SUMMARY CYBERSECURITY

AI – den nye angrebsflade

Indledning

Kristian og Tue sætter fokus på AI som et teknologisk skifte, der samler tidligere paradigmer som objektorienteret programmering, virtualisering og cloud – men i et langt højere tempo. Pointen er, at AI markant sænker barriererne for at udvikle og idriftsætte funktionelle løsninger, samtidig med at sikkerhed ofte ikke følger med i samme hastighed.

AI præsenteres ikke som et nicheværktøj, men som en teknologi, der allerede bruges bredt i organisationer – ofte uden fælles rammer, overblik eller klare sikkerhedsprincipper.

Hastighed som ny risikofaktor i AI udvikling

Vejen fra idé til produktionsklar løsning er i dag så kort, at klassiske sikkerheds- og governance processer ikke når at blive aktiveret i forløbet. AI-genererede løsninger kan hurtigt få adgang til data og systemer, uden at organisationen har overblik eller tilstrækkelig kontrol.

Kristian og Tue bruger et konkret eksempel til at illustrere dette skifte.

Case: AI-genereret bookingsystem

Kristian lavede en live demo, hvor han viste, hvordan et komplet bookingsystem til en fiktiv restaurant "La Tasca" kan bygges på få minutter ved hjælp af generativ AI:

- Kode genereres via prompt (frontend, backend og forretningslogik)
- AI-agent håndterer dialog med kunder
- Integrationer til e-mail (Office 365) og vagtplaner etableres
- Løsningen deployes automatisk via GitHub og containerisering

Formålet med eksemplet er ikke selve systemet, men at vise, hvor hurtigt en løsning med reelle integrationer og rettigheder kan sættes i drift og det uden at udvikleren fuldt ud forstår, hvad der faktisk bliver oprettet i baggrunden.

Risici i AI-drevne løsninger

Med udgangspunkt i casen peger Kristian og Tue på flere konkrete risici:

- Eksponering af credentials og data, når API-nøgler og konfigurationsdata indgår direkte i prompts og kode
- Manglende governance, hvor IT og sikkerhedsafdelingen ikke har indsigt i, hvem der bygger AI-løsninger, som hurtigt bliver forretningskritiske
- Usikre standardvalg, fx brug af forældet software med kendte sårbarheder
- Overprivilegerede AI-agenter, der kan udføre handlinger på tværs af systemer uden klare begrænsninger
- Udvidet angrebsflade, når kode, arkitektur og logik er åbent tilgængelige

Et centralt punkt er, at "proof of concept"-løsninger i praksis sjældent forbliver midlertidige.

Når angriberen også bruger AI

Tue supplerer med erfaringer fra Palo Alto Networks' incident response-arbejde, som viser, at angribere anvender AI på samme måde:

- Malware og ransomware kan udvikles på minutter
- Dataeksfiltration starter ofte inden for ca. en time efter kompromittering
- Sårbarheder kan hurtigere udnyttes til fjendtlige formål
- Avancerede AI-modeller kan kombinere små svagheder hurtigere, end mennesker kan analysere dem

Konsekvensen er, at menneskelig reaktion alene ikke kan følge med tempoet, og at AI må bruges aktivt i virksomhedens forsvar.

Organisering og rammer for sikker AI-brug

Indlægget understreger, at sikker AI-anvendelse kræver tværgående samarbejde i virksomheden, fordi manglende involvering fra én af disse grupper øger risikoen markant. Der er behov for klare rammer for, hvad der må bygges og bruges samt tydelige forventninger til databrug og ansvar.

Det drejer sig især om samarbejde i:

- Ledelse og bestyrelse: der har ansvar for forretningsmæssig forankring
- Udviklere og AI/ML specialister: der må sikre sikker teknisk implementering
- Brugere og ledere: må sikre korrekt og ansvarlig anvendelse
- CISO, Legal og HR: sikrer risikohåndtering og compliance

Key take aways

- AI har samlet tidligere teknologiske skift i ét og drastisk øget hastigheden fra idé til produktion, hvilket udfordrer traditionelle sikkerhedsmodeller.
- AI genererede løsninger kan hurtigt få adgang til data og systemer, uden at organisationen har overblik eller tilstrækkelig kontrol.
- Når angribere bruger AI, reduceres tiden fra sårbarhed til aktivt angreb til et niveau, hvor manuel respons ikke er tilstrækkelig.
- Sikker anvendelse af AI kræver både tekniske kontroller og klare organisatoriske rammer, hvor ansvar, rettigheder og overvågning er defineret fra start.

Vil du vide mere?

Kontakt vores specialist Kristian. Vil du i dialog med Tue Nørgaard fra Palo Alto networks? Send os en mail, så vil Tue kontakte dig.

Kristian er vores specialist
Kontakt ham til en snak om dine virksomhedsbehov.

Kristian von Staffeldt
Principal Advisor, Conscia
kvs@conscia.com

Conscia
Conscia A/S
Østbanegade 135,
2100 København Ø
Denmark

Kontakt
+45 70 20 77 80
conscia.com