HISOLUTIONS - SCHWACHSTELLENREPORT

Eine Analyse der identifizierten Schwachstellen in Penetrationstests des Jahres 2015

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 46 Penetrations- und Schwachstellentests, die im Jahr 2015 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:

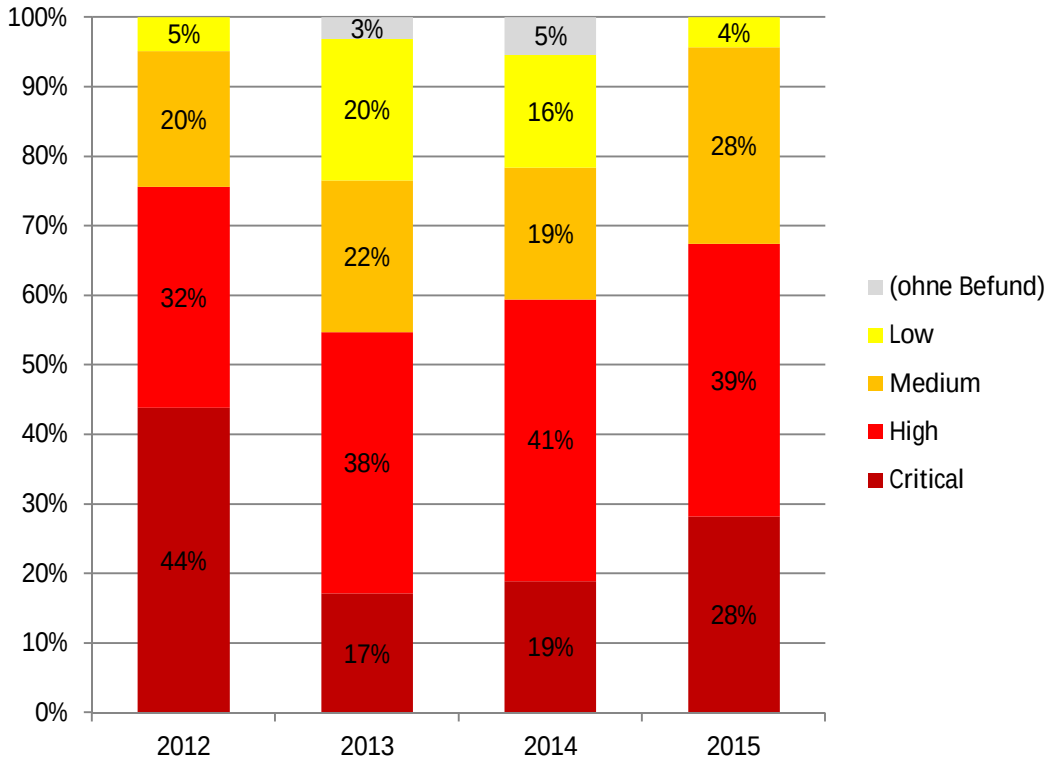
CRITICAL (C)	Die getesteten Systeme sind akut gefährdet, umgehendes Handeln ist (in der Regel noch während der Testdurchführung) erforderlich.
HIGH (H)	Die Schwachstelle hat eine hohe praktische Relevanz und sollte priorisiert behoben werden.
MEDIUM (M)	Die Schwachstelle besitzt ein relevantes Schadenspotenzial, 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 unserer Schwachstellenreports von 2012 bis 2014 verglichen.

