

Risk för bristande säkerhet när allt fler satsar på AI under 2019

2019 kan bli året då Artificiell Intelligens (AI) på allvar förändrar flera branscher. Många företag ligger i startgroparna för satsningar, men samtidigt finns risker för att säkerhetsfrågorna kopplade till AI prioriteras för lågt. Detta enligt en ny rapport från PwC.

Idag är många företagsledningarna på det klara med att AI kan ha stor påverkan på deras affärsmodeller. Enligt beräkningar kan AI bidra med hissnande 15 700 miljarder dollar till den globala ekonomin 2030. Men enligt PwC:s rapport *2019 AI Predictions* så är det många beslutsfattare som missar en av nyckelfrågorna.

– Idag satsar allt fler företag på AI och 2019 lär vi få se en explosion inom området, men samtidigt måste säkerhetstänket hänga med. Här finns mycket att göra inom många organisationer, såväl privata som offentliga, berättar Jakob Bundgaard ansvarig Cyber Security, PwC Sverige.

Även om det finns en medvetenhet om utmaningen så visar rapporten att det fortfarande återstår mycket arbete när det gäller fokus på AI-säkerhet. Bara 47 procent av de svarande planerar att öka fokus på tester när det gäller påverkan av datamodeller och användning av algoritmer. Dessutom är det bara drygt hälften som tänker satsa på att förbättra styrning av driftsmodeller och processer kopplade till AI.

– Det har funnits en diskussion och ökad oro för hur AI kan påverka integritet och sysselsättning, men inte lika ofta kopplat till cybersäkerhet. Samtidigt märker vi nu att allt fler ställer sig frågan om det går att lita på AI. Så det är ingen överraskning att cheferna i den här undersökningen säger att AI-systemens pålitlighet lyfts som en av deras största utmaningar för 2019.

Det här behöver organisationer tänka på för att skapa en ökad säkerhet kring AI:

- Opartiskhet - minskar riskerna för påverkan med de data- och AI-modeller som ni använder, eller är det tvärtom så att de ökar?
- Tolkningsbarhet - kan ni förklara hur en AI-modell fattar beslut och kan ni säkerställa att besluten är korrekta? Om inte, vems är ansvaret?
- Robust och säker - kan ni lita på AI-systemets prestanda och hur sårbart systemet är för angrepp?
- Styrning - vem är ansvarig för AI-system och finns rätt kontroller på plats?
- Etiskt perspektiv - överensstämmer era AI-system med regler och lagar och hur kommer de att påverka anställda och kunder?

– För att hantera alla dessa delområden behövs en organisation med tydliga ansvar för AI. En trend som vi ser är att allt fler företag nu skapar etiska råd och inrättar en Chief Ethic Officer-roll med teknikkompetens och där AI är en del av uppdraget. Framöver kommer det helt klart behövas fler arbetsroller som kombinerar teknisk expertis med kunskap om både juridik-, etik- och varumärkesfrågor, menar Jakob Bundgaard och avslutar;

– Sen tror vi även att vi får se fler företag under 2019 som vill göra AI-besluten mer transparenta, tolkningsbara och möjliga att se nyttan av. Lite förenklat handlar det om algoritmer som förklarar sig själva. Målet är med andra ord då en AI-lösning som kan förklara dess rationalitet, styrkor och svagheter och förmedla hur den kommer att fungera i framtiden. Framöver tror jag att våra beslutsfattare kommer att trycka mer på de här tolkningskraven och bygga in dem i regelverken.

Om undersökningen

I undersökningen *2019 AI Predictions* har PwC frågat 1 000 chefer i USA om hur deras organisationer ser på AI och där ett av huvudområdena handlar om säkerhetsfrågorna. Undersökningen genomfördes under hösten 2018.

Mer information om rapporten och undersökningen:

<https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions-2019.html>

För mer information

Jakob Bundgaard ansvarig Cyber Security, PwC Sverige

jakob.bundgaard@pwc.com

070-929 13 23

Om PwC:

PwC Sverige är marknadsledande inom revision, redovisning, skatte- och affärsrådgivning med 2 800 medarbetare på 34 kontor runt om i landet. Med erfarenhet och unik branschkunskap utvecklar vi värden för våra 45 000 kunder vilka utgörs av globala företag, svenska storföretag och organisationer, mindre och medelstora, främst lokala företag samt den offentliga sektorn.

PwC Sverige drivs som en självständig och oberoende juridisk enhet. Vi ingår i det globala nätverket PwC och delar våra kunskaper, erfarenheter och lösningar med 250 000 medarbetare i 158 länder för att utveckla nya perspektiv och praktiska råd.