AI ÆNDRER SPILLEREGLERNE FOR CYBERSIKKERHED

IT-BRANCHENS TJEKLISTE TIL VIRKSOMHEDER

AI åbner nye muligheder for virksomheder til at udvikle innovative løsninger, skabe forretningsværdi og øge produktiviteten. Samtidig ændrer AI også cybertrusselsbilledet markant. Teknologien gør eksisterende cyberangreb hurtigere og mere effektive og introducerer nye risici, når AI-systemer får adgang til følsomme data, kritiske systemer og mulighed for at handle selvstændigt.

Virksomheder skal derfor både styrke den grundlæggende cybersikkerhed og håndtere de nye risici, som AI medfører. Samtidig skal der skabes rammer for sikker og ansvarlig anvendelse af AI uden at bremse innovationen.

Med denne tjekliste peger IT-Branchen på syv centrale indsatsområder med konkrete anbefalinger til, hvordan virksomheder kan omsætte disse hensyn til handling i praksis. Anbefalingerne henvender sig bredt til danske virksomheder, velvidende at deres modenhed inden for AI og cybersikkerhed, ressourcer og organisering varierer betydeligt. Tjeklisten bør derfor tilpasses den enkelte virksomheds behov og forudsætninger, og skal ikke anses som udtømmende.

AI dækker i denne tjekliste over en bred vifte af teknologier fra generativ AI og sprogmodeller til AI-agenter og systemer til automatiseret analyse og beslutningsstøtte. Teknologierne indebærer forskellige sikkerhedsrisici afhængigt af deres anvendelse og de data, de behandler. Derfor bør virksomheder anlægge en risikobaseret tilgang, hvor sikkerhedsforanstaltningerne tilpasses de konkrete løsninger og risici.

IT·BRANCHEN

01

AI OG CYBERSIKKERHED STARTER I LEDELSESLOKALET

Virksomhedens ledelse skal tage ansvar for både at beskytte virksomheden mod AI-forstærkede cybertrusler og håndtere de sikkerhedsrisici, der følger med virksomhedens egen anvendelse af AI. Det kræver tydelig ansvarsfordeling, de rette kompetencer, og at der afsættes tilstrækkelige ressourcer til sikkerhed og risikostyring.

- **Forankr det overordnede ansvar i virksomhedens ledelse** og sørg for, at AI og cybersikkerhed indgår i virksomhedens samlede risikostyring.
- **Sørg for at ledelsen har de nødvendige kompetencer** til at forstå virksomhedens væsentligste AI-relaterede muligheder og risici, så den kan træffe kvalificerede beslutninger om anvendelse, investeringer og sikkerhed.
- **Placer et tydeligt ansvar for virksomhedens AI-anvendelse**, herunder hvem der har ansvar for AI-systemers resultater og handlinger. Det kan fx være en eller flere udpegede AI-ansvarlige eller en eksisterende funktion, der har mandat til at koordinere sikkerhed, risikostyring og overholdelse af relevante regler.
- **Inddrag virksomhedens eksisterende sikkerhedsfunktion** i udvikling, indkøb og implementering af AI-løsninger, og sørg for at den har de nødvendige kompetencer, ressourcer og mandat.
- **Afsæt dedikerede midler til øget cybersikkerhed** i lyset af de AI-forstærkede trusler og vurder investeringerne op imod de økonomiske konsekvenser af driftstop, tabte data mv.
- **Sikr løbende ledelsesmæssig opfølgning** på virksomhedens AI-anvendelse og sikkerhed, herunder om AI-løsningerne skaber den forventede forretningsværdi, og om risici og sikkerhedsforanstaltninger er acceptable.

02

SÆT RAMMER FOR SIKKER AI-ANVENDELSE OG SKAB PLADS TIL INNOVATION

Virksomheder skal fastlægge deres risikovillighed og skabe klare rammer for udvikling, eksperimenter og anvendelse af AI. Sikkerhedskravene skal tilpasses de konkrete risici, så medarbejderne kan udnytte teknologiens muligheder uden at kompromittere virksomhedens sikkerhed. Klare retningslinjer og attraktive alternativer skal samtidig reducere risikoen for *shadow AI*, hvor medarbejdere anvender AI-værktøjer uden virksomhedens godkendelse eller kontrol.

- **Fastlæg virksomhedens risikovillighed** ved at vurdere, hvor AI kan skabe værdi, hvilke risici anvendelsen indebærer, og hvilke konsekvenser fejl eller misbrug kan få. Beslut på den baggrund, hvilke risici der kan accepteres, hvilke der kræver særlige sikkerhedsforanstaltninger, og hvornår AI bør fravælges, fordi risiciene overstiger den forventede værdi.

