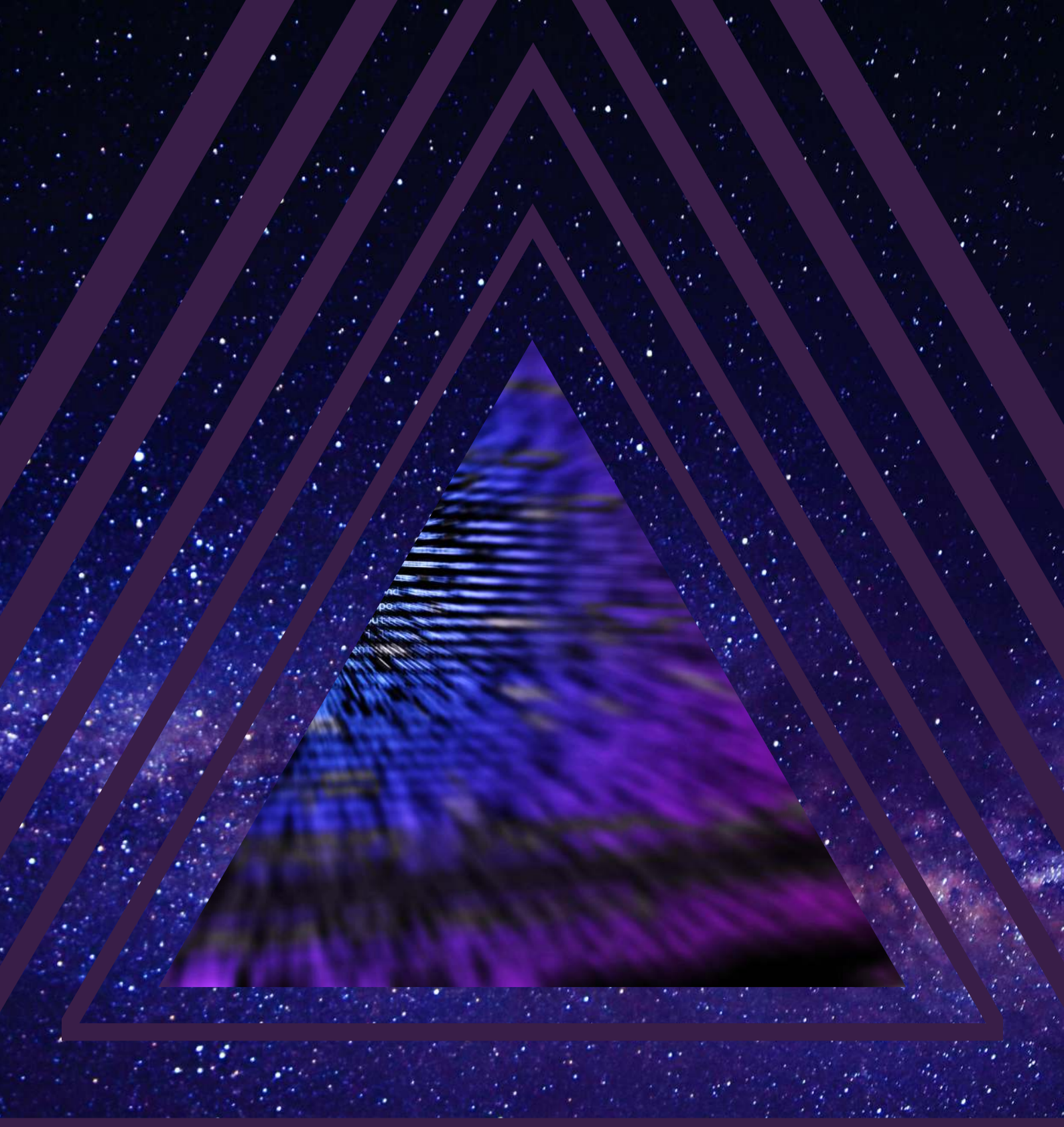


PENETRATIONSTEST

Hinweise rund um das Thema Penetrationstest
von der AWARE7 GmbH

I Bedrohungen

II Wer wird angegriffen?

