Veiligheidscheck van de hele vloot

Datum: 28 juli 2026
Aanleiding: het nieuws dat AI-agenten van OpenAI uit hun omgeving ontsnapten en een ander AI-bedrijf binnendrongen. Dat riep de vraag op: hoe staat het met onze eigen bots?
Gecontroleerd: 5 machines, 10 websites, de database, de VPS en alle koppelingen.

> Alles hieronder is zelf gemeten. Waar een meting een vals antwoord kon geven, heb ik het nagelopen en staat dat erbij.

In het kort

1. **Er is niets ingebroken.** Geen gelekte wachtwoorden of sleutels gevonden in de code.
2. **Maar de bewaker was zelf dood.** Het programma dat je bots in de gaten houdt, lag stil sinds 25 juli. Gerepareerd, draait weer.
3. **De code-scanner was helemaal verdwenen** van de MacBook. Daardoor stond er groen in het rapport terwijl er niets gescand was. Teruggehaald en opnieuw gedraaid.
4. **Het enige zware alarm is loos.** Ik heb het nagelopen: er lekt niets.
5. **Wel echt: haartips.nl geeft je gebruikersnamen weg.** Iedereen kan opvragen dat je inlogt als "admin" en "jamal".
6. **Inloggen kan onbeperkt geprobeerd worden** op beide WordPress-sites. Geen rem.
7. **De VPS heeft 32 updates openstaan.**
8. **Het WhatsApp-lek van vorige week raakt onze Macs niet.**

---

1. De bewaker lag stil

Wat is het?
Er draait een programma dat elke 10 minuten kijkt of je bots nog leven, en ze anders

herstart. Dat programma crashte bij elke ronde. 542 keer achter elkaar, zonder dat iemand het merkte.

Waarom het pijn doet:
Als er in die drie dagen een bot was omgevallen, had niemand het gezien. Dit is precies het gat dat je niet wilt: de wachter die zelf weg is en dat niet meldt.

De oorzaak (drie dingen tegelijk):
- Een tijdstempel uit de database had vijf cijfers achter de komma. Het programma kon alleen met drie of zes cijfers omgaan en klapte eruit.
- De gegevens over Coco waren verouderd. Er werd gezocht naar een programma dat niet meer bestaat, en drie dagen lang elke 10 minuten een dienst herstart die er niet meer is.
- Kimi stond er nog in als Windows-machine, terwijl hij op 25 juli naar de MacBook is verhuisd.

De fix: alle drie hersteld. En er zit nu een rem op: na drie mislukte herstartpogingen stopt hij en meldt hij het, in plaats van eindeloos door te gaan.

Bewijs: de taak eindigt nu met code 0 (was code 1) en meldt alle drie de bots gezond.

---

2. De code-scanner was er niet meer

Wat is het?
De scanner die de code doorzoekt op gelekte wachtwoorden en sleutels stond niet meer op de MacBook. Het overkoepelende rapport zette daar netjes "overgeslagen" bij, maar de samenvatting die naar Telegram gaat toonde gewoon: 0 kritiek, 0 hoog, 0 medium.

Waarom het pijn doet:
Dat leest als "alles is veilig", terwijl het in werkelijkheid "ik heb niet gekeken" betekent. Een leeg resultaat is geen goed resultaat.

De fix: de scanner staat terug (hij stond nog wel op GitHub) en is opnieuw gedraaid over alle sites.

Uitkomst van die scan: 42 bevindingen. 0 kritiek, 1 hoog, 25 midden, de rest klein.

3. Het zware alarm is loos

Het rapport meldde: **wp-config.php op haarvisie.nl geeft antwoord**. Dat is het bestand met je databasewachtwoord erin, dus dat klinkt ernstig.

Ik heb het bestand echt opgehaald. Het antwoord is **1 teken groot en leeg**. Er staat niets in. Dat is normaal: de server voert het bestand uit in plaats van het te tonen.

Conclusie: vals alarm. De scanner kijkt alleen of er antwoord komt, niet of er iets in dat antwoord staat.

Let op: dit soort loze alarmen zijn gevaarlijk. Als je er drie keer per maand een krijgt, ga je ze negeren, ook de echte.

---

4. Wel echt: je gebruikersnamen liggen op straat

Wat is het?
Op haartips.nl kan iedereen deze pagina opvragen: `/wp-json/wp/v2/users`. Daar staat in dat er twee gebruikers zijn: **admin** en **jamal**.

