HISOLUTIONS

SCHWACHSTELLEN-REPORT 2020

Entwicklungen & Trends 2013-2019

Stand 7. Mai 2020

HISOLUTIONS

INHALTSVERZEICHNIS

MOTIVATION

HiSolutions führt jedes Jahr eine große Anzahl von unterschiedlichen Penetrations- und Schwachstellentests durch. Immer wieder taucht dabei die Frage auf, wie die Ergebnisse des einzelnen Tests im Vergleich mit „typischen" Pentest-Ergebnissen einzustufen sind und ob die identifizierten Probleme bei anderen Unternehmen in ähnlicher Form und Schwere bestehen.

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

VORGEHEN

Dieser Report beruht auf einer Auswertung der Ergebnisse aus insgesamt 90 Penetrations- und Schwachstellentests, die im Jahr 2019 durchgeführt wurden. Zusätzlich wurden die Befunde mit den Ergebnissen der Schwachstellenreports aus den Jahren 2013 bis 2018 verglichen.

Die Tests betreffen verschiedene Zielumgebungen, von Netzwerkinfrastrukturen über Web-Anwendungen bis hin zu einzelnen Systemen und Verfahren, weswegen sie nicht direkt miteinander vergleichbar sind. Durch die Kategorienbildung bei den Schwachstellen lassen sich dennoch interessante Beobachtungen ableiten.

Für die Kategorien wurde sich zunächst an den „OWASP Top 10" orientiert. Diese Veröffentlichung des OWASP-Projektes aus dem Jahr 2017[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 zum Teil auch auf andere Testziele gut übertragen, decken jedoch nicht alle Befunde vollständig ab, sodass einige selbst erstellte Kategorien ergänzt wurden. Diese umspannen den gesamten Zyklus der Softwareentwicklung und des Betriebs von Architektur und Design über Implementierung bis hin zur Systempflege. Dadurch lassen sich auch entsprechende Sicherheitslücken jenseits von Web-Anwendungen feingranular einordnen.

In diesem Jahr wurden die Kategorien gegenüber den Vorjahren aktualisiert, um vollständig mit der aktuellsten „OWASP Top 10" Liste übereinzustimmen. Die Kategorien „Insecure Direct Object Reference (OWASP A4)" und „Missing Function Level Access Control (OWASP A7)" wurden zu der

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

Kategorie „Broken Access Control (OWASP A5)“ zusammengefasst. Die Kategorie „Client-Side (OWASP A3/ A8) Injection“ wurde in „Cross-Site Scripting (OWASP A5)“ umbenannt. Diese Kategorie fasste in Vorjahresberichten die Kategorien „Cross-Site Scripting“ und „Cross-Site Request Forgery“ zusammen. Da letztere jedoch aus der OWASP Top 10 Liste verschwunden ist, wird sie nicht mehr separat aufgelistet. Neu hinzugekommen ist außerdem die Kategorie „Insufficient Logging and Monitoring (OWASP A10)“. Nicht geführt werden die Kategorien „XML External Entities (OWASP A4)“ und „Insecure Deserialization (OWASP A8)“, da diese selten zur Einteilung verwendet wurden.

Die Aggregation der Daten bringt einige praktische Schwierigkeiten mit sich: Aufgrund der Verschiedenartigkeit der durchgeführten Tests ließen sich keine relevanten Aussagen zur Häufigkeit von Schwachstellen in einem bestimmten System oder einer Anwendung ermitteln. Auch werden in den Projektberichten gleichartige Schwachstellen auf verschiedenen Systemen häufig zu einem Befund zusammengefasst, sodass eine Zählung der Befunde hier ebenfalls nur begrenzte Aussagekraft hat. Aufgrund dessen wurde beschlossen, als Maß die relative Häufigkeit von Projekten, in welchen ein Befund der entsprechenden Kategorie auftaucht, zu verwenden. Dadurch wird deutlich, welchen Schwachstellen man in unterschiedlichen Projekten besonders häufig begegnet und welche eher selten oder nur in besonderen Zielumgebungen auftauchen.

Für die Bewertung der Relevanz einer Schwachstelle wird in den Prüfberichten ein standardisiertes Schema verwendet, welches aus der Bewertung der Komplexität des Angriffs und des zu erwartenden Schadens zu einer Einordnung in die folgenden Kategorien führt:

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 Auswertung nicht berücksichtigt.

ERGEBNISSE

Die Erkenntnisse der Auswertung aller Penetrationstests des letzten Jahres sollen im Folgenden vorgestellt werden. Dazu werden die durch Tests aufgedeckten Sicherheitslücken im Kontext der Entwicklungen über die letzten Jahre betrachtet. Verwendet wird dafür die Kategorie und der

Schweregrad jeder Schwachstelle. Erstmals wird in diesem Jahr auch die Art des durchgeführten Tests berücksichtigt und die Effizienz der im Anschluss an Penetrationstests durchgeführten Maßnahmen bewertet.