- **Skab plads til sikker AI-anvendelse og kontrollerede eksperimenter** med klare retningslinjer for, hvilke AI-værktøjer der må anvendes, til hvilke formål og med hvilke data. Klassificér virksomhedens data og giv fx frihed til at eksperimentere med AI til generelle opgaver, mens brug af fortrolige data eller AI i kritiske processer kræver skærpet kontrol. Gør det nemt at afprøve nye løsninger, fx gennem afgrænsede testmiljøer.

- **Skab overblik over og kontrol med virksomhedens AI-anvendelse**, herunder shadow AI, gennem medarbejderdialog og kortlægning af anvendte værktøjer. Overvej tekniske løsninger, fx data loss prevention-værktøjer, der kan opdage og blokere deling af følsomme data med AI-værktøjer, under hensyntagen til databeskyttelses- og arbejdsretlige regler om medarbejderovervågning. Tilbyd samtidig godkendte, sikre og brugervenlige AI-værktøjer som alternativer.

- **Etabler en enkel og skalerbar proces for godkendelse af AI-værktøjer**, så sikker AI-anvendelse bliver lettere for medarbejderne og ikke bremses af unødigt bureaukrati.

- **Styrk medarbejdernes kompetencer** i både værdiskabende og sikker AI-anvendelse, herunder valg af relevante AI-værktøjer, hensigtsmæssig brug af AI, korrekt håndtering af forskellige typer data som fx personoplysninger og fortrolige data samt kritisk vurdering af AI-genererede resultater.

03 DET STÆRKESTE AI-FORSVAR BEGYNDER MED GOD CYBERHYGIEJNE

AI kan gøre velkendte cyberangreb hurtigere og mere effektive, fx ved at understøtte phishing, kortlægning af sårbarheder og automatisering af angreb. Derfor bliver grundlæggende cybersikkerhedsforanstaltninger som adgangsstyring, softwareopdateringer, backup og overvågning endnu vigtigere. Nye AI-baserede sikkerhedsløsninger kan supplere, men ikke erstatte, disse foranstaltninger.

- **Gennemgå og styrk virksomhedens grundlæggende cybersikkerhed**, herunder overblik over systemer, løbende softwareopdateringer, adgangsstyring, antivirus/firewall, netværkssegmentering, monitorering og backup. Generelt bør alle danske virksomheder som minimum følge de ni nationale råd om digital sikkerhed udgivet af Styrelsen for Samfundssikkerhed.

- **Reducer virksomhedens angrebsoverflade og styrk trusselsdetektionen.** Fjern bl.a. unødvendige services, begræns eksponeringen mod internettet, og sørg for at systemer og brugere kun har de nødvendige adgange og rettigheder. Sørg samtidig for løbende monitorering af systemer, netværk og brugeraktiviteter med henblik på at opdage mistænkelig aktivitet.

- **Test løbende om virksomhedens sikkerhedsforanstaltninger fungerer efter hensigten** og gennemfør regelmæssige sårbarhedsscanninger. AI kan forkorte tiden mellem opdagelse og udnyttelse af sårbarheder ("time to exploit"). Prioritér derfor hurtig udbedring af kritiske sårbarheder og installation af sikkerhedsopdateringer.

- **Styrk beskyttelsen mod AI-forstærket phishing, deepfakes og identitetssvindel**, fx gennem medarbejdertræning og procedurer for at verificere usædvanlige anmodninger om betalinger, oplysninger eller adgang.

04 BYG SIKKERHED IND I AI FRA STARTEN

Når virksomheder udvikler, indkøber eller implementerer AI-løsninger, skal sikkerhed, databeskyttelse og relevante lovkrav (fx GDPR, AI-forordningen, CRA og NIS2, hvor de finder anvendelse) tænkes ind fra begyndelsen. Det gælder både løsninger fra eksterne leverandører og virksomhedens egen AI-udvikling. AI-assisteret softwareudvikling kan øge udviklingshastigheden, men stiller fortsat krav til sikkerhedstest, kvalitetssikring og medarbejdernes kompetencer.

- **Byg videre på virksomhedens eksisterende sikkerhedsprincipper og indarbejd security by design** i udvikling, indkøb og implementering af AI-løsninger. Tilpas sikkerhedskravene til løsningernes anvendelse og risikoniveau, så sikkerheden ikke gøres unødigt kompleks.

- **Stil samme krav til gennemgang, sikkerhedstest og kvalitetssikring af AI-genereret kode som til anden softwareudvikling** før ibrugtagning, især ved *vibe coding*, hvor software kan udvikles uden tilstrækkelig forståelse for kodens funktion og sikkerhedsrisici.

- **Stil sikkerhedskrav til eksterne AI-leverandører ud fra løsningens betydning for virksomheden.** Undersøg leverandørens dokumentation for sikkerhed og databehandling, fx anerkendte certificeringer efter standarder som ISO/IEC 27001 og ISO/IEC 42001, og vær særligt opmærksom på kritiske afhængigheder, hvis AI-løsningen understøtter centrale forretningsprocesser eller kritiske systemer.

