# HISOLUTIONS SCHWACHSTELLEN-REPORT 2021

Entwicklungen & Trends bei Schwachstellen 2013-2020

**Stand 29. September 2021**

**HiSolutions AG © 2021**

## 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, sowohl die Vertraulichkeit der Projektergebnisse gegenüber unseren Kunden zu wahren als auch 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 89 Penetrations- und Schwachstellentests, die im Jahr 2020 durchgeführt wurden. Zusätzlich wurden die Befunde mit den Ergebnissen der Schwachstellenreports aus den Jahren 2013 bis 2019 verglichen.

Die durchgeführten 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.

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 System häufig zu einem Befund zusammengefasst, sodass eine Zählung der Befunde hier ebenfalls nur begrenzte Aussagekraft hat. Aufgrund dessen wird als Maß die relative Häufigkeit von Projekten, in welchen ein Befund der entsprechenden Kategorie auftaucht, verwendet. Dadurch wird deutlich, welche Schwachstellen

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

besonders häufig in Projekten auftreten und welche eher selten oder nur in besonderen Zielumgebungen vorkommen.

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

Im Folgenden werden die Erkenntnisse aus der Auswertung der Penetrationstests des letzten Jahres vorgestellt. Es werden die durch die Tests gefundenen Sicherheitslücken im Vergleich der Ergebnisse der letzten Jahre begutachtet. Hierfür werden die Kategorie und der Schweregrad der Schwachstellen betrachtet. Die Auswertung von Nachtest-Ergebnissen erlaubt auch in diesem Jahr wieder eine Untersuchung über die Effizienz der im Anschluss an Penetrationstests durchgeführten Maßnahmen.

Bei der Auswertung der Projekte des Jahres 2020 müssen die Besonderheit des Jahres in Bezug auf die globale Covid-19-Pandemie im Blick behalten werden. So ist es dieses Jahr besonders wichtig, die Entwicklung der Ergebnisse der Penetrations- und Schwachstellentests im Zusammenhang mit den Einschränkungen zur Pandemiebekämpfung und den Auswirkungen auf die verschiedenen Projektarten zu begutachten und zu bewerten.

Die erste Abbildung zeigt die Entwicklung des Schweregrades von Sicherheitslücken von 2013 bis 2020. In diesem Fall werden alle Funde eines Penetrationstests betrachtet. Jedem Test wird die höchste Kritikalität seiner Funde zugeordnet, da eine einzige Schwachstelle des entsprechenden Schweregrades genügen kann, die Sicherheit des gesamten Systems zu beeinträchtigen.

Von 2013 bis 2015 gab es einen klaren Anstieg der kritischen, hohen und mittleren Befunde. Die Anzahl dieser sank in den nächsten Jahren bis 2018 zwar deutlich, um 2019 erneut stark zu steigen. Wie bereits im Bericht des letzten Jahres vermutet, liegt der starke Anstieg der als hoch eingestuften Funde in 2019 vermutlich im Rahmen der kurzzeitigen Schwankungen, welche zwar nicht direkt einen Negativtrend darstellt, aber dennoch beobachtet werden sollte.

Die Entwicklung der Kritikalitätsverteilung im Jahr 2020 zeigt im Vergleich zu 2019 einen Anstieg der Schwachstellen mit mittleren und niedrigen Auswirkungen und damit einhergehend eine Abnahme der kritischen und hohen Schwachstellen. Der Grund für diesen starken Unterschied liegt allerdings nicht in einem wesentlich verbesserten Sicherheitsniveau der Untersuchungsgegenstände, sondern lässt sich vielmehr durch die Auswirkungen der Covid-19-Pandemie erklären: Durch die Maßnahmen gegen die Pandemie (z. B. Lockdowns, Reisebeschränkungen und Home-Office-Regelungen) konnten im Jahr 2020 deutlich weniger interne Penetrationstests durchgeführt werden. Im Gegensatz zu externen Prüfungen über das Internet werden bei Penetrationstests in internen Netzwerken fast ausnahmslos eine wesentlich höhere Anzahl an Befunden und Schwachstellen mit hohen und kritischen Auswirkungen aufgedeckt.

Dies liegt unter anderem daran, dass extern erreichbare Systeme täglich im Fokus verschiedenster Angreifer stehen und kritische Schwachstellen kurzfristig ausgenutzt werden. Je nach den Folgen der Ausnutzung und gegebenenfalls vorhandener öffentlicher Berichterstattung zu den Schwachstellen führt dies dazu, dass Schwachstellen in externen Systemen schneller erkannt und behandelt werden. Dies gilt umso mehr, als dass heutzutage ein Großteil der Unternehmen weiterhin einen Netzwerkschutz nach dem Perimeter-System betreiben. Die Absicherung nach außen steht dabei im Fokus der Sicherheitsmaßnahmen, wobei die Behandlung von Sicherheitsrisiken in internen Systemen nachrangig behandelt wird oder durch Ressourcenmangel nicht oder nur stark verzögert erfolgen kann.