Abbildung 1 zeigt die Entwicklung des Schweregrades von Sicherheitslücken von 2013 bis 2019. Dieser Schweregrad wird im Folgenden auch als Kritikalität bezeichnet. Für die Generierung der Werte wurde jedem durchgeführten Penetrationstest die maximale Kritikalität aller von ihm aufgedeckten Sicherheitslücken zugeordnet. Ein Penetrationstest, welcher eine kritische Sicherheitslücke aufgedeckt hat, wird daher als kritisch eingestuft. Dies ist dadurch zu begründen, dass eine einzige Lücke des entsprechenden Schweregrades ausreicht, die Sicherheit des gesamten Systems zu beeinträchtigen. Seit 2013 sind Schwankungen ohne eindeutige Tendenz in der Entwicklung der Kritikalität von Penetrationstests zu verzeichnen. Nach einem Rückgang der als *kritisch* oder *hoch* eingestuften Penetrationstests von 2015 bis 2018 war im letzten Jahr erstmals wieder ein deutlicher Zuwachs zu erkennen. Nur im Jahr 2015 lieferte ein größerer Anteil der Tests schwerwiegende Befunde. Dies liegt im Rahmen der kurzzeitigen Schwankungen und muss nicht auf einen Negativtrend verweisen. Dennoch weist es darauf hin, dass trotz der erhöhten öffentlichen Aufmerksamkeit für das Thema IT-Sicherheit aus den betrachteten Untersuchungen keine grundlegende Verbesserung in diesem Bereich über die letzten Jahre abgeleitet werden kann.

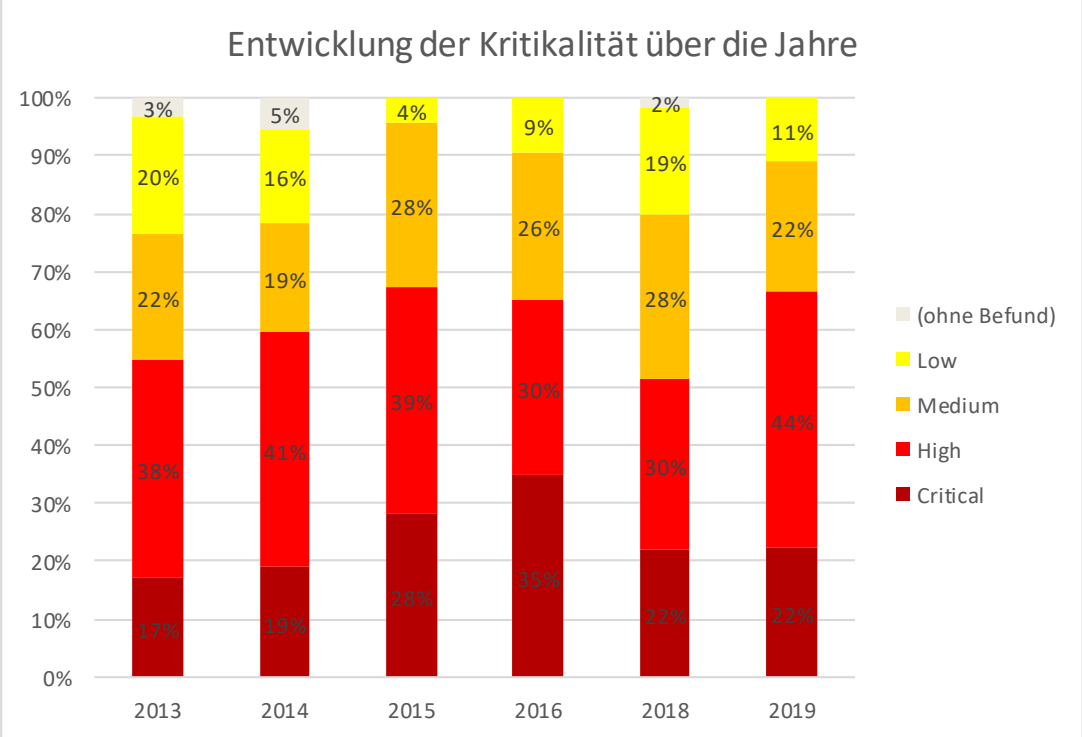

Abbildung 1: Entwicklung der Kritikalität von 2013 bis 2019

Um die Sicherheit von bestehenden Systemen zu verbessern und Sicherheitsaspekte im Entwurf neuer Systeme zu berücksichtigen, ist es wichtig zu verstehen, welche Art von Sicherheitslücken besonders häufig auftritt und welche Auswirkungen dies haben kann.
In Abbildung 2 wird daher zunächst die Entwicklung des Auftretens bestimmter Fehlerklassen in den letzten Jahren gezeigt. Dargestellt wird der Anteil der Penetrationstests, welche mindestens einen Befund der Kategorie erzeugt haben.
Abbildung 3 zeigt die Schwere der Befunde dieses Jahres aufgeschlüsselt nach Kategorie. Angegeben wird dabei der Anteil der unterschiedlichen Kritikalitätswerte an den Gesamtbefunden der jeweiligen Kategorie.

Auch für das Jahr 2019 konnten viele verschiedene Probleme bei der Entwicklung, Konfiguration und dem Betrieb von Software beobachtet werden. Die Häufigkeit, mit der sensible Daten preisgegeben wurden, nahm im Vergleich zu den Vorjahren deutlich ab. Dennoch traten diese Fehler weiterhin in über der Hälfte aller Tests auf. Deutlich zugenommen hat im Jahr 2019 erneut die Anzahl der Penetrationstests, welche fehlerhafte Konfigurationen mit Folgen für die Sicherheit eines Systems aufdecken konnten. In neun von zehn Tests wurde eine derartige Fehlkonfiguration identifiziert. Zwar entstanden aus beiden Kategorien meist lediglich geringe Sicherheitsrisiken, doch sind bei groben Fehlern auch schwerwiegende Auswirkungen möglich.

