HISOLUTIONS - SCHWACHSTELLENREPORT

Eine Analyse der identifizierten Schwachstellen in Penetrationstests des Jahres 2014

HISOLUTIONS

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.

VORGEHEN

Dieser Report beruht auf einer Auswertung der Ergebnisse aus insgesamt 37 Penetrations- und Schwachstellentests, die im Jahr 2014 durchgeführt wurden. 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:

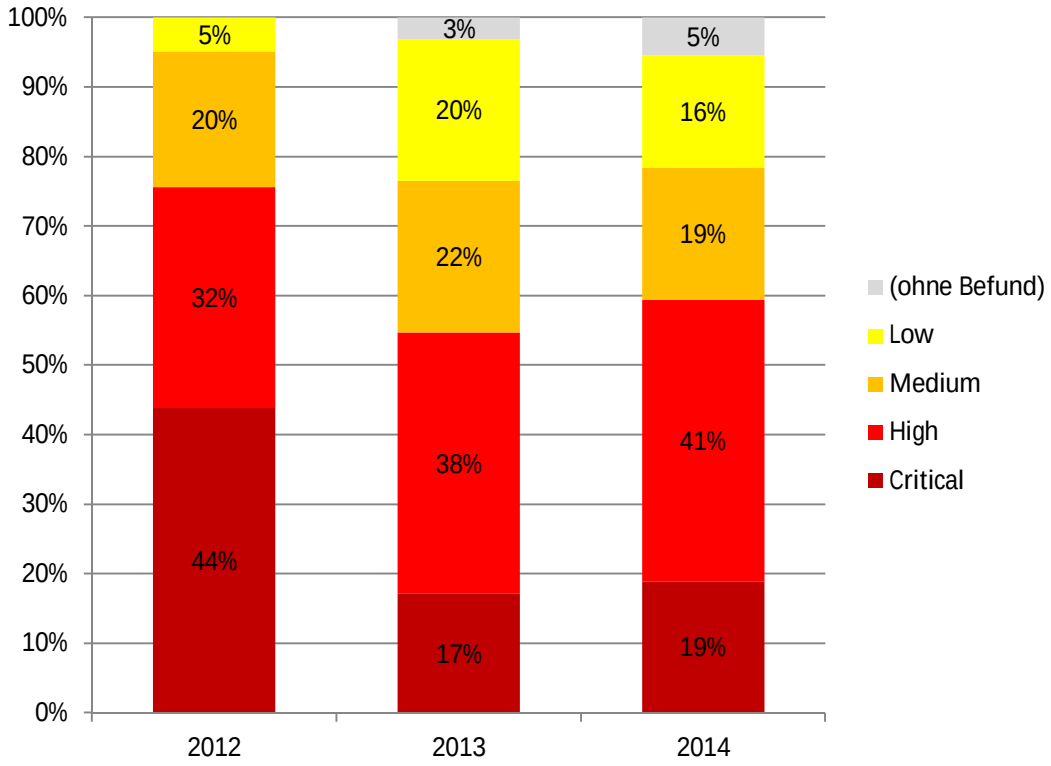
CRITICAL (C)	Die getesteten Systeme sind akut gefährdet, umgehendes Handeln ist (in der Regel noch während der Testdurchführung) erforderlich.
HIGH (H)	Die Schwachstelle hat eine hohe praktische Relevanz und sollte priorisiert behoben werden.
MEDIUM (M)	Die Schwachstelle besitzt ein relevantes Schadenspotenzial, 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.

Zusätzlich haben wir die Befunde mit den Ergebnissen unseres Schwachstellenreports 2012 und 2013 verglichen, auch wenn sich durch die Aktualisierung der OWASP Top 10 im Jahre 2013 hier einige Verschiebungen in der Kategorisierung einzelner Befunde ergeben haben.