III Unser Prozess

IV Ablauf eines Penetrationstests

Bedrohungen

Hacktivisten

Motivation: Oft politisch, dynamisch, unvorhersehbar
Business Impact: Datenlecks, Reputationsverluste

Organisiertes Verbrechen

Motivation: Finanzielles
Business Impact: Informationsdiebstahl

Insider

Motivation: Groll, Finanzielles
Business Impact: Verteilung oder Zerstörung von Informationen, Reputationsverlust

Staatliche Akteure

Motivation: Politische Vorteile, Industriespionage
Business Impact: Disruption oder Zerstörung, Datendiebstähle, Reputationsverlust

Wer wird angegriffen?

Energie

Chemie

Luftfahrt

Automotive

Militär

Banken

Gebäude-
technik

Forschung

eCommerce

Kommunikations-
technik

Maschinenbau

Ver- &
Entsorgung

Unser Prozess

Verständnis der Anforderungen

Wir evaluieren gemeinsam mit Ihnen die operativen und geschäftsspezifischen Risiken. Dadurch können wir den Fokus beim Pentest auf die für Ihr Unternehmen bedeutsamsten Risiken lenken. Wir führen diese Analyse auf Basis unterschiedlicher Informationen durch:

- Interviews oder Workshops mit den Produkteigentümern oder deren Vertretern
- Review von existierenden Dokumenten der zu analysierenden Umgebung

Zu diesem Zeitpunkt definieren wir also die für Sie relevanten Risiken und Risikobereiche. In der Regel sind diese technisch, unter Umständen aber auch regulatorisch oder geschäftlich.

Test und Analyse

Wir führen den Sicherheitstest durch und identifizieren Ihre individuellen Risikoquellen. Dabei halten wir uns an standardisierte Methodiken, beispielsweise OWASP, PCI-DSS oder OSSTMM. Dabei werden vorher identifizierte und priorisierte Risiken bevorzugt identifiziert. Wir beginnen das Reporting der identifizierten Schwachstellen und benachrichtigen Sie, falls dringend Aufmerksamkeit gefordert ist.

Business Impact & Empfehlungen

Die identifizierten Schwachstellen werden bei Bedarf nach Business Impact klassifiziert und zusammengestellt. Jede Schwachstelle wird mit Handlungsempfehlungen versehen, die eine Ausnutzung durch Dritte verhindern. Je nach Schwere wird definiert, ob die Schwachstelle kurz-, mittel- oder langfristig angegangen werden sollte. Unsere Reports sind für folgende Zielgruppen geschrieben:

- Executives & Senior Management: Klare, verständliche Executive Summary in verständlicher Business Language. Es werden Strategieempfehlungen gegeben, falls möglich.
- Mittleres Management: Diagramme und Schaubilder ermöglichen schnelle Entscheidungen in Bezug auf Gegenmaßnahmen.
- Umsetzungsteam: Die Verantwortlichen für die Umsetzung der Maßnahmen erhalten detaillierte Einsichten und technische Beschreibungen der gefundenen Schwachstellen. Es werden spezifische Empfehlungen gegeben, Schwachstellen zu beseitigen.

AWARE7 Qualitätsversprechen

Jeder von uns durchgeführte Penetrationstest wird nach höchsten Qualitätsstandards von menschlichen, zertifizierten Analysten durchgeführt. Wir bieten immer qualifizierte und motivierte Mitarbeiter*innen die nach bestem Wissen und Gewissen testen. Dabei halten wir uns an ethische und regulatorische Vorgaben ebenso wie an technische Best Practices. Jeder Bericht wird durch unsere Geschäftsführung auf höchste Qualität geprüft.

