgrund geschäftlicher Anforderungen ändert oder weiter entwickelt.

Unerreichte Erfahrung

Die Dienste rund um die Penetration-Tests von Trustwave werden von den SpiderLabs® bereitgestellt – einem hoch spezialisierten Team des Unternehmens, das sich auf Forensik, White-Hat-Hacking und Anwendungssicherheit spezialisiert hat. Das Team führte weltweit bereits über 1.500 forensische Untersuchungen, tausende White-Hat-Hacks und Tests zur Anwendungssicherheit durch. Unser manueller Prozess geht weit über das hinaus, was automatische Bewertungs-Tools in Form von generischen Rückmeldungen bieten können, und vermeidet deren Fehlalarme und Beschränkungen.

In unserem Team arbeiten einige der weltweit führenden ITSecurity-Experten. Das Team bringt fachliche Erfahrungen aus den Bereichen der Corporate Information Security mit, von der Sicherheitsforschung bis hin zur Strafverfolgung. Die Mitglieder der Trustwave SpiderLabs werden regelmäßig als Referenten zu Sicherheitskonferenzen auf der ganzen Welt eingeladen.

Portalbasierte Sicherheitstests nach Bedarf

- Einfache Zeitplanung: Melden Sie das Ziel einfach an und wählen Sie ein passendes Datum und einen Zeitraum für den Test aus.
- Überblick über das Budget: Betrachten Sie Ihren verbleibenden Kontostand und den Verlauf Ihrer Buchungen.
- Zentrale Dashboards: Vereinfachen Sie die Verwaltung von Penetration-Tests mit einfachen Zugängen zum Projekt- und Teststatus sowie zu den Ergebnissen.
- Projekt- und Testdetails: Zeigt die Beziehung zwischen Projekten und Tests an, um Sicherheitsprogramme der Organisation einfacher zu organisieren.
- Detaillierte Ergebnisse: Belege einschließlich Bildern und Videos bieten detaillierte Hintergrundinformationen zu erkannten Schwachstellen. Spezielle Präsentationsansichten erklären die Sicherheitsrisiken dem Führungspersonal.
- Berichte über Angriffssequenzen: Grafische Darstellung der Beziehungen zwischen mehreren Schwachstellen und vereinfachte Angriffsszenarien für ein schnelles Verständnis.
- Benachrichtigung in Echtzeit: Benachrichtigungen werden sofort per E-Mail versandt, wenn Tests ihren Status ändern und Schwachstellen identifiziert oder behoben werden.
- Sichere Dokumentenübertragung: Sichere Weitergabe sensibler Dateien wie Code, Netzwerkdiagramme, Medien usw.
- Selbstverwaltete Konten: Erstellen Sie neue Nutzer und delegieren Sie Berechtigungen.
- Virtuelle Patches für Web Application Firewall (WAF): Virtuelle Patches, die von den SpiderLabs individuell erstellt werden, blockieren Angriffe sofort.
- Grafiken zur Bedrohung von Daten: Erkennen Sie auf detaillierten Grafiken, welche Daten während eines Tests offengelegt wurden.

UMFANG VON NETZWERKTESTS

Lokales Netzwerksegment	Unternehmensinfrastruktur
VLAN Hopping	Active Directory/LDAP
ARP-Spoofing	Quellcode-Repositories
Unsichere Netzwerkprotokolle	Infrastruktur-Services
Man in the Middle (MITM)	Datenbanken
Netzwerkinfrastruktur	Mainframes
Router/Switches/Lastausgleich	Middleware
Remote Access-Geräte	SSO
Gemeinsame Services	Remote Administration
HTTP	Backup
SMTP	File Sharing
POP/IMAP	Zugriffskontrolle
FTP	Betriebssystem
Einfache Webseiten	Betriebssystemspezifische Services
XSS	Weitergehende taktische Maßnahmen
SQL-Injection	Nicht-IP-Protokolle
Known Command Injection	Mehrstufige Angriffsvektoren

Leistungsfähige Berichterstattung

Das Trustwave SpiderLabs-Portal bietet eine Vielzahl an Berichtsvarianten, um die Anforderungen an internes Reporting, Audits, Compliance und andere Maßnahmen zu erfüllen. Dazu zählen:

- Online-Berichte und -Metriken: Schwachstellendaten werden im Portal für jeden Test erfasst, einschließlich des Risikos, des Fortschritts der Abhilfebemühungen, der kompromittierten Daten und des Status, auch über Projektgrenzen hinweg. Ein vollständiger Zugriff auf den Verlauf der Testergebnisse für Trendanalysen liefert Ihnen eine Übersicht über die Sicherheitslage des Unternehmens im Zeitverlauf.
- Voreingestellte Berichte: Die Online-Reports umfassen ein Executive Summary, eine Zusammenfassung der Empfehlungen, detaillierte Informationen zu den Testmethoden und Ergebnissen. Ein PDF-Export ist ebenfalls verfügbar.
- Individuelle Berichte: Anwender können individuelle Berichte auf verschiedene Arten erstellen, beispielsweise nach Risiko, nach Status der Ergebnisse, über mehrere Projekte hinweg, nach eigenen Kriterien, für einzelne Tests und Testvarianten.
- Common Vulnerability Scoring System (CVSSv2) für alle Schwachstellen: CVSS bietet eine Standardmethode zur Bewertung von Risiken und zur Priorisierung von sicherheitskritischen Schwachstellen, um die Abhilfe zu optimieren.
- Berichte in verschiedenen Formaten: Datenexport in PDF, Excel, XML, CSV, HTML und andere.

UMFANG VON ANWENDUNGSTESTS

Authentifizierung und Autorisierung	Kryptographie
Unbegrenzte Anmeldeversuche	Schwache Algorithmen
Umgehung der Authentifizierung	Schlechtes Key Management
Umgehung der Autorisierung	Logikfehler
Schwache und Standardpasswörter	Missbräuchliche Nutzung
Session Management	Umgehung des Workflow
Vorhersehbarkeit der Session-Kennung	Datenschutz
Übernahme einer Session	Transport
Wiederauflage einer Session	Speicherung
Festhalten einer Session	Offenlegung von Informationen
Fehlerhaftes Auslaufen einer Session	Verzeichnisindizierung
Injection	Detaillierte Fehlermeldungen
SQL-Injection	HTML-Kommentare
Cross-Site-Scripting	Standardinhalte
LDAP-Injection	Variablenkontrolle
HTML-Injection	Stack-basiert
XML-Injection	Heap-basiert

Erfahren Sie mehr unter trustwave.com

Trustwave ist ein führender Anbieter von Sicherheitslösungen für Compliance, Web-, Anwendungs-, Netzwerk- und Datensicherheit, die als Cloud, Managed Security Services, Software und Appliance zur Verfügung stehen. Organisationen, die sich mit dem heutigen, fordernden Sicherheitsumfeld auseinander setzen müssen, erhalten von Trustwave einen einmaligen Ansatz mit umfassenden Lösungen, die das TrustKeeper®-Portal und andere proprietäre Sicherheitslösungen umfassen. Trustwave hat bereits hunderte Organisationen, von Fortune-500-Unternehmen und großen Finanzinstitutionen bis hin zu kleinen und mittleren Einzelhändlern, unterstützt, ihre Compliance zu managen und die Netzwerkinfrastruktur, Kommunikation und geschäftskritische Datenbestände zu schützen. Trustwave hat seinen Hauptsitz in Chicago und weltweite Filialen.

Trustwave®

Weitere Informationen finden Sie unter: www.trustwave.com

MIDS_PCI3.1_1015