Sowohl OWASP A3 als auch OWASP A6 sind typische Fehlerklassen, welche aus Fehlern im Betrieb von Software und nicht in deren Entwicklung entstehen. Die erhoffte Verbesserung im Umgang mit IT-Systemen kann also bedauerlicherweise nicht oder nur in Teilen beobachtet werden.

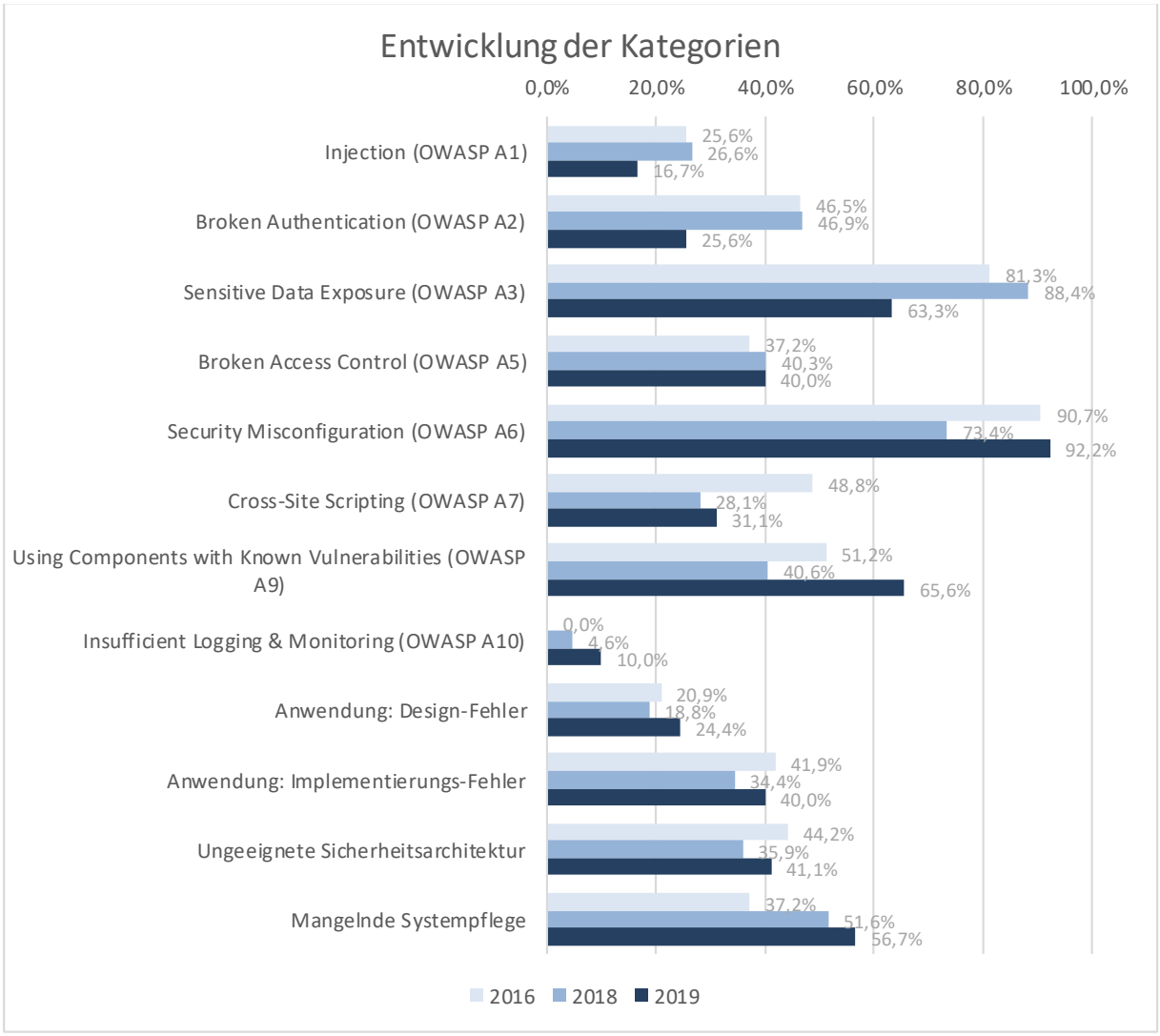

Abbildung 2: Häufigkeit der Kategorien von 2016 bis 2019

Besonders bedenklich ist die deutliche Zunahme der Häufigkeit von 41% auf 66%, mit der Komponenten mit bekannten Schwachstellen eingesetzt wurden. Da Informationen zu diesen Schwachstellen und in vielen Fällen darüber hinaus Exploits, welche sie ausnutzen, öffentlich verfügbar sind, haben Fehler dieser Art besonders häufig kritische oder schwere Auswirkungen[2] auf die Sicherheit eines IT-Systems. Diese Schwachstellen entstehen in der Regel durch ein mangelhaftes Patch-Management, welches sicherstellen sollte, dass verwundbare Software aktualisiert wird. Die Etablierung eines funktionierenden Patch-Managements bzw. einer kontinuierlichen Systempflege stellt also weiterhin eine

[2] Schwachstellen oder Sicherheitslücken, welche mit der Kritikalität „hoch" eingestuft wurden, werden im Folgenden häufig auch als „schwere Sicherheitslücken" oder „Sicherheitslücken mit (potentiell) schweren Folgen" bezeichnet.

Herausforderung für viele Unternehmen dar. Dies verdeutlicht auch die Kategorie „mangelnde Systempflege“, welche allgemeine Fehler dieser Art beinhaltet und in mehr als der Hälfte aller Tests gefunden wurde. Dadurch entstanden häufig kritische oder schwere Sicherheitslücken.

