5 OMRÅDER DIN VIRKSOMHET KAN LIGGE FORAN TRUSSELBILDET

MÅLRETTEDE SVINDELFORSØK FREMSTÅR TROVERDIGE

Med nok tid, nok informasjon fra nett og samarbeid på tvers av grenser kan svindlere kartlegge virksomheten nøye og sende troverdige hendvendelser med godt språk.

- ☐ Kartlegg virksomhetens trusselbilde slik at ansatte er bedre rustet til å avsløre svindelforsøk.
- ☐ Ha klare regler og rutiner rundt transaksjoner. Sentrale spørsmål er: Hvordan kan kontonummer endres på en trygg måte? Hvilke kommunikasjonskanaler er trygge nok? Hvor mange og hvem må godkjenne endringen?

USIKRE UNDERLEVERANDØRER

Underleverandører med lavt nivå av sikkerhet benyttes som en inngang til det egentlige målet.

- ☐ Sørg for å vurdere risiko når man velger leverandører som får tilgang til viktig informasjon. Vurder både leverandøren OG landet den opererer i for å sikre deg at informasjonen blir tatt vare på.

NÅR ER DET NOK MAKSINER OG ENHETER?

Det blir stadig flere enheter og selv i kjente produkter oppdages svakheter og sikkerhetshull.

- ☐ Hold oversikt over all maskinvare som brukes i virksomheten og etabler et system for å regelmessig oppdatere programvare, operativsystem og firmware.
- ☐ Utsatte virksomheter bør vurdere risikoen i private enheter som brukes i arbeidsammenheng. Hvilke arbeidsoppgaver kan trygt utføres fra private maskiner? Hvilke oppgaver kan ikke?

DATAKOMPROMITTERING KAN KOSTE MER ENN OMDØMME

Uansett om datalagringen håndteres av virksomheten selv eller en leverandør er det viktig å vurdere sikkerheten i lagringen. Personvernlover håndheves strengere og uansvarlig datalagring kan få enda større konsekvenser enn tidligere.

- ☐ Still krav til skyleverandør og velg en leverandør som tilfredstiller dine krav til tilgjengelighet, sporbarhet og kontrollmekanismer.
- ☐ En komplett backuprutine reduserer risiko på mange områder. Både utilsiktede feil og alvorlige dataangrep kan føre til tap av data og en god backuprutine reduserer konsekvense betydelig. Test at backuprutinen fungerer ved å tilbakerulle IT-systemer jevnlig.

BENYTT MER ENN PASSORD

Mange bruker samme passord på tvers av tjenester, og mange passord blir skrevet ned slik at «nestemann» får logget inn. Her finnes det enkle løsninger som styrker sikkerheten betraktelig.

- ☐ Unngå kompromitterte brukere og e-poster ved å styrke autentiseringsprosessen:
  - Bruk 2-faktor autentisering med mobil eller annen enhet.
  - Bruk biometrisk data, som fingeravtrykk eller øyeskanning.¨