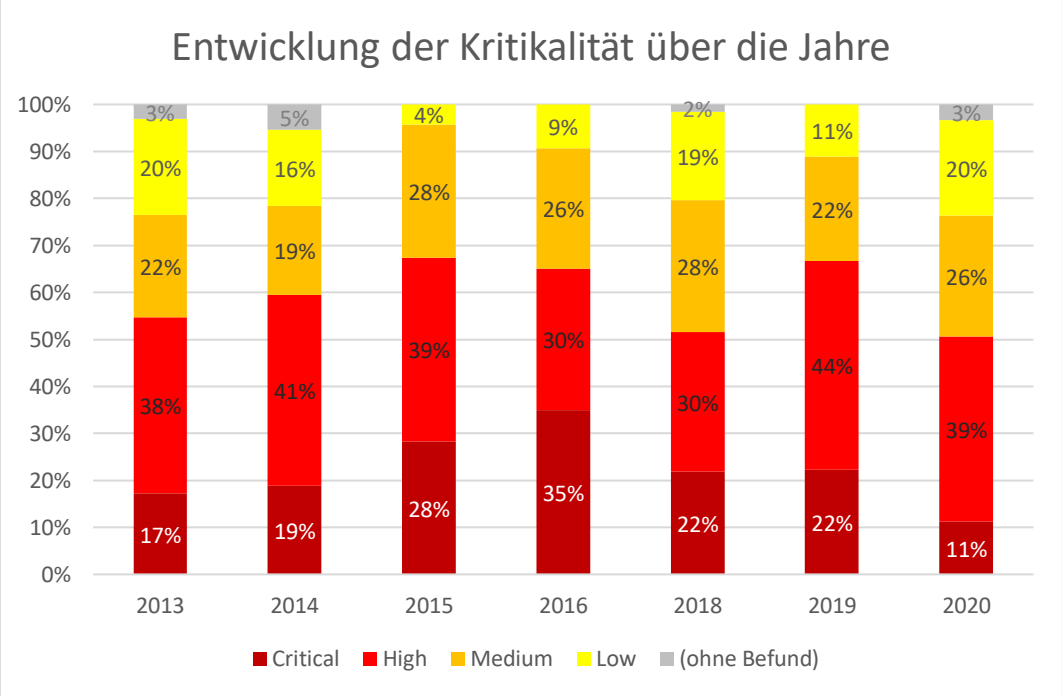



Abbildung 1: Entwicklung der Kritikalität von 2013 bis 2020

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.

Im abgelaufenen Jahr ist besonders zu bemerken, dass eine Preisgabe von schützenswerten Daten, welche im letzten Jahr stark gesunken war, erneut enorm angestiegen und nun wieder in 8 von 10 Fällen zu finden ist. Zugleich ist aber die Anzahl der fehlerhaften Konfigurationen mit Auswirkung auf die Sicherheit eines Systems nach einem dramatischen Anstieg im letzten Jahr wieder gesunken, wobei eine solche noch immer in 80 % der Penetrationstests aufzufinden ist. Auch Funde im Bereich der Injektion und fehlerhafter Authentifizierung oder Sitzungsverwaltung sind im Vergleich zum vorherigen Jahr wieder häufiger geworden, wobei in diesen Fällen der Anstieg um ca. 5 % im Bereich normaler Schwankungen liegt.