Auch Schwachstellen, welche durch Fehler im Entwurf und in der Entwicklung von Softwaresystemen entstehen, wurden durch Penetrationstests im Jahr 2019 aufgedeckt. Besonders eine ungeeignete Systemarchitektur führt dabei zu schwerwiegenden Fehlern. Dennoch konnte eine solche in 41% aller Penetrationstests festgestellt werden. Ähnlich häufig treten Implementierungsfehler auf. Design-Fehler konnten in etwa einem Viertel aller Penetrationstests festgestellt werden. Wie schwerwiegend die Folgen fehlerhafter Softwareentwicklung sein können, verdeutlicht die Kategorie *fehlerhafte Zugriffskontrolle*, welche über die letzten Jahre in etwa 40% der Penetrationstests zu finden war und wenn vorhanden in mehr als 40% der Fälle als *kritisch* oder *hoch* eingestuft wurde. Laut unserer Erfahrungen aus Sicherheitsaudits werden Sicherheitsfragen in IT-Projekten häufig erst im Zuge der Betriebseinführung betrachtet, also nachdem vormals genannte Probleme bereits entstanden sind. Dies ist besonders problematisch, da die Auswirkungen von Fehlern schwerer sind, je früher der Entwicklungsschritt ist, in dem sie auftauchten. So wiegen im Mittel Fehler in Architektur und Design deutlich schwerer als solche in der Implementierung.

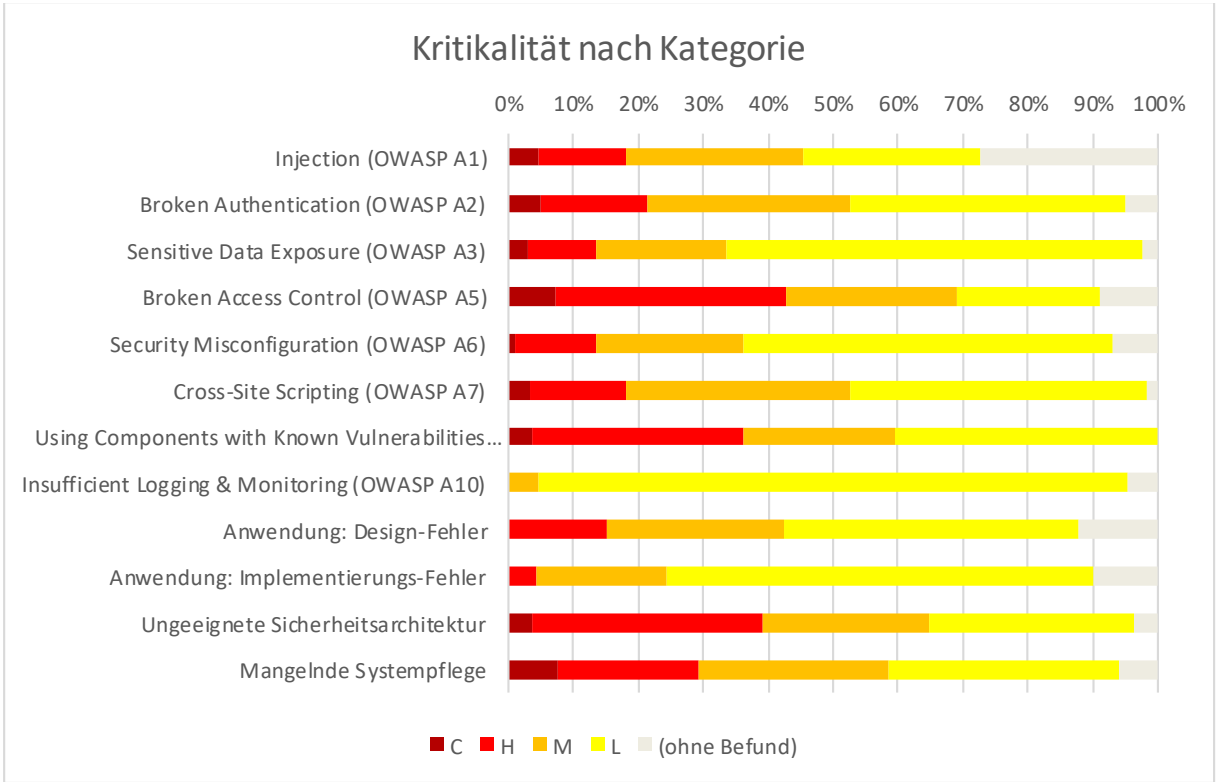

Abbildung 3: Kritikalität der Befunde nach Kategorie

Unzureichendes Monitoring und Logging wird im diesjährigen Bericht erstmals betrachtet. Es tritt in lediglich 10% der Tests auf und birgt ein lediglich geringes bis mittleres Risiko. Es kann jedoch das Aufspüren von Angriffen und deren Aufklärung deutlich verzögern und erschweren und sollte daher nicht vernachlässigt werden.

Die meisten kritischen Sicherheitslücken nach absoluten Zahlen waren eine Folge von mangelnder Systempflege. Auf den nächsten Plätzen folgt die Verwendung von Komponenten mit bekannten Sicherheitslücken und die Preisgabe sensibler Informationen. Auch Fehlkonfigurationen, Fehler bei der Authentifizierung und eine ungeeignete Systemarchitektur führten häufig zu kritischen Sicherheitsproblemen.
Betrachtet man ebenfalls Sicherheitsprobleme mit einer hohen Kritikalität, so liegen eine fehlerhafte Zugriffskontrolle und eine ungeeignete Systemarchitektur noch vor der Nutzung unsicherer Komponenten und mangelnder Systempflege.

