ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

09

BAND

Autorisierung, kontrollierte Prüfung und nachprüfbare Verbesserung

Spanische Ausgabe · 2026

Handbuch für evidenzbasierte Pentests:

Validierung, Behebung und Retest für Unternehmen

Einsatzregeln, Feststellungen, abgegrenzte Auswirkungen, Behebung und Überprüfung

Ein Sicherheitstest wird in einen autorisierten und nachprüfbaren Prozess überführt, in dem jede Feststellung durch angemessene Evidenz gestützt wird und jede Behebung überprüft werden kann, ohne ein weiteres Ereignis zu verursachen.

Für Sicherheits-, Technologie- und Führungsverantwortliche, Compliance, Versicherer, Auditoren und Dienstleister. Enthält keine Anleitung zur Ausnutzung von Schwachstellen und autorisiert keine Tests an Systemen ohne ausdrückliche Genehmigung.

Redaktionskoordination: Jocsan Laguna · Amerikanischer Rat für Cybersicherheit und digitale Forensik

Allgemeine technische Anleitung und offenes Bildungsmaterial. Sie stellt keine Rechtsberatung, kein sachverständiges Gutachten und keine Anleitung zum unbefugten Zugriff auf Systeme dar. Beispiele und Daten sind fiktiv; Abbildungen sind redaktionelle Rekonstruktionen.

Inhalt

Die sichtbare Seitennummerierung entspricht der PDF-Ausgabe. Word kann dieses Verzeichnis beim Öffnen des Dokuments aktualisieren; die interne Navigation der Überschriften bleibt erhalten.

Einleitung: Ein Scan beweist nicht alles, was wichtig ist 3
Kapitel 1. Autorisierung und Regeln 3
1.1 Umfang ohne Interpretationsspielraum 3
1.2 Betriebliches Risiko und Exitplan 4
Kapitel 2. Technische Vorbereitung und Validierung 5
2.1 Architektur und Sicherheitsfragen 5
2.2 Werkzeuge und Kontrolldaten 5
2.3 Protokolle und Synchronisierung 5
Kapitel 3. Sichere Durchführung und Protokollierung 5
3.1 Protokoll je Aktion 5
3.2 Abbruch, Eskalation und Kommunikation 6
3.3 Umgang mit erlangten Informationen 6
Kapitel 4. Evidenz für jede Feststellung 7
4.1 Reproduzierbares Formular 7
4.2 Falschpositive und Duplikate 7
4.3 Auswirkung und Priorität 7
Kapitel 5. Behebung und Risikomanagement 8
5.1 Ursachenorientierte Behebung 8
5.2 Plan nach Auswirkung und Abhängigkeit 8
5.3 Evidenz der Behebung 9
Kapitel 6. Retest und Abschluss 9
6.1 Vergleichbare Bedingungen wiederholen 9
6.2 Abschlussstatus 9
6.3 Abschlussbericht und Erkenntnisse 10
Anhang A. Einsatzregeln und Formular 11
A.1 Einsatzregeln 11
A.2 Feststellungsformular 11
A.3 Retest-Bericht 11
Anhang B. Rechtsrahmen und Abschlusskontrolle 12

Einleitung: Ein Scan beweist nicht alles, was wichtig ist

Ein Bericht mit Hunderten von Warnmeldungen kann die wesentlichen Fragen unbeantwortet lassen: Welches Risiko besteht tatsächlich, bei welchem Asset, unter welchen Bedingungen, mit welcher Auswirkung und wie lässt sich überprüfen, ob die Behebung wirksam war? Ein Penetrationstest ist kein Wettlauf um Zugriff um jeden Preis. Er ist eine autorisierte Bewertung, die Evidenz zur Risikominderung liefert, ohne Menschen, Daten oder den Geschäftsbetrieb zu schädigen.

NIST SP 800-115 unterscheidet Techniken zur Überprüfung, Identifizierung, Analyse und Validierung von Schwachstellen. Ein Scanner kann ein Baustein sein, ersetzt jedoch weder Planung und Analyse noch die anschließende Bewertung. Der Mehrwert der Fachkraft liegt nicht darin, möglichst viele Werkzeuge auszuführen, sondern zu entscheiden, welches Werkzeug erforderlich ist, in welchem Umfang es eingesetzt wird und wann abgebrochen werden muss.[1]

Die Evidenz wird vor dem Test konzipiert. Sie muss die Überprüfung von Asset, Konfiguration, Bedingungen, Vorgehen, Ergebnis, Auswirkung und Grenzen ermöglichen. Reale Geheimnisse werden nicht erfasst, nur um deren Existenz zu beweisen, wenn dieser Nachweis mit fiktiven Daten, Teilantworten oder einer kontrollierten Umgebung möglich ist. Behebung und Retest gehören von Anfang an zum Auftrag und werden nicht improvisiert, nachdem der Bericht übergeben wurde.