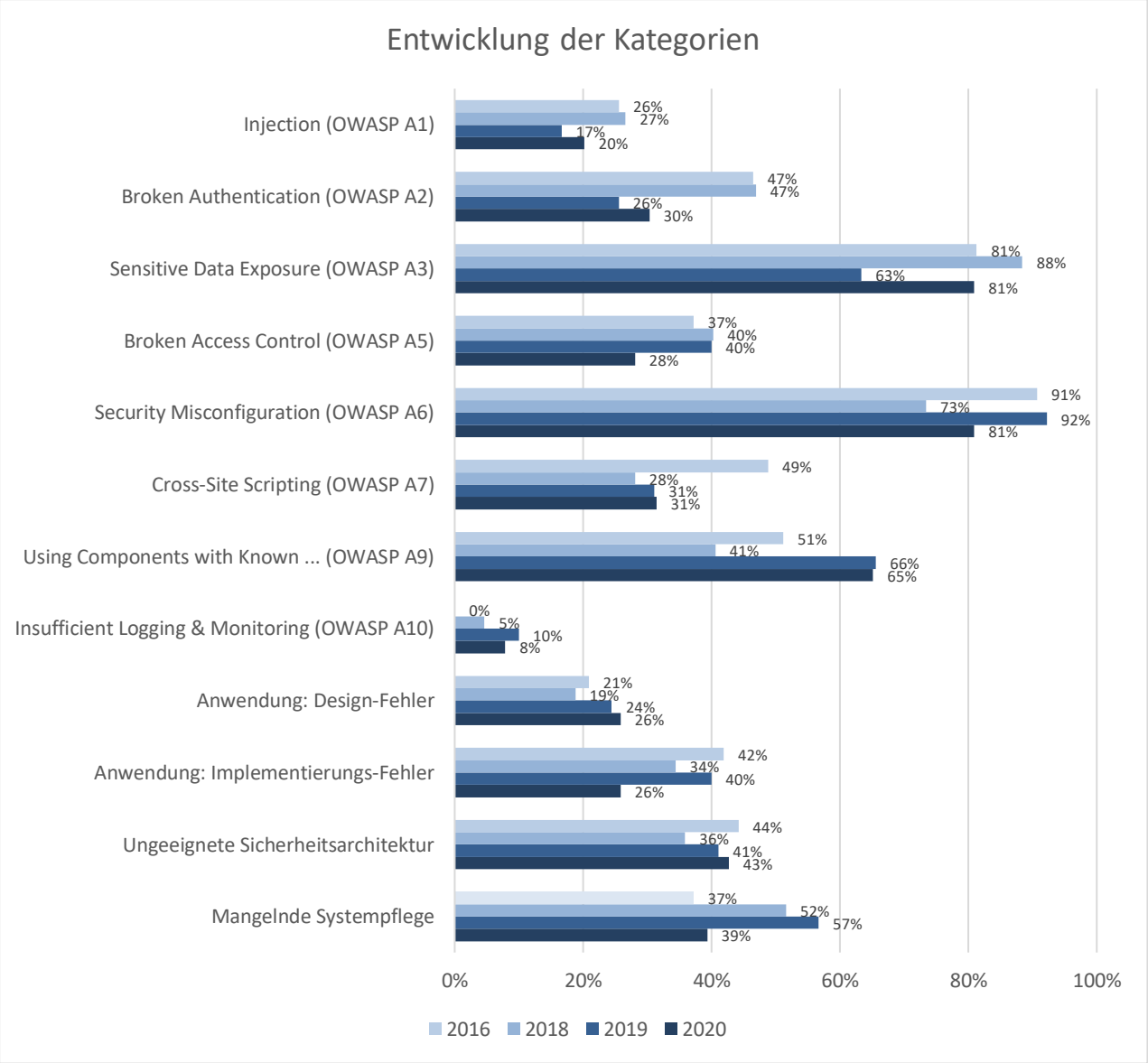



Abbildung 2: Relative Häufigkeit der Kategorien[2] von 2016 bis 2020

[2] Die Kategorien „*XML External Entities (OWASP A4)*“ und „*Insecure Deserialization (OWASP A8)*“ sind aufgrund der geringen absoluten Zahlen aktuell nicht aufgeführt.

Positiv zu vermerken scheint, dass der Anteil der Funde im Bereich von Implementierungsfehlern, mangelnder Systempflege und fehlerhafter Authentifizierung oder Sitzungsverwaltung im Vergleich zu 2019 wieder stark sank. Wie schon bei der Kritikalitätsentwicklung sind jedoch auch diese Entwicklungen mit großer Wahrscheinlichkeit den Auswirkungen der Covid-19- Pandemie zuzurechnen, da Fehler in diesen Bereichen zum Großteil bei internen Penetrationstests bemerkt werden.

Abbildung 3 zeigt die Schwere der Befunde im vergangenen Jahr aufgeschlüsselt nach Kategorie und im Vergleich zu den Befunden des vorangegangenen Jahres. Angegeben wird dabei der Anteil der unterschiedlichen Kritikalitätswerte an den Gesamtbefunden der jeweiligen Kategorie.

