ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

08

Volumen

Erhaltung von Inhalt und überprüfbarem Kontext

Spanische Ausgabe · 2026

Handbuch zur Zertifizierung von E-Mails, Online-Veröffentlichungen und Social-Media-Inhalten

EML, Header, URLs, Dateien, Veröffentlichungen, Nachvollziehbarkeit und Präsentation

Bewahren, was eine Überprüfung einer Nachricht oder Veröffentlichung vor deren Verschwinden ermöglicht, ohne einen Screenshot mit der Quelle oder ein Datum auf dem Bildschirm mit einem Herkunftsnachweis zu verwechseln.

Für Rechtsanwälte, Sachverständige, Compliance- und Kommunikationsverantwortliche, Ermittler und alle, die eine E-Mail, eine Veröffentlichung oder ein Online-Gespräch sichern müssen. Notarielle, sachverständige oder administrative Zertifizierung hängt vom Gebiet und Verfahren ab.

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: Sichern, bevor sich Inhalte ändern 3
Kapitel 1. Umfang und Vorbereitung 3
1.1 Welche Behauptung nachgewiesen werden muss 3
1.2 Vorbereitung der Erfassungsumgebung 4
Kapitel 2. Die vollständige Nachricht 4
2.1 EML: Text, Header und Anhänge 4
2.2 Weiterleitung, Herunterladen und Konvertierung 4
2.3 Anhänge und Übergabe durch Dritte 5
Kapitel 3. Authentifizierung des Kanals 6
3.1 Received-Header und Übertragung 6
3.2 DKIM, SPF und DMARC 6
3.3 Datum, Message-ID und Inhalt 7
Kapitel 4. Dateien, URLs und Veröffentlichungen 8
4.1 Vollständige Erfassung einer URL 8
4.2 Veröffentlichung, Thread und Multimedia 8
4.3 Webarchiv und Datumsangaben Dritter 8
Kapitel 5. Bewahrung und dokumentierte Zertifizierung 9
5.1 Erfassungsprotokoll 9
5.2 Verwahrung und Zugriffskontrolle 9
5.3 Sachverständige, notarielle oder administrative Zertifizierung 10
Kapitel 6. Entfernung, Meldung und Medienschaden 10
6.1 Vor dem Entfernen sichern 10
6.2 Schaden und Umfang 10
6.3 Integrierter Fall 10
Anhang A. Formate der Bewahrung 11
A.1 E-Mail-Protokoll 11
A.2 Veröffentlichungsprotokoll 11
A.3 Objektmanifest 11
A.4 Protokoll des Entfernungsantrags 11
Anhang B. Rechtsrahmen und Abschlussliste 12

Einleitung: Sichern, bevor sich Inhalte ändern

Eine Veröffentlichung kann bearbeitet, ein Konto geschlossen, eine Anlage ersetzt und ein Link ungültig werden. Die Bewahrung soll dokumentieren, was zu einem bestimmten Zeitpunkt vorhanden war, wo es sich befand, wie es erlangt wurde und welche Darstellung erhalten blieb. Ein Screenshot kann einen Ausschnitt zeigen; die Überprüfung erfordert jedoch das vollständige Objekt und seinen Kontext: URL, Konto, Datum, Zeitzone, Dateien, Antworten, Metadaten und Erfassungsprozess.

E-Mails bieten ein klares Beispiel. Wer nur ein Bild der Nachricht aufbewahrt, verliert Header, Struktur und Anhänge. Wer nur die Anlage speichert, verliert die Erklärung, die ihren Inhalt beschreibt, und in einigen Fällen den Hash zu deren Überprüfung. EML vereint diese Komponenten und ermöglicht ihre Verknüpfung. Es beweist weder die Wahrheit aller Aussagen noch, dass eine bestimmte Person den Text verfasst hat.

„Zertifizierung“ bezeichnet hier ein dokumentiertes Verfahren, keine universelle Garantie. Eine notarielle Handlung, ein Sachverständigengutachten, eine Aufbewahrungsbestätigung und eine bezeugte Bildschirmaufnahme können unterschiedliche Funktionen und Wirkungen haben. Wer bewahrt, muss angeben, was getan wurde und was bewiesen werden kann; Feierlichkeit darf eine unvollständige Quelle nicht verdecken.