> **Leitprinzip**
> Etwas testen zu können bedeutet nicht, dazu autorisiert zu sein. Die Autorisierung legt Assets, Techniken, Zeitfenster, Daten, Kontakte und Abbruchkriterien fest; die Methode wahrt diese Grenze.

Kapitel 1. Autorisierung und Regeln

1.1 Umfang ohne Interpretationsspielraum

Das Autorisierungsdokument umfasst Assets nach Domain, Adresse, Anwendung, Konto, Umgebung und Eigentümer; erlaubte und verbotene Techniken; Datumswerte und Zeitzonen; Testdaten; Umgang mit Informationen; Kontakte; Kommunikation; Abbruch- und Übergabebedingungen. „Du kannst alles auditieren“ sagt nichts darüber aus, ob Social Engineering, Denial of Service, Exploitation, Brute Force, physischer Zugriff oder die Einsicht in reale Daten erlaubt sind.

Dritte und Abhängigkeiten werden identifiziert: Cloud, CDN, E-Mail-Anbieter, Zahlungs-Gateways, gemeinsam genutzte Dienste, externe APIs und Kundennetzwerke. Eine autorisierte Domain kann auf Infrastruktur eines Dritten auflösen, für die eine separate Autorisierung erforderlich ist. Der Test erweitert sich nicht durch eine Entdeckung: Wird ein neues Asset gefunden, wird es protokolliert und vor jeder Kontaktaufnahme eine Erweiterung des Auftrags beantragt.

Element	Schriftlich festzuhaltender Inhalt	Fiktives Beispiel
Ziel	Geschäftsrisiko und Bewertungsfrage.	Zugriffskontrollen auf das Kundenportal validieren.
Assets	Domains, Bereiche, Anwendungen, Konten und Umgebung.	demo.empresa.invalid und zwei fiktive Konten.

[1] NIST SP 800-115. Technischer Leitfaden für Sicherheitstests und -bewertungen: Planung, Durchführung und anschließende Analyse. Ein automatisierter Scan allein entspricht weder einem Penetrationstest noch einer vollständigen Validierung. Offizielle Online-Quelle

Element	Schriftlich festzuhaltender Inhalt	Fiktives Beispiel
Techniken	Erlaubte, eingeschränkte und ausgeschlossene Techniken.	Kein Denial of Service, kein Brute Force in der Produktivumgebung, kein Spam.
Zeitfenster	Beginn, Ende, Zeitzone und Kontaktzeiten.	10–12 nov, 22:00–02:00 −06.
Daten	Fiktive Daten, Maskierung, Umgang und Löschung.	Keine reale Datenbank herunterladen und keine Geheimnisse exportieren.
Abbruch	Bedingung, verantwortliche Person und Benachrichtigungsweg.	Beeinträchtigung, unerwarteter Zugriff auf Dritte oder unklarer Umfang.
Übergabe	Format, Empfänger, Kanal und Löschung.	Verschlüsselter Bericht an die autorisierte verantwortliche Person.

1.2 Betriebliches Risiko und Exitplan

Mögliche Blockierungen, Ressourcenverbrauch, Protokolle, Warnmeldungen, Zustandsänderungen, Restdaten und Auswirkungen auf Benutzer werden geprüft. Der Plan umfasst gegebenenfalls Backups, technische Kontakte, Konfigurationsrollback, das Aussetzen von Aufgaben und Kommunikation. Eine irreversible Aktion wird nicht eingeleitet, um ein Risiko zu demonstrieren, das sich auf andere Weise nachweisen lässt.

Der Test erfolgt vorzugsweise mit fiktiven Konten, Datensätzen und Objekten. Soll unberechtigter Zugriff nachgewiesen werden, wird eine Abbruchbedingung festgelegt, bevor reale Inhalte angezeigt werden. Der Screenshot beschränkt sich auf das Nötigste: Antwort, Code, Struktur und Referenz, ohne Kundendaten zu verbreiten. Die Evidenz für eine Feststellung darf keine zweite Verletzung darstellen.

> **Startkriterium**
> Solange nicht beantwortet ist, wer die Autorisierung erteilt, welche Assets einbezogen sind, welche Aktionen zulässig sind, wer zu kontaktieren ist und wann abzubrechen ist, ist der Test noch nicht durchführungsbereit.

