Website-Logs, Besucherzählung und Server-Sicherheit

Oct 21, 2026 · @Sebastian Ebner · Quelle: KI Werkzeug Cloude

Überblick

Diese Zusammenfassung bündelt, was sich bei der Auswertung von Server-Logs einer kleinen Website (Webhosting mit DirectAdmin und LiteSpeed, dazu ein eigener Ubuntu-Server) im September und Oktober 2026 als nützlich erwiesen hat. Sie ist zum Weitergeben gedacht: persönliche IP-Adressen, Schlüssel, Kanalnamen und Ordnernamen sind entfernt.

SSH-Login-Alarm mit ntfy

Bei jeder erfolgreichen SSH-Anmeldung schickt der Server eine Push-Nachricht aufs Handy: leise bei bekannten Adressen, als Alarm bei allen anderen. Fehlversuche lösen bewusst nichts aus, sonst kämen über 9.000 Meldungen am Tag. Versand über ntfy (kostenlos, ohne Konto, App im Play Store und bei F-Droid).

1. **Geheimen Kanalnamen erzeugen** und in der ntfy-App abonnieren: `echo "ssh-$(head -c 12 /dev/urandom | base64 | tr -dc a-zA-Z0-9)"`
2. **Skript** nur für root schreibbar ablegen, z. B. `/root/login-alarm.sh`, Rechte 700:

```
#!/bin/sh
PATH=/usr/sbin:/usr/bin:/sbin:/bin
[ "$PAM_TYPE" = "open_session" ] || exit 0
KANAL="HIER-DEN-GENERIERTEN-KANALNAMEN-EINTRAGEN"
IP="${PAM_RHOST:-lokal}"
ZEIT=$(TZ=Europe/Berlin date '+%d.%m.%Y %H:%M:%S')
case "$IP" in
  EIGENE-IP-ADRESSE-1|EIGENE-IP-ADRESSE-2)
    PRIO=low;    TITEL="SSH-Anmeldung (bekannte Adresse)" ;;
  *)
    PRIO=urgent; TITEL="ACHTUNG: SSH-Anmeldung von unbekannter Adresse" ;;
esac
curl -s -m 10 -H "Title: $TITEL" -H "Priority: $PRIO" -H "Tags: key" \
  -d "Benutzer $PAM_USER auf $(hostname) von $IP am $ZEIT" \
  "https://ntfy.sh/$KANAL" >/dev/null 2>&1 &
exit 0
```

3. **Testen:** `PAM_TYPE=open_session PAM_USER=root PAM_RHOST=1.2.3.4 /root/login-alarm.sh` muss einen Alarm auslösen. Ob ntfy ihn erhalten hat, zeigt `curl -s "https://ntfy.sh/<KANAL>/json?poll=1"`.
4. **Einhängen:** `echo 'session optional pam_exec.so /root/login-alarm.sh' >> /etc/pam.d/sshd`. Das Wort `optional` verhindert, dass ein Fehler im Skript die Anmeldung sperrt. Vor dem Schließen der Sitzung in einem zweiten Fenster neu anmelden.

Kommt nichts am Handy an, obwohl ntfy die Nachricht hat: Kanalname in der App exakt prüfen (Groß- und Kleinschreibung), Benachrichtigungen und Akku-Ausnahme für die App erlauben, ntfy nicht vom VPN ausnehmen. Anmeldungen per Web-Konsole des Anbieters deckt dieselbe Zeile in `/etc/pam.d/login` ab.

Datei-Wächter fürs Webhosting

Auf Webhosting ohne root lässt sich keine Anmeldung überwachen, wohl aber jede veränderte Datei. Ein Cronjob prüft alle 10 Minuten die Webordner und meldet per ntfy neue, geänderte und gelöschte Dateien. Wer eine Website übernimmt, verändert fast immer Dateien, egal ob er per FTP, Kundenmenü oder über eine Lücke hereinkam.

```
#!/bin/sh
KANAL="HIER-DEN-GENERIERTEN-KANALNAMEN-EINTRAGEN"
BASIS="/home/HIER-BENUTZERNAME-EINTRAGEN"
MARKE="$BASIS/.waechter-marke"
export LC_ALL=C

melde() {   # $1 Titel  $2 Liste  $3 Ordner
  [ -z "$2" ] && return
  N=$(printf '%s\n' "$2" | wc -l)
  T=$(printf '%s\n' "$2" | sed "s#^$3##" | head -20)
  curl -s -m 15 -H "Title: $1 ($N)" -H "Tags: warning" \
       -d "$T" "https://ntfy.sh/$KANAL" >/dev/null
}

pruefe() {  # $1 Name  $2 Ordner  $3 Ausnahme  $4 zweite Ausnahme (optional)
  A2="${4:-$3}"
  BESTAND="$BASIS/.waechter-liste-$1"
  find "$2" -type f ! -path "$3" ! -path "$A2" 2>/dev/null | sort >
"$BESTAND.neu"
  GEAENDERT=$( {
    [ -f "$MARKE" ]   && find "$2" -type f -cnewer "$MARKE" ! -path "$3" ! -
path "$A2" 2>/dev/null
    [ -f "$BESTAND" ] && comm -13 "$BESTAND" "$BESTAND.neu"
  } | sort -u )
```

```
  GELOESCHT=""
  [ -f "$BESTAND" ] && GELOESCHT=$(comm -23 "$BESTAND" "$BESTAND.neu")
  mv "$BESTAND.neu" "$BESTAND"
  melde "Neu/geaendert auf $1" "$GEAENDERT" "$2"
  melde "Geloescht auf $1" "$GELOESCHT" "$2"
}

touch "$MARKE.neu"
pruefe "HIER-DOMAIN-EINTRAGEN" "$BASIS/domains/HIER-DOMAIN-
EINTRAGEN/public_html" \
       "*/HIER-AUSGENOMMENEN-ORDNER-EINTRAGEN/*"
mv "$MARKE.neu" "$MARKE"
```

