ACCCF / BIBLIOTHEK FÜR ANGEWANDTES WISSEN

03

BAND

Eindämmung mit Augenmaß und überprüfte Wiederherstellung

Spanische Ausgabe · 2026

Handbuch zur Ransomware-Reaktion:

Eindämmung, Beweise und Geschäftskontinuität

Erste Minuten, Sicherung, Beseitigung, Wiederherstellung und Lernen

Schnelle Reaktion, ohne die Informationen zu vernichten, die das Verständnis des Vorfalls ermöglichen, Menschen zu schützen und den Betrieb mit überprüfbaren Kontrollen wieder aufzunehmen.

Für Geschäftsleitung, Sicherheits-, Technologie- und Kontinuitätsteams, Rechts- und Versicherungsabteilungen, First Responder und forensische Spezialisten. Die Anweisungen beschränken sich auf Verwaltung und defensive Sicherung; sie enthalten weder die Ausführung von Malware noch Verhandlungen mit Angreifern.

Redaktionelle Koordination: Jocsan Laguna · Consejo Americano de Ciberseguridad y Cómputo Forense

Allgemeine technische Anleitung und offenes Bildungsmaterial. Diese Unterlagen ersetzen keine Rechtsberatung oder forensische Begutachtung und enthalten keine Anleitung zum unbefugten Zugriff auf Systeme. Beispiele und Daten sind fiktiv; die 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: Die Krise beseitigt die Methode nicht 3
Kapitel 1. Die ersten fünfzehn Minuten 3
1.1 Die Akte eröffnen, bevor Dateien geöffnet werden 3
1.2 Ausschalten, vom Netz trennen oder eingeschaltet lassen 4
Kapitel 2. Umfang, Verbreitung und Prioritäten 5
2.1 Das sichtbare Gerät ist nicht der gesamte Vorfall 5
2.2 Priorität nach Dienst statt nach Lärm 6
Kapitel 3. Sicherung während der Eindämmung 6
3.1 Arbeitsspeicher, Datenträger, Protokolle und Zustand 6
3.2 Protokolle vor Kontosperrung oder Neuinstallation 6
3.3 Beweise aus Erpressernotiz und Kontaktkanal 7
Kapitel 4. Untersuchung: Herkunft, Persistenz und Exfiltration 8
4.1 Chronologie mit sichtbarer Unsicherheit 8
4.2 Hypothesen zu Einstieg und Persistenz 8
4.3 Exfiltration: Fehlen eines Beweises und Beweis des Nichtvorhandenseins 9
Kapitel 5. Eradikation und Entscheidung über das Lösegeld 9
5.1 Die Ursache beseitigen, nicht nur das Symptom 9
5.2 Zahlung oder Nichtzahlung: dokumentierte Entscheidung statt Impuls 9
5.3 Kommunikation und Verpflichtungen 10
Kapitel 6. Wiederherstellung und Kontinuität 10
6.1 Wiederherstellungspunkt auswählen und validieren 10
6.2 Schrittweise Wiederherstellung 11
6.3 Abgleich von Informationen und Lernen 11
Anhang A. Rechtsrahmen und sektorale Aufzeichnungen 12
Anhang B. Antwortformate 13
B.1 Chronologie des Vorfalls 13
B.2 Entscheidungsmatrix für die Eindämmung 14
B.3 Erfassungsprotokoll 14
B.4 Abnahmekriterien für die Wiederherstellung 14
Anhang C. Übung und Checkliste 15
C.1 Tabletop-Übung mit fiktiven Daten 15
C.2 Kurzliste vor dem Abschluss 15

Einleitung: Die Krise beseitigt die Methode nicht

Wenn Dateien nicht mehr geöffnet werden und ein Bildschirm Lösegeld fordert, besteht die erste Reaktion häufig darin, alles auszuschalten, scheinbar Infiziertes zu löschen und eine beliebige Sicherungskopie wiederherzustellen. Diese Maßnahmen können den Schaden in einem Kontext begrenzen und Beweise in einem anderen vernichten. Sie können auch eine ungeprüfte Persistenz in die Produktion zurückbringen. Es geht nicht darum, zwischen Geschwindigkeit und Beweisführung zu wählen: Erforderlich ist, das Notwendige zu bewahren und den Schaden zu begrenzen, mit einer verantwortlichen Person für jede Entscheidung.

Dieses Handbuch verfolgt von Beginn an zwei parallele Linien. Die erste schützt Menschen, Dienste und Kontinuität. Die zweite bewahrt Quellen, Entscheidungen und Beweise. Die zweite darf eine dringende Sicherheitsmaßnahme nicht verzögern, und die erste darf die Möglichkeit, den Vorfall zu verstehen, nicht unregistriert beseitigen. Bei jeder Maßnahme muss dokumentiert werden, wer sie mit welchen Informationen autorisiert hat, was sich geändert hat und welches Risiko dadurch entstanden ist.

NIST SP 800-61 Rev. 3 gliedert die Reaktion in Vorbereitung, Erkennung, Reaktion, Wiederherstellung und kontinuierliche Verbesserung. NIST SP 800-86 stellt die Beziehung zwischen Sammlung, Untersuchung, Analyse und Bericht her. Die Reaktion ist keine Liste von Schaltflächen mehr, wenn Umfang, Werkzeuge, Ergebnisse und Grenzen dokumentiert werden. Eine verschlüsselte Datei beweist Verschlüsselung; sie beweist für sich allein nicht, wann der Zugriff begann, ob eine Exfiltration stattfand oder wer sie verursacht hat.[1][2]

> **Leitregel**
> Schützen Sie zuerst Menschen. Dämmen Sie danach mit dem geringsten vertretbaren Schaden ein, sichern Sie alles, was verloren gehen könnte, und behaupten Sie nicht, das System sei wieder sauber, nur weil es eingeschaltet wurde.

