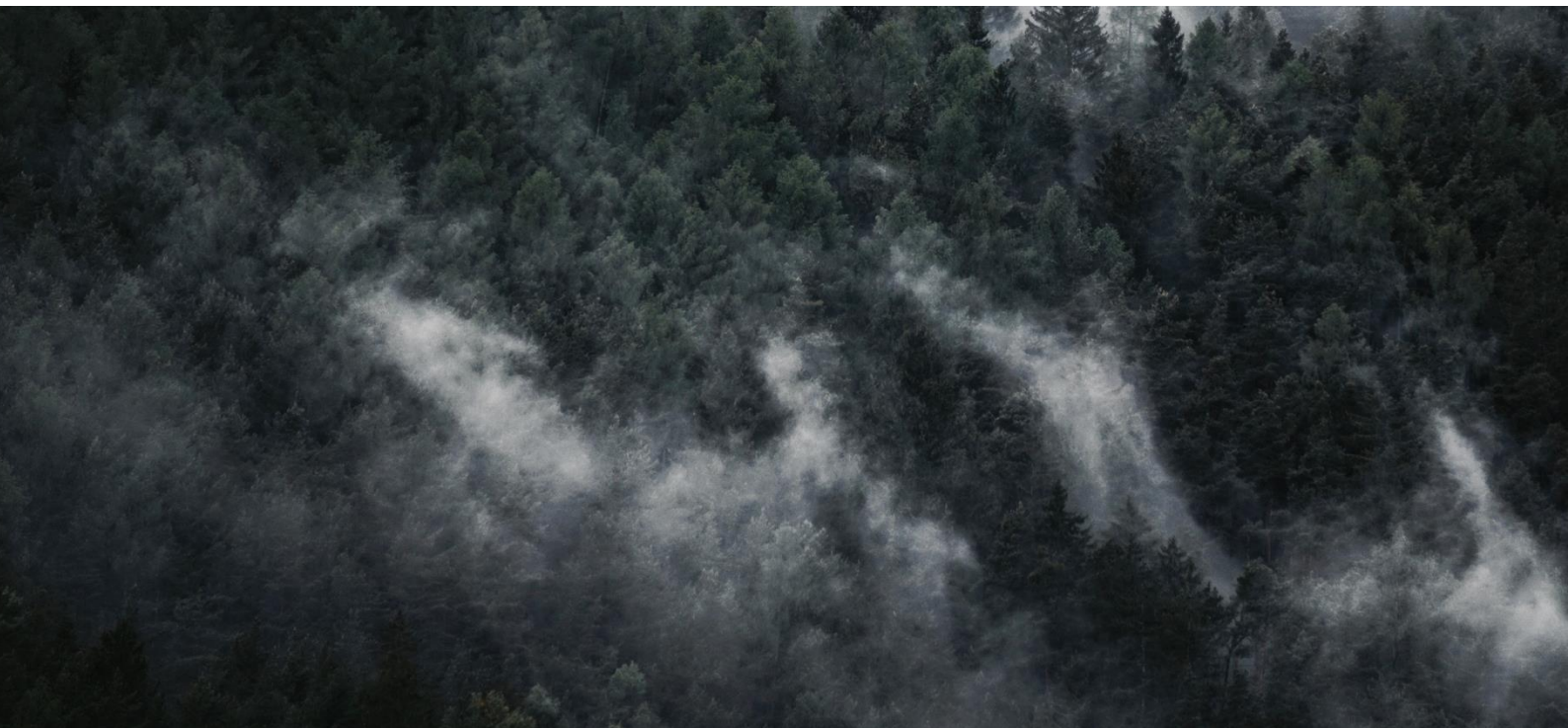




Digital identitetsmanipulasjon



Digital identitetsmanipulasjon: Når deepfakes blir et sikkerhetsproblem for norsk næringsliv

Av Árvakr

Utviklingen innen kunstig intelligens har revolusjonert hvordan vi jobber, kommuniserer og skaper verdi. Men den samme teknologien gir også trusselaktører nye og kraftfulle verktøy. Deepfakes – manipulerte video-, bilde- eller lydopptak som er tilnærmet umulige å skille fra virkeligheten – er ikke lenger et fremtidsscenario. De brukes allerede aktivt i svindel, påvirkning og industrispionasje. For norske virksomheter betyr dette at en av de mest grunnleggende forutsetningene i sikkerhetsarbeid står for fall: **tillit til identitet**.

Et nytt landskap for manipulasjon

Tidligere har sikkerhetsbrudd ofte krevd fysisk tilstedeværelse, teknisk kompetanse eller tydelige spor. Med dagens AI-verktøy kan hvem som helst – også lite sofistikerte aktører – generere troverdige opptak av ledere, ansatte eller samarbeidspartnere på få minutter.

