```php
<?php
/**
 * config_snippets.php
 *
 * Sammlung aller Ergaenzungen fuer die phpList config.php.
 * Dies ist KEIN eigenstaendig lauffaehiges Skript, sondern eine
 * Referenzsammlung - die einzelnen Bloecke werden in die produktive
 * config.php uebernommen, nicht diese Datei selbst eingebunden.
 *
 * Reihenfolge in diesem Dokument = empfohlene Reihenfolge beim Einfuegen.
 */


// ============================================================
// 1) Server-seitiger Basis-Spamschutz (Wiki-Kapitel 4.1)
// ============================================================
define('USE_SPAM_BLOCK', 1);
define('NOTIFY_SPAM', 1);


// ============================================================
// 2) Bounce-Postfach-Konfiguration (Wiki-Kapitel 6.3)
// ============================================================
$bounce_mailbox_host = 'DEIN-SERVER';
$bounce_mailbox_user = 'bounces@nl.DEINE-DOMAIN.de';
$bounce_mailbox_password = 'DEIN_PASSWORT';
$bounce_mailbox_port = "995/pop3/ssl/novalidate-cert";
$bounce_mailbox_purge = 1;
$bounce_mailbox_purge_unprocessed = 1;
$bounce_unsubscribe_threshold = 5;

// Wichtig: Envelope-Absender auf die Bounce-Adresse setzen,
// sonst laufen Bounces weiterhin beim persoenlichen Postfach auf
$message_envelope = 'bounces@nl.DEINE-DOMAIN.de';


// ============================================================
// 3) Remote Processing Secret fuer Bounce-Cron (Wiki-Kapitel 6.6)
// Generieren mit: openssl rand -hex 20
// WICHTIG: Muss als $GLOBALS['config'][...] gesetzt werden,
// eine einfache Variable wird von getConfig() NICHT erkannt!
// ============================================================
$GLOBALS['config']['remote_processing_secret'] = 'DEIN_GENERIERTES_SECRET';


// ============================================================
// 4) IP-Sperrliste: Lese-Check (Wiki-Kapitel 8.4)
// Wird von blocklist_update.php befuellt.
// ============================================================
$blocklistFile = '/pfad/zu/private/ip_blocklist.php';
```

```php
if (file_exists($blocklistFile)) {
    $blocked_ips = include $blocklistFile;
    $remote_ip = $_SERVER['REMOTE_ADDR'] ?? '';
    if (in_array($remote_ip, $blocked_ips, true)) {
        header('HTTP/1.1 403 Forbidden');
        exit('Access denied.');
    }
}


// ============================================================
// 5) Subscription-Bombing-Schutz (Wiki-Kapitel 9.2)
// Rate-Limiting pro Zieladresse statt pro IP - wirksam gegen
// Angreifer, die dieselbe (oft fremde) Zieladresse ueber
// wechselnde IPs wiederholt einreichen.
// ============================================================
if (isset($_GET['p']) && $_GET['p'] === 'subscribe' &&
!empty($_POST['email'])) {
    $targetEmail = trim($_POST['email']);

    try {
        $bpdo = new PDO(
            "mysql:host=127.0.0.1;dbname=DEINE_DB;charset=utf8mb4",
            'DEIN_DB_USER',
            'DEIN_DB_PASSWORT'
        );
        $stmt = $bpdo->prepare("
            SELECT COUNT(*) FROM phplist_user_user_history h
            JOIN phplist_user_user u ON u.id = h.userid
            WHERE u.email = :email
              AND h.summary IN ('Subscription', 'Re-Subscription')
              AND h.date >= (NOW() - INTERVAL 24 HOUR)
        ");
        $stmt->execute(['email' => $targetEmail]);
        $recentAttempts = (int) $stmt->fetchColumn();

        if ($recentAttempts >= 2) {
            header('HTTP/1.1 429 Too Many Requests');
            exit('Please wait before trying again.');
        }
    } catch (Exception $e) {
        // Bei DB-Fehler nicht blockieren, normal weiterlaufen lassen
    }
}
```