> **Goldene Regel**
> Inhalt und Kontext müssen gemeinsam bewahrt werden. Ein scharfes Bild einer Veröffentlichung ohne URL und Datum ist eine nützliche Referenz, aber keine vollständige Rekonstruktion des Objekts.

Kapitel 1. Umfang und Vorbereitung

1.1 Welche Behauptung nachgewiesen werden muss

Es ist nicht dasselbe, zu beweisen, dass eine Veröffentlichung existierte, dass ein Konto sie veröffentlichte, dass eine Person sie verfasste, dass sie öffentlich zugänglich war, dass sie eine Drohung enthielt oder dass eine bestimmte Datei übergeben wurde. Die Behauptung bestimmt die Quelle: sichtbare Veröffentlichung, Export, EML, Plattformprotokolle, Empfänger, Administrator oder Zeuge. Wenn nur die Existenz an einem Datum nachgewiesen werden soll, darf die Analyse nicht zur Urheberschaft ausgedehnt werden.

Zeitraum, Konten, URLs, Schlüsselwörter, Beteiligte, Inhaltstypen und Drittdaten werden abgegrenzt. Außerdem wird festgelegt, ob die Bewahrung für eine Meldung, Entfernung, ein Verfahren, eine interne Untersuchung oder eine Archivbestätigung dient. Dringende Bewahrung enthebt weder der Genehmigung noch dem Schutz Dritter.

Ziel	Vorrangige Quelle	Zu erklärende Grenze
Existenz einer Veröffentlichung	URL, Inhalt, Seite und dokumentierte Bewahrung.	Sie beweist weder menschliche Urheberschaft noch die Vollständigkeit des Kontos.
E-Mail-Inhalt	EML mit Text, Header und Anhängen.	Sie beweist nicht die Wahrheit des Textes.
Dateiübergabe	Anhänge, Text, Hash, Download und Manifest.	Sie beweist nicht die Abdeckung des Quellsystems.

Ziel	Vorrangige Quelle	Zu erklärende Grenze
Öffentliche Reichweite	Sichtbarkeit, Zielgruppe, Link und Zugriffsnachweis.	Sie entspricht nicht der tatsächlichen Leserzahl.
Urheberschaft oder Kontrolle	Konto, Sitzungen, Geräte und Kontext.	Ein sichtbarer Name identifiziert keine Person.
Sequenz	Datumsangaben, Zeitzone, Antworten, Bearbeitungen und Referenzen.	Ein isolierter Screenshot lässt nicht den gesamten Verlauf rekonstruieren.

1.2 Vorbereitung der Erfassungsumgebung

Ein autorisierter Computer und ein autorisierter Account werden verwendet, mit dokumentiertem Datum und Zeitzone, bekanntem Browser und kontrolliertem Speicher. Die Anmeldung mit einem persönlichen Konto soll vermieden werden, da dadurch unnötige Daten in die Beweise gelangen. Mit der Veröffentlichung wird nur so viel wie nötig interagiert: Antworten, Melden oder Teilen kann ihre Reichweite verändern und den Autor benachrichtigen.

Für Original, Arbeitskopie, Screenshots, Exporte, Protokolle und Manifest werden getrennte Ordner angelegt. Potenziell rechtswidrige oder schädliche Inhalte werden nicht an das gesamte Team verteilt. Das Vorhandensein wird dokumentiert und über einen eingeschränkten Kanal übergeben. Gefährdet eine Person etwas, haben ihre Sicherheit und die Kontaktaufnahme mit den zuständigen Stellen Vorrang vor zusätzlichem technischem Nachweis.

> **Vorherige Entscheidung**
> Kann die Veröffentlichung verschwinden und liegt eine Genehmigung zur Bewahrung vor, werden zuerst Objekt und Kontext dokumentiert. Erst danach werden Entfernung oder Überprüfung beantragt. Eine Entfernung vor der Bewahrung kann eine Behauptung ohne Quelle hinterlassen.