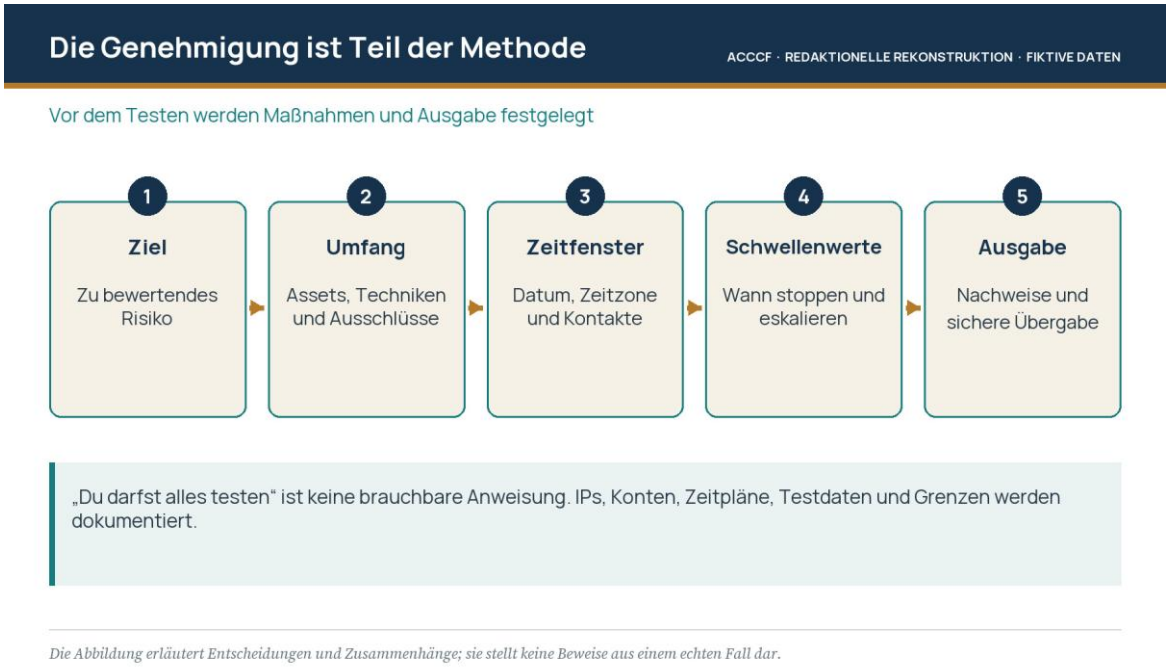


Abbildung 1. Die Autorisierung ist Teil der Methode. Vor dem Test werden Aktionen und Ausstiegsweg abgegrenzt. Redaktionelle Rekonstruktion; keine reale Evidenz.

Kapitel 2. Technische Vorbereitung und Validierung

2.1 Architektur und Sicherheitsfragen

Architektur, Inventar, Authentifizierungsflüsse, Rollen, Protokolle, Abhängigkeiten, jüngste Änderungen und Geschäftsanforderungen werden zusammengetragen. Die Dokumentenprüfung kann Schwachstellen aufzeigen, ohne den Dienst zu berühren. Die Architektur gibt die Richtung für Tests von Autorisierung, Konfiguration, Sitzungsverwaltung, Datenexposition und Integrationskontrollen vor. Nicht jede Frage erfordert eine Ausnutzung.

Der Plan priorisiert nach Auswirkung und Wahrscheinlichkeit, nicht nach einfacher Ausnutzbarkeit. Eine Warnmeldung bei einem Dienst ohne Daten kann eine geringere Priorität haben als eine Funktion, die das Ändern von Begünstigten erlaubt. Die Bewertung unterscheidet technisches Risiko, Umgebungsbedingung und geschäftliche Folge. Ist die Funktion des Assets unbekannt, wird die Aussage zur Auswirkung eingeschränkt.

2.2 Werkzeuge und Kontrolldaten

Werkzeuge werden mit bekannten Zielen und fiktiven Daten validiert: Identifikation, Ausgabe, Grenzen, Rate, Wiederholungsversuche, Format und Auswirkungen auf Protokolle. Name, Version, Konfiguration und Ergebnis werden festgehalten. Ein Scanner kann Falschpositive erzeugen oder einen Zustand übersehen, weil er eine generische Antwort interpretiert. Die Ausgabe wird nicht ungeprüft in den Bericht kopiert.

Kontrolldaten ermöglichen den Vergleich von erwartetem und beobachtetem Verhalten: Benutzer ohne Berechtigung, Benutzer mit eingeschränkter Rolle, eigene Ressource, fiktive Ressource eines Dritten, gültige Anfrage und veränderte Anfrage. Die unterschiedliche Antwort kann einen Zustand belegen, ohne sensible Inhalte zu lesen. Erlaubt das System nur Tests in der Produktivumgebung, werden strengere Schwellenwerte und eine verfügbare verantwortliche Person vereinbart.

2.3 Protokolle und Synchronisierung

Vor dem Test wird geprüft, welche Protokolle das System erzeugt, wer sie einsehen kann und ob die Uhrzeit synchronisiert ist. Originalwerte und Zeitzone jeder Quelle werden festgehalten. Eine WAF-Warnmeldung, ein Anwendungsereignis und eine Anfrage des Prüfers können auf unterschiedlichen Uhren beruhen. Die Korrelation wird anhand von Identifikatoren erläutert, nicht nur durch zeitliche Nähe.

> **Qualitätskontrolle**
> Hinterlässt der Test keine verständlichen Protokolle, sind die möglichen Aussagen darüber eingeschränkt. Die Lösung besteht nicht darin, einen vollständigen Ablauf zu erfinden, sondern geeignete Quellen zu aktivieren oder das Fehlen zu erklären.