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

Auch wenn sich im Vergleich der letzten Jahre immer wieder leichte Verschiebungen ergeben haben, bleibt doch die Befundlage über die Jahre insgesamt relativ gleich. 2015 hat dabei insbesondere der Anteil von kritischen Schwachstellen in unseren Tests wieder deutlich zugenommen:



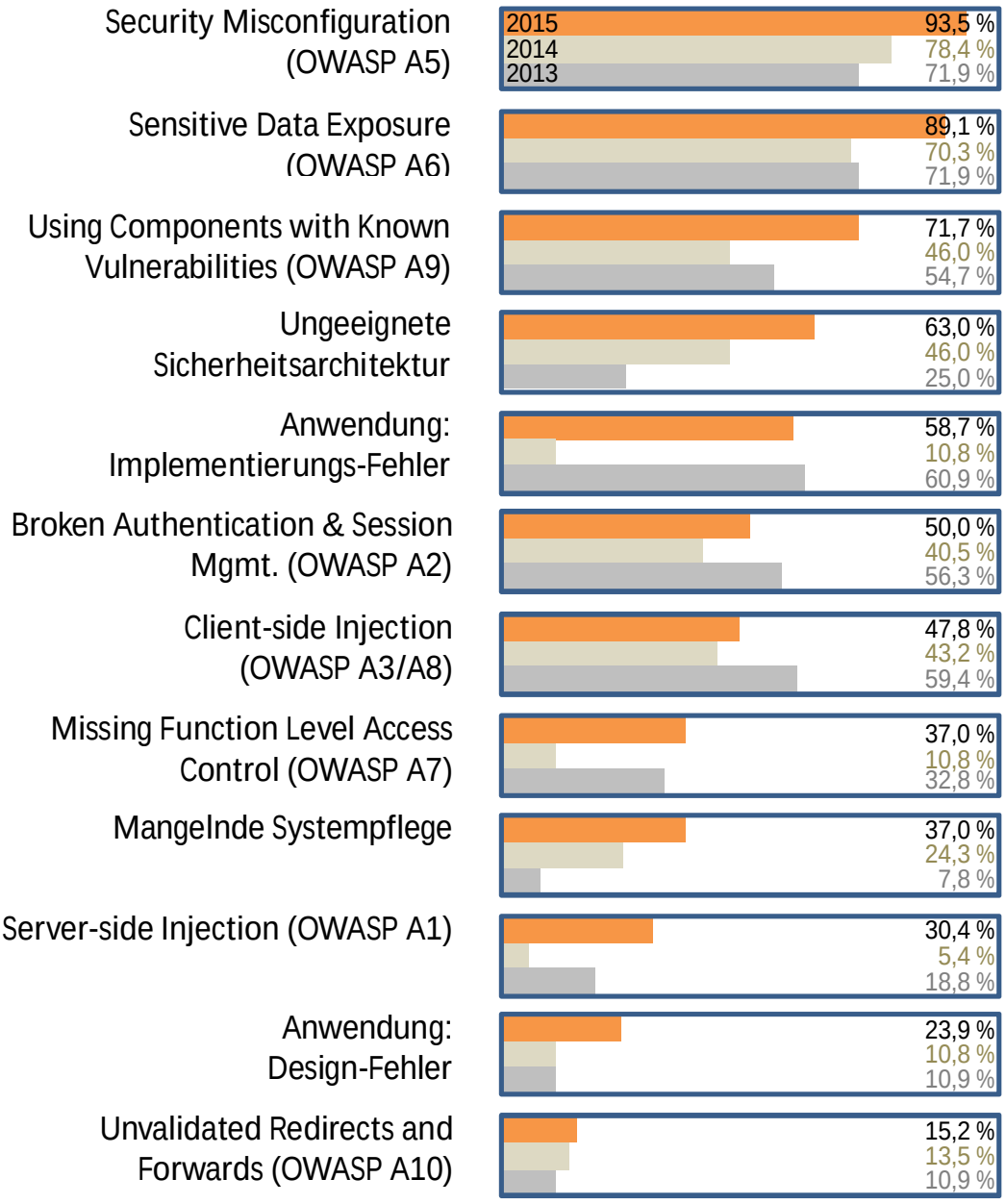
Maximale Kritikalität in Untersuchungen der letzten vier Jahre

Das Phänomen der letzten beiden Jahre, in denen wir zumindest vereinzelt auch Prüfungen ohne Befund abgeschlossen haben, hat sich 2015 nicht fortgesetzt. Auch Tests mit nur geringen Verbesserungsmöglichkeiten waren 2015 eine deutliche Ausnahme (4 %). Der Anteil von Tests mit schweren und kritischen Befunden ist wieder gestiegen und umfasst jetzt gut zwei Drittel unserer Projekte (67 %). Bei mehr als jedem vierten Projekt bestand unmittelbarer Handlungsbedarf (28 % kritische Befunde).

