HISOLUTIONS – SCHWACHSTELLENREPORT 2013

Eine Analyse der identifizierten Schwachstellen in Penetrationstests

MOTIVATION

HiSolutions führt jedes Jahr eine große Anzahl von unterschiedlichen Penetrations- und Schwachstellentests durch. Immer wieder werden wir dabei gefragt, wie die Ergebnisse des einzelnen Tests gegenüber „typischen“ Ergebnissen einzustufen sind, und ob die identifizierten Probleme bei anderen Unternehmen ähnlich bestehen.

Wir haben diese Fragen zum Anlass genommen, die von uns in den letzten Jahren durchgeführten Tests jahresweise auszuwerten und die jeweils identifizierten Schwachstellen in Kategorien zusammenzufassen. Diese Aggregation erlaubt uns, einerseits die Vertraulichkeit der Projektergebnisse gegenüber unseren Kunden zu wahren, andererseits aber Aussagen abzuleiten über typische Testergebnisse und besondere Problembereiche, die entweder besonders häufig auftauchen oder besonders schwerwiegende Lücken darstellen. Durch die Fortschreibung der Auswertung über die Jahre hinweg können dabei auch Trends und Entwicklungen in der Sicherheitslage deutlich werden.

HISOLUTIONS

VORGEHEN

Dieser Report beruht auf einer Auswertung der Ergebnisse aus insgesamt 64 Penetrations- und Schwachstellentests, die im Jahr 2013 durchgeführt wurden. Bereits letztes Jahr hatten wir eine vergleichbare Auswertung für 41 Tests des Jahres 2012 durchgeführt, deren Ergebnisse wir nun zum Vergleich heranziehen können. Die Tests betreffen verschiedene Zielumgebungen, von Netzwerkinfrastrukturen über Web-Anwendungen bis hin zu einzelnen Systemen und Verfahren, sind also nicht direkt miteinander vergleichbar. Durch die Kategorienbildung bei den Schwachstellen lassen sich dennoch interessante Beobachtungen ableiten.

Für die Kategorien haben wir uns zunächst an den „OWASP Top 10“ orientiert. Diese Veröffentlichung des OWASP-Projektes aus dem Jahr 2013[1] umfasst eine Systematik der schwerwiegendsten Schwachstellen *für Web-Anwendungen*, die dort auf der Grundlage einer Berechnung der Schweregrade auf der Basis von Häufigkeiten und Auswirkungen erstellt wurde. Die Kategorien lassen sich dabei z. T. auch auf andere Testziele gut übertragen, decken jedoch nicht alle unsere Befunde vollständig ab, so dass wir einige eigene Kategorien ergänzt haben.

Die Aggregation bringt einige praktische Schwierigkeiten mit sich: Wegen der Unterschiedlichkeit der durchgeführten Tests ließen sich keine relevanten Aussagen zur Häufigkeit einer Schwachstelle pro System oder Anwendung ermitteln. Auch fassen wir in den Projektberichten gleichartige Schwachstellen auf verschiedenen Systemen häufig zu einem Befund zusammen, so dass eine Zählung der Befunde hier ebenfalls nur begrenzte Aussagekraft hat. Wir haben uns daher entschlossen, als Maß die Häufigkeit des Auftretens eines Schwachstellentyps pro Projekt anzusetzen. Dadurch wird deutlich, welchen Schwachstellen wir in unterschiedlichen Projekten besonders häufig begegnen, und welche eher selten oder nur in besonderen Zielumgebungen auftauchen.