Kapitel 1. Die ersten fünfzehn Minuten

1.1 Die Akte eröffnen, bevor Dateien geöffnet werden

Die erste Person, die das Problem erkennt, dokumentiert Datum, Uhrzeit und Zeitzone, was sie auf welchem Gerät gesehen hat, wer es gemeldet hat und welche Maßnahmen bereits erfolgt sind. Sie muss keine Diagnose stellen. Sie darf die Erpressernotiz nicht mit unbekannten Programmen öffnen, Anhänge ausführen oder Links folgen, um ihre Echtheit zu prüfen. Die Nachricht wird ohne Interaktion fotografiert oder registriert und das Originalobjekt nach Möglichkeit aufbewahrt.

Benennen Sie einen Vorfallkoordinator und einen Kommunikationskanal außerhalb der potenziell kompromittierten Systeme. Das Verzeichnis enthält Verantwortliche für Technik, Kontinuität, Recht, Datenschutz, Kommunikation, Versicherungen und Anbieter. Falls die Unternehmens-E-Mail betroffen sein könnte, verwenden Sie sie nicht, um Indikatoren, Anmeldedaten oder sensible Berichte zu teilen. Mündliche Entscheidungen werden mit Uhrzeit und Verantwortlichem dokumentiert.

[1] NIST SP 800-61 Rev. 3 (April 2025). In CSF 2.0 integrierte Empfehlungen für die Reaktion auf Vorfälle: Vorbereitung, Erkennung, Reaktion, Wiederherstellung und Verbesserung. Ersetzt Revision 2. Offizielle Online-Quelle

[2] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die Zulässigkeit. Offizielle Online-Quelle

Ausgangsfrage	Mindestdokumentation	Warum sie die nächste Entscheidung verändert
Sind Menschen oder kritische Dienste gefährdet?	Dienst, Abhängigkeit und unmittelbare Folge.	Bei der Eindämmung haben Leben und Sicherheit Vorrang vor Beweisen.
Was wurde genau beobachtet?	Nachricht, Erweiterung, Verhalten, Asset und Uhrzeit.	Unterscheidet einen Alarm von einer Hypothese.
Breitet sich der Vorfall weiter aus?	Geräte, Segmente, Ressourcen und beobachtete Aktivität.	Bestimmt Isolierung und Dringlichkeit.
Was kann verloren gehen?	Arbeitsspeicher, Sitzungen, Protokolle, Links und Sicherungskopien.	Priorisiert Sicherung vor Veränderungen.
Wer entscheidet und kommuniziert?	Koordinator, Befugnis, Kanal und Vertretung.	Vermeidet widersprüchliche Handlungen und Gerüchte.

1.2 Ausschalten, vom Netz trennen oder eingeschaltet lassen

Es gibt keine allgemeingültige Antwort. Ausschalten kann Prozesse stoppen und gleichzeitig Speicherinhalte, Sitzungen und Schlüssel vernichten, die für Analyse oder Wiederherstellung benötigt werden. Die Netztrennung kann Verbreitung und Exfiltration begrenzen, ohne flüchtige Daten zu vernichten, kann jedoch auch ein vom Angreifer vorgesehenes Verhalten auslösen oder einen kritischen Dienst unterbrechen. Eingeschaltet lassen ermöglicht Beobachtung und Live-Erfassung, kann aber Daten weiter verändern und den Schaden vergrößern.

Die Entscheidung beruht auf Zustand, Verbreitung, Dienst, Verschlüsselung, flüchtigen Daten, Werkzeugen und Befugnis. Besteht die Fähigkeit zur Live-Erfassung, wird sie vor dem Ausschalten bewertet. Fehlt sie, wird diese Einschränkung dokumentiert und die am wenigsten destruktive, mit der Sicherheit vereinbare Eindämmung gewählt. Ein First Responder darf keine forensische Speichererfassung improvisieren, wenn er nicht qualifiziert ist; er kann den Zustand fotografieren, nach Verfahren isolieren und den Fall weiterleiten.

> **Ausnahmeentscheidung**
> Wenn ein Leben oder ein wesentlicher Dienst vom System abhängt, darf die Beweissicherung nicht als Argument für einen Aufschub des Schutzes dienen. Dokumentiert werden die Notwendigkeit, die geprüften Alternativen und die Beweise, die vor und nach der Maßnahme gesichert werden konnten.



Abbildung 1. Eindämmen bedeutet zu entscheiden, was zuerst geschützt wird. Es gibt keine allgemeingültige Anweisung zum Ausschalten oder Trennen. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 2. Umfang, Verbreitung und Prioritäten

2.1 Das sichtbare Gerät ist nicht der gesamte Vorfall

Ein Endgerät mit verschlüsselten Dateien kann das letzte Glied einer Kette sein, die Wochen zuvor in einem anderen Konto begann. Die Übersicht umfasst Identitäten, VPN, E-Mail, Server, Hypervisoren, Kopien, Anbieter, für die Arbeit autorisierte persönliche Geräte, Verwaltungssysteme und Cloud-Dienste. Die Erweiterung erfolgt anhand von Beweisen und nicht mit der Aussage „alles ist kompromittiert“, die zu unnötigen Abschaltungen führen und Prioritäten verdecken kann.

Erstellen Sie eine Asset-Matrix mit Kritikalität, Eigentümer, Zustand, möglichem Kompromiss, Abhängigkeit, Protokollquelle und Entscheidung. Ein Gerät kann infiziert sein, ein anderes lediglich unerreichbar, weil ein Switch isoliert wurde, und ein drittes gesund, aber von einem gestoppten Server abhängig. Der Bericht unterscheidet diese Zustände, statt sie als eine einzige bestätigte Infektion darzustellen.

Zustand	Erforderliche Beweise	Dokumentierte Entscheidung
Bestätigt	Artefakt, Ausführung, Protokoll oder nachweisbare Verschlüsselung auf dem Asset.	Nach Priorität eindämmen und sichern.
Verdächtig	Verwandter Indikator ohne ausreichende Bestätigung.	Überwachen, selektiv isolieren oder erfassen.
Durch Abhängigkeit betroffen	Dienst, der durch eine andere Maßnahme oder ein anderes System gestoppt wurde.	Abhängigkeit wiederherstellen, ohne sie als Infektion zu bezeichnen.
Keine Hinweise im untersuchten Umfang	Abfrage, Filter, Zeitraum und geprüfte Quellen.	Nicht außerhalb dieser Abdeckung für sauber erklären.
Unbekannt	Fehlender Zugriff, Protokolle oder Inventar.	Verantwortlichen und Grenze der Schlussfolgerung zuweisen.