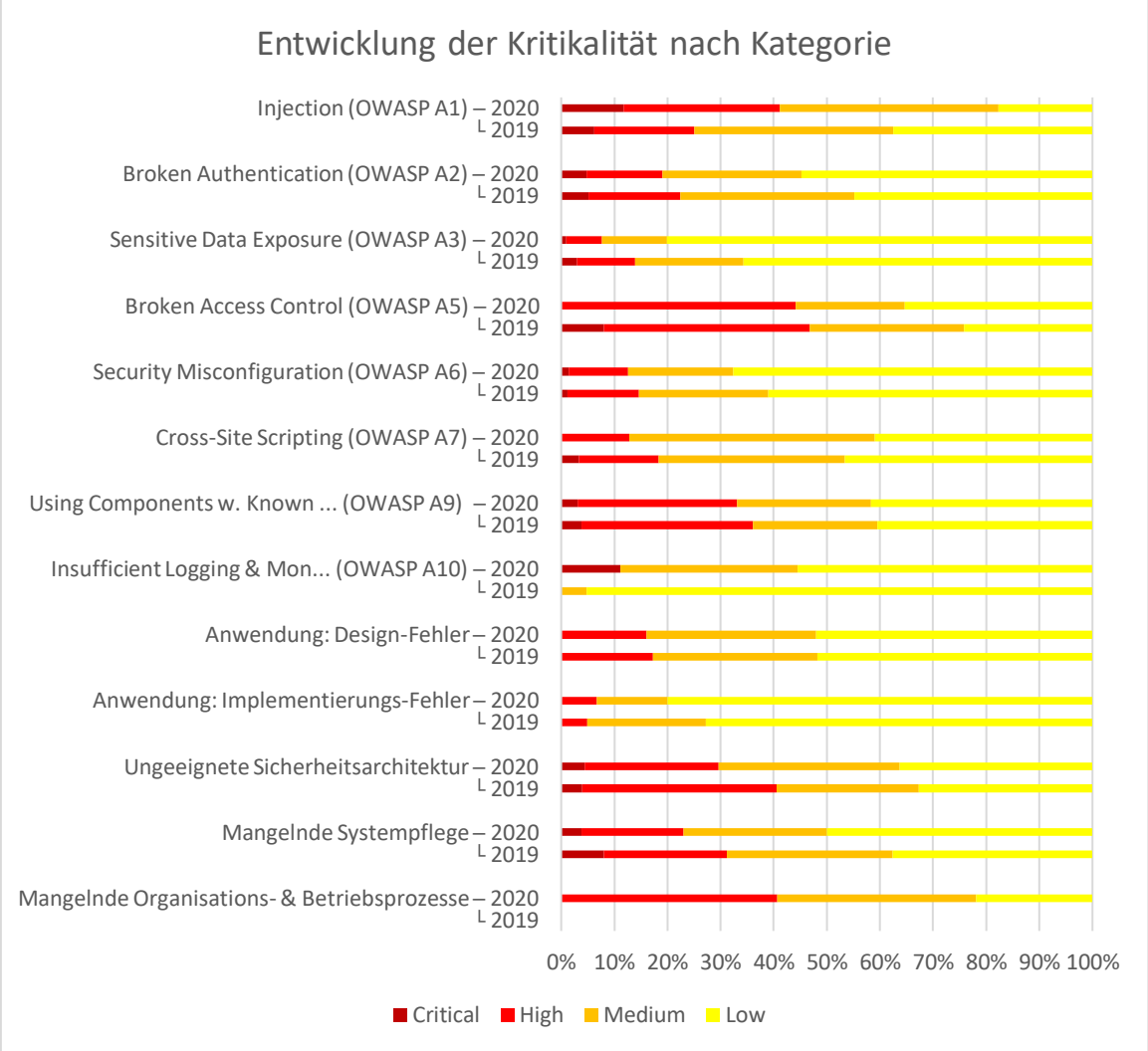



Abbildung 3: Entwicklung der Kritikalität[3] der Befunde nach Kategorie im Vergleich zum Vorjahr

Betrachtet man die Entwicklung der Häufigkeit der Kategorien zusammen mit der Kritikalität nach Kategorien, ergeben sich einige bemerkenswerte Veränderungen. So ist zwar die Häufigkeit der Funde

[3] Ohne Befunde, aus welchen sich keine direkten sicherheitsrelevanten Auswirkungen ergaben.

im Bereich „Injektion“ nur leicht angewachsen, jedoch ist die Kritikalität der Funde in diesem Bereich, besonders von kritischen und hohen Funden, deutlich stärker gestiegen.
Im Gegenteil hierzu ist jedoch die Häufigkeit im Bereich „Fehlerhafter Authentifizierung oder Sitzungsverwaltung“ ähnlich zur Kategorie „Injektion“ gewachsen. Hier hat sich die Verteilung der Kritikalität allerdings in Richtung niedrig (low) verschoben.
Auch die Anzahl von Funden im Bereich des „Preisgebens von sensiblen Daten“ ist stark gestiegen – und ähnlich wie beim vorherigen Punkt ist auch hier die Verteilung der Kritikalität der Funde sogar noch eindeutiger in Richtung niedrig gewandert.

Während die Häufigkeit von Funden im Bereich des unzureichenden Loggings & Monitorings gesunken ist, ist hier die Kritikalität besonders stark angestiegen. Im Jahr 2020 wurden allerdings in diesem Bereich nur neun Funde entdeckt, im Gegensatz zum Vorjahr, wo es 22 Funde gab, weshalb die allgemeingültige Aussagekraft der Veränderung kritisch zu hinterfragen ist. Nichtsdestotrotz sollte dieser Bereich umso genauer im Blick behalten werden, da ein gutes Logging und Monitoring nicht nur bei der Fehlersuche, sondern auch bei der rechtzeitigen Erkennung und Behandlung von Angriffen essenziell ist.

Als letzter bemerkenswerter Punkt ist hervorzuheben, dass 40 % der Funde im Bereich von mangelnden Organisations- und Betriebsprozessen eine hohe Kritikalität vorzeigen und sogar bis zu 80 % als mittlere Kritikalität eingestuft werden.

### Auswertung nach Testtyp

HiSolutions bietet eine Vielzahl unterschiedlicher Sicherheitsüberprüfungen an. Vergleichsweise häufig und insbesondere periodisch wiederkehrend werden externe Penetrationstests und Web-Penetrationstests ausgeführt, bei denen das Testteam die gleichen Möglichkeiten wie externe Angreifer besitzt. Zusätzlich wird auch eine Vielzahl an internen Penetrationstests durchgeführt, welche die Untersuchung der Auswirkungen eines erfolgreichen Angriffes in der Praxis ermöglichen. Bei diesen stehen dem Testteam wesentlich mehr Möglichkeiten zur Verfügung, da sie sich im internen Netz des Auftraggebers befinden. Auch diverse Pentests und gezielte Prüfungen von Hardware-Systemen, Anwendungen und ICS-Umgebungen sowie Überprüfungen von Quellcode, System- und Netzwerk-Architekturen und der Konfiguration von IT-Systemen wurden im Jahr 2020 von HiSolutions durchgeführt.

