IT-sikkerhet i regnskaps-systemer

Bilde: Stockbilder

Hans Ellefsen

Direktør teknologi, innovasjon og bærekraft

REGNSKAP NORGE

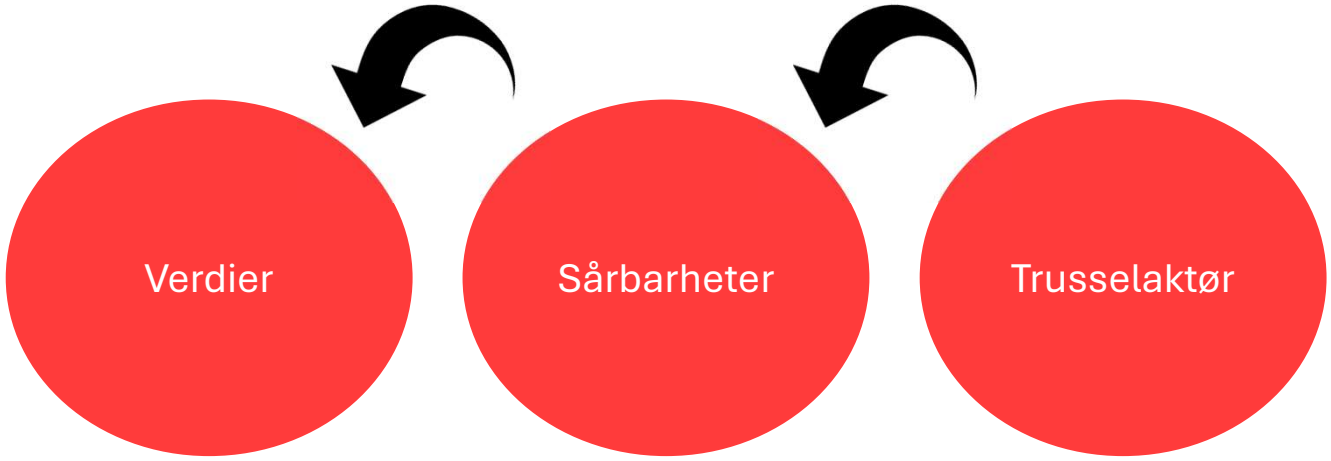

«JEG HAR SYSTEMENE MINE I SKYEN. LEVERANDØRENE HAR SIKKERHETS-REVISJONER. DA HAR JEG IVARETATT SIKKERHETEN PÅ EN GOD MÅTE»
Sitat: CFO som liker å leve farlig!

ERP-systemenes sentrale rolle

- ERP-systemer håndterer kritiske forretningsfunksjoner og utgjør den digitale ryggraden i organisasjoner, avgjørende for stabil drift
- Regnskapssystemer inneholder verdifulle data som kan misbrukes til svindel og økonomisk kriminalitet
- Vi opplever økende sikkerhetsutfordringer
- Økt digitalisering og skyintegrasjon utvider ERP-systemenes angrepsflate og krever derfor omfattende sikkerhetstiltak
- Vi må ha en helhetlig sikkerhetstilnærming
- Effektiv IT-sikkerhet kombinerer tekniske, organisatoriske og juridiske tiltak, inkludert risikovurderinger og opplæring

Bilde: Stockbilder

Hva er problemstillingen?



