TEKNOLOGI

'ChatGPT udgør sikkerhedsrisiko for samfundet' - ingeniører efterlyser regler for brugen af AI

Vi tror ikke, folk er opmærksomme på problemet, lyder det fra ingeniørforeningen IDA.

Når du skriver noget i ChatGPT, så bruger den efterfølgende informationen som en del af den data, den bliver trænet på. (Foto: © LIONEL BONAVENTURE, Ritzau Scanpix)

LÆS OP ORDBOG TEKST

AF
Allan Nisgaard

3. MAJ KL. 07:53

Den kan hjælpe skribenter med at skrive nyheder, guides og reklametekster. Og den kan hjælpe programmører med at udvikle koder til komplekse opgaver.

Chatbotten ChatGPT er på kort tid blevet et populært redskab blandt virksomheder verden over.

Men når man bruger den slags kunstig intelligens, som også bliver kaldt sprogmodeller, bør man tænke over, hvad man fodrer dem med.

LÆS OGSÅ: Skal vi være bekymrede? eksperter er uenige om faren ved kunstig intelligens

> **Der er særlig stor risiko for lækage, hvis du eksempelvis skriver virksomheds- eller statshemmeligheder.**
>
> JOHANNES BJERVA, LEKTOR PÅ INSTITUT FOR DATALOGI PÅ AALBORG UNIVERSITET I KBH.

ChatGPT og andre sprogmodeller kan nemlig risikere at lække de oplysninger, som virksomhederne fodrer dem med, når de spørger dem om hjælp, advarer ingeniørforeningen IDA.

- Har du nogen interesse i at holde noget fortroligt, så skal du nok holde det væk fra ChatGPT. Det gælder især, hvis du arbejder med kritisk infrastruktur, da det kan udgøre en risiko for samfundet, siger Jørn Guldberg, it-sikkerhedsekspert for IDA.

Derfor bør myndighederne, ifølge Jørn Guldberg, udarbejde nogle retningslinjer for virksomheders brug af ChatGPT og andre lignende sprogmodeller. Og når det kommer til offentlige institutioner, bør de retningslinjer være et krav, mener foreningen.

© Ritzau Scanpix

Samsung lækkede hemmeligheder til ChatGPT

Medarbejdere i det sydkoreanske firma Samsung er i flere tilfælde

- Vi tror nemlig ikke, at folk er opmærksomme på det her. Så vi skal have nogle retningslinjer for, hvad vi må bruge det til og ikke må bruge det til, siger han.

OpenAI - firmaet bag ChatGPT - vil i de kommende måneder rulle chatbotten ud til virksomheder på et erhvervsabonnement <https://www.dr.dk/nyheder/viden/teknologi/openai-vil-rulle-chatgpt-ud-til-virksomheder-og-revolutionere-arbejde> .

Ekspert: Der er risiko for lækage

Når ingeniørerne frygter, at ChatGPT kan lække fortrolig information, skyldes det den måde, den kunstige intelligens fungerer på.

ChatGPT og andre lignende sprogmodeller bliver trænet med enorme mængder data i form af tekster, heriblandt kodesprog. Ud fra den data lærer de at gengive og skabe ny information.

- Sprogmodeller har ikke et begreb om, hvad sandhed er. De er blot gode til at efterligne information, siger Johannes Bjerva, der er lektor på Institut for Datalogi på Aalborg Universitet i København og forsker i sprogteknologi.

Når du så spørger ChatGPT om noget og giver den ny information via dit spørgsmål, så leverer du samtidig ny data, som den kan blive trænet på. Derfor skal man være opmærksom, mener Johannes Bjerva.

- Der er særlig stor risiko for lækage, hvis du eksempelvis skriver virksomheds- eller statshemmeligheder. Så giver du den træningsdata, og det betyder, at hvis en anden stiller et spørgsmål i den retning, så vil de få et svar, som måske er fortrolig information.