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), Probleme bei der Zugriffskontrolle auf funktionaler Ebene (OWASP A7) sowie eine mangelhafte Sicherheitskonfiguration (OWASP A5) oder ungeeignete Architekturen. Einen großen Anteil an mit „hoch“ bewerteten Problemen machen darüber hinaus Informationen aus, die ohne ausreichenden Schutz abrufbar waren (Sensitive Data Exposure, OWASP A6). Es findet sich also weiterhin eine breite Mischung aus Problemen in der Entwicklung, der Konfiguration und dem Betrieb von IT-Infrastrukturen.

Die folgende Grafik zeigt die von uns definierten Schwachstellenkategorien jeweils mit der Häufigkeit ihres Auftretens im Projekt, verglichen mit den beiden Vorjahren:



Zunächst sind die sehr hohen Häufigkeiten von Konfigurationsfehlern (OWASP A5) und ungeschützt abrufbaren Informationen (OWASP A6) auffällig, die jeweils in ungefähr 9 von 10 Projekten aufgetreten sind. Ungefähr jeder dritte Fund war dabei als schwerwiegend oder kritisch einzustufen. Dies zeigt unseres Erachtens, wie schwierig es für Unternehmen heute ist, die Komplexität von IT-Infrastrukturen ausreichend zu beherrschen.

Auch das Patchmanagement, das eigentlich sicherstellen müsste, dass Softwareversionen mit bekannten Schwachstellen aktualisiert werden, bleibt eine Herausforderung, die nur wenige Unternehmen durchgängig meistern. In fast drei Vierteln unserer Tests haben wir veraltete Software mit bekannten Schwachstellen im Betrieb gefunden.

Einen beständigen Anstieg haben wir in den letzten drei Jahren in der Kategorie „ungeeignete Sicherheitsarchitektur“ verzeichnen können. Diese Kategorie umfasst fehlende oder falsch implementierte Sicherheitsmechanismen, häufig jedoch auch eine ungeeignete Segmentierung von Netzen oder Platzierung von Systemen in Sicherheitszonen. Solche Architekturprobleme sind im Betrieb oft nur mit hohem Aufwand zu beheben. IT-Sicherheitsaspekte sollten daher in IT-Projekten möglichst frühzeitig berücksichtigt werden.

Der im vorigen Jahr beobachtete starke Rückgang bestimmter Problemarten (Implementierungsfehler, Missing Function Level Access Control und Server-Side-Injections) hat sich im laufenden Jahr nicht fortgesetzt, sondern scheint einen einmaligen „Ausreißer“ darzustellen. Da es sich hierbei durchgängig um typische Fehler in der Entwicklung von serverseitigen Anwendungen handelt, könnte sich dieser Effekt darin begründen, dass solche Anwendungen 2014 unter den zu prüfenden Umgebungen einfach weniger vertreten waren.

Auch im Bereich des Session Managements zeichnet sich keine klare Verbesserung der Situation ab, die Befundquote pendelt hier um einen Wert von 50 %. Obwohl etablierte Frameworks für das Session Management bereitstehen, werden hier immer wieder Fehler durch eigene Implementierungen gemacht, die eigentlich leicht vermeidbar wären.