Einrichten: Skript neben dem Ordner `domains` ablegen, nicht im Webordner (im DirectAdmin-Dateimanager ist das die oberste Ebene `/`, auf dem Server `/home/BENUTZERNAME`). Rechte 755. Cronjob mit Minute `*/10`, Rest `*`, Befehl `/bin/sh /home/BENUTZERNAME/w.sh >/dev/null 2>&1`. Der erste Lauf legt nur Zeitmarke und Liste an.

Worauf achten:

- **`-cnewer` statt `-newer`:** FTP-Apps übertragen oft das alte Dateidatum. Die Statuszeit (ctime) setzt der Server selbst, sie lässt sich nicht zurückdatieren.
- **Ordner ausnehmen, die sich von selbst ändern:** Zählerdaten, Caches, PHP-Sitzungen (`tmp/sess_*`), Datenordner von own-/Nextcloud (oft mit Zufallsnamen wie `.ht….data`). Beim Ändern der Ausnahmen kommt einmalig eine Meldung „neu“ bzw. „geloescht“; vermeidbar durch Löschen der `.waechter-*`-Dateien vorher.
- **Grenzen:** Was zwischen zwei Läufen entsteht und wieder verschwindet, sieht er nicht. Reine Zugriffe und Anmeldungen meldet er nicht. Pro Meldung werden höchstens 20 Dateien gelistet.
- **Zeitplan:** `*/10` läuft zu den vollen Zehnern, nicht zehn Minuten nach dem Anlegen.

Sicherheitshinweise

- **FTP nur als FTPS oder SFTP.** Einfaches FTP überträgt Passwort und Dateien im Klartext. Bei DirectAdmin nutzt FTP meist dasselbe Passwort wie das Kundenmenü, aber ohne zweiten Faktor. Unbenutzte FTP-Konten löschen.
- **Zwei-Faktor-Anmeldung** im Kundenmenü und in der Cloud einschalten. Die Anmeldeseiten einer Cloud werden von Suchmaschinen gefunden und gezielt angegriffen.

- **SSH mit Passwort** hält nur, wenn das Passwort lang und zufällig ist. Auf beiden Servern gingen rund 100.000 Rateversuche pro Monat allein auf root. Ein anderer Port als 22 senkt das Grundrauschen deutlich.
- **Nichts Sensibles in den Webordner.** Datenbankdateien (z. B. `owncloud.db`), PHP-Sitzungen und Konfigurationen müssen per `.htaccess` gesperrt sein. Kontrolle: die Adresse im Browser aufrufen, erwartet wird 403 oder 404.
- **Indexseiten für das Web-Archiv** listen alles, was im Ordner liegt. Archive.org hat so auch Statistik-Rohdaten und Geo-Datenbanken mitgenommen. Solche Ordner aus der Liste nehmen und zusätzlich sperren, z. B. `<FilesMatch "\.(csv|bin|json)$"> Require all denied </FilesMatch>`. Was im Archiv liegt, bleibt dort öffentlich.
- **IP-Listen sind personenbezogen.** Auswertungen mit IP-Adressen nur für sich behalten, nicht veröffentlichen.
- **ntfy-Kanalnamen geheim halten.** Wer den Namen kennt, liest alle Meldungen mit (Servername, Benutzer, IP, Dateinamen).

Bewusst weggelassen

Damit das Dokument gefahrlos weitergegeben werden kann, fehlen: die eigenen IP-Adressen und Adressbereiche, die ntfy-Kanalnamen, Zugangsschlüssel, Server-Hostnamen, die Adresse der privaten Cloud und der Name ihres Datenordners sowie alle Listen fremder IP-Adressen. In den Skripten stehen dafür Platzhalter in Großbuchstaben.