Ifølge OpenAI's egen politik kan ansatte dog selv gøre noget for at nedsætte risikoen for, at samtaler eller programmerings-koder blive brugt som data.

Når du bruger ChatGPT, kan du under indstillinger vælge, at chatbotten ikke må anvende dine samtaler som data, den kan træne sig selv på. Men det skal du selv aktivt gå ind og vælge, og dine data bliver alligevel gemt i 30 dage, oplyser virksomheden.

- De to ting passer ikke helt sammen i mit hoved. Altså at man ikke vil bruge dataene, men samtidig vælger at gemme dem i 30 dage, siger Johannes Bjerva.

- Selvom man måske er mere bange for data på kinesiske servere, så er det nok ikke optimalt, at en privat virksomhed i USA får fat i al den slags info.

Johannes Bjerva mener, at man som minimum bør slå funktionen til, hvis man bruger ChatGPT og fodrer den med information, der er fortrolig eller personfølsom.

- Men jeg tror ikke, det er nok. Det kræver nok, at man som land eller EU som helhed sætter nogle krav for, hvad virksomheder må og ikke må.

Virksomhed laver selv regler

Start-up-virksomheden Neurospace i Hørning i Jylland har selv taget initiativ til at lave nogle sikkerhedsregler, når deres medarbejdere bruger værktøjer som ChatGPT.

Det er jo kritisk infrastruktur, vi arbejder med. Derfor er det også vigtigt, at vi har styr på sikkerheden, hvis vi bruger ChatGPT.

MARIA JENSEN, MEDSTIFTER AF NEUROSPACE.

Neurospace hjælper blandt andre forsyningsvirksomheder, som arbejder med fjernvarme, vand og spildevand, med at behandle data, så de får så meget værdi ud af dem som muligt.

For eksempel kan de hjælpe et fjernvarmeselskab med at få et bedre overblik over forsyning, efterspørgsel, køling og lækager.

- Det er jo kritisk infrastruktur, vi arbejder med. Derfor er det også vigtigt, at vi har styr på sikkerheden, hvis vi bruger ChatGPT, siger Maria Jensen, der er machine learning-ingeniør og medstifter af virksomheden.

Hos virksomheden Neurospace i Hørning må de ansatte ikke dele programmeringskoder og andre følsomme oplysninger med ChatGPT. De må bruge botten til at få inspiration, på samme måde som via almindelige Google-søgninger. (Foto: © Caroline Christensen, DR)

Medarbejderne har fået tilladelse til at bruge ChatGTP til at finde eksempler på koder, hvis de mangler inspiration til at løse et problem. Men de deler aldrig deres egne koder med botten.

- Når vi blandt andet taler fjernvarme, så går det ikke, at vi for eksempel deler en kode med en nøgle, der giver adgang til netværkene, siger Maria Jensen.

Jørn Guldberg mener, det kan være en farligt, hvis man som virksomhed arbejder med kritisk infrastruktur og bruger ChatGPT uden at tænke over

sikkerheden.

- Vi har lige set, at russiske trawlere rejser rund <https://www.dr.dk/drtv/episode/skyggekrigen_-putins-spioner-i-norden_382096> t og ser, hvor vores gasledninger og elledninger ligger under vandet. Det havde de ikke behøvet at gøre, hvis nogen havde lagt informationerne ind i ChatGPT. Så kunne russerne jo bare spørge botten om det, siger han.

Digitaliseringsminister Marie Bjerre (V) er i dag kaldt i samråd for at redegøre for, om regeringen har nogle planer om nye initiativer, set i lyset af den aktuelle udvikling inden for kunstig intelligens, for eksempel ChatGPT.

DR Nyheder har kontaktet OpenAI og spurgt virksomheden, hvordan den helt konkret bruger brugernes data, og hvorvidt det lever op til databeskyttelsesforordningen (GDPR). OpenAI er ikke vendt tilbage med svar.