Auch in Betrachtung der Einzelkategorien ist über die letzten Jahre keine Verbesserung der Sicherheitseigenschaften von IT-Systemen zu beobachten. Es bestehen weiterhin eine Vielzahl unterschiedlicher Fehlerquellen, welche die Sicherheit von Systemen beeinträchtigen können. In der Aufteilung der Fehlerkategorien setzen sich die Trends der Vorjahre fort. Es ist deutlich zu beobachten, dass es bei Konfiguration, Betrieb und Wartung von IT-Systemen zu den meisten sicherheitskritischen Fehlern kommt. Probleme in diesem Bereich werden wie in den Vorjahren in fast jedem Penetrationstest festgestellt. Auch Probleme in der Entwicklung bleiben eine Gefahrenquelle mit großem Schadenspotenzial. Sie konnten zwar in weniger Penetrationstests aufgedeckt werden, bergen jedoch, falls vorhanden, teilweise gravierende Risiken.

Auswertung nach Testtyp

Die HiSolutions AG bietet eine Vielzahl unterschiedlicher Sicherheitsüberprüfungen an. Besonders häufig werden externe Penetrationstests und Web-Penetrationstests ausgeführt, bei denen das Testteam die gleichen Möglichkeiten wie externe Angreifer besitzen. Es werden jedoch auch interne Penetrationstests vorgenommen. Bei diesen stehen dem Testteam wesentlich mehr Möglichkeiten zur Verfügung, da sie sich im internen Netz des Auftraggebers befinden. Auch die Überprüfung von Quellcode, Architektur und Konfiguration von IT-Systemen wird von der HiSolutions angeboten. Ebenso können fertige Applikationen oder Betriebsstrukturen und Dokumentationen erprobt werden.

Abbildung 4 zeigt die Kritikalität abhängig von dem Typ des durchgeführten Tests. In einem Penetrationstest können mehrere Überprüfungen unterschiedlicher Art vorhanden sein. Für die Auswertung werden die einzelnen Testbestandteile aller Penetrationstests betrachtet.
Die in Abbildung 4 dargestellte Kritikalitätsverteilung ergibt sich, wie in vorherigen Auswertungen, aus der Zuordnung jedes Testbestandteils zu seiner maximal enthaltenen Kritikalität. Für eine bessere Vergleichbarkeit werden relative Häufigkeiten dargestellt.

Verallgemeinert lässt sich die Auswertung der Befunde auf die Aussage komprimieren: Je mehr Zugang das Testteam hat, desto kritischer die aufgedeckten Sicherheitslücken. In internen Penetrationstests konnten in etwas weniger als 40% der Fälle kritische und in knapp 80% der Fälle mindestens schwere Sicherheitslücken entdeckt werden. Auch in Dokumentations- oder Organisationsaudits und Applikations- oder API-Tests wurden häufig kritische Schwachstellen aufgedeckt. Auch wenn

Konfigurationsaudits oder Architekturreviews in verhältnismäßig wenigen Fällen kritische Sicherheitslücken aufgedeckt haben, so konnten sie doch eine erhebliche Anzahl schwerer Mängel finden. Externe und Web-Pentests, bei welchen das Testteam deutlich weniger Zugriffsrechte hat als in den vorangegangenen Testtypen, konnten in deutlich weniger Fällen kritische oder schwere Sicherheitslücken aufdecken. Dennoch wurden auch bei diesen Tests in etwa 30% bis 40% der Fälle kritische oder schwere Sicherheitslücken gefunden, sodass ihre Effektivität nicht zu unterschätzen ist. Lediglich in einer sehr kleinen Anzahl von Tests wurden keine Befunde festgestellt.[3]

