

BEISPIELBERICHT

# Sicherheits- und Betriebsbericht

Server  
**server01.example.com**

Berichtszeitraum  
**18.10.2026 00:15 – 19.10.2026 00:15**

Erstellt  
**19.10.2026 17:13**

**Beispielbericht:** Server, Domains, Mailadressen, IP-Adressen und alle Zahlen sind erfunden. Der Bericht zeigt Aufbau und Inhalt der regelmäßigen Auswertung.



## Handlungsbedarf

2 kritische Befunde – bitte zeitnah bearbeiten. Details und Empfehlungen folgen in diesem Bericht.

2

Kritische Befunde

3

Warnungen

12

Hinweise

## Auf einen Blick

183.607

Web-Anfragen

1.341

Mail-Anmeldungen

3.935

Abgewehrte Anmeldeversuche

4.959

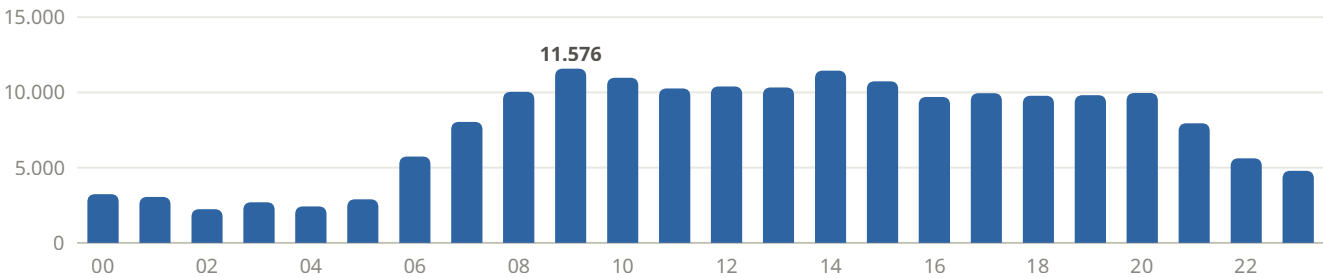
Blockierte Web-Angriffe

101

Gesperrte IP-Adressen

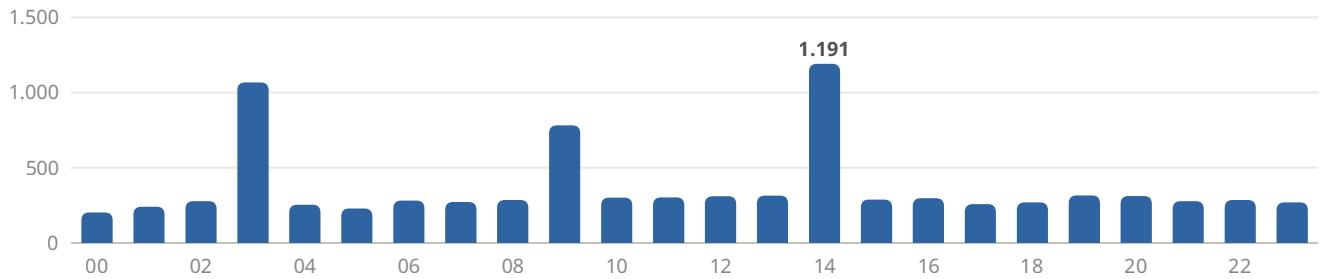
## Web-Anfragen je Stunde

18.10.2026 00:00 – 18.10.2026 23:59 Uhr



## Angriffsversuche je Stunde

Fehlgeschlagene Anmeldungen (Mail, Plesk), von der Web-Firewall blockierte Anfragen und 404-Anfragen erkannter Scanner · Werte je Stunde im Anhang



## Kritische Befunde (2)

**KRITISCH** M5

### Erfolgreicher Mail-Login nach vielen Fehlversuchen (Passwort erraten?)

Betrifft: buchhaltung@example.org · Anzahl: 37

- 203.0.113.77 (BR): 37 Fehlversuche (User) / 0 ohne User, dann Login 2026-10-18 03:12 via imap

**Empfehlung:** Passwort wurde vermutlich erraten: sofort ändern, IP sperren (fail2ban/Firewall), Versand prüfen.

**KRITISCH** W8

### Mögliches Datenleck: sensible Datei mit HTTP 200 ausgeliefert

Betrifft: shop.example.com · Anzahl: 3

- 198.51.100.14 GET /.env → 200, 1184 Bytes
- 198.51.100.14 GET /.git/config → 200, 312 Bytes
- 203.0.113.201 GET /backup/shop.sql.gz → 200, 48213771 Bytes

**Empfehlung:** Prüfen, ob die Datei wirklich ausgeliefert wurde (Antwortgröße!). Datei entfernen/sperrern und enthaltene Zugangsdaten ändern.