Kapitel 2. Die vollständige Nachricht

2.1 EML: Text, Header und Anhänge

RFC 5322 beschreibt das Format von Internetnachrichten mit Headerfeldern und Text. EML ermöglicht die Bewahrung einer Darstellung der E-Mail mit diesen Komponenten und etwaigen Anhängen. Die Herkunft wird dokumentiert: Export vom Client, Download vom Server oder Übergabe durch eine andere Person. Sie verändert die Interpretation und darf nicht hinter einer bekannten Dateiendung verborgen werden.[1]

Vor dem Öffnen mit Werkzeugen, die die Datei verändern könnten, wird sie bewahrt. Hashes der EML und der Anhänge werden getrennt berechnet und im Manifest verknüpft. Der Text kann Algorithmus und Wert einer Datei angeben: dieser wird geprüft und nicht in eine separate Notiz kopiert. Bei einer Abweichung wird die erste Übergabe aufbewahrt und eine Klärung angefordert.

2.2 Weiterleitung, Herunterladen und Konvertierung

Das Weiterleiten einer E-Mail kann Header hinzufügen und die Beziehung zwischen Nachricht und Dateien verändern. Das Drucken als PDF bewahrt eine Ansicht, nicht die Struktur. Der Download aus

[1] RFC Editor. RFC 5322, Internet Message Format: Struktur der Nachricht, Header und Textkörper. Dies ist eine technische Referenz zur Aufbewahrung und zum Verständnis von E-Mails, kein automatischer Nachweis menschlicher Identität. Offizielle Online-Quelle

Webmail kann unterschiedliche Formate erzeugen. Jeder Vorgang wird dokumentiert und Versionen werden aufbewahrt, ohne die Weiterleitung automatisch als Originalnachricht zu behandeln.

Eine weitergeleitete Nachricht kann weiterhin nützlicher Beleg dafür sein, was eine Person zu einem bestimmten Zeitpunkt erhalten hat; ihr früherer Inhalt wird jedoch mit Headern und ergänzenden Quellen analysiert. Soll die Übergabe einer Datei nachgewiesen werden, ist die ursprüngliche EML des Anbieters einem Screenshot der Weiterleitung vorzuziehen. Ist sie nicht verfügbar, wird diese Einschränkung erklärt und die Nachricht in einem anderen Postfach oder auf einem anderen Server gesucht.

Darstellungsform	Was erhalten bleibt	Was ergänzt werden muss
Ursprüngliche EML	Text, Header und verfügbare Anhänge.	Herkunft und Inhaltsprüfung.
Weitergeleitete EML	Neue Übergabe und Darstellung des früheren Inhalts.	Verlauf der Weiterleitung und frühere Herkunft.
E-Mail-PDF	Layout und lesbarer Text.	Header, Anhänge und Struktur.
Screenshot	Auf dem Bildschirm angezeigter Ausschnitt.	URL, Konto, Datum, Kontext und Datei.
Nur Anhang	Daten einer Datei.	Nachricht, Erklärung, Beziehung und Prozess.

2.3 Anhänge und Übergabe durch Dritte

Die Anlage wird vor der Bewahrung weder bearbeitet noch konvertiert, um das Lesen zu erleichtern. Der Hash wird berechnet, mit dem angegebenen Wert verglichen und Öffnung sowie Abdeckung dokumentiert. Öffnet sich eine CSV-Datei ohne Feldwörterbuch, wird die Bedeutung der Felder angefordert. Der Hash beweist nur die Gleichheit der verglichenen Objekte, nicht die Vollständigkeit oder Wahrheit der Zeilen.

> **Fiktiver Fall**
> Ein Anbieter liefert eine CSV- und eine PDF-Datei und nennt im Nachrichtentext für jede einen Hashwert. Die CSV-Datei stimmt überein, die PDF-Datei nicht. Alles wird aufbewahrt, eine erneute PDF-Lieferung angefordert und dokumentiert, dass die CSV-Datei mit der Erklärung übereinstimmt, ohne die Vollständigkeit der Anbieterinhalte zu behaupten. Die zweite Lieferung erhält einen anderen Identifikator und ersetzt die erste nicht.