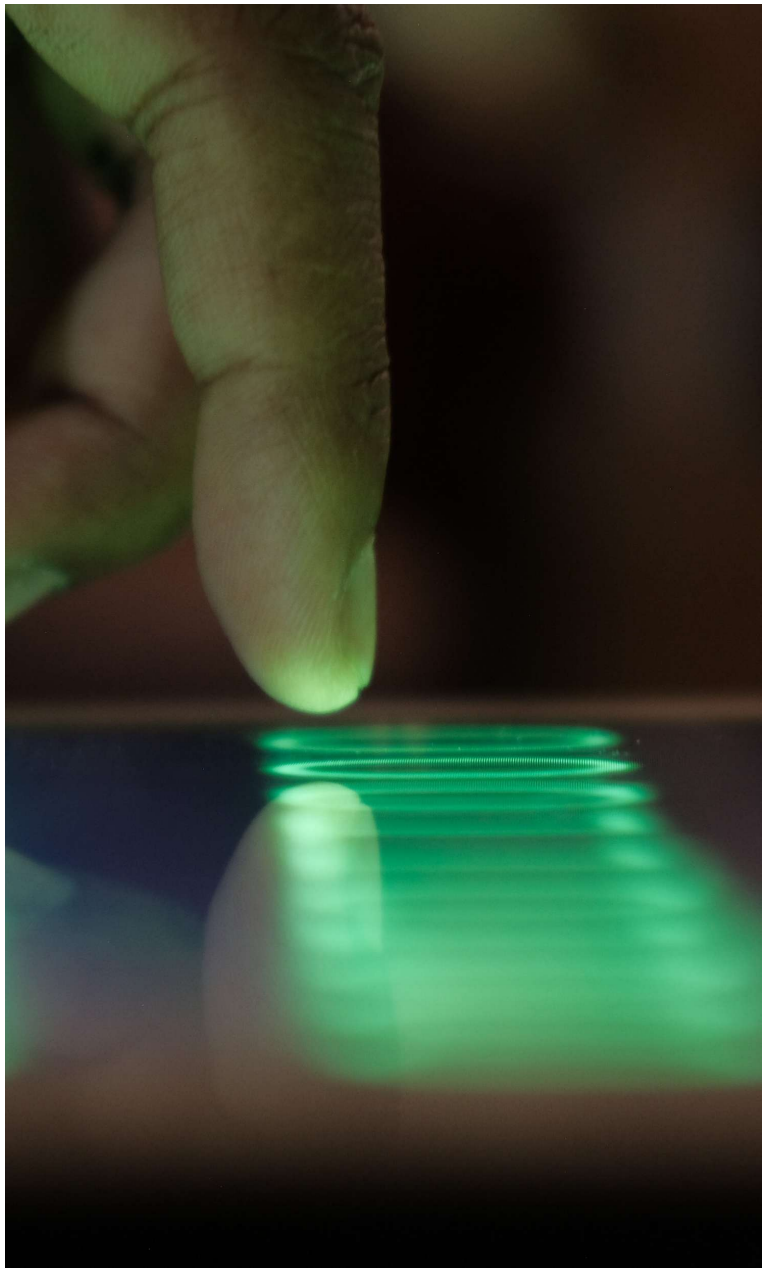
Økende cybertrusler

- Cyberkriminalitet rettet mot ERP-systemer øker gjennom avanserte angrep, spesielt mot regnskapsvirksomheter og andre som forvalter verdier
- Vanlige angrepsmetoder er phishing, sosial manipulering, løsepengevirus og innsidertrusler. CaaS – Crime as a Service kjøpes på darkweb. Aktørene har til og med support og penger-tilbake-garanti!
- En betydelig andel av databrudd skyldes menneskelige feil og det tar lang tid å oppdage databruddet, noe som understreker viktigheten av opplæring

Bilde: Stockbilder

Risikodeling?

- Systemleverandører tar sjelden ansvar for sikkerhetsbrudd i løsningene
- Det er brukers ansvar å konfigurere og følge opp sikkerheten på en god måte
- Systemleverandør tar kun ansvar for angrep på egne serverparker og infrastruktur

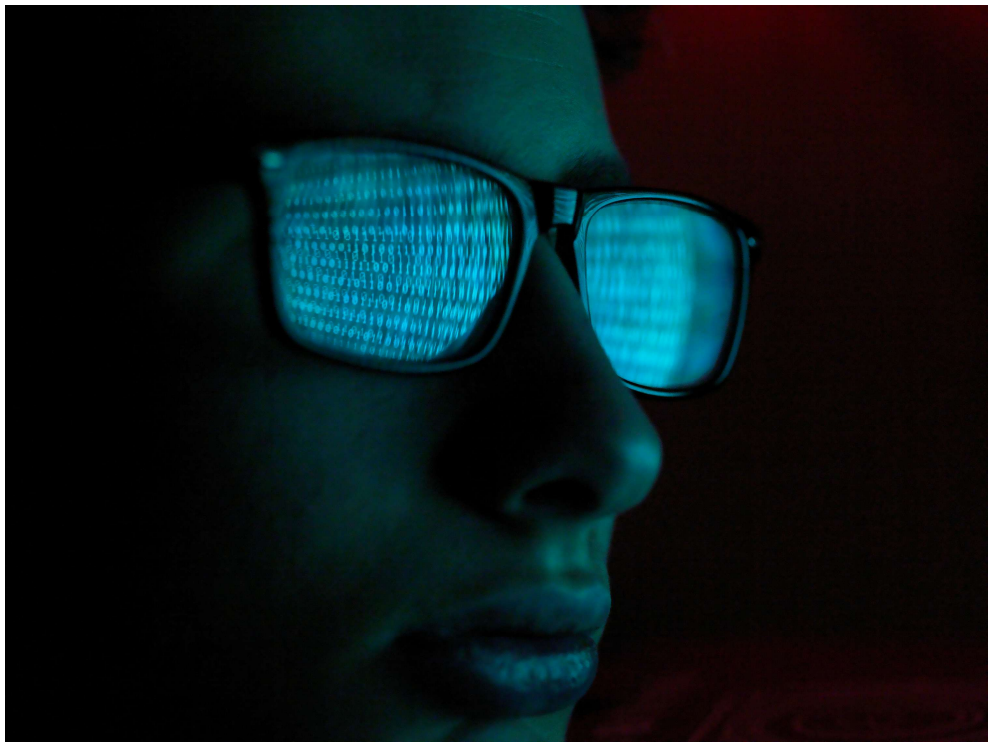


Grunnprinsipper innen IT-sikkerhet

- **Konfidensialitet** – Data er kun tilgjengelige for autoriserte personer
- **Integritet** – Dataene skal være korrekte og ikke endret uautorisert
- **Tilgjengelighet** – Dataene skal være tilgjengelige når de trengs

