MUSTERBERICHT / SAMPLE-2026-001 / FIKTIVE DATEN

Musterbericht zum WordPress-Sicherheitsvorfall

Transparenzhinweis: Alle Namen, Zeitangaben, Systeme und Befunde in diesem Dokument sind fiktiv. Das Beispiel ist kein Kundenfall und kein Leistungsnachweis.

1. Kurzfassung

Auf der Beispielwebsite wurden unerlaubte Spam-Seiten und eine externe Weiterleitung festgestellt. Die Ausgangslage wurde gesichert, die Schadwirkung eingedämmt und Dateien, Datenbank, Konten sowie geplante Aufgaben auf Persistenz geprüft. Eine absolute Aussage zu einem möglichen Datenabfluss war wegen einer Loglücke nicht möglich.

2. Umfang und Grenzen

Geprüft	WordPress-Installation, Datenbank, Konten, geplante Aufgaben, verfügbare Hosting-Logs
Nicht geprüft	Betriebssystem-Forensik, externe Mailkonten, rechtliche Bewertung
Logabdeckung	Webserver: 7 Tage; WAF: 30 Tage; SFTP: nicht verfügbar

3. Zeitlicher Ablauf

T+00:00	baseline.captured	Ausgangslage und Logs gesichert
T+00:45	redirect.contained	Externe Weiterleitung deaktiviert
T+03:20	persistence.removed	Datei- und Datenbankfund entfernt
T+06:10	verification.complete	Funktions- und Integritätsprüfung

4. Befunde und Einordnung

BEFUND	Manipulierte Plugin-Datei mit ausführbarem Redirect-Code; Hash und Vergleichsquelle dokumentiert.
INDIZ	Unbekannter Administrator ohne dokumentierten Zweck; Anlagezeitpunkt im Zeitraum des Vorfalls.
GRENZE	Webserverlogs deckten nur sieben Tage ab; der früheste Zugriff blieb offen.

5. Durchgeführte Maßnahmen

OK	Ausgangslage und relevante Logs vor Änderungen gesichert
OK	Aktive Weiterleitung kontrolliert eingedämmt
OK	Betroffene Komponente aus verifizierter Quelle ersetzt
OK	Dateien, Datenbank, Konten, Sessions und Cronjobs geprüft
OK	Zugänge und Schlüssel in abgestimmter Reihenfolge rotiert
OK	Frontend, Login, REST, Formulare und Kernfunktionen getestet

6. Datenabflussindikatoren

In den verfügbaren Protokollen wurde kein bestätigter Export gefunden. Der Schadcode konnte jedoch auf Anwendungskonfiguration zugreifen, und die Logabdeckung war unvollständig. Ergebnis: kein bestätigter Abfluss, aber keine belastbare Negativaussage.

7. Restpunkte und Freigabe

OK	Logaufbewahrung und zentrale Alarmierung verlängern
OK	Mehrfaktor-Authentifizierung für privilegierte Konten aktivieren
OK	Wiederherstellungstest des getrennten Backups dokumentieren
OK	Kontrollprüfung nach 30 Tagen durchführen

Abschlussstatus: BEREINIGT UND TECHNISCH GEPRÜFT.
Zeitpunktbezogene Abnahme - keine Garantie, dass ein System niemals erneut angegriffen werden kann.