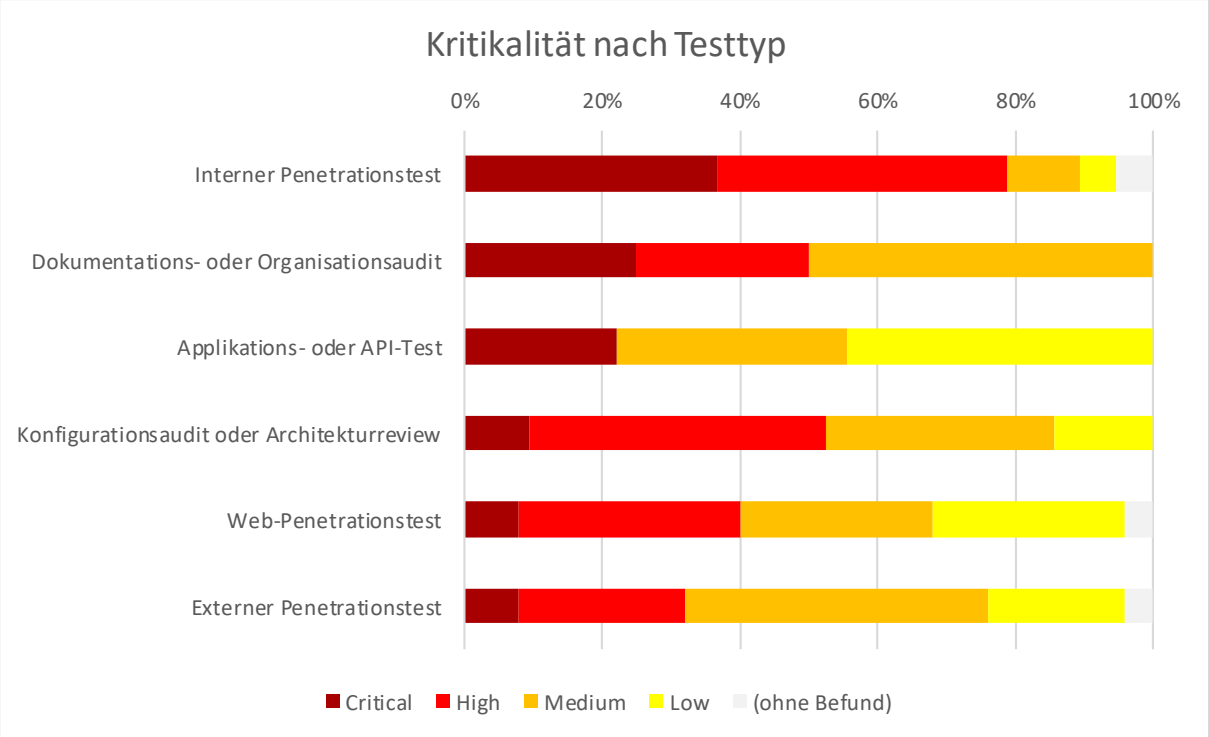

Abbildung 4: Kritikalität nach Testtyp

Auswertung der Nachtests

Anbieter von Penetrationstests empfehlen in der Regel eine Verifikation der im Anschluss umgesetzten Maßnahmen als wirkungsvolles Mittel zur Verbesserung der Sicherheitseigenschaften von IT-Systemen. Die tatsächliche Wirksamkeit wird im Folgenden überprüft. Zu diesem Zweck werden Befunde betrachtet, bei denen ein Nachtest stattgefunden hat, also eine Überprüfung der nach dem Penetrationstest implementierten Maßnahmen.

[3] Differenzen zu Abbildung 1 in welcher kein einziger Penetrationstest ohne Befund zu verzeichnen ist, sind dadurch zu erklären, dass ein Penetrationstest aus mehreren Teilen bestehen kann und somit lediglich ein Teil des Tests ergebnislos geblieben sein kann.

Abbildung 5 zeigt die Anzahl der Befunde und deren Kritikalität nach Kategorien. Der obere Balken bezieht sich dabei auf die Befunde im Penetrationstest, der untere auf die Befunde im Nachtest.[4]

Alles in allem ist eine Abnahme der Kritikalität von ursprünglichem Penetrations- zu Nachtest zu erkennen. Insbesondere sicherheitskritische Fehlkonfigurationen und Fehler bei der Zugriffskontrolle wurden häufig vollständig beseitigt, da dies in vielen Fällen mit geringem Aufwand möglich ist. Dahingegen kam die Preisgabe sensibler Informationen auch in vielen Nachtests weiterhin zum Tragen. Allgemein kann beobachtet werden, dass ein Befund eher behoben oder zumindest teilweise behoben wurde, je höher seine Kritikalität eingestuft war.

Insgesamt wurde gut die Hälfte aller Sicherheitsmängel bis zum Nachtest komplett beseitigt. Die Anzahl der kritischen und schweren Befunde reduzierte sich auf weniger als ein Drittel der ursprünglichen Befunde. Es lässt sich also bestätigen, dass mit Hilfe von Penetrationstest die Sicherheitseigenschaften einer Systemlandschaft deutlich verbessert werden können. Zu beachten bleibt jedoch, dass knapp die Hälfte der entdeckten Sicherheitslücken bis zum Nachtest nicht befriedigend geschlossen wurde. Dies zeigt, dass in einigen Fällen die Risiken der durch den Penetrationstest offengelegten Schwachstellen ernster genommen werden müssen und schneller reagiert werden muss.

[4] Da lediglich Befunde betrachtet werden, für welche ein Nachtest stattgefunden hat, können nur etwa 20% der Befunde verwendet werden. Es kann daher zu Abweichungen zu Abbildung 3 kommen, da für diese mehr Datenpunkte zur Verfügung stehen. Die Kategorie „Insufficient Logging & Monitoring (OWASP A10)“ wird mangels Daten nicht berücksichtigt.