2.2 Priorität nach Dienst statt nach Lärm

Die Kontinuitätsmatrix bestimmt wesentliche Prozesse, die maximal tolerierbare Unterbrechungsdauer, die für den Betrieb mindestens erforderlichen Daten, Abhängigkeiten, Verantwortliche und vorübergehende manuelle Wege. Ein Server mit vielen Warnmeldungen kann weniger prioritär sein als ein Verzeichnis, von dem alle abhängen. Die Reihenfolge der Wiederherstellung richtet sich nach den tatsächlichen Auswirkungen, nicht danach, welche Datei zuerst in der Notiz erschien.

Reaktions- und Kontinuitätsteams arbeiten mit derselben Chronologie, aber mit unterschiedlichen Ergebnissen. Die Sicherheit muss wissen, welche Persistenz besteht; die Kontinuität muss wissen, welche Version wiederhergestellt werden kann und welche Abhängigkeiten bestehen. Der Abgleich verhindert, dass ein System wiederhergestellt wird, das erneut mit der Ursache des Vorfalls verbunden wird, oder dass ein gesunder Dienst aus Unkenntnis abgeschaltet bleibt.

> **Fiktiver Fall**
> Ein Unternehmen entdeckt Verschlüsselung auf dem Dokumentenserver. Die Gehaltsabrechnung ist nicht verschlüsselt, funktioniert jedoch nicht, weil sie von demselben Verzeichnis abhängt. Das Team kennzeichnet die Gehaltsabrechnung nicht als infiziert: Es dokumentiert eine Beeinträchtigung durch Abhängigkeit. Die Wiederherstellung priorisiert Identität und Protokolle, bevor die Dienste wieder verbunden werden.

Kapitel 3. Sicherung während der Eindämmung

3.1 Arbeitsspeicher, Datenträger, Protokolle und Zustand

Die Sicherung wird nach Volatilität und der Fähigkeit zur Beantwortung von Fragen priorisiert. Der Arbeitsspeicher kann Prozesse, Verbindungen, Schlüssel oder Sitzungsfragmente enthalten; der Datenträger bewahrt Dateien und Artefakte; Protokolle erklären Ereignisse; die Konfiguration zeigt die Verbindungen des Systems. Nicht jeder Fall erfordert eine vollständige Erfassung jedes Assets. Ausgewählt wird, was Herkunft, Verbreitung, Persistenz, Exfiltration und Wiederherstellung unterscheiden kann.

Jede Erfassung dokumentiert Quelle, Methode, Werkzeug und Version, Datum und Zeitzone, Befugnis, Abdeckung, Ausgabe, Fehler und Überprüfung. Die Ausgabe wird geöffnet, bevor sie als gültig gilt. Eine Datei, die vorhanden, aber nicht lesbar ist, ist kein brauchbarer Beweis. Vorkommnisse werden in der Akte aufbewahrt, einschließlich unvollständiger Erfassung oder inkompatibler Werkzeuge. Eine Wiederholung erzeugt ein weiteres verknüpftes Objekt und löscht den ersten Versuch nicht.[3][4]

3.2 Protokolle vor Kontosperrung oder Neuinstallation

Vor der Deaktivierung eines Kontos werden Anmeldeprotokolle, Faktorregistrierungen, Wiederherstellungsänderungen, E-Mail-Regeln, Delegierungen, Token und verfügbare administrative Aktivitäten exportiert. Vor einer Neuinstallation werden Image, Konfiguration, Protokolle, Aufgaben und einschlägige Artefakte gesichert. Sind diese Maßnahmen in einer Notlage unmöglich, werden Verlust und Grund dokumentiert, statt eine ideale Abfolge zu erfinden.

Die Aufbewahrung kann während der Diskussion des Umfangs rotieren. Der Anbieter wird um Sicherung mit Zeitraum, Konten, Feldern, Zeitzone, nativem Format, Feldverzeichnis, Filtern und Einschränkungen

[3] ISO/IEC 27037:2012. Leitlinien für Identifizierung, Sammlung, Erfassung und Erhaltung digitaler Beweise. Die Ausgabe wurde von ISO als gültig bestätigt. Offizielle Online-Quelle

[4] NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Methodischer Leitfaden, weder Rechtsvorschrift noch Garantie für die Zulässigkeit. Offizielle Online-Quelle

ersucht. Die Übermittlung wird mit vollständiger EML-Datei, Nachrichtentext, Kopfzeilen und Anhängen aufbewahrt. Gibt der Anbieter einen Hashwert für jede Datei an, wird dieser lokal überprüft und jede Abweichung dokumentiert, ohne die Quelle zu verändern.[5]

3.3 Beweise aus Erpressernotiz und Kontaktkanal

Die Erpressernotiz wird als Objekt aufbewahrt: Bildschirmfoto, gegebenenfalls Originaldatei, Standort, Name, Beobachtungsdatum, Format und Beziehung zum Gerät. Der Text kann falsche Behauptungen über Exfiltration, Überwachung oder Zugriffszeit enthalten. Er wird als Erklärung des Angreifers behandelt, nicht als erwiesene Tatsache. Zahlungs- und Kontaktkennungen werden dokumentiert, ohne Transaktionen durchzuführen oder Anweisungen zu folgen.

Objekt	Erforderliche Dokumentation	Vermiedener Fehler
Erpressernotiz	Originalobjekt, Standort, Datum, Beziehung und wörtlicher Inhalt.	Ihren Text als technisches Geständnis behandeln.
Verschlüsselte Datei	Kontrollierte Probe, Name, Größe, vorheriger Zustand und aufbewahrte Kopie.	Viele Dateien öffnen und die Beweislage verändern.
Vorfallsbezogene E-Mail	EML-Datei, Anhänge, Kopfzeilen, Datum und Empfänger.	Nur ein Bildschirmfoto der Nachricht aufbewahren.
Supportkonto	Rolle, Berechtigungen, Aktivität und Export.	Zugriff teilen oder den Vorfall erweitern.
Sicherungskopie	Datum, Version, Abdeckung, Standort und Zugriffsstatus.	Ohne Bewertung der Kontamination verbinden.

