Hva betyr «Just-in-time» privileger for driftspersonalet?

- Sivilingeniør **Imran Mushtaq** har vært involvert i prosjekter med meget høy grad av teknisk kompleksitet som krever lang erfaring og dyp kompetanse
- Har gjort alt fra programmeringsoppgaver til å lede større offshore team og gi råd på mer strategisk nivå.
- Epost: imr@a-2.no / Mobil: +47 93841638

Om A-2 (http://www.a-2.no)

- Ca. 50 konsulenter
- I snitt har hver av oss over 20 års erfaring fra å lede store, komplekse IT-prosjekter. Operativ erfaring.
- Ca. 10 konsulenter innen teknologi rådgivning/arkitektur
- Vi ansetter nå også folk med IT-sikkerhetskompetanse

Tema for foredraget

- Brukere med privilegier er yndlingsmål
- Tilgang til sensitive opplysninger i målsystem
- Identitet og tilgangsstyring (IAM) og Privilegert tilgangsstyring
  - Kontohvelv vs Just-in-time tilganger
  - Styring av privilegerte tilganger
  - PAM praksis

Brukere med privilegier - ER privilegerte MÅL

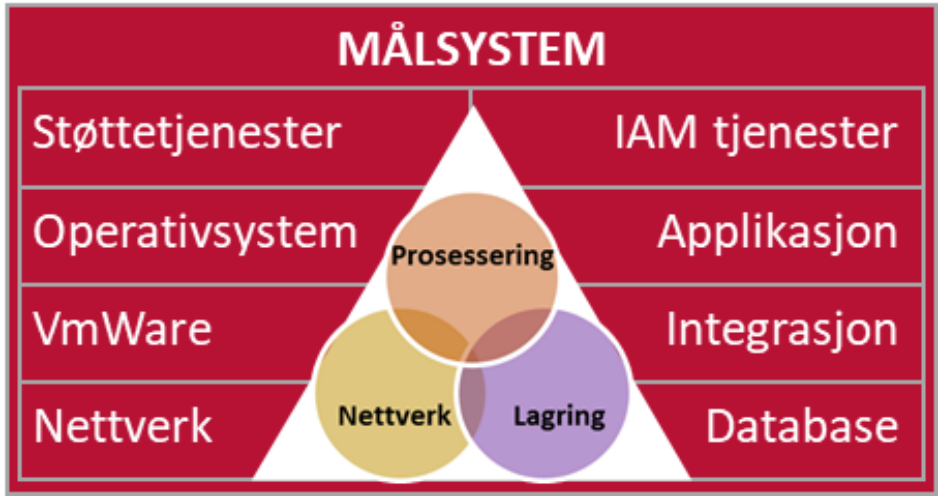
- Brukere med administrative rettigheter er blant de som får målrettet angrep mot seg.
- En driftsressurs opparbeider seg gjerne mange privilegier over tid. Risiko?
- Hva slags praksis og rutiner bør en drifts-organisasjon etablere for å øke datasikkerheten?
- Bør privilegerte tilganger begrenses?

Brukere med privilegier - kun «Just-in-time»?

- I et konsern med tusenvis av sluttbrukere, er det nødvendig med tiltak for også å beskytte seg mot dem som skal beskytte IT systemene.
- Er «Just-in-Time» privilegier et levedyktig modell og en god fremtidig kultur i en driftsorganisasjon?

Tilgang til sensitive opplysninger – Kontroll med målsystem!

- Tilstrekkelig kontroll på HVEM som har gjort HVA og NÅR og i henhold til hvilke tjenstlig behov!
- Redusert sikkerhetsrisiko for uautorisert tilgang til sensitive opplysninger i MÅLSYSTEM!
- Beskytte målsystem fra de som har privilegerte tilganger!



Ha kontroll med de som kontrollerer MÅLSYSTEM eller de som angriper brukere med privilegier!

Tilgang til sensitive opplysninger - Sikkerhetsutfordringer

- **Brukere** med privilegerte tilganger har rettigheter til å kunne se sensitiv info
- Manglende oversikt over hvem som har hvilke tilganger, manglende sporbarhet og manglende oversikt over **misbruk**
- Manglende kontroll på hvem som har tildelt/godkjent privilegerte tilganger
- Manglende rutiner for tilgangsstyring

According to the Verizon 2012 Data Breach Investigations Report, 69 percent of confirmed security incidents were perpetuated by insiders, which represents a 300 percent increase between 2011 and 2012.

In this particular Fannie Mae incident, there are a few things that went wrong, any one of which could have prevented the breach if addressed:

- Too many people shared the UNIX root account with no individual accountability
- There was no concept of 'least privilege' access associated with the administrative account. Every administrator had access to the full power of the administrative credential, even capabilities that were far outside the scope of their responsibilities
- There was no mechanism in place to audit or watch what administrators do with their rights
- There was no concept of governance for privileged accounts
- There was no mechanism to find and remove instances of permissions that exceeded those appropriate for an individual's role

Tilgang til sensitive opplysninger Sikkerhetsutfordringer

- **Behov**: Sørge for at rett person har den rette tilgangen til den rette ressursen på rett tid for det rette formålet.
- Prinsipp om "**minste privilegium**" for privilegert tilgang
- Unngå sikkerhetsrisiko ved overdreven eller upassende tilgang
- Privilegert tilgangsstyring (PAM) brukes for å kontrollere de som kontrollerer!

