METHODIK- UND SERVICE-LEVEL-VERGLEICH

Security Testing Services

September 2019

Die Trustwave Security Testing Services (STS) geben Ihnen die Möglichkeit, Probleme und Schwachstellen in Netzwerken, Anwendungen und Datenbanken zu identifizieren. Sie können feststellen, wo und wie Daten kompromittiert werden könnten, und zudem Risiken messen und verwalten. Die STS verbinden Vulnerability Scans und Penetrationstests zu einem Rundum-Service für Schwachstellenbewertung und Security Testing.

Dieses Dokument bietet eine Übersicht über die Security-Testing-Methodik sowie einen Service-Level-Vergleich der Testing- und Scanning-Services.

Methodik der Penetrationstests

Die Penetrationstests (Pentesting) werden von Trustwave SpiderLabs® durchgeführt, einer Gruppe hochqualifizierter Forscher, Penetrationstester und Ethical Hacker. Die bewährte Methodik dieser Penetrationstests umfasst:

- Untersuchung
- Manuelle Tests
- Reporting
- Support

Untersuchung

Im ersten Schritt wird vollständig ermittelt, was genau getestet werden soll. In dieser Phase der Informationserfassung werden die potentiellen Ziele identifiziert und der Testumfang – von einer bestimmten Anwendung bis hin zu Netzwerkbereichen – festgelegt. Beim Testen einer Anwendung muss deren Struktur verstanden, der zu erreichende Detaillierungsgrad bestimmt und die Informationsarchitektur der Anwendung identifiziert werden.

Bei der Prüfung eines Netzwerkbereichs werden erste nicht-destruktive Tests durchgeführt, um die Verfügbarkeit eines Hosts zu prüfen. Dies erfolgt meist durch Ping-Sweeps und die Identifizierung gemeinsamer Ports. Sobald Trustwave SpiderLabs® feststellt, dass ein Host erreichbar ist, wird versucht, alle Ports (TCP und UDP) zu identifizieren. Sobald alle Testparameter umfassend ermittelt wurden und die Untersuchung abgeschlossen ist, kann die manuelle Testphase beginnen.

Manuelle Tests

Auf den Identifizierungsprozess folgen gründliche Tests, um Probleme und Schwachstellen in den zu testenden Anwendungen oder Netzwerkbereichen zu ermitteln. Anschließend wird versucht, diese Schwachstellen auszunutzen, um Zugriff auf einen Host oder eine Anwendung zu erlangen. Sobald SpiderLabs® Fuß gefasst hat, versuchen die Experten die Auswirkungen eines Problems zu ermitteln, indem sie weiter in das System eindringen.

Vulnerability Scans untersuchen ein System auf mögliche Schwachstellen oder unsichere Konfigurationen. Im Anschluss erfolgen Penetrationstests, bei denen die SpiderLabs®-Experten mit Ihrem Einverständnis versuchen, sich in Ihr Netzwerk oder Ihre Anwendung zu hacken. Dabei nutzen die Spezialisten dieselben Tools, Taktiken und Techniken wie moderne Cyberkriminelle und gehen nach folgendem High-Level-Workflow vor:

- Erkundung des Systems
- Identifizierung von Schwachstellen
- Bestätigung von Schwachstellen
- Versuch der Datenextraktion
- Durchführung einer umfassenden Qualitätssicherung (QS)

Bei der Feststellung großer oder kritischer Schwachstellen werden Sie umgehend gewarnt. Es werden keine Denial-of-Service-Tests (DoS) mit Unternehmensassets durchgeführt. Sobald der Tester seinen Bericht fertiggestellt hat, wird dieser der QS vorgelegt. Die QS wird von einem leitenden Teammitglied durchgeführt, um zu gewährleisten, dass Trustwaves strikte Prozesse und Methoden angewandt werden.

Reporting

Sie erhalten während des gesamten Testprozesses dynamisch Einsichten in die Ergebnisse. Nach Abschluss des Reportings werden Ihre Berichte und Nachweise über die Trustwave Fusion-Plattform bereitgestellt. Die unterstützenden Nachweise korrelieren mit den vorliegenden Ergebnissen. So werden beispielsweise Textnachweise zu Raw Requests und Responses zur Verfügung gestellt. Wenn es für die entdeckten Schwachstellen relevant ist und die SpiderLabs®-Experten es für notwendig halten, die Ergebnisse auf eine andere Weise zu präsentieren, werden zudem Videos erstellt. Dies kommt beispielsweise bei komplexen Logikfehlern oder Angriffsketten zum Einsatz.