## Warnungen (3)

**WARNUNG** W1

### PHP memory\_limit erreicht (Allowed memory size exhausted)

Betrifft: shop.example.com · Anzahl: 14

- 14x memory\_limit 256 MB – /var/www/vhosts/example.com/shop.example.com/wp-content/plugins/woocommerce/includes/class-wc-product-query.php

**Empfehlung:** PHP memory\_limit der Domain erhöhen (Plesk > Domain > PHP-Einstellungen) oder Script/Plugin prüfen.

**WARNUNG** W3

**PHP-FPM-Pool ausgelastet (pm.max\_children erreicht)**

Betrifft: **shop.example.com** · Anzahl: 3

- 3x pm.max\_children = 10 erreicht (2026-10-18 11:38 bis 2026-10-18 11:51)

**Empfehlung:** pm.max\_children des PHP-FPM-Pools erhöhen (Plesk > PHP-Einstellungen) – verfügbaren RAM beachten; bei Angriffen (viele wp-login/xmlrpc-Requests) zuerst die Angreifer sperren.

**WARNUNG** W14

**Veraltete PHP-Version 7.4 ohne Sicherheitsupdates (End of Life)**

Betrifft: **PHP 7.4** · Anzahl: 2

- alt.example.net, verein.example.org
- Quelle: Plesk-Datenbank (live, alle Domains)

**Empfehlung:** PHP-Version der Domains auf eine unterstützte Version umstellen (Plesk > Domain > PHP-Einstellungen), vorher Kompatibilität der Website testen.

**Hinweise (12)**

| Hinweis                                                                                                                                                                                                                                                                                                                                   | Betrifft          | Anzahl |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------|
| <b>Brute-Force auf Mail-Logins – IPs NICHT von fail2ban gesperrt</b><br>412 Fehlversuche 203.0.113.77 (BR)<br>187 Fehlversuche 198.51.100.62 (VN)                                                                                                                                                                                         | Mail              | 3      |
| <b>Eingehender Spam (SpamAssassin), RBL- und sonstige Abweisungen</b><br>SpamAssassin-Treffer: 214, RBL-Abweisungen: 1873, sonstige Abweisungen: 96<br>Spam an info@example.com: 88x                                                                                                                                                      | Mail              | 2.183  |
| <b>MariaDB/MySQL: InnoDB-Buffer-Pool sehr klein (Performance)</b><br>innodb_buffer_pool_size = 128 MB, 12 Memory-Pressure-Ereignisse im Zeitraum<br><b>Empfehlung:</b> innodb_buffer_pool_size an Datenbestand und RAM anpassen (z.B. 1–2 GB bei 8 GB RAM), z.B. in / etc/mysql/mariadb.conf.d/50-server.cnf; danach MariaDB neu starten. | MySQL/<br>MariaDB | 12     |
| <b>Zertifikat / Let's Encrypt fehlgeschlagen</b><br>3x praxis.example.org<br>1x shop.example.com                                                                                                                                                                                                                                          | Zertifikate       | 4      |
| <b>SSH-Fehlversuche</b><br>611x 203.0.113.9 (CN) [fail2ban]<br>402x 198.51.100.150 (RU) [fail2ban]                                                                                                                                                                                                                                        | SSH               | 1.893  |
| <b>fail2ban: erkannte und gesperrte IPs je Jail</b><br>plesk-dovecot 61 IPs erkannt, 38 Sperren<br>plesk-postfix 44 IPs erkannt, 27 Sperren                                                                                                                                                                                               | fail2ban          | 101    |