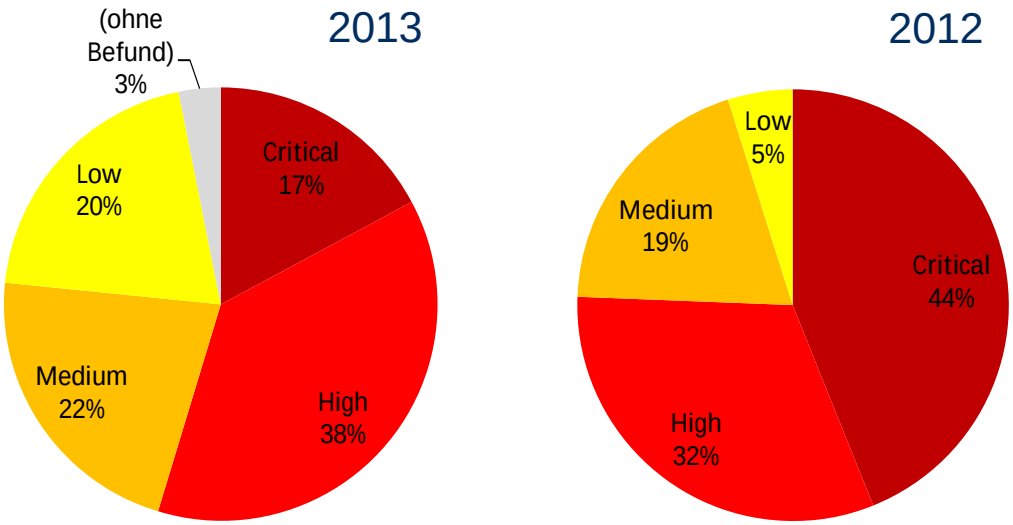
Für die Bewertung der Relevanz einer Schwachstelle verwenden wir in unseren Prüfberichten ein standardisiertes Schema, in dem wir aus der Bewertung der Komplexität des Angriffs und des zu erwartenden Schadens zu einer Einordnung in die folgenden Kategorien kommen:

CRITICAL (C)	Die getesteten Systeme sind akut gefährdet, umgehendes Handeln ist (in der Regel noch während der Testdurchführung) erforderlich.
HIGH (H)	Die Schwachstelle hat eine hohe praktische Relevanz und sollte priorisiert behoben werden.
MEDIUM (M)	Die Schwachstelle besitzt ein relevantes Schadenspotenzial, dieses kann aber nur in bestimmten Umständen oder in Verbindung mit anderen Problemen realisiert werden.
LOW (L)	Die Schwachstelle stellt für sich keine unmittelbare Gefahr dar, kann jedoch Angriffe über andere Schwachstellen erleichtern oder verstärken.

Rein informative Befunde (z. B. festgestellte funktionale Fehler ohne Sicherheitsbezug) wurden in der Zählung nicht berücksichtigt.

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Insgesamt hat sich die Situation seit dem Vorjahr etwas verbessert, bleibt jedoch aus unserer Sicht kritisch:



Höchste Einstufung einer Schwachstelle je Projekt

In fast allen durchgeführten Tests (97 %) wurden Sicherheitslücken gefunden, die nur in einem Fünftel der Fälle (20 %) als ungefährlich eingestuft werden konnten. Nur in zwei Berichten wurden keine bzw. nur sicherheitsunkritische Tatbestände festgestellt.

Deutlich über die Hälfte aller Projekte zeigte hingegen sogar Probleme mit potenziell schweren Auswirkungen. Zwar hat in unserer Stichprobe die Zahl der kritischen Lücken im Vergleich zum Vorjahr abgenommen, sie erforderten aber immer noch in jedem sechsten Fall (17%) unmittelbares Handeln.

Analysiert man die gefundenen Schwachstellen thematisch, ergibt sich folgendes Bild:

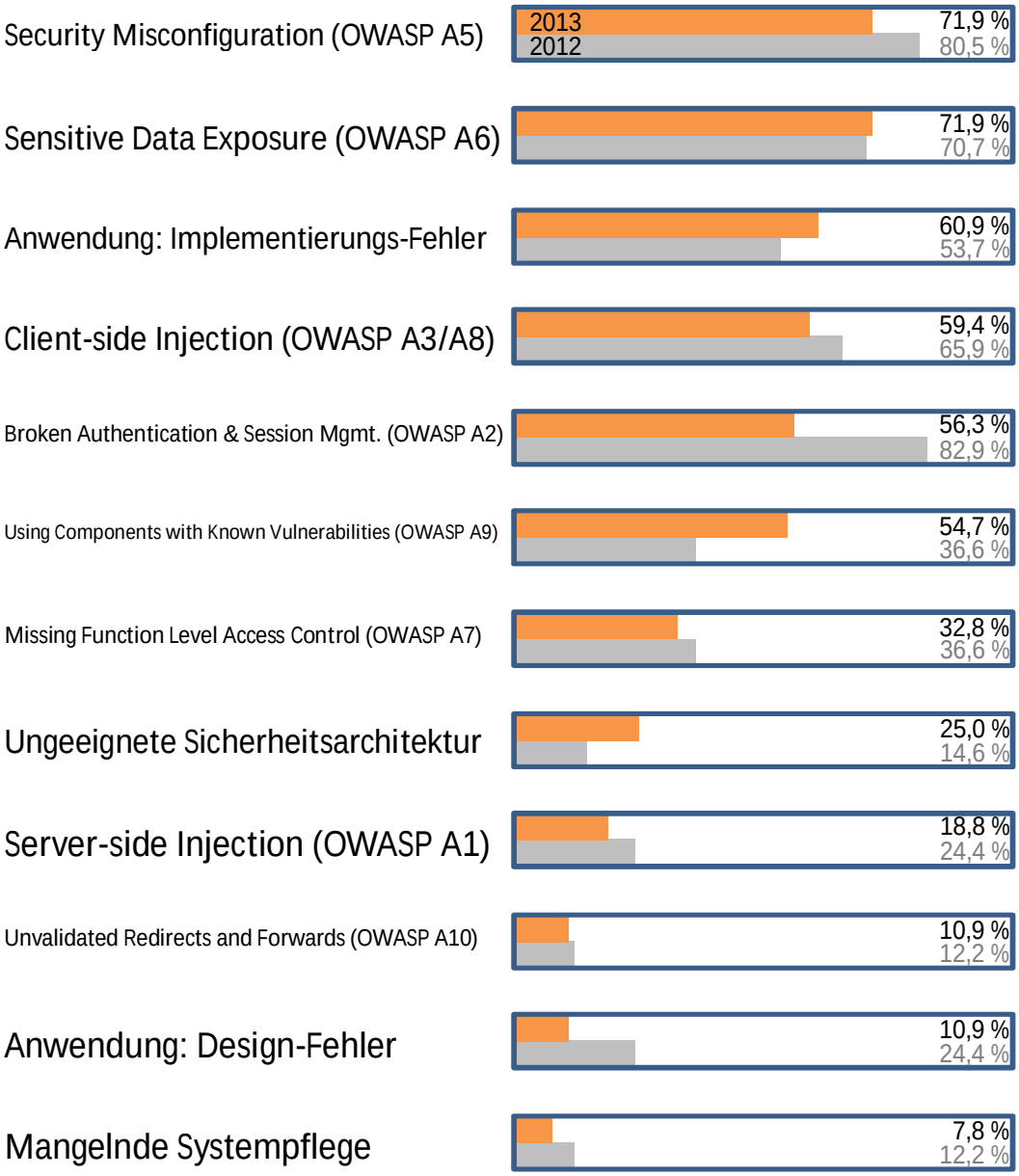
Die Gruppe der Schwachstellen mit der häufigsten Einstufung als „kritisch“ umfasst serverseitige Injection-Angriffe (insbesondere SQL-Injections) sowie Probleme bei der Zugriffskontrolle und beim Rechtemanagement. Diese beiden Gruppen tauchen zwar nur vergleichsweise selten in den Tests auf, was auf ein langsam steigendes Bewusstsein der Anwendungsentwickler (oder der Framework-Autoren…) für diese Probleme hinweist.

Andere Schwachstellen, insbesondere bei der sicheren Systemkonfiguration und der Absicherung sensibler Daten, tauchen deutlich häufiger auf – in über 70 % der durchgeführten Tests –, wiegen aber oft weniger schwer. Die gefunden Fehler sind dort nicht immer unmittelbar ausnutzbar oder haben nur geringere Auswirkungen. Kritische Befunde kommen aber auch in diesen Bereichen vereinzelt vor.

Der Klassiker *Cross-Site Scripting* – in den OWASP Top 10 von 2007 noch auf Platz 1, in der Version von 2013 auf Platz 3 – tritt gemeinsam mit anderen clientseitigen Injections zwar etwas weniger häufig auf (59 %), bringt aber nach wie vor ein hohes Schadenspotenzial mit sich.

Neu hinzugekommen zur OWASP Top 10 ist der Bereich *Using Components with Known Vulnerabilities*, den wir bei unserer letzten Erhebung durch eine eigene Kategorie *Fehlende Patches & Updates* quasi vorweggenommen haben: In über der Hälfte der Prüfungen wurden derartige Schwachstellen identifiziert. Die Schwere der Befunde ist überdurchschnittlich hoch. Ein funktionierender Patch-Management-Prozess erweist sich auch hier wieder als unerlässlich für den sicheren Betrieb von IT-Systemen.

