YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[Unternehmensangaben zu ergänzen]

Bericht-Nr.: YH-DEMO-2026-04
Ausstellungsdatum: 19. November 2026
WIEDERHERSTELLUNGSPLAN

INCIDENT RESPONSE & SANIERUNG • ERGEBNIS NR. 4

Vorfallsanalyse & Systemwiederherstellung

Diagnose eines kurzen 502-Fehlers, forensische Untersuchung unbefugter Zugriffe sowie Bereinigungs- und Härtungsplan.

AUFTRAGGEBER

Unternehmen: Horizons Médias & Édition SARL (Fiktiv)
Domains: portail-horizons.example (+ Multi-Sites)
Host-Server: srv-demo-03.yoorhosting.com (Nginx/Apache)
Konten: horizons_adm · horizons_wp

HTTP-502-FEHLER GEKLÄRT
12 s · 85 Req
Apache-Neustart nach System-Update

INITIALER ZUGANGSVEKTOR
1 FTP-Konto
Agentur-Login ohne Root-Chroot

SERVERWEITE AUSBREITUNG
0 Ausbreitung
Andere cPanel-Konten und SSH intakt

SANIERUNGSPROTOKOLL
10 Schritte
Sauberer Neuaufbau und Härtung

KUNDENANFRAGE

„Nach Warnmeldungen über einen kurzen Ausfall (Fehler 502) sowie dem Verdacht auf unbefugte Zugriffe und massiven Spam-Versand auf einem Multi-Site-Konto forderte der Kunde: (1) die exakte technische Erklärung der 502-Unterbrechung, (2) eine vollständige forensische Untersuchung des Einbruchs und seines Umfangs sowie (3) ein detailliertes technisches Protokoll zur sauberen Wiederherstellung und dauerhaften Härtung."

1 Teil 1 — Analyse des Kurzzeitausfalls (HTTP-502-Fehler über 12 Sekunden)

PROTOKOLL-CHRONOLOGIE (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : Auto-Update openssl, systemd,
ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload und
eingereihte Neustarts
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : Upstream-Abbruch
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused während
Apache-Stopp
[14:28:00-01] Apache neu gestartet (OpenSSL/3.5.8) →
100 % HTTP 200 OK
```

Befund: 100 % der **85 HTTP-502-Fehler** traten in diesen 12 Sekunden auf. Keine beschädigten Dateien, kein Angriff, kein Hardwaredefekt. Prüfungen nach Neustart: Startseite (~180 ms), Produktseite (~210 ms) und Admin (~150 ms) liefern `200 OK`.

SEPARATER BACK-OFFICE-TIMEOUT & EMPFEHLUNGEN

Die Anwendungsprotokolle (`/home/horizons_adm/public_html/var/logs/`) zeigten einen separaten Fehler beim Öffnen von *Systeminformationen* durch `operateur@portail-horizons.example` :

