heise+ | Promptware: Wie weit Malware für KI-Systeme schon ist

2026-04-07 08:30

Attacken auf große Sprachmodelle gehen mittlerweile weit über reine Prompt-Injections hinaus. Zeit für eine Bestandsaufnahme.