Abbildung 4 zeigt die Kritikalität abhängig vom Typ des durchgeführten Tests und im Vergleich die Ergebnisse des Vorjahres. In einem Penetrationstest können mehrere Überprüfungen unterschiedlicher Art vorkommen. 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 maximalen ermittelten Kritikalität. Für eine bessere Vergleichbarkeit werden relative Häufigkeiten dargestellt.

Um im Vergleich einen Mindestwert an Aussagekraft zu erzielen, werden nur Testtypen berücksichtigt, für welche im Jahr 2020 mindestens 10 Projekte durchgeführt wurden.

Die Auswertung nach Testtyp zeigt, dass die generelle Verteilung der in den Projekten beobachteten Kritikalitäten größtenteils konstant geblieben ist.

Nach wie vor gilt nachweisbar: Je mehr Zugang das Testteam hat, desto kritischer sind die aufgedeckten Sicherheitslücken. Zwar wurden im Fall der internen Penetrationstests nur noch in ungefähr 35 % der Prüfungen Befunde identifiziert, die als kritisch eingestuft wurden, der Anteil der sonstigen internen

Pentests, die dann mindestens einen als „hoch“ eingestuften Befund enthalten, ist von ca. 40 % auf ca. 60 % der Gesamtzahl angestiegen.

Da durch die Corona-Pandemie deutlich mehr Überprüfungen von über das Internet erreichbaren Testgegenständen stattgefunden haben, ist die Entwicklung hier besonders interessant. Sowohl bei externen als auch bei Web-Penetrationstests sind besonders die Funde von kritischen und hohen Schwachstellen zurückgegangen. Das könnte darauf hinweisen, dass die Absicherung nach außen sich bei einigen Systemen im Vergleich zum Vorjahr verbessert hat. Ob dies dadurch begründet werden kann, dass durch die Pandemie deutlich mehr Personal im Home-Office arbeitete und somit die Schnittstellen nach außen stärker abgesichert werden mussten, muss durch andere Untersuchungen beleuchtet werden.

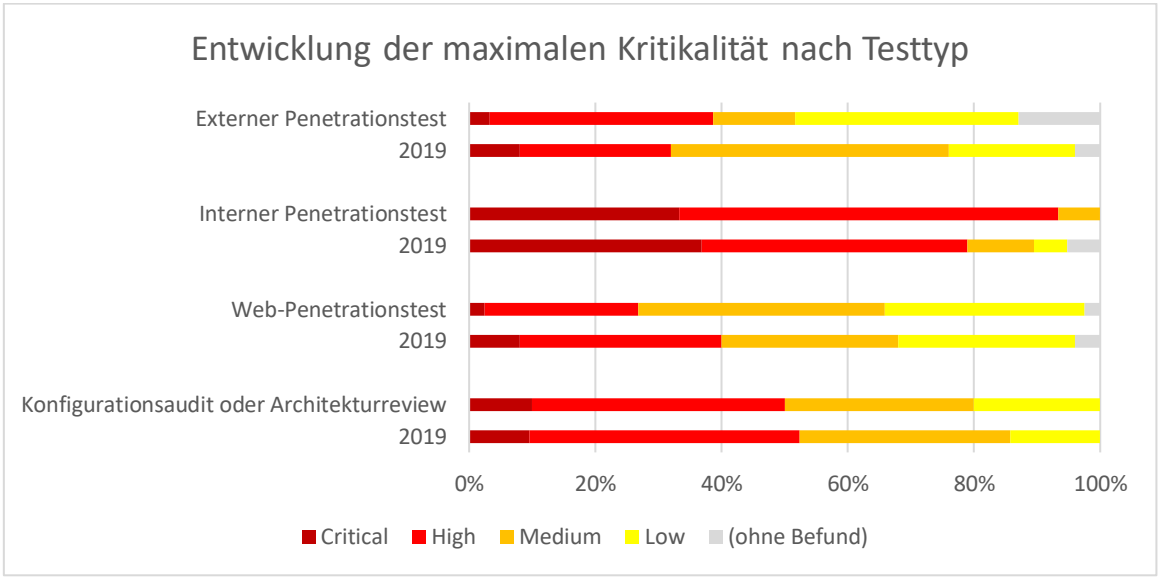



Abbildung 4: Entwicklung der maximalen Kritikalität nach Testtyp im Vergleich zum Vorjahr

## 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 der umgesetzten Maßnahmen wird im Folgenden an Beispielen aus der Praxis überprüft. Zu diesem Zweck werden Befunde betrachtet, bei denen ein Nachtest durch HiSolutions stattgefunden hat, also eine Überprüfung der nach dem Penetrationstest implementierten Maßnahmen.

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

Im Allgemeinen kann erneut hervorgehoben werden, dass besonders kritische und hohe Schwachstellen bis auf wenige Ausnahmen erfolgreich behoben wurden. Allerdings waren in den

[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.