Kapitel 3. Sichere Durchführung und Protokollierung

3.1 Protokoll je Aktion

Für jede Aktion werden Datum und Zeitzone, Operator, Asset, Werkzeug und Version, Konfiguration, Ziel, autorisierte Anfrage beziehungsweise das autorisierte Vorgehen, Antwort, Artefakte und Auswirkungen protokolliert. Reale Anmeldedaten oder Tokens werden nicht im Protokoll gespeichert.

Ausgabedateien werden mit einem Manifest verknüpft und der Zugriff eingeschränkt. Screenshots dienen dazu, das Erforderliche zu zeigen, nicht Bilder zu sammeln.

Das Protokoll enthält auch, was nicht funktioniert hat. Ein negatives Ergebnis unter einer dokumentierten Bedingung kann eine falsche Risikobehauptung verhindern, beweist jedoch keine universelle Nichtexistenz. Wenn ein Werkzeug fehlschlägt, werden Version, Fehler und Umfang notiert. Eine Testwiederholung erzeugt eine neue, verknüpfte Ausführung und löscht nicht den vorherigen Versuch.

Feld	Fiktives Beispiel	Überprüfung
Aktion	Autorisierte Anfrage an die Ressource DEMO-02 mit eingeschränkter Rolle.	Innerhalb des Umfangs und mit fiktiven Daten.
Uhrzeit und Zeitzone	2026-11-10T22:14:03−06:00.	Stimmt mit dem Serverprotokoll überein.
Ergebnis	Antwort 200 mit der Struktur einer fremden Testressource.	Unberechtigter Zugriff, ohne reale Daten zu lesen.
Evidenz	Anfrage, Teilantwort, Identifikator und minimaler Screenshot.	Ohne Tokens oder personenbezogene Daten.
Auswirkung	Keine Zustandsänderungen und keine sichtbaren Auswirkungen auf den Dienst.	Überwachung und Kontakt bestätigt.
Entscheidung	Pfad abbrechen und Feststellung dokumentieren.	Nicht auf andere reale Datensätze ausweiten.

3.2 Abbruch, Eskalation und Kommunikation

Abgebrochen wird bei Beeinträchtigung, unvorhergesehenen Auswirkungen, unklarem Umfang, ungeplanten realen Daten, einer Sicherheitswarnmeldung, die eine Reaktion erfordert, oder auf Anweisung des autorisierten Kontakts. Die Meldung enthält Asset, Aktion, Status, verfügbare Evidenz und offene Entscheidung. Der Test wird nicht fortgesetzt, um eine Gelegenheit zu nutzen, die in der Autorisierung nicht vorgesehen war.

Der reale Vorfall wird vom Test getrennt. Entdeckt das Team eine Aktivität, die es nicht selbst ausgelöst hat, wird diese als eigenständige Feststellung protokolliert und über einen sicheren Kanal gemeldet. Sie wird nicht automatisch dem Pentest zugeschrieben, und ihre Spuren werden nicht gelöscht. Die Chronologie muss unterscheiden, wer jede Aktion ausführte und was zeitgleich geschah.

3.3 Umgang mit erlangten Informationen

Greift der Test auf unerwartete Daten zu, wird die Untersuchung gestoppt, der Zustand dokumentiert, ohne weitere Inhalte zu kopieren, und geklärt, wie mit dem Erlangten umzugehen ist. Die Übergabe erfolgt über einen verschlüsselten Kanal an einen eingeschränkten Empfängerkreis. Schlüssel werden getrennt übermittelt. Die Löschung von Testdateien wird mit Umfang und Grenzen dokumentiert; Evidenz der Aktion wird nicht ohne Absprache gelöscht.

> **Prinzip der minimalen Beweisführung**
> Wenn eine Teilantwort und ein fiktiver Identifikator das Problem belegen, darf nicht die gesamte Datenbank heruntergeladen werden. Die Aussagekraft der Evidenz wird nicht an der Menge offengelegter Daten gemessen.

Kapitel 4. Evidenz für jede Feststellung

4.1 Reproduzierbares Formular

Das Formular enthält Identifikator, Titel, Asset, Version, Bedingung, Quellen, Vorgehen, Ergebnis, Auswirkung, Umfang, Einschränkungen, vereinbarten Schweregrad, Empfehlung und Retest-Kriterium. Der Test wird so detailliert beschrieben, dass eine autorisierte Person ihn wiederholen kann; der allgemeine Bericht vermeidet jedoch die Veröffentlichung von Geheimnissen oder Pfaden, die das Risiko außerhalb des Empfängerkreises erhöhen.

Die Evidenz muss Anfrage und Antwort dem richtigen Asset zuordnen. Ein Screenshot ohne URL und Datum identifiziert das Objekt nicht. Eine Fehlermeldung beweist keine Ausnutzung. Ein mit „kritisch“ gekennzeichnetes Scanner-Ergebnis belegt keine geschäftliche Auswirkung. Die Fachkraft prüft und erläutert, was getan wurde und welche Auswirkung tatsächlich nachgewiesen wurde.