Abbildung 1. EML, Anhänge und Erklärung: miteinander verbundene Objekte. Jede Integrität bezieht sich auf ein anderes Objekt. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 3. Authentifizierung des Kanals

3.1 Received-Header und Übertragung

Received-Felder liefern eine erklärte Sequenz von Servern, Datumsangaben und Transportdaten. Sie werden in der durch die Nachrichtenstruktur festgelegten Reihenfolge geprüft, ohne pauschal alle für zuverlässig zu halten und ohne das erste sichtbare Feld als menschlichen Ursprung zu interpretieren. Einige Felder können durch Zwischensysteme hinzugefügt werden. Die Analyse vergleicht Server, Zeiten, Domains und weitere Authentifizierungsergebnisse.

Die sichtbare From-Adresse kann von der authentifizierten Domain oder dem Versandserver abweichen. Eine IP-Adresse im Header kann Infrastruktur identifizieren, nicht die Person. Datumsangaben können von unterschiedlichen Uhren abhängen. Eine komplexe Kopfzeile ist kein magischer Beweis; die Analyse muss erläutern, welche Komponenten verifizierbar sind und welche auf Vertrauen beruhen.

3.2 DKIM, SPF und DMARC

DKIM verknüpft eine Domain durch eine kryptografische Signatur mit der Nachricht und ermöglicht die Überprüfung der signierten Komponenten. SPF veröffentlicht, welche Hosts für eine Domain im Protokollkontext zugelassen sind; DMARC liefert Ausrichtung und Domain-Richtlinie. Diese Mechanismen helfen bei der Bewertung von Kanal und Domain, beweisen aber weder den Verfasser des Textes noch seine Richtigkeit. Ein Fehler kann auch eine Prüfung von Weiterleitung, Konfiguration oder Umwandlungen erfordern.[2][3]

Der Bericht dokumentiert, sofern verfügbar, Domain, Selektor, signierte Felder, Ergebnis, Datum und Abfragequelle. „DKIM pass“ reicht nicht als persönliche Identifizierung. Auch „SPF fail“ beweist für sich

[2] RFC Editor. RFC 6376, DomainKeys Identified Mail (DKIM) Signatures: Verantwortung einer Domain und kryptografische Überprüfung der signierten Komponenten. Dies allein belegt weder, wer den Text geschrieben hat, noch die Richtigkeit des Inhalts. Offizielle Online-Quelle

[3] RFC Editor. RFC 8616 und technische Referenzen SPF RFC7208, DKIM RFC6376 und DMARC RFC7489: Autorisierung von Hosts, Domain-Signatur, Ausrichtung und Richtlinie. Sie helfen bei der Bewertung des Kanals; allein belegen sie weder menschliche Identität noch die Richtigkeit des Inhalts. Offizielle Online-Quelle

allein keine böswillige Täuschung: Übertragungsweg und Konfiguration müssen geprüft werden. Die technische Analyse bewahrt die Originalnachricht, damit andere sie überprüfen können.

3.3 Datum, Message-ID und Inhalt

Die Message-ID kann beim Verknüpfen von Nachrichten und Systemen helfen, aber ihre Einzigartigkeit und Struktur hängen vom Generator ab. Datumsangaben werden wörtlich mit ihrer Zeitzone bewahrt und mit Serverprotokollen und Empfangsereignissen verglichen. Das Download-Datum ist nicht das Versanddatum. Das Datum einer Anlage ist eine weitere Ebene.

Behauptung	Was überprüft werden kann	Was nicht daraus folgt
Authentifizierte Domain	Signatur, Ausrichtung und Kanalkonfiguration.	Eine natürliche Person hat die Nachricht verfasst.
Versanddatum	Header und Protokolle sind konsistent.	Der Text wurde genau zu diesem Zeitpunkt erstellt.
Nachricht erhalten	Postfach, EML und Serverprotokolle.	Die Person hat sie gelesen oder verstanden.
Wahrer Inhalt	Unabhängige Quellen für das erzählte Ereignis.	DKIM oder Hash beweist das Ereignis.
Konto kompromittiert	Sitzungen, Wiederherstellung und anomale Aktivität.	Eine andere Adresse allein beweist Diebstahl.

Leseregel

Header werden als Nachweis von Transport und Domain analysiert, nicht als Geständnis einer Person. Urheberschaft erfordert zusätzliche Bestätigung.