Bereichen sicherheitskritische Fehlkonfiguration und Nutzen von Komponenten mit bekannten Schwachstellen selbst im Nachtest noch immer Schwachstellen der Kritikalität „hoch“ zu finden.

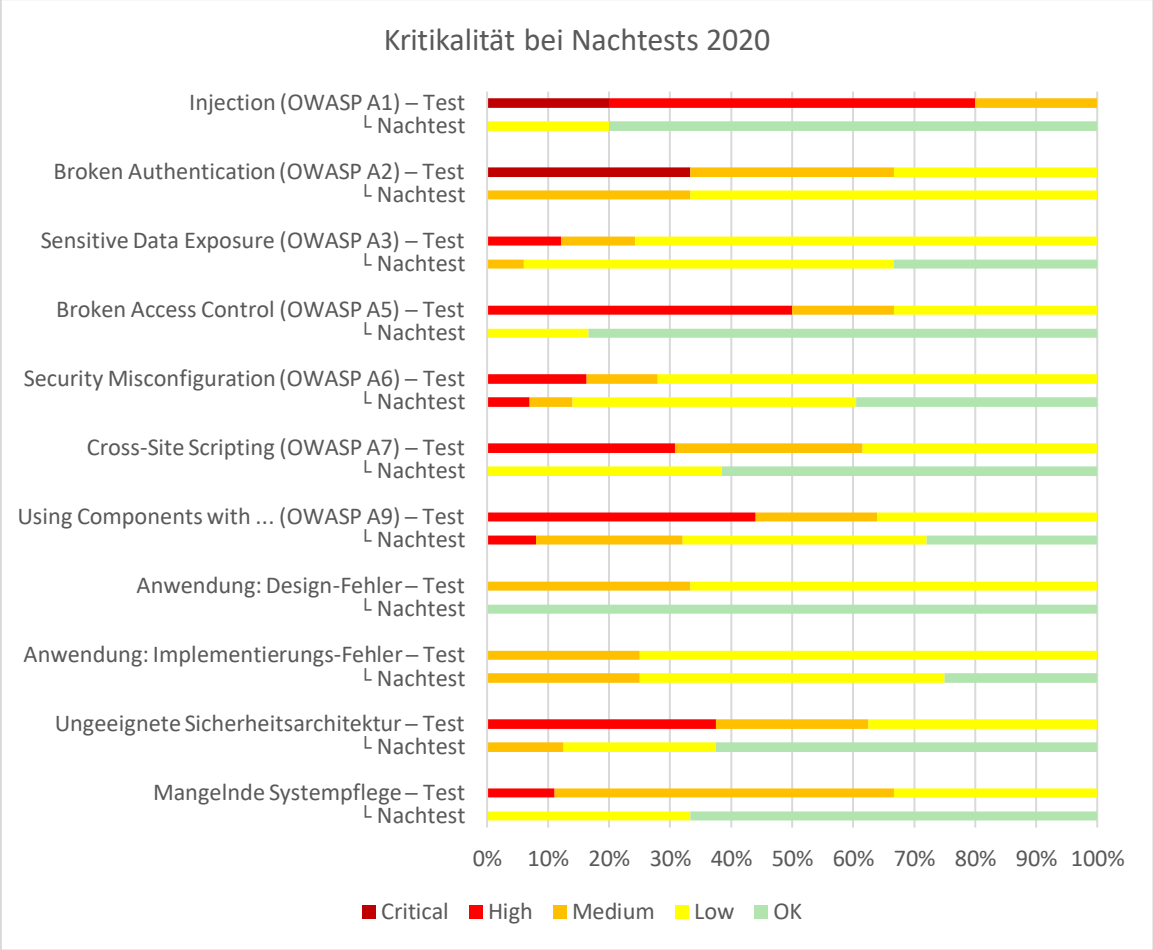



Abbildung 5: Kritikalität im Vergleich vom Penetrationstest zum Nachtest 2020

Der Grund für die Unterschiede bei diesen beiden Kategorien war dabei häufig, dass es sich um schwerwiegende systematische Schwachstellen handelt, deren Behebung längere Zeit in Anspruch nimmt oder größere Umstrukturierungen notwendig macht. Bei Schwachstellen etwa, die auf veraltete Systeme und Komponenten zurückzuführen sind, ist ein funktionierendes Patch- und Life-Cycle-Management essenziell, um die Probleme dauerhaft zu beheben. Sind diese Management-Prozesse nicht ausreichend etabliert, werden Systeme im Nachgang an einen Penetrationstest oft einmalig aktualisiert, sind aber bis zum Zeitpunkt des Nachtests erneut veraltet. Vor dem Hintergrund, dass Ransomware-Trojaner und -Angreifer immer wieder Schwachstellen in veralteten Systemen ausnutzen, empfiehlt HiSolutions auch in internen Netzwerken dringend die Umsetzung eines zeitnahen Patch- und Life-Cycle-Managements.

## FAZIT

Auch dieses Jahr zeigten die identifizierten Befunde, wie wichtig und notwendig Penetrationstests und praktische technische Sicherheitsüberprüfungen sind.

