

MASSNAHMEN · HANDLUNGSEMPFEHLUNGEN

Maßnahmenkatalog & Handlungsempfehlungen

Beobachtete technische Befunde werden in eine priorisierte, nachvollziehbare Arbeitsfolge übersetzt: erst sichern, dann umsetzen, anschließend im Originalsystem erneut verifizieren.

FALL

PA-DEMO-20261011-HELMSTEDT-001

ZIEL

www.demo-report.de

SCANZEIT

2026-10-24T20:04:38+00:00

PROFIL

Technischer Bericht

Abgeleitet aus den im Prüfbericht dokumentierten Signalen. Evidence-Referenzen, Quellen und technische Grenzen bleiben im Hauptbericht und im übrigen Beweispaket maßgeblich. Keine Rechtsberatung.

Befunde verstehen. Maßnahmen priorisieren.

Wofür dieser Katalog dient: Der Katalog bündelt die automatisch aus den technischen Befunden abgeleiteten Handlungsempfehlungen. Jede Empfehlung beschreibt den Auslöser, die sofortige Begrenzung, die dauerhafte Umsetzung, eine zuständige Rolle und den Nachtest.

Die Reihenfolge ist technisch priorisiert. Sie bestätigt weder einen Rechtsverstoß noch eine bestimmte Rechtsfolge. Zweck, Rechtsgrundlage, Erforderlichkeit und tatsächliche Verarbeitung sind durch Betreiber, DSB oder Fachpartner manuell zu bewerten.

3

Maßnahmen

1

Hohe Priorität

2

Erhöhte Priorität

0

Hinweise

Prioritätssicht: Hoch: 1 · Erhöht: 2 · Hinweis: 0 · **Version:** 8.5-demo · Export 8.5-demo

01 HOCH

UMSETZUNG

Clientseitig erreichbare Zugangsdaten sofort rotieren

BEFUND / AUSLÖSER

Passwort im Local Storage simuliert · API-Key im JavaScript simuliert · Live-Zugangsdaten im Frontend simuliert

Zugeordnete Befunde: DEMO-SYN-003 · Passwort im Local Storage simuliert · DEMO-SYN-004 · API-Key im JavaScript simuliert · DEMO-SYN-013 · Live-Zugangsdaten im Frontend simuliert

SOFORTMASSNAHME

Betroffene Zugangsdaten widerrufen/rotieren und Nutzungs- sowie Authentisierungslogs prüfen.

ZUSTÄNDIGE ROLLE

Anwendungsbetrieb, Informationssicherheit und API-Verantwortliche

WARUM DIE EMPFEHLUNG

Ein clientseitig erreichbarer Zugangsdaten- oder Secret-Hinweis wurde im Quelltext-/Bundle-Befund erfasst.

DAUERHAFTE UMSETZUNG

Secrets serverseitig verwalten, Proxy mit Minimalrechten und dokumentierte Rotation einsetzen.

NACHTEST / EVIDENCE

Quelltext-, Bundle- und HAR-Nachtest ohne Klartext-Secret; alte Credentials müssen scheitern.

DEMO-SYN-003 · 01_vor_einwilligung.har · E-LAW-003 · E-STORAGE-002 · 01_vor_einwilligung.har · E-STORAGE-002 · DEMO-SYN-004 · E-LAW-004 · DEMO-SYN-013 · E-LAW-006

Technischer Kontext: Passwörter, Bearer-/Basic-Auth-Daten, private Schlüssel und nicht als öffentlich ausgewiesene Tokens als kompromittiert behandeln, widerrufen oder rotieren und die Nutzungslogs prüfen. Künftige privilegierte Aufrufe über einen serverseitigen Proxy mit minimalen, kurzlebigen Berechtigungen ausführen; die konkrete Fundstelle nicht erneut als Klartext in einen Bericht oder ein Beweispaket übernehmen.