4.2 Falschpositive und Duplikate

Ein Falschpositiv kann auf eine abgeleitete Version, eine individuelle Antwort, einen Proxy, eine Konfiguration oder eine fehlerhafte Scanner-Signatur zurückzuführen sein. Es wird durch manuelle Überprüfung, Protokolle und erwartetes Verhalten gegengeprüft. Kann es nicht bestätigt werden, wird es als unbestätigt markiert und nicht zur Gesamtzahl der Feststellungen gezählt. Duplikate mit derselben Ursache werden miteinander verknüpft, ohne betroffene Assets zu verschweigen.

Situation	Methodische Behandlung	Zu vermeiden
Unbestätigte Warnmeldung	Quelle, Version und Verhalten prüfen; Grenze angeben.	Als nachgewiesene Schwachstelle darstellen.
Dieselbe Ursache bei mehreren Assets	Nach Ursache gruppieren und die jeweilige Abdeckung auflisten.	Assets verschweigen oder Anzahl künstlich erhöhen.
Intermittierendes Ergebnis	Bedingungen, Wiederholungsversuche und Umgebung dokumentieren.	Nur die günstige Ausführung auswählen.
Nicht nachgewiesene Auswirkung	Technische Bedingung von möglicher Folge trennen.	Vollständige Kontrolle über das System annehmen.
Asset außerhalb des Umfangs	Anhalten und eine Erweiterung beantragen.	Testen, weil es verwandt erscheint.

4.3 Auswirkung und Priorität

Der technische Schweregrad wird durch Exposition, Berechtigungen, Daten, Ausnutzbarkeit, Kompensationskontrollen und geschäftliche Auswirkungen ergänzt. Eine schwer ausnutzbare Schwachstelle in einem kritischen Asset kann eine andere Priorität erfordern als eine leicht ausnutzbare in einer isolierten Umgebung. Es wird weder aus Rücksicht auf Geschäftsbeziehungen verharmlost noch zur Beeindruckung übertrieben.

Die Management-Zusammenfassung erläutert, was geschehen kann, welche Assets betroffen sind, unter welchen Bedingungen und welche Entscheidung erforderlich ist. Sie enthält keine endlose Liste kontextloser Begriffe. Der technische Anhang enthält Testnachweise, Logs und Einschränkungen. Die Geschäftsleitung erhält Entscheidungsgrundlagen; die Sicherheitsabteilung den Reproduktionspfad; die Compliance-Abteilung Evidenz für die Nachverfolgung.

Fiktiver Fall

Eine Funktion ermöglicht durch Ändern eines Identifikators den Zugriff auf ein Testdokument eines anderen Benutzers. Vor dem Zugriff auf reale Dokumente wird gestoppt. Die Feststellung belegt einen Autorisierungsfehler beim fiktiven Objekt. Sie behauptet weder, dass alle Dokumente zugänglich sind, noch dass der Angreifer die Datenbank heruntergeladen hat: Die Auswirkung wird durch zusätzliche autorisierte Tests abgegrenzt.

Ein Feststellungsformular ermöglicht eine Überprüfung ohne erneuten Schaden

ACCCF · REDAKTIONELLE REKONSTRUKTION · FIKTIVE DATEN

Minimaler Test, abgegrenzte Auswirkung und Korrekturweg

Feld	Inhalt	Kontrolle
Asset und Version	DEMO-Dienst und beobachtete Konfiguration.	Eindeutiges Objekt innerhalb des Umfangs.
Vorgehen	Schritte in kontrollierter Umgebung und fiktive Daten.	Wiederholbarkeit ohne echte Anmeldedaten.
Ergebnis	Technische Antwort und zugehörige Nachweise.	Warnung nicht mit Ausnutzung verwechseln.
Auswirkung	Asset, Zustand und nachgewiesene Folge.	Nicht auf das gesamte Unternehmen hochrechnen.
Behebung	Vorgeschlagene Änderung und Priorität.	Verantwortliche Person, Datum und Kriterium für den erneuten Test.

Die Abbildung erläutert Entscheidungen und Zusammenhänge; sie stellt keine Beweise aus einem echten Fall dar.

Abbildung 2. Ein Feststellungsformular ermöglicht die Überprüfung, ohne den Schaden zu wiederholen. Minimaler Nachweis, abgegrenzte Auswirkung und Behebungspfad. Redaktionelle Rekonstruktion; keine reale Evidenz.

Kapitel 5. Behebung und Risikomanagement

5.1 Ursachenorientierte Behebung

Die Empfehlung benennt die Bedingung, die geändert werden muss, und nicht nur ein allgemeines Update. Liegt das Problem in der Autorisierung, werden die serverseitige Validierung und die Beziehung zur Ressource geprüft; das Ausblenden des Links löst das Problem nicht. Liegt es in der Konfiguration, werden die Auswirkungen auf andere Umgebungen und Komponenten geprüft. Die Behebung umfasst Eigentümer, Zieldatum, Abhängigkeit, Test und mögliche Regression.