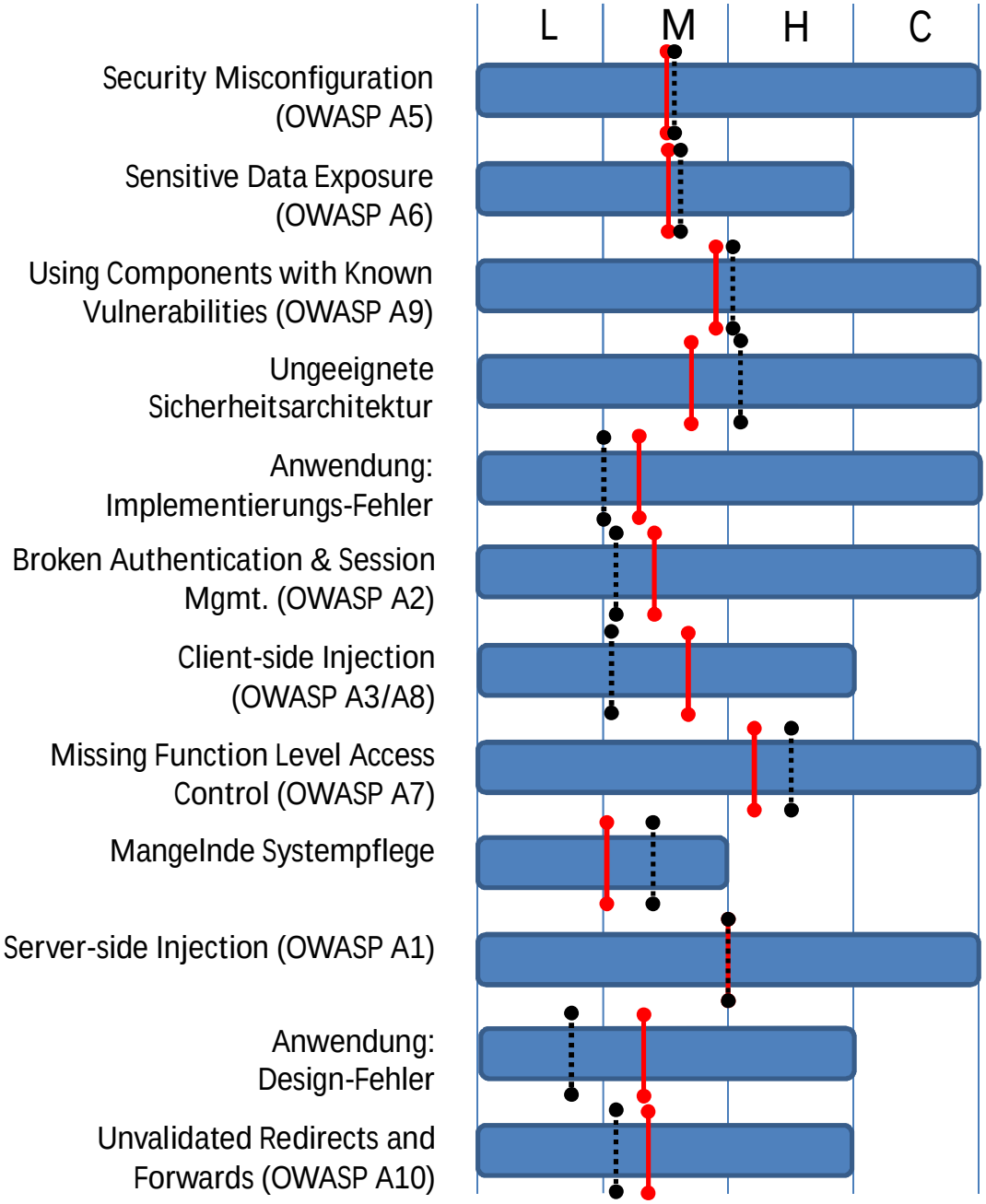
Ähnlich häufig bleiben client-seitige Injection-Angriffe, bei denen immer noch das sogenannte Cross-Site-Scripting dominiert. Auch wenn solche Probleme alles andere als harmlos sind, weil sie insbesondere die Nutzer einer Anwendung täuschen und zur Preisgabe von Informationen und Kennwörtern verleiten können, stellen sie meistens keine Gefahr für die Anwendung insgesamt dar und sind daher zwar gelegentlich als „hoch“, aber in keinem Fall als kritisch eingestuft worden. Der mittlere Schweregrad solcher Schwachstellen hat aber im Vergleich zum Vorjahr deutlich zugenommen (siehe folgende Grafik).