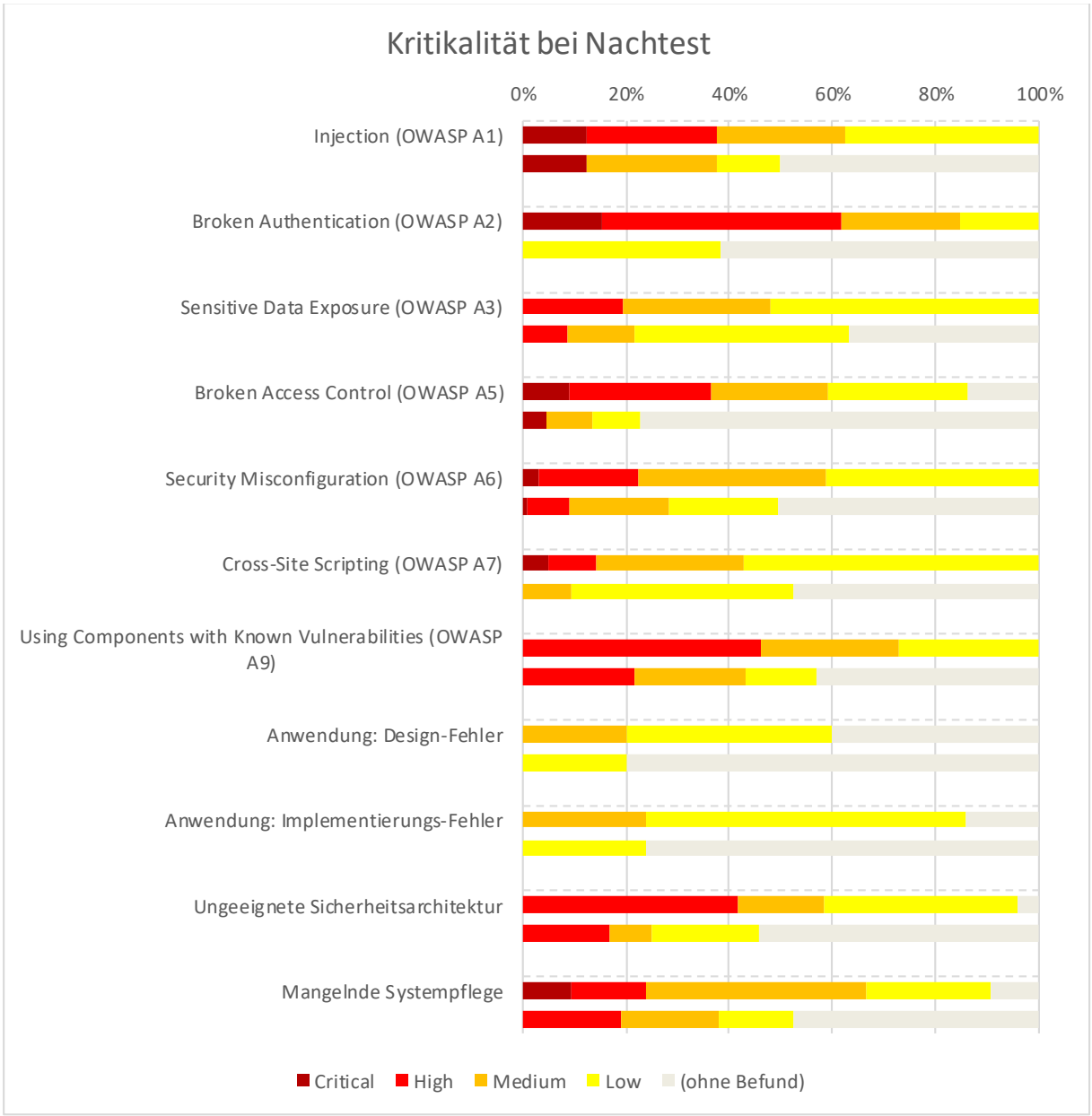

Abbildung 5: Kritikalität von Penetrationstest zu Nachtest

INJECTION (OWASP A1)

Ähnlich wie bei Cross-Site-Scripting-Angriffen bringt bei der Injection ein Angreifer einen 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.

BROKEN AUTHENTICATION (OWASP A2)

In diese Kategorie fallen Fehler, die mit fehlerhafter Authentifizierung oder Sitzungsverwaltung zusammenhängen. Durch diese wird es Angreifern erlaubt Passwörter, Schlüssel oder Sitzungs-Tokens zu kompromittieren oder auf andere Weise temporär oder permanent eine falsche Identität anzunehmen. In den letzten Jahren konnten über 30 verschiedene Arten von Einzelbefunden identifiziert werden. 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.

SENSITIVE DATA EXPOSURE (OWASP A3)

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.

BROKEN ACCESS CONTROL (OWASP A5)

Fehler dieser Kategorie entstehen, falls Restriktionen hinsichtlich der Handlungserlaubnis authentifizierter Nutzer nicht korrekt umgesetzt werden. Angreifern ist es dadurch möglich, unerlaubt auf Daten oder Funktionen zuzugreifen. So kann es ihnen möglich sein die Daten anderer Nutzer einzusehen oder zu verfälschen, andere sensible Dateien zu lesen oder Zugriffsrechte zu manipulieren.

SECURITY MISCONFIGURATION (OWASP A6)

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, sodass die meisten Einstufungen hier niedrig bis mittel ausgefallen sind. Kritisch sind lediglich bestimmte Fälle der Preisgabe von Informationen über technische Konfigurationsdaten, Directory-Listings oder nicht gelöschte Beispiel- und Hilfedateien, die in den entsprechenden Fällen jeweils einen unmittelbaren Ansatzpunkt für Angriffe gaben.

CROSS-SITE SCRIPTING (OWASP A7)

Cross-Site-Scripting-Angriffe basieren auf dem Prinzip, dass der Angreifer in die Anwendung einen Programmcode einbringt, der auf dem Client eines Anwenders ungewollt zur Ausführung gelangt. Dabei handelt es sich meist um reflektiertes XSS (also dem Anwender über einen Link untergeschobenes), vereinzelt auch um persistentes XSS (dauerhaft in die Anwendung eingebrachten Schadcode).

USING COMPONENTS WITH KNOWN VULNERABILITIES (OWASP A9)

Unter diese Kategorie fällt eine Vielzahl von Schwachstellen, die insbesondere aus einem mangelhaften Software- und Patchmanagement resultiert: 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.

INSUFFICIENT LOGGING & MONITORING (OWASP A10)

Unzureichendes Logging und Monitoring verzögert die Entdeckung einer Kompromittierung. Durch die zusätzliche Zeit ist es Angreifern möglich weitere Systeme zu infizieren, mehr Daten zu sammeln oder zu manipulieren. Des Weiteren wird die Identifizierung des Einfallstores eines Angreifers sowie des Angreifers selbst erschwert.