Bilde: Stockbilder

Risikovurdering



- Hvilke verdier skal vi beskytte?
- Hva er sannsynlige sårbarheter?
- Regelmessige sikkerhetsvurderinger identifiserer risiko og sårbarheter i ERP-systemer for å forhindre brudd.
- Implementer grunnprinsippene om konfidensialitet, integritet og tilgjengelighet for å sikre robust IT-sikkerhet.
- Følg NSMs grunnprinsipper for IKT-sikkerhet for å redusere risiko.
- Behandle IT-sikkerhet som en kontinuerlig prosess som involverer hele organisasjonen og spesialister.

Bilde: Stockbilder

Hva virker teknologisk?

- **Sterk autentisering**: Multifaktor-autentisering (MFA) og biometriske løsninger.
- **Kryptering**: Beskyttelse av data både i lagring og overføring.
- **Oppdateringer og patching**: Reduserer teknisk gjeld og lukker sårbarheter. Dette blir mindre viktig å passe på ved økt bruk av skytjenester som oppdateres løpende
- **Zero Trust-arkitektur**: Streng tilgangsstyring og kontinuerlig verifisering

Nærmere om Zero Trust

- Zero Trust innebærer at ingen brukere eller enheter får automatisk tillit, selv innenfor virksomhetens nettverk. Aldri stol på, alltid verifiser! Minste privilegiums prinsipp
- Krever flerfaktorautentisering, rollebasert tilgangsstyring og kontinuerlig overvåking av brukeraktivitet.
- Sikrer at kun autoriserte brukere får tilgang til sensitive data, med logging og revisjon av tilgangshistorikk.
- Bruk av identitets- og tilgangsstyringsverktøy integrert med ERP-systemer gir bedre kontroll og reduserer risiko.

Bilde: Stockbilder

Fordeler med skybaserte ERP-systemer

- «End-game» er public cloud-løsninger hvor programvare, databaser og infrastruktur deles mellom alle brukere
- Skybaserte ERP-systemer gir skalerbarhet, fleksibilitet og kostnadseffektivitet ved bruk av plattformer som Azure, AWS og Google Cloud
- Utfordringer med multisky-arkitektur og «Composable ERP»
  - Bruk av flere skyplattformer øker kompleksiteten og gjør det vanskeligere å ha oversikt over og håndtere datalagring og sikkerhet
  - Med Composable ERP vil mange systemelementer kommunisere med hverandre, herunder med bruk av AI-agenter
- Sikkerhet og etterlevelse
  - Riktig konfigurasjon og vedlikehold av sikkerhetsinnstillinger er avgjørende for å overholde Digitalsikkerhetsloven, NIS2, DORA, GDPR mv
- Sikkerhetskopiering og datastyring
  - Effektiv sikkerhetskopiering og gjenopprettingsrutiner, samt sikring av datalagring innenfor EU/EØS, er viktig for risikostyring

Fremtidens utfordringer innen IT-sikkerhet

- De kriminelle bruker avansert AI i sine angrep, vi må svare med AI-baserte sikkerhetssystemer og håpe at vi ikke henger etter
- Skybaserte ERP-løsninger gir i utgangspunktet lavere risiko enn proprietære systemer, men krever riktig konfigurasjon og brukeradministrasjon.
- AI og automatisering endrer regnskapsrollen og introduserer nye sikkerhetsutfordringer.
  - Prompt-inserts i AI-agenter
  - Falske fakturaer glir lettere igjennom?
- Økende krav til leverandørstyring og kontroll av tredjepartsrisiko i en integrert systemverden.

Etterlevelse av GDPR – personopplysninger i regnskapsmaterialet

- GDPR krever sikker og lovlig behandling av personopplysninger, og begrenser overføring av data utenfor EU/EØS uten gyldig overføringsgrunnlag
- Hvor er dataene mine?
- Hvem har tilgang til dataene?
- Kan AI-agenter få tilgang til personopplysninger som de ikke skulle hatt?
- Bokføringsregelverket krever lagring og tilgjengelighet av regnskapsmateriale. Overstyrer til dels GDPR

Viktigheten av beredskap

- Beredskap sikrer kontinuitet i virksomheten ved sikkerhetshendelser gjennom dokumenterte og testede planer.
- Tydelige sikkerhetskopi-rutiner og rask gjenoppretting av data er avgjørende for å beskytte mot datatap og driftsavbrudd.
- Egenutviklede ERP-systemer på egne servere øker risikoen og krever ekstra oppmerksomhet for sikkerhetskopiering og gjenoppretting
- Skybaserte løsninger har ofte innebygde sikkerhetskopi-funksjoner, men det er viktig å verifisere at de fungerer som forventet
    - Kan også være betalbar tjeneste som må bestilles


RN
REGNSKAP
NORGE