Die folgende Grafik zeigt die von uns definierten Schwachstellenkategorien jeweils mit der Häufigkeit ihres Auftretens im Projekt:

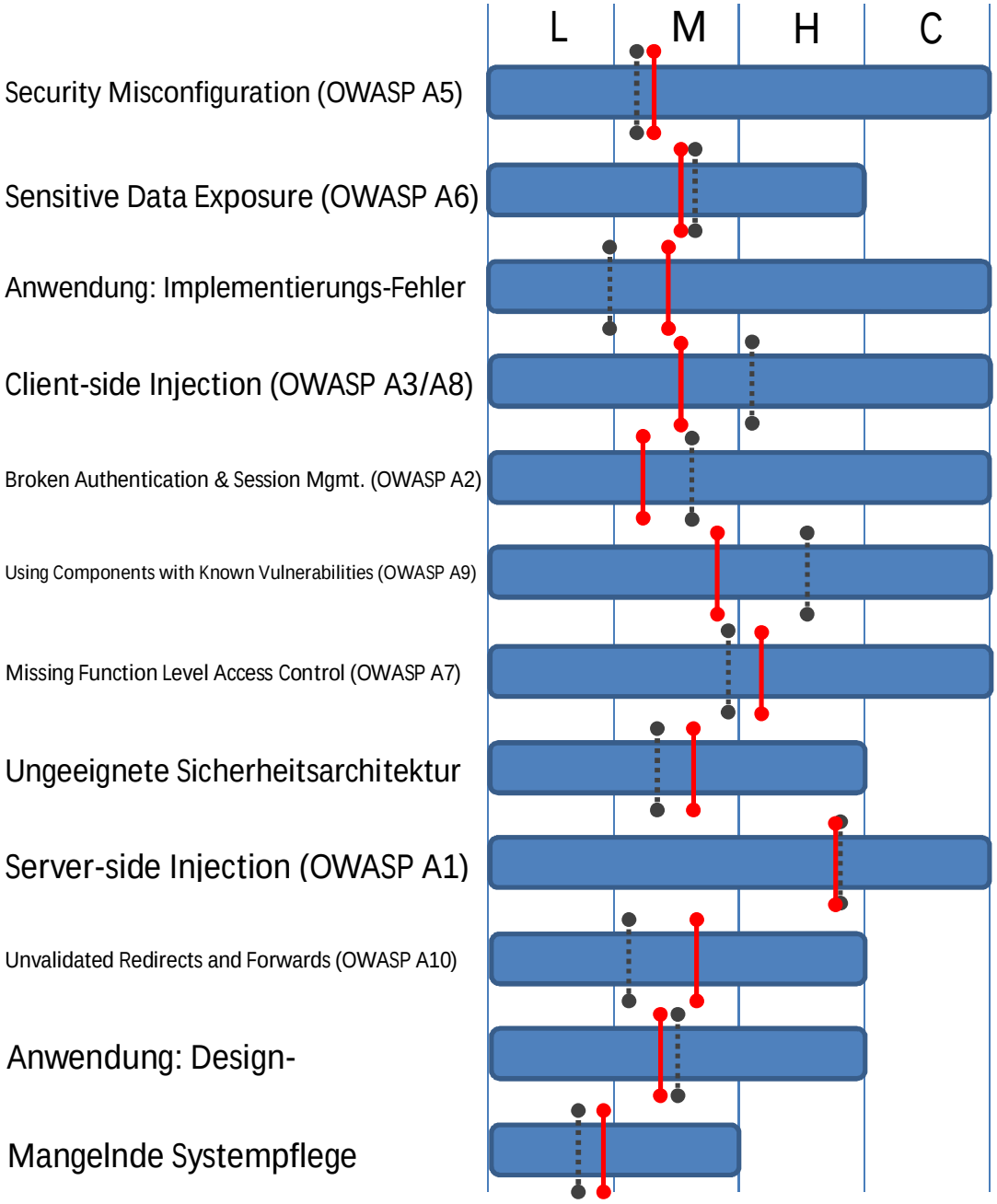


Erkennbar ist, dass es signifikante Verbesserungen beim Design von Anwendungen sowie beim Session-Management gibt. Wir führen dies auf den vermehrten Einsatz von bewährten Frameworks und eine konsequentere Beachtung bewährter Anwendungsstrukturen, wie zum Beispiel dem Schichtenmodell, zurück.