| Hinweis                                                                                                                                                                                                                                                                                                                                                                           | Betrifft | Anzahl |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------|
| <b>Angriffe auf den Plesk-Login</b><br>Versuchte Logins: admin (28x), root (10x), administrator (4x)<br>21x 203.0.113.140 (VN) [fail2ban]<br><b>Empfehlung:</b> Admin-Zugriff auf Plesk auf bekannte IPs beschränken (Tools & Einstellungen, Bereich Sicherheit), Zwei-Faktor-Authentifizierung aktivieren. Login "root" prüft das System-Passwort von root – es muss stark sein. | Plesk    | 42     |
| <b>Verteilter Brute-Force auf WordPress-Logins je Domain</b><br>1842 POST von 317 IPs blog.example.net<br>655 POST von 121 IPs www.example.org                                                                                                                                                                                                                                    | Web      | 2      |
| <b>Scanner (viele 404-Anfragen)</b><br>2412 x 404 198.51.100.201 (DE) [fail2ban]<br>1377 x 404 203.0.113.45 (NL)                                                                                                                                                                                                                                                                  | Web      | 4      |
| <b>Angriffsmuster in URLs (SQL-Injection, Path-Traversal, XSS, Log4Shell, PHP-CGI)</b><br>311x 203.0.113.45 (NL) z.B. GET /index.php?id=1%27%20UNION%20SELECT%20NULL--<br>88x 198.51.100.201 (DE) z.B. GET /cgi-bin/php-cgi.exe?-d+allow_url_include%3d1                                                                                                                          | Web      | 3      |
| <b>ModSecurity-Blockierungen (Regel-ID / Treffer)</b><br>1204x Regel 211760<br>874x Regel 214540                                                                                                                                                                                                                                                                                  | Web      | 4.959  |
| <b>PHP 8.2 erhält bald keine Sicherheitsupdates mehr</b><br>blog.example.net, kanzlei.example.com, praxis.example.org, www.example.com, www.example.org<br>Quelle: Plesk-Datenbank (live, alle Domains)<br><b>Empfehlung:</b> Umstellung auf eine aktuelle PHP-Version einplanen.                                                                                                 | PHP 8.2  | 5      |

## Serverinformationen

Bestandsaufnahme des Servers beim Sammeln der Logs (erfasst 19.10.2026 00:15 CEST). Hervorgehoben sind Werte, die Aufmerksamkeit brauchen.

### SYSTEM

|                     |                                                      |
|---------------------|------------------------------------------------------|
| Hostname            | server01.example.com                                 |
| Betriebssystem      | Ubuntu 22.04.5 LTS                                   |
| Kernel              | 5.15.0-124-generic                                   |
| Plattform           | virtuell (kvm) – QEMU Standard PC (Q35 + ICH9, 2009) |
| Laufzeit            | 3 Wochen, 4 Tage, 7 Stunden<br>seit 23.09.2026 17:12 |
| Zeitsynchronisation | synchronisiert (NTP)                                 |

### UPDATES

|                     |                                                  |
|---------------------|--------------------------------------------------|
| Paketverwaltung     | apt                                              |
| Ausstehende Updates | ● <b>12 Pakete</b><br>davon 3 Sicherheitsupdates |

### RESSOURCEN

|                         |                                                                           |
|-------------------------|---------------------------------------------------------------------------|
| CPU                     | AMD EPYC 7543P 32-Core Processor (8 Kerne)                                |
| Load 1/5/15 min         | 1,42 · 1,18 · 1,05<br>8 Kerne, Warnschwelle 16                            |
| Arbeitsspeicher         | 16,8 GB von 31,3 GB belegt<br>14,5 GB verfügbar<br><div><div></div></div> |
| Swap                    | 256 MB von 4,0 GB belegt<br><div><div></div></div>                        |
| Root-Dateisystem        | 88G von 152G belegt<br><div><div></div></div>                             |
| OOM-Kills seit Neustart | keine                                                                     |

### DIENSTE UND SICHERHEIT

|                         |       |
|-------------------------|-------|
| Fehlgeschlagene Dienste | keine |
|-------------------------|-------|

UPDATES

|                          |                                                |
|--------------------------|------------------------------------------------|
| Paketlisten aktualisiert | 18.10.2026 06:25<br>vor weniger als 24 Stunden |
| Neustart erforderlich    | nein                                           |
| Automatische Updates     | aktiv (unattended-upgrades)                    |