Schwachstellen in internen Netzwerken stellen nach wie vor den Großteil der Schwachstellen mit hohem oder kritischen Risiko für Unternehmen dar. Unter der Annahme, dass es Angreifern gelingt, die externen Sicherheitsmaßnahmen zu umgehen und in ein internes Netzwerk vorzudringen, spiegelt dieses in der Praxis ein beträchtliches Risiko wider. Auch die Erfahrungen von HiSolutions im Bereich Incident Response und Forensik und andere unabhängige Untersuchungen zeigen klar, dass Angreifer in internen Netzwerken gezielt Schwachstellen ausnutzen, um darüber ihre Berechtigungen zu erweitern und Schadsoftware auf weiteren Systemen zu verbreiten. Diverse in internen Penetrationstests identifizierte Angriffspfade ließen sich direkt oder in abgewandelter Form auch in realen Angriffen beobachten. Nur durch einen systematischen Umgang mit dem Thema IT-Sicherheit, welcher teilweise größere Umbau- und Um-Organisationsmaßnahmen und eine langfristige sicherheitsorientierte Ausrichtung in dem Bereich nach sich zieht, kann dieses komplexe Thema zukünftig verbessert werden.

Die sonstigen Entwicklungen der Zahlen aus diesem Jahr stehen stark unter dem Eindruck der durch die Covid-19-Pandemie veränderten Projektzusammensetzung. Üblicherweise in Web-Anwendungen und externen Systemen vorzufindende Schwachstellen wie die „Preisgabe schützenswerter Daten“ sind durch die gestiegene Anzahl an Projekten in diesem Bereich ebenfalls merklich angestiegen. Die Anzahl an kritischen und hoch eingestuften Schwachstellen ist, bedingt durch die geringere Anzahl an internen Penetrationstests bei Kunden vor Ort, insgesamt gesunken. Ein Blick in die Einzelprojekte zeigt jedoch kein signifikant gestiegenes Sicherheitsniveau in den einzelnen Bereichen.

Aus den Ergebnissen lässt sich auch ablesen, dass im Bereich des Loggings und Monitorings weiterhin größere Probleme existieren. Ein zielgerichtetes Logging und Monitoring wurde nur in wenigen Kundenumgebungen beobachtet. Teilweise war zwar eine umfangreiche Protokollierung eingerichtet, die Daten wurden aber nicht geeignet ausgewertet und konnten daher nicht effizient und präventiv genutzt werden. Da besonders dieser Bereich, wenn richtig durchgeführt, eine enorme Hilfe bei der Überprüfung von Systemen und insbesondere auch der frühzeitigen Erkennung von Sicherheitsvorfällen sein kann, empfehlen wir eine stärkere Fokussierung aus das Thema in der Zukunft.

Auch für das vergangene Jahr zeigen die Ergebnisse deutlich, dass anhand von Penetrationstests viele Sicherheitsprobleme in IT-Infrastrukturen erkannt werden können, die ohne externe Kontrolle (bis zu einem Angriff) verdeckt geblieben wären. Einmal identifiziert, führten die betroffenen Unternehmen in den meisten Fällen ausreichende Maßnahmen bis zum Nachtest durch, sodass die Probleme dauerhaft behoben wurden. Bei der Interpretation dieser Ergebnisse muss allerdings beachtet werden, dass die Durchführung eines Nachtests für sich bereits ein gesteigertes Sicherheitsbewusstsein oder etabliertere IT-Sicherheits-Strukturen bei Unternehmen aufzeigt. So werden Nachtests in der Regel nicht geplant und beauftragt, wenn keine Änderungen an den Systemen vorgenommen wurden. Auch wenn die Ergebnisse der Nachtests grundlegende Verbesserungen an den Systemen darlegen, zeigen sie auch deutlich, dass nicht immer alle angemahnten Schwachstellen tatsächlich effektiv behoben wurden. Die Durchführung von Nachtests ist damit weiterhin als effektives Mittel zur Bestätigung von getroffenen Maßnahmen sowie zur Identifikation möglicher Restrisiken anzusehen.

# ANHANG: BESCHREIBUNG DER KATEGORIEN

### 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.

### XML EXTERNAL ENTITIES (OWASP A4)

Die Kategorie XML External Entities (XXE) fasst Schwachstellen in der Verarbeitung von XML-Daten zusammen, welche immer dann auftreten, wenn Angreifer direkt oder indirekt Inhalte von XML-Dokumenten verändern können, welche danach unsicher verarbeitet werden. Durch das Einfügen zusätzlicher Elemente und Abhängigkeiten können häufig lokale Daten eingebettet und teilweise an externe Systeme weitergereicht werden. So ist beispielsweise der Zugriff auf schützenswerte lokale Dateien von Web- und Anwendungsservern oder die Durchführung von Denial-of-Service-Angriffen möglich.

### BROKEN ACCESS CONTROL (OWASP A5)

Fehler diese 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).