Waarom het pijn doet:
Inbreken bestaat uit twee helften: de naam raden en het wachtwoord raden. De naam is nu gratis. Op haarvisie.nl staat dit netjes dicht (die geeft een foutmelding terug), dus we weten dat het kan.

De fix: die lijst afschermen voor bezoekers die niet ingelogd zijn. Dat is een kleine toevoeging.

---

5. Onbeperkt inlogpogingen op beide sites

Wat is het?
De inlogpagina van haarvisie.nl en haartips.nl accepteert de ene poging na de andere. Er zit geen rem op.

Waarom het pijn doet:
In combinatie met punt 4 is dat een uitnodiging. De naam is bekend, en het aantal pogingen is onbeperkt.

De fix: een gratis plugin die na een paar mislukte pogingen op slot gaat. Denk aan Wordfence of Limit Login Attempts.

Eerlijk: haarvisie.nl mag ik niet zomaar aanpassen. Dit is dus een voorstel, geen uitgevoerde actie.

---

6. Kleinere punten

PUNT	WAAR	ERNST
Beveiligingskoppen ontbreken (bescherming tegen namaakvensters en scripts van buiten)	haarvisie.nl, haartips.nl en de meeste tools	midden
readme.html bereikbaar, verraadt je WordPress-versie	haarvisie.nl, haartips.nl	klein
WordPress-versie zichtbaar in de broncode	haartips.nl	klein
32 updates openstaand	VPS	midden
Beeper-koppeling ligt eruit	MacBook	klein

Verder: de database staat goed dicht. Anonieme bezoekers kunnen niets opvragen wat niet mag. Wachtwoord-inloggen op de VPS staat uit, alleen sleutels werken. Alle certificaten van de sites zijn ruim geldig, de krapste heeft nog 31 dagen.

---

7. Het WhatsApp-lek van vorige week

Er was een lek in de Adobe Acrobat-extensie voor Chrome. Wie die extensie had en tegelijk WhatsApp Web open had staan, kon door een kwaadwillende site laten meelezen in zijn gesprekken.

Ik heb alle vijf de Macs nagekeken, in elke browser die erop staat: Chrome, Arc, Brave, Edge, Opera, Vivaldi en Chromium. **De extensie staat nergens.**

De Windows-computers moeten nog gecheckt worden. Die vraag staat uit.

Los daarvan het advies uit het artikel, en dat is sowieso verstandig: kijk in WhatsApp bij "gekoppelde apparaten" en log alles uit wat je niet herkent.

---

8. Wat dit zegt over onze eigen bots

De aanleiding was het nieuws over AI-agenten die uit hun omgeving braken. Dat is bij ons niet gebeurd. Wat we deze week wel zagen, is iets anders maar net zo leerzaam:

- Sjakie herstartte zichzelf 36 keer op een dag, omdat hij zijn eigen bot opnieuw wilde starten. Daar zit sinds gisteren een rem op. Vandaag heb ik die rem ook bij Coco en bij mezelf gezet, en getest dat hij precies het juiste blokkeert: je eigen bot herstarten mag niet, een andere bot herstarten mag wel.
- De iMac is nagekeken en is schoon.
- Julio meet zichzelf, dat antwoord staat nog open.

Het patroon is niet "een bot doet iets kwaadaardigs". Het patroon is **een bot die per ongeluk zichzelf sloopt, of een wachter die stilletjes wegvalt**. Daar hoort onze aandacht te zitten.

Wat ik voorstel, op volgorde

NR	ACTIE	WAARDE	MOEITE
1	Gebruikerslijst van haartips.nl afschermen	hoog	klein
2	Rem op inlogpogingen, beide sites	hoog	klein
3	De 32 updates op de VPS installeren	midden	klein, maar even opletten

NR	ACTIE	WAARDE	MOEITE
4	Beveiligingskoppen toevoegen	midden	midden
5	readme.html weghalen	klein	klein
6	De scanner slimmer maken, zodat hij niet meer loos alarm slaat	midden	klein

Punt 1, 3, 5 en 6 kan ik zelf doen. Punt 2 en 4 raken haarvisie.nl, daar heb ik je toestemming per pagina voor nodig.

Dit is advies. Zeg welke nummers je wilt, dan pak ik ze op.