Interessant ist auch der stetige Zuwachs in der Kategorie „Mangelnde Systempflege“. Die Kategorie umfasst dabei nicht veraltete Software, die wir ja in der eigenen Kategorie OWASP A9 führen. Hier sind andere Probleme der Pflege von Systemen zusammengefasst, z. B. der Einsatz von Debugging- und Testfunktionen auf Produktivsystemen, veraltete Konfigurationseinstellungen, nicht benötigte Dienste und vergleichbare Nachlässigkeiten. Allerdings erreichten diese Probleme in keinem Fall eine Bewertung als „hoch“ oder „kritisch“.

Serverseitige Injection-Schwachstellen sind zwar im Vergleich zu den übrigen Kategorien seltener, haben aber nach wie vor einen hohen durchschnittlichen Schweregrad: In der Regel erlauben diese Schwachstellen einem Angreifer weitreichende Manipulationsmöglichkeiten von Daten oder sogar die Übernahme kompletter Systeme. Vom Schweregrad wird diese Kategorie nur noch von fehlenden Berechtigungsprüfungen (OWASP A7) übertroffen, mit denen ebenfalls häufig sehr weitreichende unbefugte Zugriffe – nicht selten auch administrativer Art – möglich sind.

Zusammenfassend bleiben die Ergebnisse der Tests besorgniserregend. Auch die erhöhte Aufmerksamkeit der Öffentlichkeit für IT-Sicherheitsthemen hat offenbar kaum zu erkennbaren Verbesserungen in den tatsächlich betriebenen IT-Infrastrukturen geführt.

In der folgenden Grafik zeigen wir die minimal und maximal vorgenommenen Einstufungen (blaue Balken) und den dabei durchschnittlich gewählten Schweregrad (rote Markierung). Die gestrichelten schwarzen 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 unter „medium“ und liegt etwas niedriger 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.

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.

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.

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.

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.

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.

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.

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.

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.

FAZIT

Die Ergebnisse unserer Erhebung von 2015 weisen in vielen Kategorien wieder eine hohe Deckung mit den Ergebnissen der vorangegangenen Untersuchung auf und bestätigen damit die Aussagekraft, auch wenn einzelne „Ausreißer“ des Vorjahres zeigen, dass die Ergebnisse natürlich auch gewissen Schwankungen unterliegen.

Die Schwere der gefunden Schwachstellen hat wieder deutlich zugenommen. Insbesondere der Anteil von Projekten mit kritischen Schwachstellen hat sich im letzten Jahr deutlich erhöht – auf jetzt immerhin 28 %. Der Anteil von Projekten mit mindestens einem schweren Befund ist auf insgesamt zwei Drittel angestiegen. In keinem einzigen Test war die geprüfte Umgebung frei von Sicherheitsmängeln.

Innerhalb der einzelnen Fehlerkategorien sind Verschiebungen bei der Kritikalität in beide Richtungen zu beobachten, weisen aber auch hier eher eine Tendenz nach oben auf. Auch klassische Fehler in der Anwendungsentwicklung werden nicht weniger. Die zunehmende Verfügbarkeit ausgereifter Entwicklungsframeworks, die uns noch im letzten Jahr Hoffnung auf ein weiteres Abnehmen von Standardproblemen gemacht hat, hat die Erwartungen dahingehend enttäuscht. Vielleicht sind hier doch noch längere Zeiträume erforderlich, bis sich dieser Effekt in der Praxis erkennbar niederschlägt.

Den Spitzenplatz bei der durchschnittlichen Kritikalität hat wie im Vorjahr die fehlende Zugriffskontrolle auf funktionaler Ebene eingenommen. Solche Befunde erfordern 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 – auch dies war schon im Vorjahr der Fall.

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