Support

Während der gesamten Laufzeit Ihres Abonnements steht Ihnen über die Trustwave Fusion-Plattform eine operative Support-Hotline zur Verfügung.

Trustwave Security Testing: Service-Level-Vergleich

Dieser Abschnitt bietet einen Service-Level-Vergleich der folgenden Test- und Scan-Services:

- Interne/externe Netzwerkscans
- Interne/externe Netzwerk-Penetrationstests
- Interne/externe Application Scans
- Interne/externe Application-Penetrationstests
- Datenbankscans

Externer Netzwerktest

Umfasst:	Scans		Penetrationstests†			
	Self-Serve-Scan — External Vulnerability Scan (EVS)	Managed Scan	Basic Pen Test	Opportunistic Threats Pen Test	Targeted Threats Pen Test	Advanced Threats Pen Test
Network Vulnerability Scan	X	X	X	X	X	X
Scans nicht authentifizierter Web-Apps		X	X	X	X	X
Untersuchungsbericht	X	X	X	X	X	X
Validierung der Scanergebnisse		X	X	X	X	X
Manueller Pentest: am meisten ausnutzbare Funde			X	X	X	X
Manueller Pentest: alle ausnutzbaren Schwachstellen				X	X	X
Vertikale Eskalation				X	X	X
Horizontale Eskalation				X	X	X
Videobeweis				X	X	X
Angriffsketten					X	X
Eskalation auf benachbarte Systeme					X	X
Limited Phishing					X	X
Test-Nachbesprechung					X	X
Clientseitige Angriffe						X
Social Engineering						X
Angriffe nach benutzerdefiniertem Protokoll						X
Eskalation auf das interne Netzwerk						X
Erkundung des Dark Web						X

† Einige der in der Tabelle aufgeführten Bestandteile werden je nach Auftragsumfang und Testergebnissen angewendet.

Interner Netzwerktest

Umfasst:	Scans		Penetrationstests†			
	Self-Serve-Scan — External Vulnerability Scan (EVS)	Managed Scan	Basic Pen Test	Opportunistic Threats Pen Test	Targeted Threats Pen Test	Advanced Threats Pen Test
Network Vulnerability Scan	X	X	X	X	X	X
Scans nicht authentifizierter Web-Apps		X	X	X	X	X
Credentialed Network Vulnerability Scan	X	X	X	X	X	X
Untersuchungsbericht	X	X	X	X	X	X
Validierung der Scanergebnisse		X	X	X	X	X
Manueller Pentest: am meisten ausnutzbare Funde			X	X	X	X
Layer-2-Test (Broadcast, ARP)			X	X	X	X
Vertikale Eskalation			X	X	X	X
Segmentation-Test			X	X	X	X
Manueller Pentest: alle ausnutzbaren Schwachstellen (Ziele)				X	X	X
Horizontale Eskalation (Ziele)				X	X	X
Angriffsketten				X	X	X
Datenexfiltrationstest				X	X	X
Videobeweis				X	X	X
Unternehmenseskalation					X	X
Test aus Client-Subnetzen					X	X
Horizontale Eskalation (Unternehmen)					X	X
Manueller Pentest: alle ausnutzbaren Schwachstellen (Unternehmen)					X	X
Test-Nachbesprechung					X	X
Clientseitige/Browserseitige Angriffe						X
Erweiterte Protokollangriffe						X
Passwortanalyse						X
Erkundung des Dark Web						X

† Einige der in der Tabelle aufgeführten Bestandteile werden je nach Auftragsumfang und Testergebnissen angewendet.

Application-Penetrationstest

Umfasst:	Scans		Penetrationstests†			
	Self-Serve-Scan — External Vulnerability Scan (EVS)	Managed Scan	Basic Pen Test	Opportunistic Threats Pen Test	Targeted Threats Pen Test	Advanced Threats Pen Test
Application Vulnerability Scan	X	X	X	X	X	X
Untersuchungsbericht	X	X	X	X	X	X
Validierung der Scanergebnisse		X	X	X	X	X
Manueller Injection-Test			X	X	X	X
Manueller Sessionmanagement-Test			X	X	X	X
Manuelle Prüfung der Kontorichtlinien			X	X	X	X
Manuelle Prüfung der Offenlegung v. Informationen			X	X	X	X
Manueller Datenschutztest			X	X	X	X
Manueller Authentifizierungstest				X	X	X
Manueller Autorisierungstest				X	X	X
Manueller Test auf einfache Logikfehler				X	X	X
Videobeweis				X	X	X
Manueller Test auf komplexe Logikfehler					X	X
Manueller Test auf kryptografische Schwachstellen					X	X
Manuelles Bounds Checking					X	X
Manuelle Überprüfung des Application Resource Handling					X	X
Test-Nachbesprechung					X	X
Umfangreicher Test						X
Manueller Test aller Benutzerrollen						X

† Die Experten von Trustwave SpiderLabs® untersuchen Ihre Anwendung unabhängig vom gewählten Service-Level des Application-Penetrationstests auf jede Schwachstelle, die Trustwaves Tools identifizieren können. Anschließend führen die Experten die jeweils in der Tabelle aufgeführten manuellen Tests durch.

