BYGG DIN PERSONLIGA AI-AGENT

Säkerhet. Verkliga incidenter och hur du skyddar dig

8 min läsning | Nybörjare | Lektion 15 av 21

DEL 1 AV 6

Översikt

- AI-agenter är kraftfulla.
- Men med kraft kommer risk.
- Jag vill att du förstår vad som faktiskt har hänt, inte vad som KAN hända i teorin.

DEL 2 AV 6

Tre verkliga incidenter

- OpenClaw-krisen (2026)

DEL 3 AV 6

Vad alla de här incidenterna har gemensamt

- Problemet är inte att AI i sig är farlig.
- Problemet är att en AI-agent med bred åtkomst till dina system skapar en stor attackyta.
- Ju fler saker agenten kan göra, desto mer kan gå fel.

DEL 4 AV 6

Prompt injection, förklarat enkelt

- Det finns ett speciellt trick som angripare använder mot AI-agenter.
- Det kallas "prompt injection".

DEL 5 AV 6

Sex gyllene regler för säker agentanvändning

- Kör aldrig en AI-agent på din jobbdator utan IT-avdelningens godkännande.
- Om något går fel är det ditt ansvar.
- Prata med IT först.

DEL 6 AV 6

Välj din egen nivå

- Nästa kapitel: Agenter bortom grunderna. Kodagenter, browser-agenter, forskningsagenter och en blick mot framtiden. ->

Tack för att du lärde dig med oss.

Nästa lektion: Instruktionsdesign för agenter. Fortsätt där du slutade på snabbprompt.se.

snabbprompt.se

Scanna för att fortsätta