Wenn keine sofortige Behebung erfolgt, werden akzeptiertes Risiko, vorübergehende Mitigation, verantwortliche Person und Überprüfungsdatum dokumentiert. Die Akzeptanz wird nicht als Behebung dargestellt. Eine WAF kann einen Pfad einschränken, beseitigt aber nicht die Ursache; Evidenz beider Zustände wird aufbewahrt und geprüft, ob die Regel legitime Funktionen beeinträchtigt.

5.2 Plan nach Auswirkung und Abhängigkeit

Aktion	Verantwortliche Person und Datum	Akzeptanzkriterium
Vorübergehende Mitigation	[Eigentümer, Umsetzung und Gültigkeitsdauer]	[Verringert Exposition, ohne den Betrieb zu beeinträchtigen]
Endgültige Behebung	[Änderung, Version und Deployment]	[Ursache im Umfang beseitigt]

Aktion	Verantwortliche Person und Datum	Akzeptanzkriterium
Überprüfung weiterer Assets	[Gleiches Muster und Abdeckung]	[Keine versteckten Duplikate]
Regressionstest	[Kritische Funktionen und Rollen]	[Keine Beeinträchtigung legitimer Benutzer]
Aktualisierung der Dokumentation	[Diagramm, Konfiguration und Verfahren]	[Realität und Dokumente stimmen überein]
Restrisikoakzeptanz	[Wer, Grund und Ablaufdatum]	[Nicht mit technischem Abschluss verwechseln]

5.3 Evidenz der Behebung

Konfigurationsänderung, Version, Datum, verantwortliche Person, Deployment, Tests und Auswirkungen werden aufbewahrt. Ein Screenshot des Panels mit der Angabe „aktualisiert“ beweist nicht, dass der Pfad behoben wurde. Bei mehreren Umgebungen wird dokumentiert, wo die Änderung angewendet wurde. Der ursprüngliche Bericht wird nicht verändert, um die Feststellung zu entfernen: Eine neue, verknüpfte Bewertung wird hinzugefügt.

> **Grundsatz der Ehrlichkeit**
> „Der Anbieter sagt, dass das Problem bereits behoben ist“ ist eine Aussage, kein Retest. Die Evidenz für den Abschluss erfordert eine technische Überprüfung oder eine ausdrückliche Entscheidung über das Restrisiko und dessen Umfang.

Kapitel 6. Retest und Abschluss

6.1 Vergleichbare Bedingungen wiederholen

Der Retest verwendet nach Möglichkeit dasselbe Objekt, dieselbe Rolle, dieselben Bedingungen und dasselbe Verfahren, jedoch mit neuer Version und neuem Datum. Der Vergleich erfolgt mit der ursprünglichen Feststellung, ohne die frühere Evidenz zu verändern. Änderungen an Anwendung oder Umgebung werden dokumentiert, da sie ein abweichendes Ergebnis erklären können. Ein negatives Ergebnis bezieht sich nur auf den aktuellen Test und seine Abdeckung.

Auch die Regression wird getestet: Der legitime Benutzer kann arbeiten, und die Funktion legt keine weiteren Daten offen. Wird die schädliche Anfrage blockiert, aber der normale Zugriff beeinträchtigt, kann der Status teilweise behoben sein. Funktioniert die Behebung nur für einen Pfad und gibt es gleichwertige Pfade, werden diese innerhalb des Umfangs geprüft. Der Abschlusstest beschränkt sich nicht auf einen Screenshot des erwarteten Fehlers.

6.2 Abschlussstatus

Status	Kriterium	Evidenz
Behoben	Die Bedingung ist im Umfang nicht reproduzierbar, und es wurde keine Regression beobachtet.	Retest, Datum, Version und legitime Funktionen.
Teilweise behoben	Einige Assets oder Pfade wurden verbessert; bei anderen besteht die Bedingung weiter.	Abdeckung und offene Punkte je Asset.

Status	Kriterium	Evidenz
Mitigiert	Eine vorübergehende Kontrolle verringert die Exposition, ohne die Ursache zu beseitigen.	Regel, Test, Gültigkeitsdauer und Grenze.
Akzeptiert	Die verantwortliche Person akzeptiert das Restrisiko mit Begründung und Ablaufdatum.	Entscheidung, Umfang und Überprüfung.
Offen	Die Bedingung ist reproduzierbar oder es liegt keine ausreichende Evidenz vor.	Ursprüngliche Feststellung und offene Aktionen.

6.3 Abschlussbericht und Erkenntnisse

Der Abschlussbericht verknüpft ursprüngliche Feststellung, Änderung, Retest und Status, ohne frühere Inhalte zu löschen. Er enthält Restrisiko, Einschränkungen und das Datum der nächsten Überprüfung. Die Management-Zusammenfassung verspricht kein „sicheres System“; sie gibt an, welche Risiken bewertet wurden und welche Evidenz für Verbesserungen vorliegt. War ein Test nicht möglich, wird dies erklärt, statt ihn als bestanden zu markieren.