ANWENDUNG: DESIGNFEHLER

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: IMPLEMENTIERUNGSFEHLER

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.

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.

MANGELNDE SYSTEMPFLEGE

Mangelnde Systempflege kann auf verschiedene Weisen zu Sicherheitsproblemen in einem IT-System führen. Die Kategorie wird daher für eine Vielzahl von Fehlerarten, welche sich nicht in die bestehenden Kategorien einordnen lassen, genutzt. Besonders häufig treten Mängel im Patch-Management auf. Diese können wiederum zu Fehlern der Kategorie „Using components with known vulnerabilities (OWASP A9)“ führen. Weitere häufige Fehler bestehen im Weiterbetrieb von ungenutzten Systemen, Test- und Beispielsystemen oder Systemen, welche nicht nach außen offen sein sollten oder abgelaufene Zertifikate besitzen. Ebenso kommen ungenutzte und undokumentierte Firewall-Regeln, fehlerhafte Systemzeiten und Login-Möglichkeiten mit Standard-Zugangsdaten vor.

FAZIT

Im Jahr 2019 bestand weiterhin eine Vielzahl unterschiedlicher Sicherheitsprobleme in den von der HiSolutions überprüften IT-Systemen. Besonders die Zahl der fehlerhaften Konfigurationen und die Häufigkeit, mit der verwundbare Komponenten eingesetzt wurden, haben sich in diesem Jahr deutlich erhöht. Abgenommen hat hingegen die Anzahl der Fehler, bei denen sensible Informationen preisgegeben wurden oder die Authentifizierung nicht korrekt funktionierte. Trotz dieser Abweichungen ergibt sich in Summe ein ähnliches Bild wie das der letzten Jahre.

Schwere und kritische Sicherheitslücken wurden, nach leichtem Rückgang 2018, im vergangenen Jahr wieder häufiger festgestellt. Es gab keinen einzigen Penetrationstest, welcher keine Befunde hervorbrachte. Insgesamt besteht folglich kein Grund für Entwarnung. Ganz im Gegenteil besteht weiterhin akuter Handlungsbedarf beim Schutz von IT-Systemen.

Für die kommenden Jahre ergibt sich insbesondere die Notwendigkeit, den Entwicklungsprozess von Software weiter zu optimieren. Besonders schwerwiegende Probleme treten bei Fehlern in der Architektur oder im Design auf. Es ist daher dringend ratsam, IT-Sicherheitsexperten am Entwicklungsprozess zu beteiligen und möglichst früh in die Planung mit einzubeziehen. Um Implementierungsfehler zu reduzieren, können ein Secure Development Lifecycle, Entwicklertrainings und Source-Code-Reviews probate Mittel sein.

Mehr denn je bestehen die größten Herausforderungen in der korrekten Konfiguration und Wartung von Software. Insbesondere ist es für die kommenden Jahre für viele Unternehmen besonders drängend, das Patch-Management zu verbessern. Wird vermieden, dass Systeme hinter den aktuellen Stand der Entwicklung zurückfallen, können schwerwiegende Risiken durch öffentlich bekannte Schwachstellen verhindert werden.

Durch die Diversität der Probleme und den Variantenreichtum, der in der Praxis vorgefundenen Schwachstellen, wird ein einfaches und schnelles Auffinden beispielsweise durch automatisierte Verfahren erschwert. Das Testen auf ausgewählte „Top 10“-Lücken erweist sich weiterhin als nicht hinreichend.

Welche Schwachstellen durch einen Penetrationstest aufgedeckt werden, hängt auch von der Art des Tests ab. Im vergangenen Jahr wurden durch die HiSolutions besonders häufig externe und Web-Penetrationstests durchgeführt. Die Auswertung zeigt jedoch, dass viele besonders schwerwiegende Sicherheitslücken erst aufgedeckt werden können, wenn dem Testteam mehr Zugangsrechte eingeräumt werden. Für viele Unternehmen kann es daher für die Zukunft sinnvoll sein, über eine externe Untersuchung der Systeme hinauszugehen und auch interne Strukturen prüfen zu lassen.

Der Bericht verdeutlicht, dass anhand von Penetrationstests viele Sicherheitsprobleme in IT-Infrastrukturen erkannt werden können, die ohne externe Kontrolle (bis zu einem Angriff) verdeckt geblieben wären. In vielen Fällen wurde auf Befunde korrekt reagiert. So wurden vor allem kritische und schwere Sicherheitslücken bis zu einem Nachtest drastisch reduziert. Insgesamt haben sich die

Sicherheitseigenschaften der getesteten Systeme nach einem Penetrationstest unbestreitbar verbessert.

In anderen Nachtests wurde jedoch deutlich, dass Sicherheitslücken teilweise nicht adäquat geschlossen werden. Außerdem können sich die Sicherheitseigenschaften eines Systems über die Zeit verändern. Daher sehen wir wiederholte Penetrationstests mit wiederholter Überprüfung identifizierter Sicherheitslücken und der zu ihrem Schließen eingesetzten Sicherheitsmaßnahmen als einen wichtigen Schritt zu mehr Sicherheit in IT-Systemen.

KONTAKT

Dominik Oepen
Managing Consultant & Team Manager
Penetrationstests/Technische Audits
Fon +49 30 533289-0
oepen@hisolutions.com

HiSolutions AG
Schloßstraße 1
12163 Berlin

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