Abbildung 2. Header lesen, ohne daraus eine menschliche Identifizierung abzuleiten. Hinweise auf Transport, Domain und Inhalt. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 4. Dateien, URLs und Veröffentlichungen

4.1 Vollständige Erfassung einer URL

Vollständige URL, Parameter, Domain, Datum und Zeitzone, sichtbares Konto, Zugriffsart, Rolle, Sprache, Browserversion und Seitenstatus werden bewahrt. Weiterleitungen, Anmeldungen, geografische Einschränkungen oder Fehler werden dokumentiert. Bei gleicher URL kann sich der Inhalt ändern; deshalb werden Objekt und Beschaffungsprozess bewahrt.

Der Screenshot muss genügend Kontext enthalten, um die Seite zu erkennen, ohne unnötige Daten offenzulegen. Wenn nützlich und zulässig, werden HTML-Datei, Multimedia-Ressourcen, nativer Export und eine Beschreibung dessen ergänzt, was nicht beschafft werden konnte. Eine dynamische Seite kann jedem Besucher andere Inhalte zeigen; der Bericht darf sie nicht als universelle Ansicht verallgemeinern.

4.2 Veröffentlichung, Thread und Multimedia

Text, scheinbarer Autor, Veröffentlichungs-ID, sichtbares Datum, URL, relevante Antworten, Zitate, Weiterleitungen, Reaktionen und Multimedia werden bewahrt. Die Reihenfolge der Antworten kann sich durch Algorithmen oder Moderation ändern. Bei der Erfassung eines Threads werden Navigationsweg und Abdeckungsgrenze dokumentiert. Eine einzelne Antwort außerhalb des Kontexts kann die Unterhaltung verzerren.

Bild- oder Videodateien werden nach Genehmigung heruntergeladen und separat gehasht. Veröffentlichung und Datei werden im Manifest verknüpft. Bei der Untersuchung der Authentizität des Inhalts kommt der spezielle Multimedia-Band zum Einsatz; die Bewahrung beweist nur, dass diese Version zu diesem Zeitpunkt und aus dieser Quelle verfügbar war.

4.3 Webarchiv und Datumsangaben Dritter

Ein Drittarchiv kann einen nützlichen Schnappschuss bewahren, aber sein Datum gehört zur Erfassung, nicht notwendigerweise zur ersten Veröffentlichung. Dokumentiert werden, wer archiviert hat, welche Version erfasst wurde, welche Ressourcen fehlen und wie darauf zugegriffen wurde. Datumsangaben im Inhalt können vom Autor geändert worden sein oder eine andere Zeitzone verwenden. Zur Bestätigung werden Veröffentlichungen, Mitteilungen, Links und zeitnahe Aufzeichnungen herangezogen.

Element	Erforderliche Dokumentation	Grenze
URL und Weiterleitungen	Vollständige Adresse und Zugriffssequenz.	Veränderlicher oder personalisierter Inhalt.
Veröffentlichung und Thread	Kennung, Text, Antworten und erfasster Umfang.	Bei begrenzter Abdeckung nicht das gesamte Gespräch.
Multimedia	Datei, Qualität, Hash und Herkunft.	Weder Authentizität der Szene noch Urheberschaft.
Externes Archiv	Verwalter, Schnappschuss, Datum und fehlende Ressourcen.	Belegt weder Erstveröffentlichung noch Vollständigkeit des Inhalts.
Zugriff	Konto, Rolle, Sichtbarkeit und Einschränkungen.	Nicht alle Benutzer sahen dieselben Inhalte.

Präsentationsregel

Ein Webarchiv darf nicht mit „war immer so“ und ein Screenshot nicht mit „das ist alles“ argumentiert werden. Beschrieben werden Version, Datum und tatsächlich belegbare Abdeckung.



Abbildung 3. Eine Veröffentlichung wird mit ihrem Umfeld bewahrt. Der Screenshot ist eine Darstellung, nicht das gesamte Universum. Redaktionelle Rekonstruktion; kein echtes Beweismaterial.

Kapitel 5. Bewahrung und dokumentierte Zertifizierung

5.1 Erfassungsprotokoll

Das Erfassungsprotokoll nennt Fall, Bediener, Genehmigung, Ort, Datum und Zeitzone, Gerät, Browser oder Werkzeug, Konto und Rolle, erfasste Objekte, Maßnahmen, Formate, Vorkommnisse und Hash. Bei Bildschirmaufnahmen werden Pfad und Filter, bei Exporten Parameter und Ausgabe und bei Anbietern Antwort und Kanal dokumentiert. Es beschreibt die tatsächlich durchgeführten Schritte, nicht einen idealen Ablauf, der nie stattfand.