Laborsicherheit

Die Proben werden nicht auf persönlichen Geräten oder in Produktionsnetzen ausgeführt. Die dynamische Analyse erfordert eine isolierte Umgebung, ein definiertes Ziel, Autorisierung, Netzwerkkontrolle und Dokumentation. Für die erste Reaktion genügt es häufig, zu sichern und weiterzuleiten.

[5] RFC Editor. RFC 5322, Internet Message Format: Aufbau der Nachricht, Kopfzeilen und Nachrichtentext. Technische Referenz zur Aufbewahrung und zum Verständnis von E-Mails, kein automatischer Beweis der Identität einer natürlichen Person. Offizielle Online-Quelle

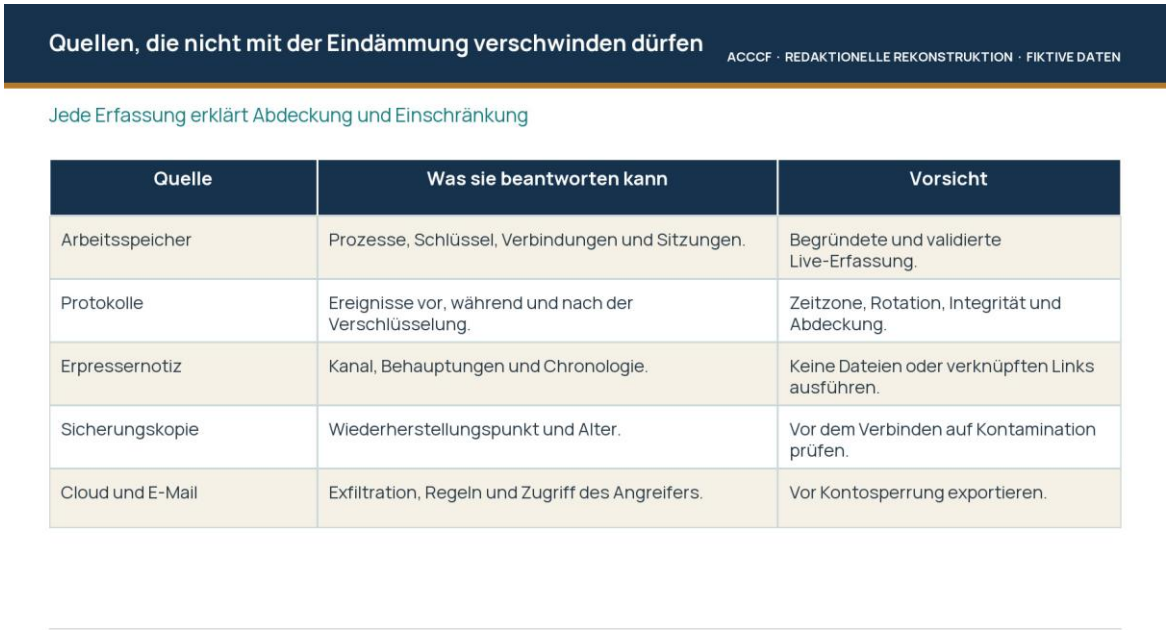


Abbildung 2. Quellen, die nicht mit der Eindämmung verschwinden dürfen. Jede Erfassung erklärt Abdeckung und Einschränkung. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Kapitel 4. Untersuchung: Herkunft, Persistenz und Exfiltration

4.1 Chronologie mit sichtbarer Unsicherheit

Die Chronologie bewahrt jeden wörtlichen Datumswert, Zeitzone, Quelle, Genauigkeit und Umrechnung. Ein UTC-Protokoll, eine falsch gehende Computeruhr und eine lokale E-Mail werden nicht ohne Erklärung der Umrechnung so geordnet, als verwendeten sie dieselbe Uhr. Die erste Erkennung ist nicht notwendigerweise der erste Zugriff. Das Änderungsdatum einer Datei beweist nicht, wann der Verschlüsseler ausgeführt wurde; es kann den Zeitpunkt der Erstellung des Ergebnisses anzeigen.

Beobachtete, von einer Person angegebene, berechnete und abgeleitete Ereignisse werden getrennt. Eine Ableitung wird nicht als Protokoll dargestellt. Fehlt eine Quelle für eine Etappe, wird „im untersuchten Umfang nicht belegt“ geschrieben. Das Fehlen von Aufzeichnungen kann auf Rotation, Konfiguration, Filter oder Löschung beruhen und beweist nicht, dass das Ereignis nicht stattgefunden hat.

4.2 Hypothesen zu Einstieg und Persistenz

Mögliche Hypothesen sind gestohlene Anmeldedaten, eine exponierte Schwachstelle, eine schädliche E-Mail, ein Anbieter, ein externes Gerät oder eine Kombination. Die Analyse vergleicht jede Hypothese mit Quellen, die sie schwächen könnten: Authentifizierung, Faktoränderungen, Regeln, Prozesse, Aufgaben, Dienste, neue Konten, Verbindungen und Verwaltungsaktivitäten. Gewählt wird die Erklärung, die mit den meisten Tatsachen und den wenigsten Widersprüchen vereinbar ist, nicht die spektakulärste.

Hypothese	Quelle, die bestätigt oder schwächt	Einschränkung der Schlussfolgerung
Kompromittiertes legitimes Konto	Anomale Sitzungen, Faktor, Gerät, Wiederherstellung und ungefähre Geografie.	Die Verwendung des Kontos identifiziert keine Person.
Öffentliche Schwachstelle	Version, Exposition, Protokolle, kontrollierte Prüfung und Patchdatum.	Das Vorhandensein einer Schwachstelle beweist keine Ausnutzung.