Gleichzeitig beobachten wir eine negative Entwicklung bei fehlenden Updates und Patches sowie der Sicherheitsarchitektur. Den Verbesserungen in der Anwendungsentwicklung steht offenbar eine gegenläufige Tendenz im Betrieb gegenüber. Wir haben den Eindruck, dass hier häufig Ressourcen für die Aufrechterhaltung der Sicherheit zu knapp bemessen sind.

Insgesamt kann keinesfalls Entwarnung gegeben werden: Nach wie vor ist die Zahl der Schwachstellen erschreckend hoch, ihre Kritikalität ist weit gestreut.

Neben der Häufigkeit ist auch die Kritikalität der gefundenen Schwachstellen interessant: Das folgende Bild zeigt die minimal und maximal vorgenommenen Einstufungen (blaue Balken) und den dabei durchschnittlich gewählten Schweregrad (rote Markierung) je Kategorie, jeweils verglichen mit dem Schweregrad aus dem Vorjahr (in grau).



Lesebeispiel: In der Kategorie “Security Misconfiguration (OWASP A5)” reichten die vorgenommenen Einstufungen von „low“ bis „critical“; der durchschnittliche Schweregrad war knapp unter „medium“ und liegt dabei sogar etwas höher als im Vorjahr.

Die zum Teil starken Bandbreiten bei der Bewertung der Schwachstellen innerhalb der einzelnen Kategorien zeigen, dass die Einstufung je nach Art des konkreten Befunds, insbesondere aber auch der Kritikalität der betroffenen Systeme und Daten individuell zu ermitteln ist.

SECURITY MISCONFIGURATION (OWASP A5)

Diese Kategorie umfasst alle Arten von Konfigurationseinstellungen, die zu Schwachstellen oder Angriffspunkten führen und ist daher in sich sehr heterogen – wir haben über 60 verschiedene Arten von Befunden dieser Kategorie zugeordnet. Viele der Konfigurationsprobleme führen jedoch auch nur zu geringen Risiken, so dass die meisten Einstufungen hier niedrig bis mittel ausgefallen sind. Kritisch sind lediglich bestimmte Fälle der Preisgabe von Informationen über technischen Konfigurationsdaten, Directory-Listings oder nicht gelöschte Beispiel- und Hilfedateien, die in den entsprechenden Fällen jeweils einen unmittelbaren Ansatzpunkt für Angriffe gegeben haben.

SENSITIVE DATA EXPOSURE (OWASP A6)

Unter diese Kategorie fallen alle Schwachstellen, die zu einem mangelhaften Schutz sensibler Daten führen. Dazu gehören neben einer fehlerhaften Konfiguration der Transportsicherheit (SSL) auch ein mangelhafter Schutz von Passwörtern und anderen sensiblen Daten durch eine fehlende Verschlüsselung oder den Einsatz veralteter Verschlüsselungsverfahren. Gerade die Anwendung kryptografischer Algorithmen hält viele Fallstricke bereit, die von Angreifern ausgenutzt werden können. Allerdings sind solche Schwachstellen nur selten als kritisch zu bewerten, da sie zumeist nur unter bestimmten Umständen oder mit einem erheblichen Aufwand ausnutzbar sind.

ANWENDUNG: IMPLEMENTIERUNGS-FEHLER

Wie bei der Vielzahl und Vielfalt existierender Anwendungen zu erwarten, bilden die hier zusammengefassten gut zwei Dutzend Schwachstellen einen bunten Strauß an Dingen, die bei der Implementierung von Anwendungen falsch gemacht oder vergessen wurden – über die von den OWASP-Kategorien bereits erfassten Fehlermöglichkeiten hinaus. Besonders kritische Fälle stehen oft im Zusammenhang mit mangelnder Rechteprüfung beim Lesen oder Schreiben sowie beim Upload von Dateien.