Testansatz

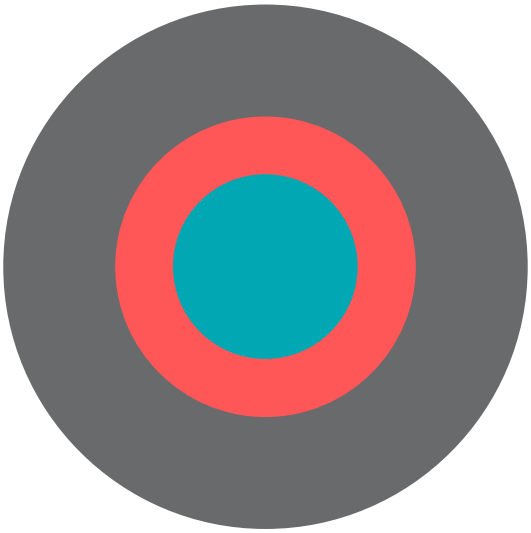
Wir haben einen innovativen Testansatz, der dazu führt, innerhalb von kürzester Zeit Sicherheitsprobleme zu identifizieren und in Bezug zu Ihren Geschäftsprozessen zu setzen. Wir analysieren Ihre Systeme nach dem Outside-In Ansatz. Wir beginnen mit so wenig Informationen wie möglich und arbeiten uns dann innerhalb Ihres Systems vor. Unser hochqualifiziertes Team aus Pentestern und Analysten stellt gemeinsam mit der Geschäftsführung sicher, dass Sie immer bestmögliche Ergebnisse bekommen.

Layer 1

Ihr System wird ohne Kenntnisse unsererseits durch unsere Experten getestet. Dieser Angriff orientiert sich nah an einem echten Angreifer der sich unauthorisiert Zugang zu Ihren Systemen verschaffen will.

Layer 2

Wir erhalten einen authorisierten Zugang zu Ihrem System und einen Teil der Dokumentation zu dem System. Ein Angreifer kann so versuchen weiter in Ihre internen Netze einzudringen.



Layer 3

Wir sind in Ihrem System und erhalten Zugang zu allem. So können wir FIrewallregeln überprüfen, interne Prozesse reviewen, Quellcode analysieren, Betriebssystemkonfigurationen kontrollieren und eine grundlegende Härtung Ihres Systems vornehmen.

Web Application Testing

Der Nutzer

- Passwort Management
- Social Engineering
- Phishing
- Waterholing Attacks
- Administrativer Zugang
- Datenhoheit
- DSGVO Konformität

Die Anwendung

- XSS
- Weak Input Validation
- Brute Force
- Vulnerable Components
- Privilege Escalation

Das Backend

- Platform Vulnerabilities
- Server Fehlkonfigurationen
- CSRF
- XSS
- Brute Force Angriffe
- Datenlecks
- SQL Injection
- Privilege Escalation
- Ausführung von Betriebssystem-kommandos

Web Application Testing - Ansatz

Blackbox Test

Ihr System wird ohne Kenntnisse unsererseits durch unsere Experten getestet. Wir geben nur Ihren Firmennamen an unsere Tester und diese starten mit der Informationsrecherche. Dieser Angriff orientiert sich nah an einem echten Angreifer, jedoch dauert die initiale Informationsrecherche je nach Umfang des Systems entsprechend lange, sodass ein großer zeitlicher Rahmen gewählt werden muss, um aussagekräftige Ergebnisse zu erhalten.

Whitebox Test

Beim Test der Konsole wird die Konfiguration der Cloudumgebung überprüft. Es wird evaluiert, welche Nutzer welche Rechte haben, ob Zugangskontrollen korrekt gesetzt sind und alle Konfigurationen korrekt implementiert sind. So können Privilege Escalation Vektoren und Informationslecks effizient und nachhaltig geschlossen werden.

Greybox Test

Die notwendigsten Informationen über das Zielsystem wurden ausgetauscht. Dazu zählt z.B. die URL der Anwendung sowie Benutzeranmeldeinformationen, welche die verschiedene Benutzerrollen darstellen. Der Greybox-Test ist die effektivste Methode zur Untersuchung Ihrer Anwendung. Durch die fehlende, umfangreiche Informationsrecherche im Vergleich zum Black Box Test, kann der Entdeckung und Ausnutzung von Sicherheitslücken mehr Aufmerksamkeit gewidmet werden.

