Application Security Assessment

Egal, ob Sie Ihre Unternehmensanwendungen intern entwickeln oder diese extern einkaufen, Sie wissen, dass ein einziger Fehler im Code zu einer Schwachstelle führen kann, die bei Angriffen erhebliche finanzielle Verluste und Imageschäden nach sich ziehen könnte. Während des Programm-Lebenszyklus können außerdem weitere Schwachstellen hinzukommen, etwa durch Softwareupdates oder eine unsichere Konfiguration der Komponenten bzw. durch neue Angriffsmethoden.

Unsere Application Security Assessments decken Schwachstellen in beliebigen Anwendungstypen auf, von umfangreichen Cloud-basierten Lösungen, ERP-Systemen, Online-Banking und anderen speziellen Geschäftsanwendungen bis hin zu integrierten und mobilen Anwendungen auf unterschiedlichen Plattformen (iOS, Android und andere).

Dank einer Kombination aus Praxiswissen und Erfahrung mit international anerkannten Best Practices entdecken unsere Experten Sicherheitslücken, die Ihr Unternehmen anfällig für unterschiedliche Angriffstypen machen könnten, u. a.:

- Abschöpfen vertraulicher Daten
- Infiltration und Manipulation von Daten und Systemen
- DoS-Attacken
- Betrügerische Aktivitäten

Auf Grundlage unserer Empfehlungen lassen sich die in den Programmen entdeckten Schwachstellen beheben und die aufgeführten Angriffstypen vermeiden.

Servicevorteile

Die Application Security Assessments von Kaspersky Lab bieten den Programmeigentümern und -entwicklern folgende Vorteile:

- **Keine finanziellen und betrieblichen Verluste sowie Imageschäden** durch frühzeitige Erkennung und Behebung von Schwachstellen, die für Angriffe genutzt werden könnten
- **Keine Korrekturkosten**, da Programmschwachstellen noch während der Entwicklung identifiziert werden, bevor sie die Produktionsumgebung erreichen, wo die Behebung meist mit erheblichen Störungen und Kosten verbunden ist.
- **Unterstützung des Secure Software Development Lifecycle** (S-SDLC) für Entwicklung und Betrieb sicherer Softwareprogramme.
- **Einhaltung von Verordnungen sowie von Branchen- und internationalen Unternehmensstandards** zur Programmsicherheit, z. B. PCI DSS oder HIPAA

Serviceumfang und Optionen

Zu den getesteten Programmen gehören u. a. offizielle Webseiten und Unternehmensprogramme (herkömmlich oder Cloud-basiert), darunter auch integrierte oder mobile Programme.

Die Tests werden an Ihre Bedürfnisse und die Besonderheiten der zu testenden Software angepasst. Zu den Services gehören u. a.:

- **Black-Box-Tests** zur Simulation eines externen Angreifers
- **Grey-Box-Tests** zur Simulation von autorisierten Benutzern mit verschiedenen Profilen
- **White-Box-Tests** zur Analyse mit umfassendem Zugriff auf die Anwendung, einschließlich des Quellcodes. Dieser Ansatz ist am effektivsten, wenn es darum geht, möglichst viele Schwachstellen zu entdecken.
- **Application Firewall Effectiveness Assessment**: Programme werden mit und ohne Firewall-Schutz getestet, um Schwachstellen zu ermitteln und festzustellen, ob potentielle Exploits geblockt werden

Ergebnisse

Zu den durch die Assessmentservices von Kaspersky Lab ermittelten Schwachstellen gehören:

- Fehler bei Authentifizierung und Autorisierung, inklusive Multifaktor-Authentifizierung
- Code-Injektion (SQL-Injektion, OS-Commanding usw.)
- Logische Schwachstellen, die Betrugsversuche begünstigen
- Schwachstellen auf Clientseite (Cross-Site-Scripting, Cross-Site Request Forgery usw.)
- Schwache Kryptografie
- Schwachstellen in Client-Server-Verbindungen
- Unsicheres Speichern und Übertragen von Daten, z. B. fehlende PAN-Maskierung in Bezahlsystemen
- Konfigurationsfehler, z. B. Fehler, die zu Attacken auf Sitzungen führen
- Offenlegung vertraulicher Informationen
- Weitere Schwachstellen, die zu den im Bericht „WASC Threat Classification v2.0" und in den „OWASP Top Ten" aufgeführten Bedrohungen führen können

Die Ergebnisse werden in einem abschließenden Bericht zusammengefasst. Dieser umfasst auch detaillierte technische Informationen zu Testvorgang, Ergebnissen, entdeckten Schwachstellen und Empfehlungen für Korrekturmaßnahmen sowie eine Kurzübersicht, in der mögliche Folgen für die Geschäftsführung beschrieben werden. Auf Anfrage können auch Videos und Präsentationen für Ihre technische Abteilung und die Geschäftsführung bereitgestellt werden.

Unsere Vorgehensweise beim Application Security Assessment

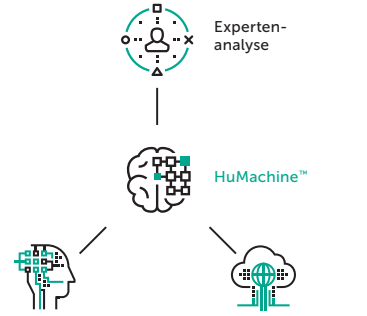
Das Application Security Assessment wird von unseren Experten sowohl manuell als auch mithilfe automatisierter Tools ausgeführt. Hierbei kommt dem Schutz von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Systeme sowie der strengen Einhaltung u. a. der folgenden internationalen Normen und Best Practices besondere Bedeutung zu:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Weitere Standards, abhängig von der Branche und dem Standort Ihres Unternehmens

Bei den Mitgliedern des Projektteams handelt es sich um erfahrene Profis mit einem tiefgreifenden und aktuellen Praxiswissen auf diesem Gebiet, inklusive der verschiedenen Plattformen, Programmiersprachen, Frameworks, Schwachstellen und Angriffsmethoden. Sie treten als Redner bei wichtigen internationalen Konferenzen auf und arbeiten als Sicherheitsberater für führende Software- und Cloud-Service-Anbieter, darunter Oracle, Google, Apple, Facebook und PayPal.

Bereitstellungsoptionen

Je nach Art des gewünschten Sicherheitsassessments und ihrer speziellen Systembedingungen und Anforderungen an die Arbeitsbedingungen können die Services entweder remote oder am Standort geleistet werden. Die meisten der Services lassen sich per Fernzugriff ausführen.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **https://de.securelist.com**
IT-Sicherheitsnachrichten: **www.business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.de