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

Noch 2013 hatte sich eine deutlich Verbesserung bei der jeweils „schlimmsten“ Schwachstelle pro Projekt ergeben. Dieser Trend hat sich 2014 nicht fortgesetzt; es ist sogar wieder eine leichte Verschlechterung zu beobachten:



Maximale Kritikalität in Untersuchungen der letzten drei Jahre

Obwohl der Anteil der Untersuchungen ohne Befunde weiter zugenommen hat, finden sich nach wie vor in den meisten durchgeführten Tests (95 %) vorhandene Sicherheitslücken, die nur in einem Sechstel der Fälle (16 %) ein geringes Risiko darstellten.

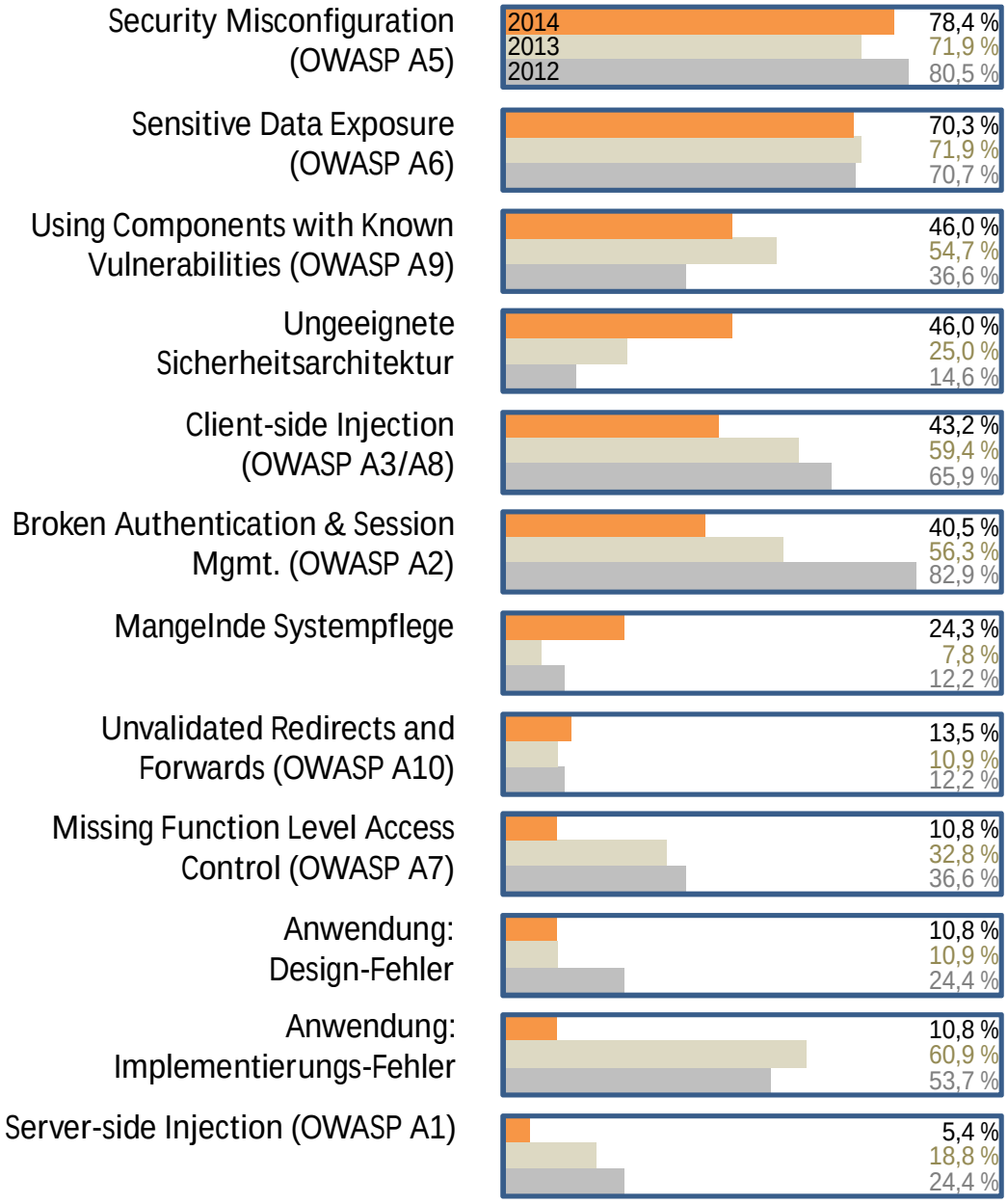
Fast zwei Drittel aller Projekte (60 %) zeigte hingegen Probleme mit potenziell schweren Auswirkungen. Die Zahl der kritischen Testergebnisse hat im Vergleich zum Vorjahr sogar wieder leicht zugenommen, sie erforderten immerhin in fast jedem fünften Fall (19 %) unmittelbares Handeln.