DIENSTE UND SICHERHEIT

|                                |                                                                          |
|--------------------------------|--------------------------------------------------------------------------|
| SSH-Server                     | Port 22<br>root-Anmeldung: nur mit Schlüssel,<br>Passwort-Anmeldung: aus |
| SSH-Schlüssel von root         | 2                                                                        |
| AppArmor / SELinux             | AppArmor aktiv                                                           |
| Zertifikat Plesk-Panel         | noch 71 Tage gültig<br>server01.example.com                              |
| Zertifikat Postfix (SMTP)      | noch 71 Tage gültig<br>server01.example.com                              |
| Zertifikat Dovecot (IMAP/POP3) | noch 71 Tage gültig<br>server01.example.com                              |
| Plesk-Zertifikate              | ● 1 läuft in weniger als 14 Tagen ab<br>6 geprüft                        |

PLESK

|             |                          |
|-------------|--------------------------|
| Version     | Plesk Obsidian 18.0.65.2 |
| Domains     | 18                       |
| Abonnements | 11                       |

Datenträger

| Einhängepunkt                | Typ  | Größe | Belegt | Frei | Belegung                       | Inodes |
|------------------------------|------|-------|--------|------|--------------------------------|--------|
| /<br>/dev/vda1               | ext4 | 152G  | 88G    | 64G  | 58 %<br><div><div></div></div> | 9 %    |
| /boot/efi<br>/dev/vda15      | vfat | 105M  | 6,1M   | 99M  | 6 %<br><div><div></div></div>  | –      |
| /var/www/vhosts<br>/dev/vdb1 | ext4 | 984G  | 792G   | 142G | 85 %<br><div><div></div></div> | 9 %    |

Netzwerk

| Schnittstelle | Adresse            | Reverse-DNS (PTR)     |
|---------------|--------------------|-----------------------|
| eth0 UP       | 192.0.2.10/24      | server01.example.com. |
| eth0 UP       | 2001:db8:10::10/64 | server01.example.com. |

Software-Versionen

|         |                          |               |                 |
|---------|--------------------------|---------------|-----------------|
| Plesk   | Plesk Obsidian 18.0.65.2 | nginx         | 1.26.2          |
| Apache  | 2.4.62 (MPM event)       | MariaDB/MySQL | 10.11.9-MariaDB |
| Postfix | 3.6.4                    | Dovecot       | 2.3.21.1        |
| OpenSSL | 3.0.2                    | OpenSSH       | 8.9p1           |

|              |        |            |          |
|--------------|--------|------------|----------|
| fail2ban     | 0.11.2 | PHP (CLI)  | 8.3.12   |
| SpamAssassin | 3.4.6  | Imunify360 | 7.12.4-1 |

## Kennzahlen

|                                        |       |                                      |         |
|----------------------------------------|-------|--------------------------------------|---------|
| Mail-Logins erfolgreich                | 1.341 | Mail-Logins fehlgeschlagen           | 2.000   |
| Mail-User mit Login                    | 38    | Angreifende IPs (Mail)               | 173     |
| Mails über SMTP-AUTH                   | 642   | Web-Requests (Domains)               | 183.607 |
| Web-Requests (Server-IP/Default)       | 2.894 | Domains mit Zugriffen                | 18      |
| WordPress-Login-POSTs                  | 2.497 | ModSecurity-Blockierungen            | 4.959   |
| SSH-Logins erfolgreich                 | 4     | SSH-Fehlversuche                     | 1.893   |
| Plesk-Panel Logins erfolgreich         | 6     | Plesk-Panel Fehlversuche             | 42      |
| fail2ban-Sperren                       | 101   | Mail-Fehlversuche bekannter Herkunft | 0       |
| M5 ignoriert: Login vorher mehrfach ok | 0     |                                      |         |