Hypothese	Quelle, die bestätigt oder schwächt	Einschränkung der Schlussfolgerung
Schädliche E-Mail	EML-Datei, Anhänge und Telemetrie zu Öffnen und Ausführen.	Der Empfang beweist keine Ausführung.
Kompromittierter Anbieter	Fernzugriff, Rollen, Änderungen und zeitliche Korrelation.	Das Vertragsverhältnis beweist nicht den Angriffsvektor.
Persistenz	Konten, Aufgaben, Dienste, Schlüssel, Regeln und Artefakte.	Nicht nur die sichtbare Datei beseitigen.

4.3 Exfiltration: Fehlen eines Beweises und Beweis des Nichtvorhandenseins

Zur Bewertung der Exfiltration werden Verbindungen, Ziele, Volumen, Komprimierung, Cloud-Synchronisation, E-Mail, Regeln, Übertragungsdienste, Proxy-Protokolle und, sofern verfügbar, DNS geprüft; die Erklärungen des Angreifers werden als separate Hypothese behandelt. Ein hohes Volumen kann eine Sicherungskopie oder legitime Aktivität sein; fehlender Verkehr kann auf fehlende Protokolle, ungeprüfte Verschlüsselung oder einen nicht erfassten Kanal hindeuten.

Die Schlussfolgerung unterscheidet zwischen Übermittlungsnachweis, vereinbaren Hinweisen, unzureichenden Daten und beobachteter Abwesenheit innerhalb einer definierten Abdeckung. Es wird nicht allein deshalb „keine Exfiltration“ behauptet, weil die Firewall keine zeigt. Auch „wir veröffentlichen Ihre Daten“ ist kein Beweis dafür, dass Daten abgeflossen sind. Wird eine veröffentlichte Probe gefunden, wird sie dokumentiert, ohne sie zu verbreiten oder unnötige Informationen herunterzuladen.

> **Vertretbare Formulierung**
> „In den Proxy-Protokollen zwischen diesen Daten und mit diesen Feldern wurden keine mit dem Vorfall verbundenen Übertragungen festgestellt. Die Abdeckung umfasst keine ungeprüften verschlüsselten Kanäle, andere Anbieter oder frühere Zeiträume; daher kann ein vollständiges Fehlen von Exfiltration nicht behauptet werden.“

Kapitel 5. Eradikation und Entscheidung über das Lösegeld

5.1 Die Ursache beseitigen, nicht nur das Symptom

Die Eradikation umfasst Konten, Wiederherstellungsmethoden, Regeln, Fernzugriffe, Persistenz, Schwachstellen, Geheimnisse und Anbieterwege. Ein Passwortwechsel genügt nicht, solange Token, Sitzungen oder Schlüssel verbleiben. Das Entfernen des Verschlüsselers beseitigt nicht den Einstiegspunkt. Die Maßnahmen werden mit Quellen und Tests überprüft und ihre Auswirkungen auf den Betrieb dokumentiert.

Ist die Ursache unbekannt, wird dies erklärt. Die Organisation kann eine Rekonstruktion aus einer vertrauenswürdigen Umgebung wählen, statt auf demselben System zu „bereinigen“. Die Entscheidung beruht auf Risiko und Beweisen, nicht auf dem Anschein von Einsparungen. Ein neu installiertes System erhält neue Konfiguration, Anmeldedaten und Überwachung; es wird nicht in den Zustand zurückversetzt, der den Vorfall ermöglichte.

5.2 Zahlung oder Nichtzahlung: dokumentierte Entscheidung statt Impuls

Die Zahlungsentscheidung liegt bei der Organisation und ihren Rechtsberatern, Versicherern und zuständigen Behörden. Zu berücksichtigen sind Rechtmäßigkeit, Sanktionen, Herkunft und Ziel der Gelder, Kontinuitätsfähigkeit, Schutz von Personen, Möglichkeit weiterer Erpressungen und das Fehlen einer Wiederherstellungsgarantie. Dieses Handbuch empfiehlt weder Zahlung noch Kontakt mit dem

Angreifer; es bietet eine Struktur, damit die Entscheidung unter Druck nicht von einer einzigen Person abhängt.

Faktor	Zu beantwortende Frage	Beweise für die Entscheidung
Rechtmäßigkeit	Besteht ein anwendbares Verbot, eine Sanktion oder eine Beschränkung?	Aktualisierte Rechtsanalyse und Genehmigungsweg.
Kontinuität	Gibt es einen anderen praktikablen Weg und wie lange dauert er?	Tests von Sicherungskopien, Alternativen und Kosten der Unterbrechung.
Wiederherstellung	Was wird versprochen und was kann nachgewiesen werden?	Keine verbalen Garantien; technische Bewertung und Einschränkungen.
Menschliches Risiko	Bestehen weitere Bedrohungen oder sensible Daten?	Sicherheit und Schutz der Betroffenen priorisieren.
Wiederholung	Welcher Anreiz oder welche Exposition bleibt?	Dokumentiertes Risiko und späterer Plan.
Befugnis	Wer kann entscheiden und kommunizieren?	Quorum, Dokumentation und einziger autorisierter Kanal.

5.3 Kommunikation und Verpflichtungen

Bei der Bewertung der Meldung wird zwischen Kunden, betroffenen Personen, Regulierungsbehörden, Versicherern, Partnern und Behörden unterschieden. Jede Gerichtsbarkeit und jeder Vertrag hat eigene Schwellenwerte und Fristen. Die technischen Informationen werden so vorbereitet, dass Tatsachen, Unsicherheit und Maßnahmen erläutert werden, ohne Details offenzulegen, die den Schaden vergrößern. Die öffentliche Kommunikation erfolgt nicht vor der Sicherung und verwandelt einen Verdacht nicht in eine Ursachenmeldung.

In Mexiko haben Kreditinstitute besondere Pflichten zur Untersuchung und Meldung von Vorfällen, zur Aufzeichnung und Aufbewahrung innerhalb der geltenden Bestimmungen; in Peru verlangt die SBS von beaufsichtigten Stellen Sicherung und forensische Analyse; in Argentinien behandelt die Comunicación A 8280 Reaktion und Abschlussbericht in ihrem Regime. Diese Fristen werden nicht auf jede Organisation oder jedes Land übertragen.[6][7][8]

> **Keine Gewissheit erzeugen**
> Die Managementdarstellung kann erklären, was bekannt ist, was getan wird und was noch zu bestimmen ist. Sie muss nicht zwischen Panik und künstlicher Ruhe wählen. Sie benötigt eine belastbare Chronologie und klare Verantwortlichkeiten.