### INSECURE DESERIALIZATION (OWASP A8)

Insecure Deserialization (Unsichere Deserialisierung) beschreibt eine Reihe von Fehlerklassen, welche bei der Deserialisierung von Objekten auftreten können. Anfälligkeiten entstehen, wenn Objekte (z. B. Cookies), welche später von der Anwendung deserialisiert werden, zuvor von Angreifern manipuliert oder verändert werden können. Schwachstellen bei der Deserialisierung haben häufig schwerwiegende Auswirkungen und erlauben oft das Ausführen von beliebigem Programmcode. Gleichzeitig sind die Schwachstellen in Black-Box-Prüfungen ohne Einsicht in den Quellcode nur schwer zu entdecken und auszunutzen.

### USING COMPONENTS WITH KNOWN VULNERABILITIES (OWASP A9)

Unter diese Kategorie fällte eine Vielzahl von Schwachstellen, die insbesondere aus einem mangelhaften Software- und Patchmanagement resultiert: Veraltete Software, vom Betriebssystem über die Anwendungsserver, Frameworks, die Anwendungssoftware und Erweiterung 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.

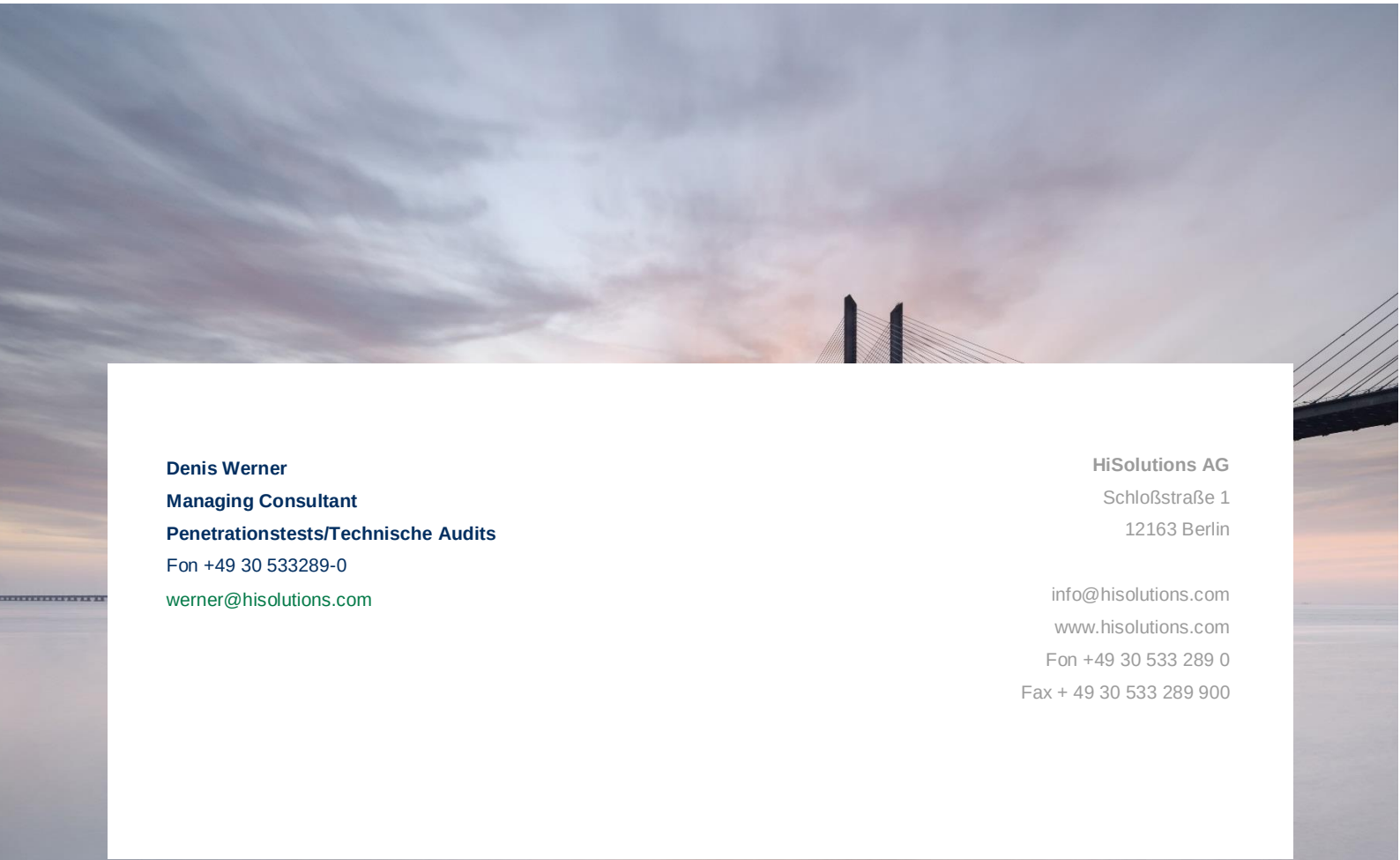
### UNGEEIGNETE SICHERHEITSARCHITEKTUR

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. Weiter häufig 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.

# KONTAKT



**Denis Werner**
**Managing Consultant**
**Penetrationstests/Technische Audits**
Fon +49 30 533289-0
werner@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