- **Inddrag relevante sikkerhedsfaglige og juridiske kompetencer**, når AI-løsninger skal anvende følsomme data, integreres med kritiske systemer eller kan medføre væsentlige risici.

05 BRUG AI TIL AT STYRKE DIT CYBERFORSVAR

AI kan styrke cyberforsvaret ved at gøre det lettere og hurtigere at opdage, analysere og reagere på trusler. Virksomhedens behov, ressourcer og modenhed er dog afgørende for, hvilke AI-baserede sikkerhedsværktøjer det er relevant at tage i brug. AI kan ikke erstatte den grundlæggende cybersikkerhed, som fortsat skal være på plads, jf. punkt 3 om basal cyberhygiejne.

- **Undersøg hvor AI og automatisering kan styrke virksomhedens cyberforsvar**, fx gennem hurtigere trusselsopdagelse, analyse af sikkerhedshændelser, prioritering af sårbarheder og understøttelse af sikkerhedsmedarbejdernes arbejde.
- **Test og kvalitetssikr AI-baserede sikkerhedsløsninger** og bevar passende menneskelig kontrol med automatiserede handlinger, særligt når de kan påvirke kritiske systemer eller virksomhedens drift.

06

GIV AI-AGENTER ADGANG MED OMTANKE OG BEVAR KONTROLLEN

AI-agenter, der selvstændigt kan tilgå data, anvende systemer og udføre handlinger på virksomhedens vegne, kan skabe nye sikkerhedsrisici. Virksomheder skal derfor sikre, at agenterne kun har de nødvendige rettigheder, at deres handlinger kan spores og kontrolleres, og at kritiske beslutninger og handlinger forbliver under passende menneskelig kontrol.

- **Giv AI-agenter egne identiteter og beskyt deres adgang til virksomhedens systemer.** Undgå at agenter deler konti med medarbejdere, beskyt deres adgange efter principperne for privilegerede konti, hvor det er relevant, og opbevar servicekontooplysninger og API-nøgler sikkert.

- **Risikovurder AI-agenter før ibrugtagning,** herunder hvilke data og systemer de har adgang til, hvilke handlinger de kan udføre, og konsekvenserne hvis de bliver manipuleret eller begår fejl. Begræns deres adgang og rettigheder til det nødvendige og gennemgå dem løbende.

- **Sikr logning, monitorering og passende menneskelig kontrol med AI-agenters aktiviteter.** Fastlæg hvilke handlinger agenterne må udføre selvstændigt, og hvilke der kræver menneskelig godkendelse, særligt når de kan påvirke kritiske systemer eller have irreversible konsekvenser.

- **Etabler mulighed for hurtigt at begrænse eller afbryde agenternes adgang og aktiviteter** ved fejl, mistanke om misbrug eller kompromittering.

- **Beskyt AI-agenter mod manipulation gennem upålidelige datakilder.** Vær opmærksom på *prompt injection*, hvor ondsindede instruktioner i fx dokumenter, websites eller e-mails kan få agenter til at udføre utilsigtede handlinger. Indfør relevante sikkerhedsforanstaltninger, herunder validering af datakilder og begrænsning af agenternes mulighed for at handle på baggrund af upålidelig information.

07

SØRG FOR AT DIN VIRKSOMHEDS BEREDSKAB OGSÅ KAN HÅNDTERE AI-RELATEREDE RISICI

AI-forstærkede cyberangreb bygger ofte på velkendte angrebsmetoder, men kan gennemføres hurtigere og i større skala. Samtidig kan virksomhedens egne AI-systemer skabe nye typer sikkerhedshændelser, fx datalæk, manipulation af AI-løsninger eller kompromitterede AI-agenter. Det kræver ikke nødvendigvis et særskilt AI-beredskab, men at virksomhedens eksisterende beredskab også kan håndtere disse risici, uanset om de kommer inde fra virksomheden eller udefra.

- **Integrér AI-relaterede risici i virksomhedens eksisterende beredskab** og vurder, om planerne dækker både AI-forstærkede cyberangreb og hændelser i virksomhedens egne AI-systemer. Tag højde for mulige konsekvenser som driftsstop, tab af data og økonomiske tab.

- **Sikr klare procedurer og ansvarsfordeling** for hurtigt at opdage, håndtere og begrænse sikkerhedshændelser, herunder mulighed for at isolere eller deaktivere kompromitterede AI-systemer. Sørg for at procedurerne også omfatter håndtering af relevante underretningspligter over for myndigheder og kunder, fx efter GDPR og NIS2, og at samarbejdet med AI-leverandører om hændelseshåndtering er aftalt på forhånd.

- **Test og drøft løbende virksomhedens beredskab** i ledelsen og bestyrelsen og inddrag relevante AI- og cyberrelaterede scenarier i eksisterende beredskabsøvelser. Tilpas beredskabet, når virksomhedens AI-anvendelse, afhængigheder eller trusselsbillede ændrer sig.