Eine Aufbewahrungsbestätigung kann den Nachweis von Integrität und Zugänglichkeit ergänzen. In Mexiko enthält die NOM-151 besondere Anforderungen für die Aufbewahrung und Digitalisierung von Datennachrichten in ihrem Anwendungsbereich; sie bescheinigt weder die Richtigkeit des Inhalts noch ersetzt sie die Erfassung der vollständigen Nachricht. Ein Zeitstempel oder Hash beweist weder menschliche Urheberschaft noch die Rechtmäßigkeit der Beschaffung.[4][5]

5.2 Verwahrung und Zugriffskontrolle

Quelle und Arbeitskopie werden getrennt und der Zugriff eingeschränkt. Elektronische Übertragungen umfassen Empfänger, Berechtigungen, Datum, Version, Schlüsselübergabekanal und Download-Verifizierung. Der Bericht enthält keine Passwörter, Tokens oder Cookies. Bei einer authentifizierten Seite wird die Rolle dokumentiert, ohne die Sitzung offenzulegen.

Die Arbeitskopie dient Analyse, Anonymisierung und Präsentation. Die öffentliche Version wird geprüft, um personenbezogene Daten, intime Bilder, Wohnadressen und nicht betroffene Dritte zu vermeiden. Die vollständig bewahrte Version wird durch eine redigierte Fassung nicht vernichtet; ihr Zugriff und ihre spätere Nutzung werden eingeschränkt.

[4]NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und elektronischen Fingerabdruck. Offizielle Online-Quelle

[5]Wirtschaftsministerium. PLATIICA. Datensatz zur NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten. Überprüfung der Gültigkeit und ergänzende Referenz zum Text des DOF. Offizielle Online-Quelle

5.3 Sachverständige, notarielle oder administrative Zertifizierung

Die Wahl hängt von Jurisdiktion, Objekt und Zweck ab. Eine notarielle Handlung kann eine Ansicht dokumentieren; ein sachverständiges Gutachten kann Herkunft, Struktur, Authentizität, Beziehungen und Kontext analysieren; eine administrative Bestätigung kann eine Handlung in ihrem Bereich belegen. Keine davon verwandelt einen Ausschnitt in einen vollständigen Beweis. Die geeignete Form wird vor Beginn angefordert, damit keine Maßnahmen auf einer veränderlichen Seite wiederholt werden.

> **Qualitätskriterium**
> Die beste Zertifizierung ist nicht die mit den meisten Stempeln, sondern die, die es einer anderen Person ermöglicht, zu verstehen, was gesehen wurde, wo, wann, mit welcher Methode und was ausgeklammert wurde.

Kapitel 6. Entfernung, Meldung und Medienschaden

6.1 Vor dem Entfernen sichern

Vor einem Entfernungsantrag werden URL, Kennung, Veröffentlichung, Konto, Multimedia, Antworten und Zugriffsdatum bewahrt. Bereits geänderte Versionen und Referenzlinks werden ebenfalls dokumentiert. Bei unmittelbarer Gefahr haben Sicherheit und Notfallkanäle Vorrang; die Bewahrung darf nicht zu einer gefährlichen Verzögerung führen.

Die Meldung an die Plattform muss konkret sein: Objekt, URL, Grund, Nachweis, Datum und Antrag. Sie enthält nur die erforderlichen personenbezogenen Daten und sendet die schädliche Datei nicht an unbestimmte Kanäle. Meldenummer, Inhalt, Datum und Antworten werden bewahrt. Das Entfernen eines Links beweist weder das Verschwinden aller Kopien noch das Ende des Schadens.

6.2 Schaden und Umfang

Die Analyse trennt Inhalt, Wiederveröffentlichung, sichtbare Reichweite, erklärte Reaktionen und Folgen. Plattformzähler können unterschiedliche Bedeutungen haben und beweisen weder einzelne Leser noch die Gesamtauswirkung. Metriken werden mit Datum und Bedeutung bewahrt, sofern bekannt. Ein wirtschaftlicher Schaden wird nicht durch unbegründete Multiplikation von Impressionen berechnet.