Kapitel 6. Wiederherstellung und Kontinuität

6.1 Wiederherstellungspunkt auswählen und validieren

Die neueste Sicherungskopie kann Persistenz oder beschädigte Dateien enthalten; die älteste kann legitime Vorgänge verlieren. Datum, Abdeckung, Integrität, Zugriff, Verlauf und Kompatibilität werden verglichen. Die Originalsicherung wird aufbewahrt und in einer isolierten Umgebung mit einer

[6] Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 bis 17: Nachweise, Verschlüsselung, Zugriff, Vorfälle, Vorkommnisse, Protokolle und Überprüfungen. Offizielle Online-Quelle

[7] Peru. SBS 504-2021, Artikel 12.6.g, 15 und 17.3–17.4: Aufbewahrung, Berichterstattung und forensische Analyse, Aufzeichnungen von Registrierung, Authentifizierung und Vorgängen. Offizielle Online-Quelle

[8] Argentinien. BCRA Comunicación A 8280: Reaktion und Wiederherstellung nach Cyber-Vorfällen; Abschlussbericht innerhalb von fünf aufeinanderfolgenden Tagen nach Eindämmung, Wiederherstellung und Lösung. Offizielle Online-Quelle

kontrollierten Kopie gearbeitet. Schlüssel werden über einen separaten Kanal übermittelt und nicht im Protokoll aufgeführt.

Die Validierung umfasst, dass die Kopie geöffnet werden kann, die erwarteten Objekte enthält, eingebunden werden kann, kohärente Versionen aufweist und keine bekannten Kompromissindikatoren zeigt. Dies beweist nicht, dass sie vollständig sauber ist, sondern dass sie die festgelegten Prüfungen bestanden hat. Fehler der Kopie werden hinsichtlich ihrer Auswirkung auf das Ziel bewertet und im Detail aufbewahrt.

6.2 Schrittweise Wiederherstellung

Begonnen wird mit minimalen Diensten in einer isolierten Umgebung und mit fiktiven Daten oder Testkonten. Anschließend werden Identität, Berechtigungen, Anwendungen, Integration, Lese- und Schreibzugriff, Export und Überwachung getestet. Erst danach wird eine schrittweise Erweiterung autorisiert. Das Produktionsnetzwerk dient nicht als Labor für die erste Wiederherstellung.

Stufe	Abnahmekriterium	Nachweis
Mindestinfrastruktur	Überprüfte Komponenten und Versionen ohne bekannte Persistenz.	Inventar und Konfiguration.
Daten	Lesbare Dateien, korrekte Abdeckung und Beziehung.	Stichprobe, Manifest und Anzahl.
Anwendung	Funktionen und Berechtigungen funktionieren mit fiktiven Konten.	Testfälle und Ergebnisse.
Integration	Autorisierte Abhängigkeiten funktionieren ohne unvorhergesehene Wege.	Protokolle und Verbindungen.
Beobachtung	Im festgelegten Zeitraum tritt keine anomale Aktivität auf.	Warnmeldungen, Abfragen und Einschränkungen.
Ausstieg	Verantwortlicher akzeptiert Restrisiko und nächste Überprüfung.	Ausstiegsprotokoll und Überwachung.

6.3 Abgleich von Informationen und Lernen

Es kann erforderlich sein, Vorgänge zu rekonstruieren, die zwischen der letzten fehlerfreien Sicherung und der Erkennung entstanden sind. Externe Aufzeichnungen, Belege, E-Mails, Nachrichten und Dokumente Dritter werden abgeglichen, ohne die Quelle zu verändern. Abweichungen werden notiert und nicht mit Schätzungen aufgefüllt, die als echte Daten ausgegeben werden.

Die gelernte Lektion verändert das Verfahren: neue Aufbewahrungsregeln, phishingresistente Authentifizierung, Segmentierung, unveränderliche Kopien, Wiederherstellungstests, Verzeichnisse, Beschränkung von Berechtigungen oder Übungen. Endet der Vorfall mit einer Präsentation, ohne dass sich ein Verhalten ändert, wird die nächste Krise dieselbe Abfolge wiederholen.

> **Abnahmekriterium**
> Wiederherstellung bedeutet, den Betrieb mit dem Nachweis fortzusetzen, dass die Kontrollen funktionieren, und mit einer ehrlichen Erklärung dessen, was weiterhin unbekannt ist. Der Abschluss umfasst Personen, Systeme, Daten, Anbieter und eine spätere Überprüfung.



Abbildung 3. Wiederherstellen bedeutet nicht, Vertrauen zurückzugewinnen. Die Ausgabe wird schrittweise und mit Abnahmekriterien geprüft. Redaktionelle Rekonstruktion; stellt keinen tatsächlichen Beweis dar.

Anhang A. Rechtsrahmen und sektorale Aufzeichnungen

Der Vorfall kann elektronische Beweise, Datenschutz, Verträge, finanzielle Verpflichtungen und Kontinuitätsregeln betreffen. Diese Funktionen werden getrennt analysiert. Eine sektorale Vorschrift begründet keine allgemeine Verpflichtung, und eine Aufbewahrungsfrist erlaubt keine unbegrenzte Aufbewahrung aller Daten. Stand der Dokumentenprüfung: 10. November 2026; ein realer Fall erfordert die Prüfung von Gültigkeit, Normadressat, Thema und Kanal.