Nicht webbasierte Anwendungen wie eigenständige APIs oder Thick Clients erfordern für Standardanwendungen mindestens die Auswahl des Levels „Targeted Threats“. Dies ist auf die inhärente Komplexität, das Fehlen sofort einsatzbereiter Tools zur Identifizierung von Schwachstellen und damit auf den erforderlichen maßgeschneiderten Testansatz zurückzuführen.

Mobile Application-Penetrationstest

Umfasst:	Scans*		Penetrationstests†	
	Self-Serve-Scan — External Vulnerability Scan (EVS)	Managed Scan	Targeted Threats Pen Test	Advanced Threats Pen Test
Application Vulnerability Scan (nur Backend)	X	X	X	X
Untersuchungsbericht	X	X	X	X
Validierung der Scanergebnisse		X	X	X
Manueller Injection-Test			X	X
Manueller Sessionmanagement-Test			X	X
Manuelle Prüfung der Kontorichtlinien			X	X
Manuelle Prüfung der Offenlegung v. Informationen			X	X
Manuelle Datenschutztests			X	X
Manuelle Authentifizierungstests			X	X
Manuelle Autorisierungstests			X	X
Manueller Test auf einfache Logikfehler			X	X
Videobeweis			X	X
Manueller Test auf komplexe Logikfehler			X	X
Manueller Test auf kryptografische Schwachstellen			X	X
Manuelles Bounds Checking			X	X
Manuelle Überprüfung des Application Resource Handling			X	X
Manuelle Binäranalyse			X	X
Manueller Laufzeittest			X	X
Manueller Transport-Security-Test			X	X
Test-Nachbesprechung			X	X
Umfangreicher Test				X
Manueller Test aller Benutzerrollen				X

† Aufgrund des benötigten Arbeitsaufwands für On-Device-Testing und die Einrichtung muss für Standardanwendungen mindestens das Level „Targeted Threats“ ausgewählt werden. Die Experten von Trustwave SpiderLabs® untersuchen Ihre Anwendung auf jede Schwachstelle, die Trustwaves Tools identifizieren können. Anschließend führen die Experten die jeweils in der Tabelle aufgeführten manuellen Tests durch.

Application Vulnerability Scanning

Umfasst:	Verfügbarkeit	
	Self-Serve	Managed
Datenbank-Injection-Fehler	X	X
Datenbankfehler	X	X
Integer Overflow	X	X
Nicht-SSL-Passwort	X	X
SSL-Prüfungen	X	X
Application Exception	X	X
Cross-Site Scripting (XSS)	X	X
Directory Browsing	X	X
Cross-Site Request Forgery (CSRF)	X	X
Cookie-Schwachstellen	X	X
Session-ID in URL	X	X
Manuelle Überprüfung der Scan-Vollständigkeit		X
Manuelle Validierung der Scanergebnisse		X
Windows/Unix Command Injection	X	X
Relativer Pfad unter Windows/Unix	X	X
Passwort-Autovervollständigung	X	X
Offenlegung von Kreditkarten	X	X
Basis-Authentifizierung über HTTP	X	X
Offenlegung der privaten IP	X	X
DOM-basiertes XSS	X	X
Open Redirect	X	X
Remote File Inclusion	X	X
Unsichere CORS-Header	X	X
Cross-Frame Scripting	X	X

Datenbankscans

Das Trustwave Managed Database Scanning umfasst vier Datenbank-Schwachstellenscans, die durch Trustwave SpiderLabs®-Experten validiert wurden. Das Scanning liefert greifbare Ergebnisse, die – nach einer Korrektur – für eine messbare Verbesserung der Sicherheit Ihrer Datenbanken sorgen.

Managed Database Scanning
Mangelhafte Zugriffskontrolle
Fehlkonfigurationen
Behebbare Schwachstellen
Schwache Passwörter
Probleme mit dem Betriebssystem
Überprüfungen der Anwendungsintegrität