Allgemeines

Der Pentest einer Webapplikation lässt sich nicht pauschalisieren und eignet sich daher nicht für eine komplette, akkurate und adäquate Automatisierung. Zu einer modernen Webapplikation gehört neben der Anwendung selbst oft noch eine API. Diese API wird von unseren Testern mitgetestet und auf Schwachstellen geprüft. Dabei halten wir uns an Industriestandards wie beispielsweise den OWASP Testing Guide.

Mobile Testing

Das Gerät & Nutzer

- Framing
- Clickjacking
- Man in the Middle
- Buffer Overflow
- Sensitive Data Storage
- Improper Platform Usage
- Configuration Manipulation
- Runtime Injection
- No Transport Encryption
- Session Hijacking

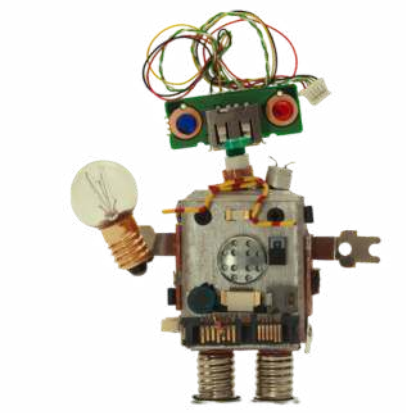
Die Anwendung

- XSS
- Weak Input Validation
- Brute Force
- Vulnerable Components
- Privilege Escalation
- Datenzugriff
- Root Detection
- SQL Injection
- Outdated Libraries

Das Backend

- Platform Vulnerabilities
- Server Fehlkonfigurationen
- CSRF
- XSS
- Brute Force Angriffe
- Datenlecks
- SQL Injection
- Privilege Escalation
- Ausführung von Betriebssystem-kommandos

Mobile Testing – Ansatz



Ansatz

Bei einem Penetrationstest einer mobilen Anwendung gehen wir grundsätzlich ähnlich vor wie bei einer Webanwendung. Das heißt, es gibt auch hier Black-, Grey- und Whiteboxansätze. Der größte Unterschied zu einer Webapplikation ist das Sicherheitsmodell rund um das Endgerät. Ein Nutzer kennt die Bedrohungen rund um das Smartphone häufig nicht und ist unter Umständen auch nicht in der Lage die totale Kontrolle auf dem Smartphone auszuüben. Applikationen sind häufig nur für einen speziellen Zweck geschrieben und nicht mannigfaltig einsetzbar. Während im Webbrowser völlig unterschiedliche Webanwendungen laufen können, ist jede mobile Applikation eine separat laufende Anwendung, die eigens getestet werden muss, egal ob die Funktionalität "Taschenlampe" oder "Bankkonto" durch die App bereitgestellt wird. Wir untersuchen bei unseren Tests also auch Punkte wie die geforderte Passwortstärke oder Vektoren für Social Engineering. Technisch orientieren wir uns an Industriestandards, beispielsweise dem OWASP Mobile Testing Guide.

Sicherheitsaspekte

Eine Applikation läuft in der Regel auf dem Endgerät und spricht mit einer entsprechenden Gegenstelle im Internet. Beide Komponenten müssen im Penetrationstest untersucht werden. In Bezug auf die Endgerätesicherheit ist es wichtig zu evaluieren auf welchem Betriebssystem die App läuft, wie Sie geschrieben und kompiliert wurde und welche Sensordaten unabdingbar für die Funktion der App sind. Benötigt die App beispielsweise Bluetoothdaten, um zu funktionieren, sollten Angriffsstrategien rund um das Bluetooth Protokoll evaluiert werden. Speichert die App sensible Daten, sollten diese nicht durch andere Applikationen auslesbar sein.

Der Server ist der Ort an dem ein Angriff dann potentiell verheerende Auswirkungen auf alle Nutzer*innen der Applikation haben könnte. Daher muss hier besonders genau getestet werden. Haben Nutzer die korrekten Berechtigungen? Können Daten ungewollt abfließen? Gibt es unsichere Testsysteme? Wir arbeiten hier nach dem Ansatz, den wir auch bei Web Anwendungen nutzen.