```
FatalError: Maximum execution time of 180 seconds
exceeded
at .../classes/ConfigurationTest.php:246 (rekursiver
Scan /img/)
```

- System-Updates in das Nachtfenster verlegen (02:00–05:00 Uhr).
- Graceful Reload (`httpd -k graceful` / `systemctl reload`) statt Stop/Start nutzen.
- Rekursiven `/img/` -Scan tagsüber in `ConfigurationTest.php` vermeiden.

2 Teil 2 — Forensische Untersuchung des unbefugten Zugriffs

INITIALER ZUGANGSVEKTOR & FEHLENDE VERZEICHNIS-ISOLIERUNG

Es wurde keine Zero-Day-Lücke ausgenutzt. Nach einem fehlgeschlagenen cPanel-Login (Port 2083) um 08:26 UTC von `203.0.113.10` meldete sich der Angreifer um 15:17 UTC per FTP (Port 21) sofort erfolgreich mit den gültigen Zugangsdaten des Dienstleisters `agence-ext@portail-horizons.example` an. **Hauptursache:** Das FTP-Konto zeigte auf das cPanel-Stammverzeichnis `/home/horizons_adm` statt auf ein *chroot* in `public_html` und legte Konfigurationsdateien sowie MariaDB-Zugangsdaten (`horizons_dbprod`) offen.

DATUM / ZEIT (UTC)	IP (ANONYMISIERT)	QUELLE / RELAY	REKONSTRUIERTE AKTIONEN (IDENTISCHE FTP-SIGNATUR + `CURL/8.7.1`)
15/09 08:26	`203.0.113.10`	VPS-Hoster A	Fehlgeschlagene Login-Versuche auf cPanel (Port 2083) mit dem Kontonamen.
15/09 15:17	`203.0.113.10`	VPS-Hoster A	Erster erfolgreicher FTP-Login (`agence-ext@...`); Abruf `tools/.htaccess` und Testskript gelöscht.
16/09 02:21	`203.0.113.10`	VPS-Hoster A	Ablage des JS-Skimmers `themes/universal/assets/js/custome1.js` (64 210 Bytes) und Änderung von `payment.tpl` .
22/09 12:29	`203.0.113.21`	Proxy-Relay B	FTP-Download von `app/config/parameters.php` (MariaDB-Passwort & Schlüssel); Backdoor `_ca_9f3a.php` abgelegt.
23/09 15:37–19:31	`203.0.113.22/23/24`	Rotierende Proxys C/D/E	Ablage von `clearcache.php` , API-Abzug von Bestellungen (`/api/orders` in 500er-Blöcken) und System-Recon (10 KB).
23/09–08/10	`203.0.113.50`	VPS-Server F	Webshells `_npgop_*.php` , Base64-SQL-Befehle, gefälschte Zahlungs-Controller, danach Löschskript `npg_purge.json` .

MANIPULATIONEN AN ANWENDUNG & SQL-DATENBANK

- **MariaDB (`horizons_db2025`):** Aktivierung `PS_WEBSERVICE` , Änderung `PS_MAIL_METHOD` , Reaktivierung von Drittmodulen, Auslesen von Bestellungen und gezieltes Löschen von Audit-Logs.
- **JS-Skimmer:** griff Zahlungsfelder ab und sendete Base64-kodierte Daten per `sendBeacon` / `fetch` an einen Drittserver (`collecte-tiers.example`).
- **Zahlungsmodul:** Einschleusung paralleler Controller (`npginit.php`) und Statusdateien unter `var/.ppext/` .

ISOLATIONSPRÜFUNG AUF SRV-DEMO-03

GEPRÜFTER BEREICH	BEFUND	STATUS
Andere cPanel-Konten (`tiers_a` , `tiers_b`)	Keine verdächtigen Dateien, Logs oder Abfragen	INTAKT
SSH- & Systemzugriff (`/var/log/secure*`)	Null Versuche von den Angreifer-IPs	INTAKT
Cron-Jobs (`/etc/cron*`)	Ausschließlich legitime Fachskripte	SAUBER
Aktive Prozesse im Speicher	Nur reguläre PHP-FPM- & Backup-Prozesse	SAUBER

3 Teil 3 — Multi-Site-Audit und vollständiger Bereinigungs- & Härtungsplan

BEFUNDE, DIE EINEN SAUBEREN NEUAUFBAU ERFORDERN (KONTO `HORIZONS_WP`)

- **KRITISCH** Über **410 000 Spam-Mails** in 30 Tagen über gekaperte Postfächer und direkte PHP-Mailer-Skripte.
- **KRITISCH** Bis zu **83 Webshells** pro Website auf 6 von 7 Domains (`editions-alpha.example` , `atelier-beta.example`).
- **KRITISCH** Unbefugte WordPress-Admin-Konten, verstecktes „Must-Use"-Plugin zum Passwortdiebstahl und SEO-Spam-Weiterleitungen.
- **49 Postfächer** durch Angreifer angelegt sowie Panel-/Webmail-Logins von unbekannten IPs (Passwörter kompromittiert).
- Veraltete Plugins mit bekannten Sicherheitslücken (`WPForms 1.7.0` , `Elementor 2.4.7` , `Yoast SEO 5.7.1`).
- Fehlende Härtung: Datei-Editor aktiv, `XML-RPC` offen, Kontaktformulare ohne Bot-Schutz.

#	SANIERUNGSSCHRITT	TECHNISCHE MASSNAHMEN IM WIEDERHERSTELLUNGSPROTOKOLL
1	**Notfall-Eindämmung**	Sofortiger Stopp des ausgehenden Spam-Versands, Sperrung der Angreiferzugriffe, vollständige Beweissicherung des betroffenen Kontos.
2	**Forensische Triage & Inventar**	Trennung der legitimen Inhalte jeder Domain von eingeschleusten Dateien, Ordnern, Konten und Datenbankeinträgen.
3	**Neues isoliertes Konto**	Einrichtung eines frischen cPanel-Kontos, komplett neue starke Passwörter (Panel, FTP, DB, Mail, WP), SSH geschlossen, ein chrooted FTP-Nutzer.
4	**Sauberer Neuaufbau**	Neuinstallation von Kern, Theme und Plugins aus offiziellen Quellen; SQL-Bereinigung fremder Admins, Links und Optionen; Medien ohne ausführbaren Code.
5	**Plugin-Modernisierung**	Aktualisierung oder Ersatz aller veralteten Erweiterungen, Funktionstests und Entfernung ungenutzter Module.
6	**Formularabsicherung**	Anti-Bot-Schutz (Turnstile oder hCaptcha), Honeypot-Feld, Rate-Limit pro IP, fester Empfänger und Versand nur über authentifiziertes SMTP.
7	**E-Mail-Bereinigung**	Beibehaltung nur bestätigter Postfächer, Löschung von Angreifer-Postfächern, Versandlimits sowie `SPF` , `DKIM` und `DMARC` .
8	**Vollständige Härtung**	Datei-Editor deaktiviert, `XML-RPC` gesperrt, PHP-Ausführung in `uploads` blockiert, 2FA für Admins, WAF-Regeln und Auto-Updates.
9	**Stilllegung fremder Domains**	Sichere Entfernung reiner Angreifer-Seiten und vollständige DNS-Prüfung jeder beibehaltenen Domain.
10	**30-Tage-Monitoring & Bericht**	Laufende Überwachung von Dateien und ausgehenden Mails, Nachkontrolle an Tag 7 und schriftlicher Abschlussbericht aller Maßnahmen.

Ergänzende Empfehlungen (Teil 2 & Teil 3): Webservice-Schlüssel (`API_KEY_REVOQUEE_DEMO_01`) und alte FTP-Konten sofort widerrufen, `custome1.js` sowie `clearcache.php` löschen, Zahlungsmodul aus offizieller Quelle neu installieren und bei möglicher Datenabschöpfung zwischen 16.09. und 08.10. die Acquiring-Bank sowie zuständige Behörden informieren.

Technische Freigabe:
CERT & Operative Sicherheit — YOORshop SAS

✓ Protokoll Validiert