Die Bewertung von Medienschäden kann Zeugenaussagen, Arbeitsdokumente, Verträge, Kommunikationen und weitere nicht digitale Quellen erfordern. Die technische Bewahrung belegt Inhalt und Sequenz, nicht den gesamten Schaden. Der Bericht erfindet weder Inhaber anonymer Konten noch leitet er aus dem Ton einer Veröffentlichung eine Absicht ab.

6.3 Integrierter Fall

Eine fiktive Veröffentlichung enthält eine Anschuldigung und mehrere Antworten. Verfügbare Threads, Dateien und datierte Metriken werden bewahrt. Anschließend ändert das Konto den Text und löscht eine Antwort. Die erste Version wird mit ihren Grenzen und die neue als verwandtes Objekt bewahrt. Die Analyse vergleicht die Änderungen, ohne den Verlauf zu löschen. Der Entfernungsantrag wird registriert, ohne zu behaupten, der Inhalt verbreite sich nicht mehr in anderen Konten.

> **Lehre**
> Der Nachweis von Medienschäden entsteht aus Versionen und Kontext. Ein später Screenshot kann weniger zeigen als der erste, doch auch der erste beweist nicht den gesamten Verlauf.

Anhang A. Formate der Bewahrung

A.1 E-Mail-Protokoll

Fiktives Protokoll

```
Fall / Objekt: EXP-DEMO-2026-008 / EML-001-R00
Quelle: [Postfach, Server, Client oder Dritte]
Beschaffung: [Export, Download oder Übergabe]
Scheinbarer Absender und Empfänger: [Protokoll]
Datum und Zeitzone der Nachricht: [wörtlich]
Datum und Zeitzone der Erfassung: [wörtlich]
Text und Erklärungen: [Referenz, Algorithmus und Hash]
Header: [vollständige Datei]
Anhänge: [Namen, Größen, Formate und Hashes]
Authentifizierung: [DKIM / SPF / DMARC, sofern geprüft]
Überprüfung: [Übereinstimmungen und Unterschiede]
Vorkommnisse: [Format, Fehlen, Fehler oder Beschränkung]
Verwahrung: [Original, Arbeitskopie und Zugriff]
```

A.2 Veröffentlichungsprotokoll

Feld	Mindestinhalt	Kontrolle
URL und Identifikator	Vollständige Adresse, Parameter und Umleitungen.	Auffindbares Objekt.
Konto und Sichtbarkeit	Scheinbarer Autor, Rolle, Zugriff und sichtbare Zielgruppe.	Keine automatische Zuschreibung.
Datumsangaben	Sichtbare Datumsangabe, Erfassung, Zeitzone und Genauigkeit.	Verwechseln Sie nicht Veröffentlichung und Download.
Inhalt	Text, Antworten, Reaktionen, Multimedia und Version.	Abdeckung des Threads.
Prozess	Werkzeug, Version, Filter und Aktionen.	Wiederholbarkeit.
Dateien	HTML, Bild, Video, Export und Hash.	Beziehung zwischen Original und abgeleitetem Objekt.
Vorkommnisse	Fehler, Zugriff, fehlende Inhalte und Einschränkung.	Abdeckung nicht verschweigen.

A.3 Objektmanifest

Inventar der Übergabe

```
ID / Originalname / Objekttyp
Quelle und Beziehung: [Original, Export, abgeleitetes Objekt]
Datum und Zeitzone des Empfangs
Methode und Werkzeug / Version
Größe und Format
Algorithmus und Hash des Objekts
Übergeordnetes Objekt und zugehörige Objekte
Öffnung und Überprüfung
Sensible Daten und Einschränkungen
Bewahrter Standort und Arbeitskopie
Übertragungen und Empfänger
Grenzen und offene Punkte
```