Die gewonnene Erkenntnis kann phishing-resistente Authentifizierung, Überprüfung von Autorisierungen, Regressionstests, ein Drittparteieninventar oder bessere Protokolle erforderlich machen. NIST SP 800-63B-4 bietet Leitlinien zur Authentifizierung und Vertrauensniveaus; die Bewertung des Wiederherstellungsablaufs wird dadurch nicht ersetzt, obwohl dieser häufig der tatsächliche Kompromittierungspfad ist.[2]

> **Tatsächlicher Abschluss**
> Der Test endet, wenn die Organisation zeigen kann, was sie festgestellt, was sie geändert, was sie überprüft hat und welches Risiko verbleibt. Er endet nicht, wenn die PDF-Datei den Namen „final“ erhält.



Abbildung 3. Der Retest überprüft das Risiko, nicht nur den Patch. Die erste Evidenz wird aufbewahrt und mit der neuen verglichen. Redaktionelle Rekonstruktion; keine reale Evidenz.

[2] NIST SP 800-63B-4 (Juli 2025). Leitlinien zur Authentifizierung und Verwaltung von Authentifizierungsmitteln, einschließlich Vertrauensniveaus und phishing-resistenter Authentifizierung. Die Wiederherstellung von Konten ist Teil des Risikos und darf nicht auf Passwörter reduziert werden. Offizielle Online-Quelle

Anhang A. Einsatzregeln und Formular

A.1 Einsatzregeln

Fiktive Vorlage zur Genehmigung

```
Projekt: DEMO-PENTEST-2026-009
Ziel und Unternehmensrisiko: [konkrete Frage]
Einbezogene Assets: [Domains, Bereiche, Anwendungen, Konten]
Ausschlüsse: [Assets, Dritte, Daten und Techniken]
Zeitfenster und Zeitzone: [Beginn, Ende, Kontakte]
Erlaubte Daten: [fiktiv, Maskierung, Verarbeitung]
Erlaubte Aktionen: [Überprüfung, Validierung, Bedingungen]
Verbotene Aktionen: [DoS, Brute Force, Social Engineering, andere]
Abbruchschwellen: [Beeinträchtigung, Daten, Umfang, Warnmeldung]
Notfallkontakt und Vertretung: [sicherer Kanal]
Evidenz: [Formate, Minimierung und Verwahrung]
Übergabe: [Empfänger, Verschlüsselung und Datum]
Löschung: [Objekte, Backup und Grenzen]
Retest: [Datum, Umfang und Akzeptanz]
Autorisierungen: [Inhaber, Dritte und Version]
```

A.2 Feststellungsformular

Feld	Erforderlicher Inhalt	Fiktives Beispiel
Identifikator	Stabiler Code mit Bezug zum Protokoll.	DEMO-AUTH-003.
Asset und Version	Anwendung, Umgebung und Konfiguration.	Portal DEMO v2.4, Testumgebung.
Bedingung	Welche Kontrolle unter welcher Rolle versagt.	Ressource eines anderen fiktiven Benutzers ist zugänglich.
Vorgehen	Autorisierte Schritte, Anfragen und Parameter.	Eingeschränkte Rolle und Kontrollressource.
Ergebnis	Antwort und Artefakte ohne Geheimnisse.	Code 200 und Teilstruktur.
Auswirkung	Nachgewiesene Folge und Umfang.	Zugriff auf das fiktive Objekt; keine Extrapolation.
Einschränkungen	Was nicht getestet wurde und warum.	Keine Einsicht in reale Dokumente.
Behebung	Änderung, Eigentümer und Priorität.	Serverseitige Validierung der Autorisierung.
Retest	Bedingungen, Datum und Ergebnis.	Gleicher Pfad und gleiche Rolle, zusätzlich Regression.

A.3 Retest-Bericht

Vergleichsprotokoll

```
Ursprüngliche Feststellung: [ID, Evidenz und Datum]
Vorgenommene Änderung: [Konfiguration, Version, verantwortliche Person]
Datum und Zeitzone des Retests: [wörtlich]
Gleichwertige Bedingungen: [Rolle, Objekt, Parameter]
Ergebnis des wiederholten ursprünglichen Tests: [beobachtet]
Regressionstests: [legitime Funktionen]
Zusätzliche Abdeckung: [Pfade oder Assets]
Status: [behoben, teilweise behoben, mitigiert, akzeptiert, offen]
Restrisiko und Grenzen: [Erklärung]
Nächste Überprüfung: [Datum und verantwortliche Person]
Anhänge: [Ausgabe, Protokolle und Manifest]
```