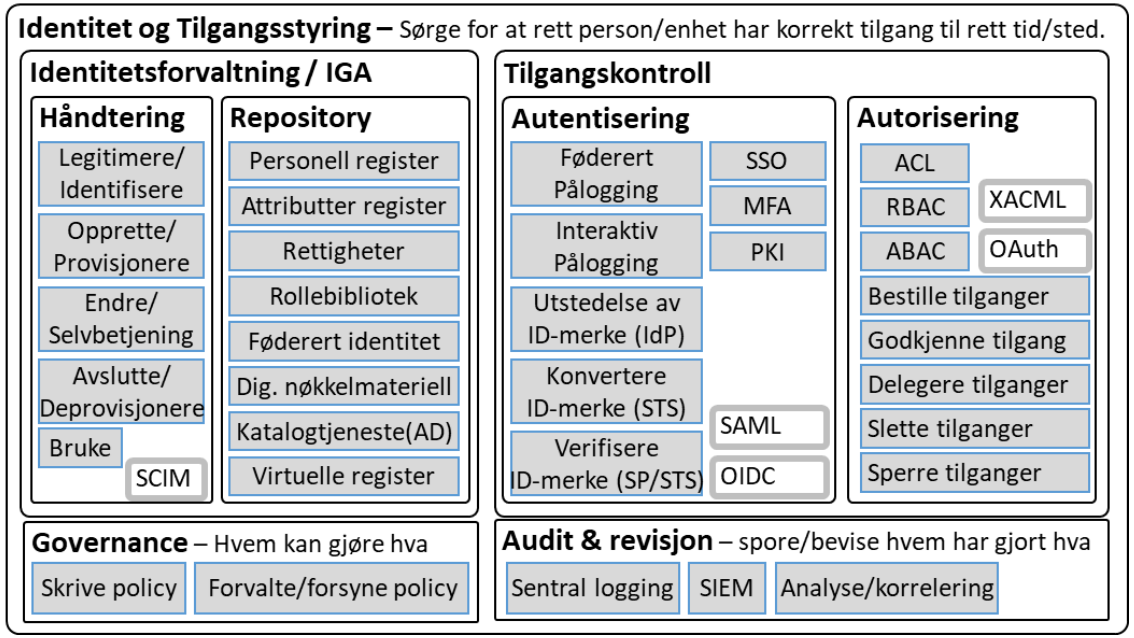
According to the Verizon 2012 Data Breach Investigations Report, 69 percent of confirmed security incidents were perpetuated by insiders, which represents a 300 percent increase between 2011 and 2012.

In this particular Fannie Mae incident, there are a few things that went wrong, any one of which could have prevented the breach if addressed:

- Too many people shared the UNIX root account with no individual accountability
- There was no concept of 'least privilege' access associated with the administrative account. Every administrator had access to the full power of the administrative credential, even capabilities that were far outside the scope of their responsibilities
- There was no mechanism in place to audit or watch what administrators do with their rights
- There was no concept of governance for privileged accounts
- There was no mechanism to find and remove instances of permissions that exceeded those appropriate for an individual's role