## Zeitverlauf je Stunde

| Stunde           | Web    | Fehler 5xx | Mail-Anm. | Mail-Fehl. | Web-Firewall | 404-Scanner | Plesk-Fehl. | PHP ausgelastet |
|------------------|--------|------------|-----------|------------|--------------|-------------|-------------|-----------------|
| 18.10.2026 00:00 | 3.240  | 12         | 24        | 35         | 128          | 40          | 0           | 0               |
| 18.10.2026 01:00 | 3.055  | 12         | 20        | 48         | 140          | 51          | 2           | 0               |
| 18.10.2026 02:00 | 2.235  | 8          | 20        | 61         | 154          | 62          | 1           | 0               |
| 18.10.2026 03:00 | 2.698  | 10         | 14        | 865        | 129          | 73          | 0           | 0               |
| 18.10.2026 04:00 | 2.418  | 9          | 18        | 58         | 147          | 47          | 2           | 0               |
| 18.10.2026 05:00 | 2.894  | 11         | 21        | 42         | 128          | 58          | 1           | 0               |
| 18.10.2026 06:00 | 5.733  | 22         | 40        | 55         | 157          | 69          | 0           | 0               |
| 18.10.2026 07:00 | 8.044  | 32         | 56        | 39         | 189          | 43          | 2           | 0               |
| 18.10.2026 08:00 | 10.033 | 40         | 76        | 52         | 178          | 54          | 1           | 0               |

| Stunde              | Web    | Fehler 5xx | Mail-Anm. | Mail-Fehl. | Web-Firewall | 404-Scanner | Plesk-Fehl. | PHP ausgelastet |
|---------------------|--------|------------|-----------|------------|--------------|-------------|-------------|-----------------|
| 18.10.2026<br>09:00 | 11.576 | 46         | 86        | 36         | 200          | 545         | 0           | 0               |
| 18.10.2026<br>10:00 | 10.972 | 43         | 80        | 49         | 174          | 76          | 2           | 0               |
| 18.10.2026<br>11:00 | 10.260 | 105        | 81        | 62         | 190          | 50          | 1           | 3               |
| 18.10.2026<br>12:00 | 10.399 | 41         | 73        | 46         | 204          | 61          | 0           | 0               |
| 18.10.2026<br>13:00 | 10.335 | 41         | 78        | 59         | 181          | 72          | 2           | 0               |
| 18.10.2026<br>14:00 | 11.446 | 45         | 77        | 43         | 1.101        | 46          | 1           | 0               |
| 18.10.2026<br>15:00 | 10.734 | 42         | 78        | 56         | 175          | 57          | 0           | 0               |
| 18.10.2026<br>16:00 | 9.698  | 38         | 76        | 40         | 188          | 68          | 2           | 0               |
| 18.10.2026<br>17:00 | 9.945  | 39         | 69        | 53         | 162          | 42          | 1           | 0               |
| 18.10.2026<br>18:00 | 9.773  | 39         | 73        | 37         | 180          | 53          | 0           | 0               |
| 18.10.2026<br>19:00 | 9.817  | 39         | 73        | 50         | 200          | 64          | 2           | 0               |
| 18.10.2026<br>20:00 | 9.956  | 39         | 72        | 63         | 173          | 75          | 1           | 0               |
| 18.10.2026<br>21:00 | 7.947  | 31         | 56        | 47         | 181          | 49          | 0           | 0               |
| 18.10.2026<br>22:00 | 5.616  | 22         | 44        | 60         | 146          | 60          | 20          | 0               |
| 18.10.2026<br>23:00 | 4.783  | 19         | 36        | 44         | 154          | 71          | 1           | 0               |

## Datengrundlage

- Beispielbericht mit erfundenen Daten: Domains aus example.com/.net/.org, IP-Adressen aus den für Dokumentation reservierten Bereichen 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24 und 2001:db8::/32.
- Ausgewertet wurden die Logdateien des Servers im Berichtszeitraum (18.10.2026 00:15 – 19.10.2026 00:15, 24 Stunden).
- Vergleich mit 30 früheren Auswertungen (neue Netze und Länder bei Anmeldungen).
- Länderzuordnung der IP-Adressen: MaxMind GeoLite2 Country, Stand 14.10.2026; Erkennung von VPN/Rechenzentren über die Netzbetreiber (MaxMind GeoLite2 ASN).  
This product includes GeoLite Data created by MaxMind, available from <https://www.maxmind.com>.
- Erstellt mit Sammelskript 2026.10.18 (aktuell), Analyse und PDF 2026.10.18.2 (WeasyPrint version 69.0).
- Alle Einzelheiten mit Beispielzeilen enthält der technische Bericht (Textdatei).