Globalt har vi sett deepfake-svindel der falske direktører beordrer økonomiavdelinger til å overføre millionbeløp, falske HR-samtaler brukes til å hente ut personopplysninger, og manipulerte videomøter benyttes for å skaffe tilgang til sensitiv informasjon. Trusselen er ikke lenger teoretisk – den er operasjonell.

Hvorfor norske virksomheter er særlig utsatt

Norsk næringsliv er preget av høy tillit, flate strukturer og raske beslutningslinjer. Dette er en styrke – men også en sårbarhet. Når kommunikasjon foregår digitalt, blir det vanskeligere å verifisere hvem som faktisk står bak en instruks, en forespørsel eller et møte.

Samtidig opererer mange norske virksomheter i bransjer av stor interesse for utenlandske aktører: energi, maritim teknologi, forsvar, fornybar, forskning og finans. For disse er digital identitetsmanipulasjon ikke bare et økonomisk problem – men et potensielt spørsmål om nasjonal sikkerhet.

Tre fremvoksende trusler virksomheter må ta på alvor

1. Deepfake-basert økonomisk svindel

Kriminelle kan allerede generere troverdige lydopptak av ledere som instruerer økonomiavdelingen til å utføre transaksjoner. Når opptakene kombineres med kjennskap til organisasjonen, kan svindelen være svært vanskelig å avdekke før skaden er skjedd.

2. Identitetsmanipulasjon i videomøter

AI-genererte ansiktsmodeller gjør det mulig å delta i digitale møter som en annen person – med korrekt mimikk, stemme og bakgrunn. Dette skaper nye muligheter for sosial manipulering, industrispionasje og tilgangsfalskning.

3. Omdømmeangrep og informasjonspåvirkning

Manipulerte videoer av ledere kan skape usikkerhet blant ansatte, investorer eller samarbeidspartnere. I et trusselbilde der påvirkningsoperasjoner blir mer sofistikerte, blir deepfakes et effektivt verktøy for destabilisering.

Fra gjenkjenning til verifikasjon – et nødvendig paradigmeskifte

Tradisjonelt har virksomheter stolt på kjente digitale identifikatorer: e-post, telefonnummer, videomøter og intern kommunikasjon. Deepfakes gjør dette utilstrekkelig. I stedet må virksomheter bevege seg mot **verifikasjonsbasert sikkerhet**, der identitet bekreftes gjennom uavhengige mekanismer – ikke magefølelse eller visuell likhet.

Dette krever både tekniske løsninger, nye rutiner og en kulturendring.

Hvordan Árvakr hjelper virksomheter å møte denne trusselen

Árvakr arbeider allerede tett med virksomheter i sektorer der digital manipulasjon kan få alvorlige konsekvenser. Vi tilbyr:

Trusselvurderinger og modenhetsanalyse

Kartlegging av virksomhetens eksponering for identitetsmanipulasjon, spesielt knyttet til økonomi, ledelseskommunikasjon og kritiske funksjoner.

Etablering av verifikasjonsprosedyrer

Utforming av praktiske rutiner for håndtering av instruksjoner, økonomiske beslutninger og digitale møter – inkludert tokenalsverifikasjon, sikker kommunikasjonsflyt og kontrollpunkter.

Opplæring i sosial manipulering og deepfake-gjenkjenning

Ansatte lærer hvordan de mest avanserte manipulasjonene fungerer, hvilke indikatorer de bør se etter, og hvordan de skal reagere.

Simuleringsøvelser og stresstesting

Árvakr kan gjennomføre realistiske scenariobaserte tester som avdekker svakheter og styrker virksomhetens responskapasitet.

Et nytt krav til ledelse og styrever

Det digitale trusselbildet utvikler seg raskere enn tradisjonelle sikkerhetsstrukturer. For styret og toppledelsen betyr dette at digital identitet må ansees som en strategisk risiko på linje med cyberangrep, korrupsjon og leverandørkjedeproblemer.

Selskaper som innfører robuste verifikasjonsrutiner og investerer i kompetanse nå, vil stå langt sterkere enn de som forsøker å håndtere hendelser i etterkant.

En tid for forberedelse – ikke for overraskelser

Deepfakes og digital identitetsmanipulasjon vil prege de neste årene. For norske virksomheter er det avgjørende å handle før teknologien blir utnyttet mot dem. Sikkerhet handler ikke lenger bare om å beskytte systemer – men om å beskytte virkeligheten.

Árvakr stár klar til á bistá virksomheter som ónsker á forstå, forebygge og hándtere denne nye generasjonen trusler. Når identitet kan forfalskes på et øyeblikk, blir sikkerhet et spørsmål om struktur, kultur – og forberedelse.