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

Die Gruppe der Schwachstellen mit der häufigsten Einstufung als „kritisch“ umfasst den Einsatz von veralteten oder bekanntermaßen unsicheren Komponenten (OWASP A9), mangelhafte Sicherheitskonfiguration (OWASP A5) sowie Probleme bei der Zugriffskontrolle auf funktionaler Ebene (OWASP A7).

Server-seitige Injection-Schwachstellen, die in den vergangenen Jahren häufig anzutreffen waren, sind 2014 nicht mehr in kritischer Konstellation vorgefunden worden – Entwarnung kann aber nicht gegeben werden, denn in vielen Fällen sind die eigentlichen Schwachstellen nur durch technische Hilfsmaßnahmen wie Web Application Firewalls oder pauschale Eingabefilterung überdeckt worden, die die eigentlichen Probleme nicht beheben, auch wenn sie Angriffe (und damit auch unsere Sicherheitstests) erschweren.

Die folgende Grafik zeigt die von uns definierten Schwachstellenkategorien jeweils mit der Häufigkeit ihres Auftretens im Projekt (zusätzlich werden die Ergebnisse von 2012 und 2013 dargestellt):



Erkennbar ist, dass es signifikante Verbesserungen bei der Implementierung von Anwendungen sowie bei der Zugriffskontrolle auf funktionaler Ebene gibt. Wir führen das auf eine weiter verbreitete Verwendung bewährter Frameworks und Entwicklungsstandards zurück, letztlich also besser ausgebildete Entwickler. Das korreliert auch mit einer Abnahme der Befunde bei Client-side und Server-side Injections.

Die umgekehrte Entwicklung zeichnet sich bei der Sicherheitsarchitektur ab. Dies mag auch dem Umstand geschuldet sein, dass sich unsere Projekte strukturell ändern. Immer öfter führen wir Penetrationstest auch zur Untersuchung der internen Sicherheit von Anwendungen und Netzen durch. Dabei zeigt sich, dass Sicherheitsaspekte beim Design interner Anwendungen oft unzureichend berücksichtigt werden – man fühlt sich im eigenen Netz sicher. Angesichts der Tatsache, dass gezielte Angriffe heute in der Regel schrittweise erfolgen, indem sich die Angreifer zunächst Kontrolle über PCs im internen Netz verschaffen und dann von dort aus weiter vorgehen, ist diese Sichtweise nicht mehr zeitgemäß.

Bei der Verwendung von Komponenten mit bekannten Schwachstellen gab es zwar kleine Verbesserungen, die aber durch die deutlich höhere Kritikalität (siehe folgende Grafik)