Jurisdiktion	Funktionale Quellen	Nutzungseinschränkung
Mexiko	CCom 89–94 und 1205; CFPC 210-A / CNPCF 348–350 je nach Übergang; CNBV 316 Bis Serie für erfasste Stellen; LFPDPPP für personenbezogene Daten.	Elektronisches Dokument, Verfahren, Bankwesen und Datenschutz trennen. Die Erklärung des CNPCF prüfen.
Peru	IOFE-Verordnung; CPC 188–197; SBS 504-2021 und 2286-2024 für beaufsichtigte Stellen.	Der Ley 27269 kein vollständiges Dokumentenregime zuschreiben und keine CNBV-Fristen kopieren.
Chile	Ley 19.799; RAN 20-7, 20-8, 20-10 je nach Stelle und Dienst.	Kontinuität, Auslagerung und Vorfälle nicht verwechseln.
Argentinien	Ley 25.506; CCyC 318–319; BCRA A 7783 und A 8280.	Eigene Fristen und Normadressaten; Authentifizierung ist nicht gleich Autorisierung.
Kolumbien	Ley 527; CPACA für Verwaltungshandlungen; SFC-Vorschriften mit der konkreten Nummer bestätigen.	Keine Anforderungen an Vorfälle aus einem ungelesenen Rundschreiben erfinden.
Ecuador	Ley 67; LOPDP; Regime des Zahlungssystems, soweit zutreffend.	Meldung und Aufbewahrung hängen von Verarbeitung und Sektor ab.
Spanien / EU	eIDAS; LEC 326 und 384; DSGVO; RD-ley 19/2018 für Zahlungsdienste.	Dokument, Verfahren, Datenschutz und nicht autorisierte Vorgänge unterscheiden.

Quellen der Tabelle:[9][10][11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27]

Bei einer Anforderung von Aufzeichnungen werden Funktion, Zeitraum, Referenz, Felder, Format, Zeitzone und Übermittlungsmethode angegeben. Ziel ist nicht, alle Server anzufordern, sondern Ereignisse, die konkrete Fragen beantworten können. Die Beweismittelkette dokumentiert, wer übergibt, wer empfängt, welches Objekt enthalten ist, wie überprüft wird und welche Einschränkungen bestehen.

Anhang B. Antwortformate

B.1 Chronologie des Vorfalls

Feld	Erforderlicher Eintrag	Kontrolle
Ereignis	Beobachtet, angegeben, berechnet oder abgeleitet.	Kategorien nicht vermischen.
Wörtliches Datum und Zeitzone	Originaltext, Umrechnung und Genauigkeit.	Quelle nicht überschreiben.
Asset und Quelle	Objekt, System, Kennung und Standort.	Nachverfolgbarkeit bis zum Manifest.
Maßnahme und Verantwortlicher	Was geschah, wer entschied und wer führte aus.	Befugnis und Beweise.

[9]Código de Comercio de México, Artikel 89–94 und 1205: Neutralität, Zurechnung, Schriftform, Original, Integrität, Zugänglichkeit und Zulassung von Datennachrichten. Amtliche Zusammenstellung. Offizielle Online-Quelle

[10]Código Federal de Procedimientos Civiles, Artikel 210-A: Zuverlässigkeit der Methode, Zurechnung, Zugänglichkeit und Integrität elektronischer Informationen. Der Code wurde durch Dekret vom 07-06-2023 aufgehoben und unterliegt einem schrittweisen Übergangsregime. Offizielle Online-Quelle

[11]Código Nacional de Procedimientos Civiles y Familiares, Artikel 348–350. Zusammenstellung mit Reform vom 15-01-2026. Die Anwendung erfolgt schrittweise und hängt von Erklärungen ab. Offizielle Online-Quelle

[12]Disposiciones de carácter general aplicables a las instituciones de crédito, Artikel 316 Bis, 316 Bis 1, 316 Bis 10 bis 17: Nachweise, Verschlüsselung, Zugriff, Vorfälle, Vorkommnisse, Protokolle und Überprüfungen. Offizielle Online-Quelle

[13]Peru. Reglamento de la IOFE, DS 052-2008-PCM, Artikel 3 und 4: Anforderung an und Zulassung von digital signierten elektronischen Dokumenten. Offizielle Online-Quelle

[14]Peru. Código Procesal Civil, Artikel 188–197 und 245.5: Zweck, Rechtmäßigkeit, Mittel, Beweislast, Bewertung und Datumsbestimmung durch technische Mittel. Offizielle Online-Quelle

[15]Peru. SBS 504-2021, Artikel 12.6.g, 15 und 17.3–17.4: Aufbewahrung, Berichterstattung und forensische Analyse, Aufzeichnungen von Registrierung, Authentifizierung und Vorgängen. Offizielle Online-Quelle

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

[17]Chile. Recopilación Actualizada de Normas, Kapitel 20-7, 20-8 und 20-10: Auslagerung, operative Vorfälle, Informationssicherheit und Cybersicherheit. Offizielle Online-Quelle

[18]Argentinien. Ley 25.506 de Firma Digital, Artikel 1 und 5–9: digitales Dokument, Beweislast bei Berufung auf eine bestrittene elektronische Signatur und begrenzte Vermutungen. Offizielle Online-Quelle

[19]Argentinien. Código Civil y Comercial, Artikel 318–319: Korrespondenz unabhängig vom Medium und Bewertung der Zuverlässigkeit von Trägern und technischen Verfahren. Offizielle Online-Quelle

[20]Argentinien. BCRA Comunicación A 8280: Reaktion und Wiederherstellung nach Cyber-Vorfällen; Abschlussbericht innerhalb von fünf aufeinanderfolgenden Tagen nach Eindämmung, Wiederherstellung und Lösung. Offizielle Online-Quelle

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

[22]Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, Artikel 2, 6–8, 10–16: Gleichwertigkeit, Schriftform, Original, Aufbewahrung, Herkunft, Versand, Empfang und elektronische Signatur. Offizielle Online-Quelle

[23]Ecuador. Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459 de 26-05-2021. Artikel 10, 37–44: Grundsätze, Sicherheitsmaßnahmen, Datenschutz durch Technikgestaltung, Risiken und Verarbeitung bei Vorfällen. Offizielle Online-Quelle

[24]Reglamento (UE) 910/2014 eIDAS, Artikel 25–26 und 46: keine Diskriminierung elektronischer Signaturen und Dokumente aufgrund ihres Formats, fortgeschrittene elektronische Signatur und Rechtswirkungen qualifizierter elektronischer Signaturen. Offizielle Online-Quelle