Cloud Testing

Nutzer

- Passwort Management
- Social Engineering
- Phishing
- Waterholing Attacks
- Administrativer Zugang
- Datenhoheit
- DSGVO Konformität

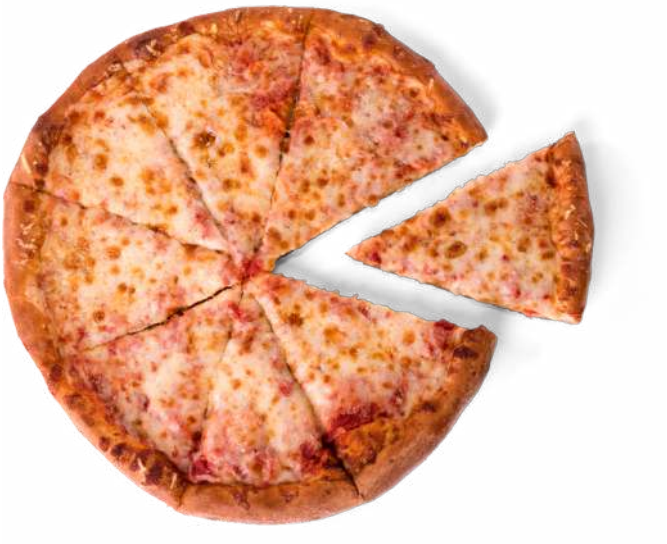
Die Anwendung

- XSS
- Weak Input Validation
- Brute Force
- Vulnerable Components
- Privilege Escalation
- Datenzugriff
- Root Detection
- SQL Injection
- Outdated Libraries
- Credential Leakage

Das Backend

- Platform Vulnerabilities
- Server Fehlkonfigurationen
- CSRF
- XSS
- Brute Force Angriffe
- Datenlecks
- Gefahr durch kompromittierte Instanzen
- SQL Injection
- Privilege Escalation
- Ausführung von Betriebssystem-kommandos

Cloud Pentest - Ansatz



Pentest gegen die Cloud

Hier werden Applikationen getestet, die als Cloud Anwendung gehostet werden. Dies können zum Beispiel Systeme sein, die von der unternehmenseigenen Infrastruktur kürzlich in die Cloud umgezogen sind oder einfach Webapplikationen. Es werden klassische Webapplikationsvektoren getestet ebenso wie fehlkonfigurierte Nutzerberechtigungen oder falsch konfigurierte Speicherinstanzen (z.B. S3 Buckets oder Metadaten von EC2 Instanzen)

Pentest auf der Konsole

Beim Test der Konsole wird die Konfiguration der Cloudumgebung überprüft. Es wird evaluiert, welche Nutzer welche Rechte haben, ob Zugangskontrollen korrekt gesetzt sind und alle Konfigurationen korrekt implementiert sind. So können Privilege Escalation Vektoren und Informationslecks effizient und nachhaltig geschlossen werden.

Pentest in der Cloud

Hier werden Systeme getestet die nicht öffentlich zugänglich sind, beispielsweise getrennt durch eine Firewall. Beim Test in der Cloud werden dem Angreifer häufig gültige Zugänge zum Backend bereitgestellt. Dies geschieht, um zu prüfen, was passiert, wenn versehentlich einmal Zugangsdaten abhanden kommen und ein Angreifer Zugang zum Backend bekommt.

Allgemeines

Diese Formen des Penetrationstests können wir unabhängig des gewählten Service Modells durchführen. Je nach Service Modell sind die Grenzen eines Penetrationstests stark definiert. Ein Infrastructure as a Service (IaaS) System hat andere Anforderungen als ein Software as a Service (Saas) System.

Kontakt

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen

pentest@aware7.de

Matteo Große-Kampmann
Geschäftsführer

+49 209 88306762
matteo@aware7.de

Moritz Gruber
Senior Manager

+49 209 88306760
moritz@aware7.de