CLIENT-SIDE INJECTION (OWASP A3/A8)

Clientseitige Injection-Angriffe basieren auf dem Prinzip, dass der Angreifer in die Anwendung Programmcode einbringt, der auf dem Client eines Anwenders ungewollt zur Ausführung gelangt. In dieser Kategorie wurden OWASP A3 (Cross-Site Scripting, XSS) und OWASP A8 (Cross-Site Request Forgery, CSRF) zusammengefasst, da letztere eher selten und in der Regel in Verbindung mit ersterer auftritt. XSS macht hier sowohl bezüglich des Auftretens als auch der Schwere den Löwenanteil aus (ca. 60 %, über 90 % der hohen und kritischen Bewertungen), wobei es meist um reflektiertes (also dem Anwender über einen Link untergeschobenes), vereinzelt auch um persistentes XSS (dauerhaft in die Anwendung eingebrachten Schadcode) geht.

BROKEN AUTHENTICATION & SESSION MGMT. (OWASP A2)

Unter diese Kategorie fällt eine Vielzahl von Schwachstellen, die mit unterschiedlicher Häufigkeit und Kritikalität vorzufinden sind (wir haben über 30 verschiedene Arten von Einzelbefunden identifizieren können). Besonders schwerwiegend sind Session-Tokens in URLs, Session-Fixation-Angriffe sowie in bestimmten Fällen mangelhaft geschützte Session-Cookies, unsichere SSH-Schlüssel, zu wenig Entropie in Session-IDs oder in Einzelfällen Logins mit Default-Credentials oder gar ohne jede Zugangskontrolle.

USING COMPONENTS WITH KNOWN VULNERABILITIES (OWASP A9)

Unter diese Kategorie fallen Schwachstellen, die insbesondere aus einem mangelhaften Software- und Patchmanagement resultieren: Veraltete Software, vom Betriebssystem über die Anwendungsserver, Frameworks, die Anwendungssoftware und Erweiterungen oder Plug-Ins können eine Vielzahl von Schwachstellen beinhalten, die nach der Veröffentlichung leicht von Angreifern ausgenutzt werden können. Wird die Software nicht sorgfältig gepflegt, können schnell Lücken entstehen, die ein großes Schadenspotenzial beinhalten.

MISSING FUNCTION LEVEL ACCESS CONTROL (OWASP A7)

Diese Kategorie umfasst Schwachstellen durch URLs, die vor unbefugtem Zugriff nicht ausreichend geschützt sind, i. d. R. weil der Anwendungsentwickler einen direkten Aufruf der URL durch einen Angreifer nicht erwartet. Dabei werden sensible Daten oder Anwendungsfunktionen ohne Authentifizierung oder für nicht berechtigte Nutzer zugänglich gemacht. Schwerere Schwachstellen in diesem Bereich betreffen vor allem bestimmte administrative Logins, die nicht von außen erreichbar sein sollten, oder administrative Bereiche, die völlig ohne Authentifizierung erreichbar sind, sowie besonders sensible Kundendaten und -dokumente.

UNGEEIGNETE SICHERHEITSARCHITEKTUR

Vereinzelt sind wir in unseren Projekten auf Sicherheitsarchitekturen gestoßen, die ihre Schutzfunktion nicht erfüllen. Dies begründet sich manchmal in fehlenden Schutzmechanismen (Firewalls), z. T. jedoch auch in vorhandenen, aber in der vorliegenden Konfiguration nicht wirksamen Sicherheitssystemen. Dieser Effekt ist besonders bei sogenannten Web Application Firewalls (WAF) häufiger zu beobachten. Ebenfalls in diese Kategorie haben wir eine aus Sicherheitssicht unzureichende Trennung von Produktiv- und Testumgebungen gezählt.

SERVER-SIDE INJECTION (OWASP A1)

Ähnlich wie bei den clientseitigen Injection-Angriffen bringt auch bei der serverseitigen Injection der Angreifer eigenen Programmcode in die Anwendung ein, der hier jedoch auf der Serverseite ausgeführt wird und dadurch ein besonders hohes Schadenspotenzial hat. Der nach wie vor überwiegende Anteil besteht dabei in SQL-Injections, bei denen der Angreifer Datenbankabfragen der Anwendung manipuliert und sich so unbefugten Zugriff auf Daten und Funktionen verschafft. Diese Angriffe stufen wir in der Regel als kritisch ein. In weiteren Fällen sind verschiedene andere Arten von Code-Injection-Lücken vorzufinden.

