

PHP2Shell: Nach dem Patch Logs, Passwörter und SaaS-Ausfall sauber nachsorgen

FÜR WEN

IT-Verantwortliche und Leitung Finanzen von KMU mit 10 bis 200 Mitarbeitenden, deren Website, Shop, Buchhaltung oder Fachanwendung auf PHP läuft oder deren SaaS-Anbieter betroffen war

AUFGABE	WER	BIS WANN
☐ Alle Systeme mit PHP erfasst, auch SaaS, Appliances und Container, mit Priorität		
☐ Pro System die Behebung belegt: Version, Backport oder schriftliche Bestätigung		
☐ PHP-Dienste neu gestartet, Container neu gebaut, laufende Version kontrolliert		
☐ session.upload_progress.enabled=0 in php.ini oder FPM-Pool gesetzt		
☐ Protokolle ab 17.10.2026 beim Hoster angefordert und ausserhalb des Servers gesichert		
☐ Protokolle auf ungewöhnliche Anfragen, Abstürze, veränderte Dateien und Prozesse geprüft		
☐ Eigene Computer auf Schadsoftware geprüft, danach Zugangsdaten erneuert		
☐ Alte API-Schlüssel und Zugänge beim Anbieter gesperrt		
☐ Entscheid zur Meldung an den EDÖB getroffen und begründet dokumentiert		
☐ Fünf Fragen an jeden SaaS-Anbieter geschickt, Antworten abgelegt		
☐ Notfallplan «Buchhaltung offline» mit Rollen, Exporten und Wiederanlauf freigegeben		
☐ Systeme mit PHP 8.2 oder älter für die Umstellung vor dem 31.12.2026 eingeplant		

ZUR ANLEITUNG

Schritte, Beispiele, Quellen, Vorlage und KI-Skill: www.vortrieb.ch/php2shell-nachsorge-kmu/