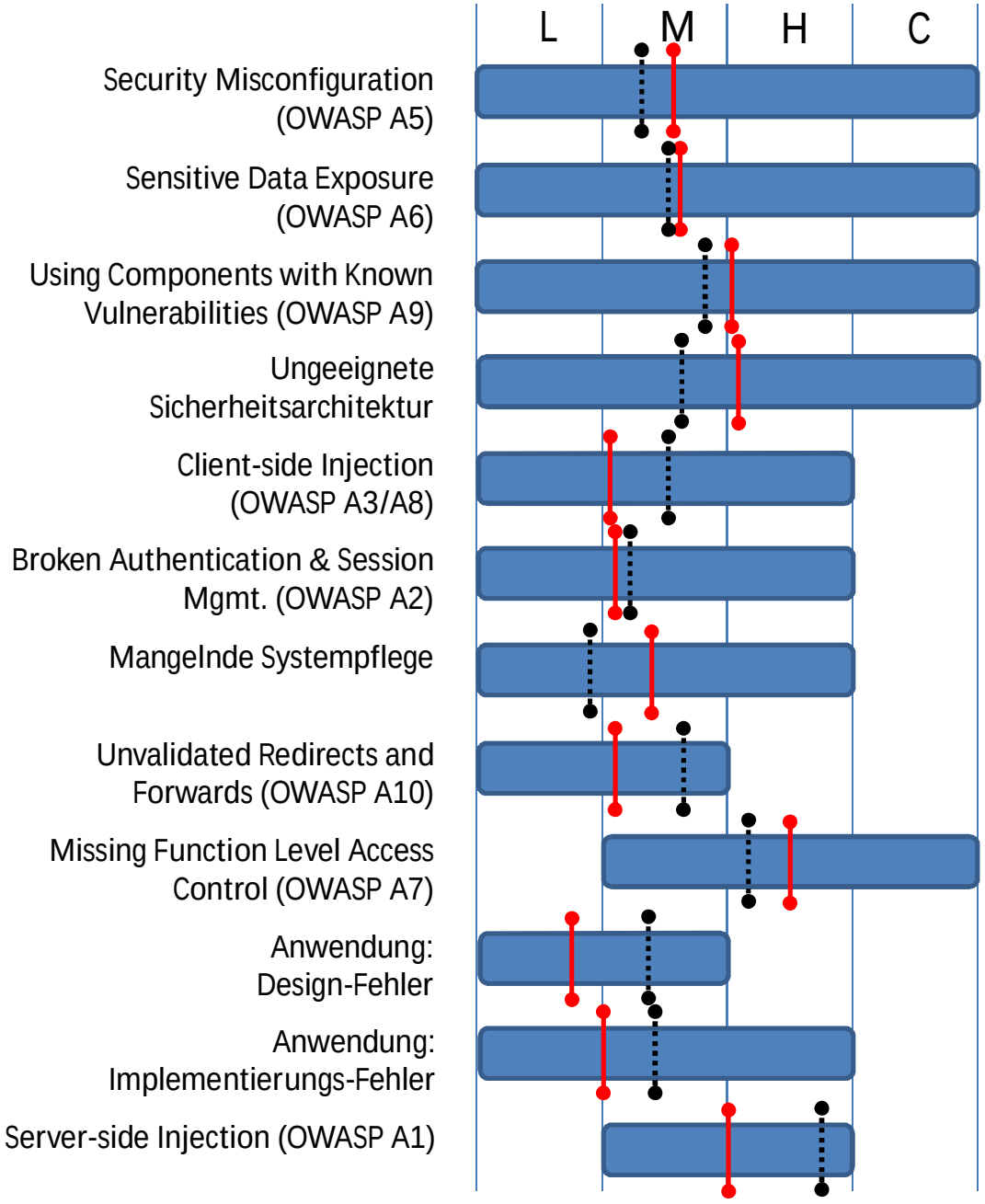
wieder aufgehoben wurden. Zudem hat sich dieser Aspekt von Platz 6 im letzten Jahr auf Platz 3 vorgeschoben. Nach wie vor stellen eine zügige Softwareaktualisierung und das Patch-Management große Herausforderungen dar.

Eng damit verwandt ist eine mangelnde Systempflege, die erheblich öfter als in den Vorjahren auffällig wurde, zudem auch noch mit deutlich höherer Kritikalität. Auch das führen wir auf einen höheren Anteil von internen Untersuchungen zurück, denn gerade interne Systeme sind oftmals nur unzureichend gepflegt, weil man auf die Sicherheit der Abschottung nach außen vertraut – wie sich häufig zeigt, zu unrecht.