Anhang B. Rechtsrahmen und Abschlusskontrolle

Die Autorisierung ist die erste Voraussetzung; elektronische Evidenz erfordert Methode, Zurechenbarkeit, Integrität und Zugänglichkeit. In Mexiko enthalten die anwendbaren CNBV-Bestimmungen besondere Anforderungen an Sicherheitsüberprüfungen und Aufzeichnungen für Kreditinstitute, einschließlich der mindestens jährlichen Überprüfung nach Artikel 316 Bis 17 in ihrem Anwendungsbereich. In Peru und Argentinien bestehen sektorale Anforderungen an Management und Reaktion; Spanien unterscheidet zwischen Zahlungen und Risiken. Diese Pflichten werden nicht auf jedes Unternehmen übertragen.[3][4][5][6][7][8]

Kolumbien, Ecuador, Chile und Spanien verfügen über Regeln zu elektronischen Dokumenten, Signaturen und Aufbewahrung, die bei der Strukturierung von Evidenz helfen; sie autorisieren für sich allein keine Intrusionstests. Der Datenschutz begrenzt, was erfasst und weitergegeben werden darf, selbst wenn das Ziel darin besteht, eine Schwachstelle nachzuweisen.[9][10][11][12][13][14]

Kontrolle	Akzeptanzfrage
Autorisierung	Sind Assets, Techniken, Daten, Zeitfenster und Abbruch genehmigt?
Sicherheit	Vermeidet der Test Schäden und unnötige Exposition?
Methode	Wurden Werkzeuge, Versionen und Ausgaben validiert?
Feststellung	Sind Asset, Vorgehen, Ergebnis und Auswirkung nachvollziehbar?
Behebung	Sind Änderung und Abdeckung dokumentiert?
Retest	Wurden dieselbe Bedingung und Regression überprüft?
Fazit	Wurden Restrisiko und Grenzen nicht verschwiegen?

Abschluss

Der beste Test ist nicht derjenige, der den größten Zugriff nachweist, sondern derjenige, der eine Risikominderung mit ausreichender Evidenz ermöglicht, ohne ein weiteres Ereignis zu verursachen.

[3] Allgemein geltende Bestimmungen für Kreditinstitute, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 bis 17: Nachweise, Verschlüsselung, Zugriff, Vorfälle, Störungen, Protokolle und Überprüfungen. Offizielle Online-Quelle

[4] Peru. SBS 504-2021, Artikel 12.6.g, 15 und 17.3–17.4: Aufbewahrung, Berichterstattung und forensische Analyse, Registrierungsaufzeichnungen, Authentifizierung und Vorgänge. Offizielle Online-Quelle

[5] Argentinien. BCRA-Mitteilung A 8280: Reaktion und Wiederherstellung bei Cybervorfällen; Abschlussbericht innerhalb von fünf Kalendertagen nach Eindämmung, Wiederherstellung und Lösung. Offizielle Online-Quelle

[6] Spanien. Königliches Dekretgesetz 19/2018, Artikel 45, 66 und 67: Rückerstattung für nicht autorisierte Transaktionen, Risikomanagement und unverzügliche Meldung schwerwiegender Vorfälle. Offizielle Online-Quelle

[7] Handelsgesetzbuch von Mexiko, Artikel 89–94 und 1205: Neutralität, Zuschreibung, Schriftform, Original, Integrität, Zugänglichkeit und Zulässigkeit von Datennachrichten. Offizielle Zusammenstellung. Offizielle Online-Quelle

[8] Nationaler Kodex für Zivil- und Familienverfahren, Artikel 348–350. Zusammenstellung mit der Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von förmlichen Feststellungen ab. Offizielle Online-Quelle

[9] Chile. Gesetz 19.799 über elektronische Dokumente und elektronische Signaturen, Artikel 1–5: Gleichwertigkeit, Schriftform, einfache/fortgeschrittene Signatur, Datum und Beweiswert. Offizielle Online-Quelle

[10] Kolumbien. Gesetz 527 von 1999, Artikel 5–13, 16–25 und 28: Datennachrichten, Schriftform, Original, Integrität, Zulässigkeit, Aufbewahrung, Versand, Empfang und digitale Signatur. Offizielle Online-Quelle

[11] Ecuador. Gesetz über elektronischen Handel, elektronische Signaturen und Datennachrichten, Gesetz 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[12] Verordnung (EU) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene Signatur und Wirkungen der qualifizierten Signatur. Offizielle Online-Quelle

[13] Mexiko. Bundesgesetz zum Schutz personenbezogener Daten in privater Hand, veröffentlicht am 20-03-2025 und geändert am 14-11-2025. Artikel 5–9, 18–20 und 31: Grundsätze, Sicherheit, Vertraulichkeit, Verletzungen und Bearbeitung von Rechten. Die derzeitige Bundesbehörde ist das Sekretariat für Korruptionsbekämpfung und gute Regierung. Offizielle Online-Quelle

[14] Europäische Union. Verordnung (EU) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit und Meldung/Kommunikation von Sicherheitsverletzungen. Spanien verlangt außerdem die Prüfung der anwendbaren nationalen und sektorspezifischen Gesetze. Offizielle Online-Quelle