UNVALIDATED REDIRECTS & FORWARDS (OWASP A10)

Diese Kategorie umfasst Aufrufe von weiteren Web-URLs durch eine Anwendung, die sich vom Anwender manipulieren oder umleiten lassen. Solche Fälle tauchten vereinzelt – insbesondere im Zusammenhang mit Empfehlungsfunktionen auf Webseiten – auf, waren jedoch nur in Einzelfällen als hoch zu bewerten.

ANWENDUNG: DESIGN-FEHLER

Designfehler in Anwendungen führen insgesamt seltener zu Befunden als Implementierungsfehler (nur ca. 10 % vs. ca. 60 %), sind dann aber oftmals gefährlich. Die Ausprägungen sind unterschiedlich. Beispiele sind Datenbankzugriffe mit administrativen Rechten, das Zulassen trivialer Passwörter, unnötige Exportfunktionen, unsichere Schnittstellen oder die ungewollte Preisgabe von Nutzerinformationen.

MANGELNDE SYSTEMPFLEGE

Vereinzelt stießen wir auf Umgebungen, die durch mangelnde Systempflege (jenseits des Patchmanagements) eine unnötig große Angriffsfläche boten, z. B. durch den Weiterbetrieb ungenutzter Systeme und Anwendungen oder Test- und Beispielanwendungen. Soweit solche Szenarien nicht zu unmittelbar ausnutzbaren Schwachstellen führten (und dann den entsprechenden anderen Kategorien zugeordnet wurden), wurden sie hier zusammengefasst.

FAZIT

Die Ergebnisse unserer Erhebung von 2013 weisen in einzelnen Kategorien eine hohe Deckung mit den Ergebnissen der vorangegangenen Untersuchung auf und bestätigen damit die Aussagekraft.

Insgesamt wurden weniger kritische Befunde verzeichnet, die Schwachstellen waren im Durchschnitt etwas weniger schwerwiegend. Positiv ist auch, dass wir erstmals Prüfungen hatten, bei denen keine sicherheitsrelevanten Schwachstellen gefunden werden konnten. Dennoch werden nach wie vor in mehr als jedem zweiten Fall schwere Befunde verzeichnet; in immer noch 17 % der Prüfungen erforderten diese unmittelbares Handeln. Trotz einer leichten Verbesserung des Gesamtbilds bleibt so in vielen Fällen deutlicher Handlungsbedarf vorhanden.

Die überarbeitete Struktur der OWASP Top 10 hat sich auch für unsere Auswertung bewährt. Mit der neuen Kategorie *Using Components with Known Vulnerabilities* werden nun auch Schwachstellen erfasst, die wir bisher in einer eigenen Kategorie abbilden mussten. Die Spitzenposition bei der Kritikalität haben aber nach wie vor die serverseitigen Injection-Angriffe. Sie treten zwar nur in etwas mehr als jedem sechsten Test auf (18,8 %), erfordern dann aber aufgrund der potenziellen Auswirkungen überdurchschnittlich oft unmittelbares, oftmals provisorisches Eingreifen.

Nach wie vor verzeichnen wir eine breite Streuung möglicher Probleme. Der Variantenreichtum der in der Praxis vorgefundenen Schwachstellen erschwert ein einfaches und schnelles Auffinden beispielsweise durch automatisierte Verfahren. Ein „Durchtesten“ ausgewählter „Top-5“- oder „Top-10“-Lücken erweist sich weiterhin als nicht hinreichend.

Regelmäßige Penetrationstests helfen, die vorhandenen Probleme zu identifizieren und abzustellen. Die Aufrechterhaltung eines angemessenen Sicherheitsniveaus gelingt am besten in der Kombination einer systematischen Risikoanalyse und der Verifikation der Wirksamkeit der umgesetzten Maßnahmen im praktischen Test.

KONTAKT

Frank Rustemeyer
Director System Security
Fon +49 30 533 289-0
rustemeyer@hisolutions.com

HiSolutions AG
Bouchéstraße 12
12435 Berlin

info@hisolutions.com
www.hisolutions.com
Fon +49 30 533 289 0
Fax + 49 30 533 289 900