Der Spitzenreiter unserer Statistik aus dem letzten Jahr, die mangelhafte Sicherheitskonfiguration, hat seinen Vorsprung wieder ausgebaut und tritt jetzt in fast vier von fünf Untersuchungen auf – das war auch schon 2012 zu beobachten (80,5 Prozent). Dabei ist auch die durchschnittliche Kritikalität der Befunde gestiegen, was auf anhaltend weit verbreitete Mängel beim Konfigurationsmanagement hinweist.

Zusammenfassend zeigt sich eine nach wie vor hohe Gefährdungslage. Einigen Verbesserungen in manchen Kategorien stehen zum Teil überraschend negative Entwicklungen in anderen gegenüber.

In der folgenden Grafik zeigen wir die minimal und maximal vorgenommenen Einstufungen (blaue Balken) und den dabei durchschnittlich gewählten Schweregrad (rote Markierung). Die gestrichelten grauen Linien zeigen die Durchschnittswerte aus dem Vorjahr:



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

Die meist große Bandbreite bei der Bewertung der Schwachstellen innerhalb der einzelnen Kategorien zeigt, 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.

USING COMPONENTS WITH KNOWN VULNERABILITIES (OWASP A9)

Unter diese Kategorie fällt eine Vielzahl von 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, kann 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.

UNGEEIGNETE SICHERHEITSARCHITEKTUR

Relativ häufig 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.

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.

MANGELNDE SYSTEMPFLEGE

In einigen Tests stießen wir auf Umgebungen, die durch mangelnde Systempflege 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.

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 in keinem Fall als hoch zu bewerten.

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.

ANWENDUNG: DESIGN-FEHLER

Designfehler in Anwendungen sind zum Glück selten, dann aber oftmals gefährlich. Die Ausprägungen sind unterschiedlich, Beispiele sind Datenbankzugriff mit administrativen Rechten, Zulassen trivialer Passwörter, unnötige Exportfunktionen, unsichere Schnittstellen oder die ungewollte Preisgabe von Nutzerinformationen.

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 Anwendung 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.

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 oftmals als kritisch ein, im letzten Untersuchungszeitraum waren jedoch nur solche Schwachstellen auszumachen, deren Schadenspotenzial beschränkt war. In weiteren Fällen sind verschiedene andere Arten von Code-Injection-Lücken vorzufinden.

FAZIT

Die Ergebnisse unserer Erhebung von 2014 weisen in einzelnen Kategorien wieder eine hohe Deckung mit den Ergebnissen der vorangegangenen Untersuchung auf und bestätigen damit die Aussagekraft.

Auch wenn die Schwere der Schwachstellen im Durchschnitt weiter abgenommen hat, wurden insgesamt wieder vermehrt Untersuchungen mit kritischen Befunden verzeichnet. Positiv ist natürlich, dass der Anteil der Prüfungen, bei denen keine sicherheitsrelevanten Schwachstellen vorgefunden wurden, weiter anwächst – wenn auch langsam.

Dennoch werden nach wie vor in deutlich mehr als jedem zweiten Fall schwere Befunde verzeichnet, in immer noch 19 % der Prüfungen erforderten diese unmittelbares Eingreifen. Der deutliche Handlungsbedarf aus den letzten Jahren bleibt weiter bestehen. Besonders bei internen Systemen und Anwendungen sehen wir großen Nachholbedarf.

Innerhalb der einzelnen Fehlerkategorien sind Verschiebungen bei der Kritikalität in beide Richtungen zu beobachten. Das zeigt, dass sich die Gesamtsituation nicht entspannt – positive und negative Entwicklungen halten sich die Waage, die Bedrohungslage verschiebt sich nur auf andere Sicherheitsprobleme.

Den Spitzenplatz bei der durchschnittlichen Kritikalität hat inzwischen die Zugriffskontrolle auf funktionaler Ebene übernommen. Solche Befunde treten zwar deutlich seltener auf als in den Vorjahren, erfordern dann aber aufgrund der potenziellen Auswirkungen überdurchschnittlich oft unmittelbares, oftmals provisorisches Handeln. Nach absoluten Zahlen jedoch hat die Verwendung von Komponenten mit bekannten Schwachstellen am häufigsten kritische Auswirkungen.

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