BYGG DIN PERSONLIGA AI-AGENT

Säkerhetsriskerna du MÅSTE känna till

8 min läsning | Nybörjare | Lektion 10 av 21

DEL 1 AV 6

Översikt

- Det här är den viktigaste lektionen i hela kursen.
- Jag säger inte det för att skrämma dig.
- Jag säger det för att jag vill att du ska vara trygg.

DEL 2 AV 6

138 säkerhetshål på 63 dagar

- Säkerhetsforskare började granska OpenClaws kod i början av 2026.
- Under bara 63 dagar hittade de 138 allvarliga sårbarheter.
- Det är i genomsnitt över två nya säkerhetshål varje dag.

DEL 3 AV 6

335 skadliga skills

- Kommer du ihåg ClawHub-marknadsplatsen med över 5 400 skills?
- Forskare gick igenom dem och upptäckte att 335 stycken var skadliga.
- Det är 12 procent av hela registret.

DEL 4 AV 6

135 000 öppna installationer

- Forskare skannade internet och hittade över 135 000 OpenClaw-installationer som var publikt tillgängliga.
- Det betyder att vem som helst på internet kunde ansluta till dem.

DEL 5 AV 6

Varför händer det här?

- OpenClaw är ett projekt som drivs av frivilliga.
- Det finns ingen supportavdelning, inget säkerhetsteam som jobbar heltid och ingen kvalitetskontroll av skills som laddas upp till ClawHub.

DEL 6 AV 6

De gyllene reglerna

- Om du ändå vill testa OpenClaw, följ de här reglerna till punkt och pricka:

Tack för att du lärde dig med oss.

Nästa lektion: Vad är Hermes Agent? Fortsätt där du slutade på snabbprompt.se.

snabbprompt.se

Scanna för att fortsätta