Browser-Speicher vor Consent klassifizieren und minimieren

BEFUND / AUSLÖSER

Vor Einwilligung · 2 Speicherindikator(en)

SOFORTMASSNAHME

Nicht erforderliche Cookies und Storage-Einträge vor Einwilligung unterbinden.

ZUSTÄNDIGE ROLLE

Frontend-/CMP-Verantwortliche und
Datenschutzkoordination

WARUM DIE EMPFEHLUNG

Im Ausgangskontext wurden 2 Cookie-/Storage-Indikatoren aufgezeichnet; Zweck und Erforderlichkeit müssen je Eintrag geprüft werden.

DAUERHAFTE UMSETZUNG

Inventar mit Zweck, Lebensdauer, Kategorie und Löschverhalten pflegen.

NACHTEST / EVIDENCE

Automatisierter Diff in leerem Kontext nach Laden, Ablehnen, Akzeptieren und Reload.
Keine Evidence-Referenz separat zugeordnet.

Technischer Kontext: Jeden Cookie- und Storage-Eintrag Zweck, Erforderlichkeit, Lebensdauer und Consent-Kategorie zuordnen. Nicht erforderliche Einträge erst nach Einwilligung setzen und den Ausgangszustand regelmäßig mit einem leeren Browserkontext prüfen.

Fehlende oder schwache Security-Header gezielt härten

BEFUND / AUSLÖSER

Content-Security-Policy fehlt simuliert · HSTS fehlt simuliert

Zugeordnete Befunde: DEMO-SYN-009 · Content-Security-Policy fehlt simuliert · DEMO-SYN-010 · HSTS fehlt simuliert

SOFORTMASSNAHME

Fehlende Header am tatsächlichen HTTPS-Endpunkt bestätigen und Basisschutz ergänzen.

ZUSTÄNDIGE ROLLE

Server-/DevOps-Verantwortliche und Webentwicklung

WARUM DIE EMPFEHLUNG

Mindestens ein Security-Header wurde als fehlend, schwach oder nicht nachgewiesen erfasst.

DAUERHAFTE UMSETZUNG

CSP schrittweise mit Nonces/Hashes aufbauen; HSTS, MIME-, Referrer-, Frame- und Permissions-Schutz setzen.

NACHTEST / EVIDENCE

Response-Header, Redirects, Assets, Browserkonsole und CSP-Reports nach Rollout kontrollieren.
DEMO-SYN-009 · E-LAW-011 · DEMO-SYN-010 · E-LAW-012

Technischer Kontext: HSTS, Content-Security-Policy, X-Content-Type-Options, Referrer-Policy, Permissions-Policy und Clickjacking-Schutz anhand des konkreten Deployment-Modells prüfen. Eine CSP schrittweise im Report-Only-Modus einführen, danach Ausnahmen reduzieren und erst anschließend erzwingen.

ABSCHLUSS · UMSETZUNG UND NÄCHSTER PRÜFSTAND

Maßnahmen umsetzen. Wirkung verifizieren.

Ein technischer Befund wird erst dann zu einer belastbaren Verbesserung, wenn die Ursache im Originalsystem behoben, die Änderung dokumentiert und der relevante Prüfzustand erneut hergestellt wurde.

Der nächste Prüfstand sollte dieselben URL-Pfade, Consent-Zustände, Browserbedingungen und Evidence-Bezüge verwenden. So bleibt sichtbar, was angepasst, was bestätigt und was weiterhin offen ist.

NÄCHSTE SCHRITTE

1. Maßnahme und Verantwortlichkeit im Ticketsystem festhalten.
2. Originalbefund mit Evidence-ID reproduzieren.
3. Änderung versioniert und kontrolliert freigeben.
4. Nachtest im frischen Chromium-Kontext durchführen.
5. Ergebnis und verbleibende Unsicherheit dokumentieren.

Dieser Katalog ist ein abgeleitetes Arbeitsdokument. Der technische Befund, die Primärbelege und die menschliche fachliche Einordnung bleiben maßgeblich.



treeology.de