[25]Spanien. Ley de Enjuiciamiento Civil, Artikel 326 und 384: private Dokumente, Anfechtung, Instrumente zur Archivierung, Kenntnisnahme oder Wiedergabe von Daten, Prüfung, Verwahrung und gesunde Kritik. Offizielle Online-Quelle

[26]Europäische Union. Reglamento (UE) 2016/679, Artikel 5, 25, 28 und 32–34: Grundsätze, Datenschutz durch Technikgestaltung, Auftragsverarbeiter, Sicherheit sowie Meldung/Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten. Für Spanien sind außerdem die einschlägigen nationalen und sektoralen Rechtsvorschriften zu prüfen. Offizielle Online-Quelle

[27]Spanien. Real Decreto-ley 19/2018, Artikel 45, 66 und 67: Rückerstattung für nicht autorisierte Vorgänge, Risikomanagement und unverzügliche Meldung schwerer Vorfälle. Offizielle Online-Quelle

Feld	Erforderlicher Eintrag	Kontrolle
Ergebnis	Ausgabe, Fehler und Zustandsänderungen.	Vorkommnisse nicht verbergen.
Nächste Überprüfung	Offene Frage und Verantwortlicher.	Vorzeitigen Abschluss vermeiden.

B.2 Entscheidungsmatrix für die Eindämmung

Fiktive Entscheidungsvorlage

```
Vorfall: DEMO-RANSOM-2026-001
Asset und Dienst: [Kennung, Funktion, Abhängigkeiten]
Beobachteter Zustand: [Bildschirm, Prozesse, Netzwerk, Verschlüsselung]
Bewertete Optionen: [ausschalten, Netz isolieren, eingeschaltet lassen, Konto sperren]
Risiko für Personen und Kontinuität: [Priorität]
Volatilität und gefährdete Beweise: [Arbeitsspeicher, Protokolle, Sitzungen]
Entscheidung und Befugnis: [Maßnahme, Person, Datum und Zeitzone]
Vorherige Sicherung: [Objekt, Methode und Ausgabe]
Vorgenommene Änderung: [Endzustand und Nebenwirkung]
Offen: [was nicht aufbewahrt oder bestätigt werden konnte]
Überprüfung: [Verantwortlicher und nächster Bewertungszeitpunkt]
```

B.3 Erfassungsprotokoll

Technisches Manifest

```
Quellen-ID / Erfassung: DEMO-SRV-001 / A01
Befugnis und Umfang: [Dokument und Ausschlüsse]
Ausgangszustand: [Fotografien und Beobachtung]
Ziel und Abdeckung: [Arbeitsspeicher, Image, Logik, Export]
Werkzeug und Validierung: [Version, Umgebung und Test]
Beginn / Ende mit Zeitzone: [wörtliche Werte]
Ausgabe: [Dateien, Format und Größe]
Integrität: [Algorithmus und genaues Objekt]
Vorkommnisse: [Fehler und fehlende Abdeckung]
Überprüfung: [Öffnen, Beziehung und Revision]
Verwahrung: [Aufbewahrung, Zugriff und Übertragungen]
```

B.4 Abnahmekriterien für die Wiederherstellung

Überprüfung	Ja / Nein / nicht zutreffend	Nachweis und Beobachtung
Sicherungskopie vor Verwendung aufbewahrt	[ ]	Kennung und Verwahrung.
Lesbare Daten und kohärente Abdeckung	[ ]	Stichprobe und Anzahl.
Rekonstruierte Konten und Faktoren	[ ]	Keine alten Sitzungen.
Bewertete Persistenz	[ ]	Quellen und Einschränkungen.
Geprüfte Funktionen und Integrationen	[ ]	Fiktive Fälle.
Zugewiesene Überwachung und Verantwortlicher	[ ]	Warnmeldungen und Überprüfung.
Durchgeführte Mitteilungen	[ ]	Versionen und Empfänger.
Akzeptiertes Restrisiko	[ ]	Unterschrift und Datum des Verantwortlichen.

Anhang C. Übung und Checkliste

C.1 Tabletop-Übung mit fiktiven Daten

Simuliert wird ein Unternehmen mit drei Servern, zwei Verwaltungskonten, nächtlicher Sicherung und einem E-Mail-Anbieter. Um 08:12 wird Verschlüsselung in Dokumenten gemeldet; um 08:16 zeigt ein anderes Gerät dieselbe Erweiterung; um 08:20 wird eine Weiterleitungsregel in einem Konto entdeckt. Das Team muss Isolierung, erste Erfassungen, Anbieterkontakt, Datenbewertung und Wiederherstellungsweg entscheiden, ohne eine Datei auszuführen.

Die Bewertung beruht auf der Qualität der Entscheidungen und Aufzeichnungen: Stellt das Team die Weiterleitung nicht auf, geht die Möglichkeit ihrer Erklärung verloren; wird das Konto vor dem Export gesperrt, wird die Einschränkung dokumentiert; bleibt ein kritischer Dienst ohne Alternative, muss dies begründet werden. Abschließend werden die Entscheidungen bewertet, nicht die schnellste Handlung.

C.2 Kurzliste vor dem Abschluss

Frage	Erwartetes Ergebnis
Sind die Personen geschützt?	Prioritäten und wesentliche Dienste berücksichtigt.
Wurden vorrangige flüchtige Beweise aufbewahrt?	Objekte, Methoden und Einschränkungen dokumentiert.
Wurden Herkunft, Persistenz und Exfiltration bewertet?	Hypothesen und Quellen ohne absolute Aussagen.
Wurden Lösegeld- und Kommunikationsentscheidungen autorisiert?	Quorum, Begründung und Versionen.
Wurde die Wiederherstellung getestet?	Daten, Funktionen, Zugriffe und Beobachtung.
Was hat sich für das nächste Mal geändert?	Tatsächliche Kontrolle, Verantwortlicher und Validierung.

Abschluss

Ruhe bedeutet nicht zu behaupten, alles sei in Ordnung. Sie bedeutet zu wissen, was mit welchen Beweisen getan wird, wer entscheidet und was noch zu überprüfen ist.