A.4 Protokoll des Entfernungsantrags

Fiktives Format

```
Plattform und Kanal: [offiziell]
URL / Veröffentlichung / Konto: [spezifisches Objekt]
Grund und beigefügte Nachweise: [Kennungen]
```

```
Antrag: [Entfernung, Überprüfung, Aufbewahrung]
Datum und Zeitzone: [Versand]
Meldenummer: [Referenz]
Antwort: [Datum, Inhalt und Aktion]
Weitere bekannte Kopien: [URL und Status]
Kommunikation mit Betroffenen: [Kanal und Version]
Offene Punkte: [Abdeckung und nächste Überprüfung]
```

Anhang B. Rechtsrahmen und Abschlussliste

Mexiko erkennt Datennachrichten in CCom 89–94 und 1205 an; CFPC/CNPCF entwickeln Zuverlässigkeit, Zuschreibung und Integrität im Rahmen der Übergangsregelung; NOM-151 regelt die Aufbewahrung in ihrem Anwendungsbereich. Peru verteilt Signatur, Verfahren und Archivierung auf verschiedene Vorschriften; Chile unterscheidet Signatur und Datum; Argentinien gewichtet die Zuverlässigkeit; Kolumbien und Ecuador verlangen die Aufbewahrung von Format, Herkunft, Bestimmung und Datumsangaben; Spanien kombiniert eIDAS, LEC und Vertrauensdienste. Keine Vorschrift macht eine Nachricht allein deshalb wahr, weil sie elektronisch ist.[6][7][8][9][10][11][12][13][14][15][16]

Die Aufbewahrung unterliegt außerdem den Grenzen des Datenschutzes und der Rechte Dritter. Rollen, Zugriff und Verbreitung werden eingeschränkt; Arbeits- und öffentliche Fassungen werden getrennt; die Veröffentlichung intimer Inhalte, Daten Minderjähriger, Geheimnisse oder Zugangsdaten wird vermieden. Das Beweismaterial wird über den autorisierten Kanal und mit einem Manifest übergeben, nicht als öffentliche Sammlung von Dateien.[17][18][19]

Abschließende Kontrolle	Abnahmefrage
Objekt	Sind EML, URL, Datei und Kontext verfügbar?
Prozess	Wurden Person, Rolle, Filter und Datum der Beschaffung registriert?
Integrität	Entspricht jeder Hash einem Objekt und einem Zeitpunkt?
Kanal	Wurden DKIM / SPF / DMARC unter Angabe ihrer Grenzen interpretiert?

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

[7] 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

[8] NOM-151-SCFI-2016, Aufbewahrung und Digitalisierung von Datennachrichten, veröffentlicht am 30-03-2017. Anforderungen an Bescheinigung, Integrität, Zugänglichkeit und elektronischen Fingerabdruck. Offizielle Online-Quelle

[9] Peru. Verordnung über die IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung und Zulassung digital signierter elektronischer Dokumente. Offizielle Online-Quelle

[10] Peru. Zivilprozessordnung, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Beweismittel, Beweislast, Beweiswürdigung und Datumsfeststellung durch technische Mittel. Offizielle Online-Quelle

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

[12] Argentinien. Zivil- und Handelsgesetzbuch, Artikel 318–319: Kommunikation auf jedem Wege und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren. Offizielle Online-Quelle

[13] 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

[14] 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

[15] 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

[16] Spanien. Gesetz über den Zivilprozess, Artikel 326 und 384: Privaturkunden, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Vervielfältigung von Daten, Prüfung, Verwahrung und vernünftige kritische Würdigung. Offizielle Online-Quelle

[17] 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

[18] Kolumbien. Statutengesetz 1581 von 2012, Artikel 4, 8, 12, 17–18 und 26: Grundsätze, Rechte, Information, Pflichten der Verantwortlichen und Auftragsverarbeiter sowie Übermittlung in Drittländer. Offizielle Online-Quelle

[19] 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

Abschließende Kontrolle	Abnahmefrage
Abdeckung	Wurden Thread, Antworten und Auslassungen dokumentiert?
Zuschreibung	Wurden Konto und Person nicht verwechselt?
Datenschutz	Vermeidet die Übergabe unnötige Offenlegung?

Abschluss

Bewahren bedeutet, eine nachprüfbare Spur dessen zu hinterlassen, was zu einem bestimmten Zeitpunkt vorhanden war. Es bedeutet nicht, Screenshots zu sammeln, bis es ausreichend erscheint.