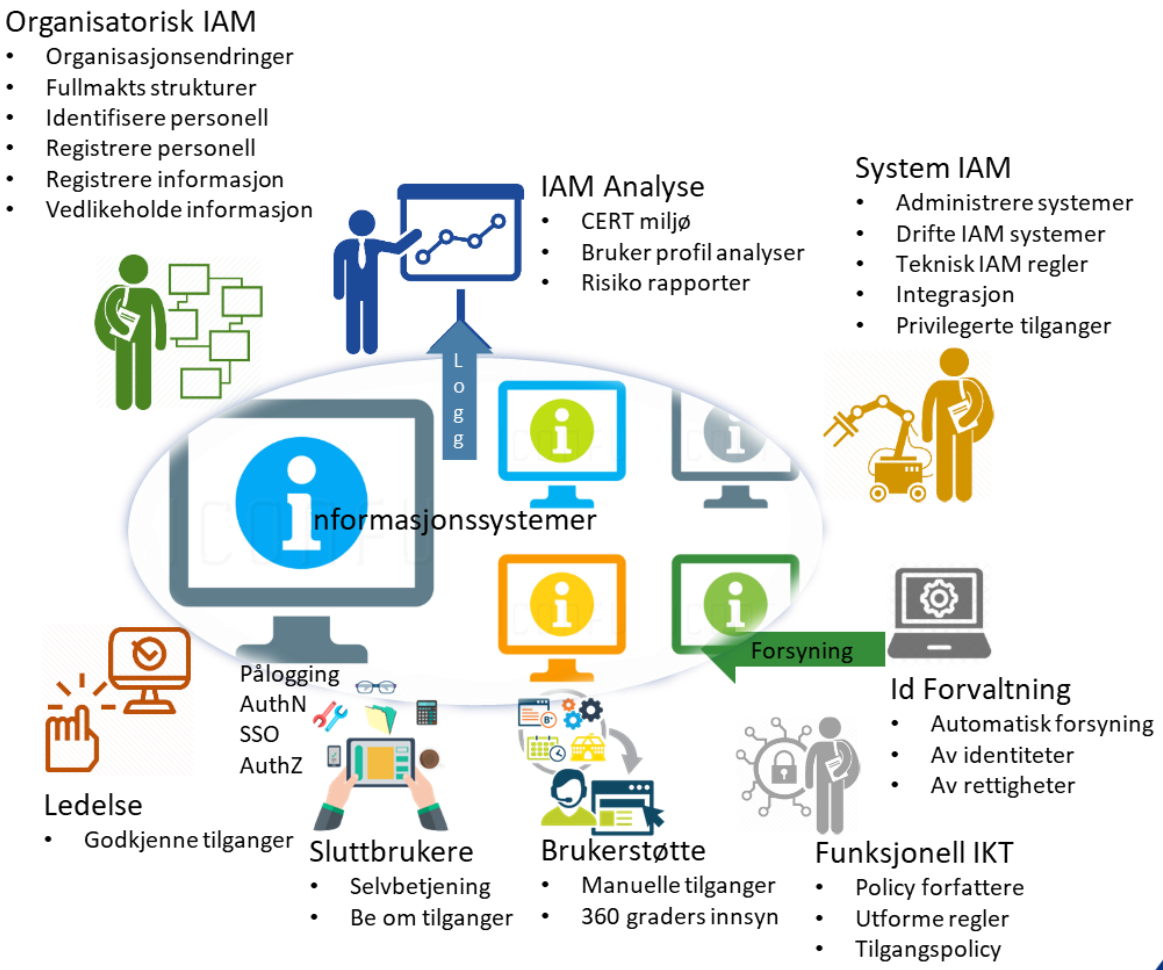
Identitet og tilgangsstyring (IAM) - Rammeverk

- **IAM** handler om å tilrettelegge med **teknologi** og **prosedyrer** for at brukere kan få **tilgang** til
  - data/informasjon og tjenester
- via applikasjoner og eller systemer på en **enkel** og **sikker** måte.
- Det skal være **tillitt** til **bruk** av data/informasjon og tjenester.
- Det påvirker hele livssyklus for **identitetsforvaltningen** og mekanismer for **tilgangskontroll** og **sporing**.



Identitet og tilgangsstyring (IAM) – Livssyklusen med rettigheter til informasjonssystemer

- Hvordan sikre at relevant personell får tilgang til relevant informasjon til riktig tid med riktig brukerkonto, og at denne aktiviteten overvåkes, logges og kontrolleres.
- Viktig at sensitiv informasjon ikke blir kompromittert.
- Enkel og brukervennlig forvaltning for tildeling av tilganger.



Identitet og tilgangsstyring (IAM) – Styring av privilegerte konto!

- Privilegerte tilganger er ekstraordinære rettigheter som har betydelig høyere sikkerhetsrisiko sammenlignet med ordinær sluttbrukertilgang.
- Handlinger utført med privilegerte tilganger skal være entydig sporbart tilbake til person med gitt identitet og knytning til gitt rolle i arbeidsforholdet.

Privilegert tilgangsstyring (PAM)

- **Passordhvelv** – Er det løsningen?
- Automatisk passord rotasjon?
- Logging og sesjonsopptak?
- Felles løsning og inngangsportal for drift?
- Etablere egnet infrastruktur for PAM?

According to the Verizon 2012 Data Breach Investigations Report, 69 percent of confirmed security incidents were perpetuated by insiders, which represents a 300 percent increase between 2011 and 2012.

In this particular Fannie Mae incident, there are a few things that went wrong, any one of which could have prevented the breach if addressed:

- Too many people shared the UNIX root account with no individual accountability
- There was no concept of 'least privilege' access associated with the administrative account. Every administrator had access to the full power of the administrative credential, even capabilities that were far outside the scope of their responsibilities
- There was no mechanism in place to audit or watch what administrators do with their rights
- There was no concept of governance for privileged accounts
- There was no mechanism to find and remove instances of permissions that exceeded those appropriate for an individual's role

Sikkerhets-Utfordringer

Privilegert tilgangsstyring (PAM)

- Etablere helhetlig eierskap til driftsløsning?
- Organisere og forbedre prosesser for tildeling, godkjenning og revokering av privilegerte tilganger
- Etablere rutiner og beste praksis for bruk av privilegerte tilganger

According to the Verizon 2012 Data Breach Investigations Report, 69 percent of confirmed security incidents were perpetuated by insiders, which represents a 300 percent increase between 2011 and 2012.

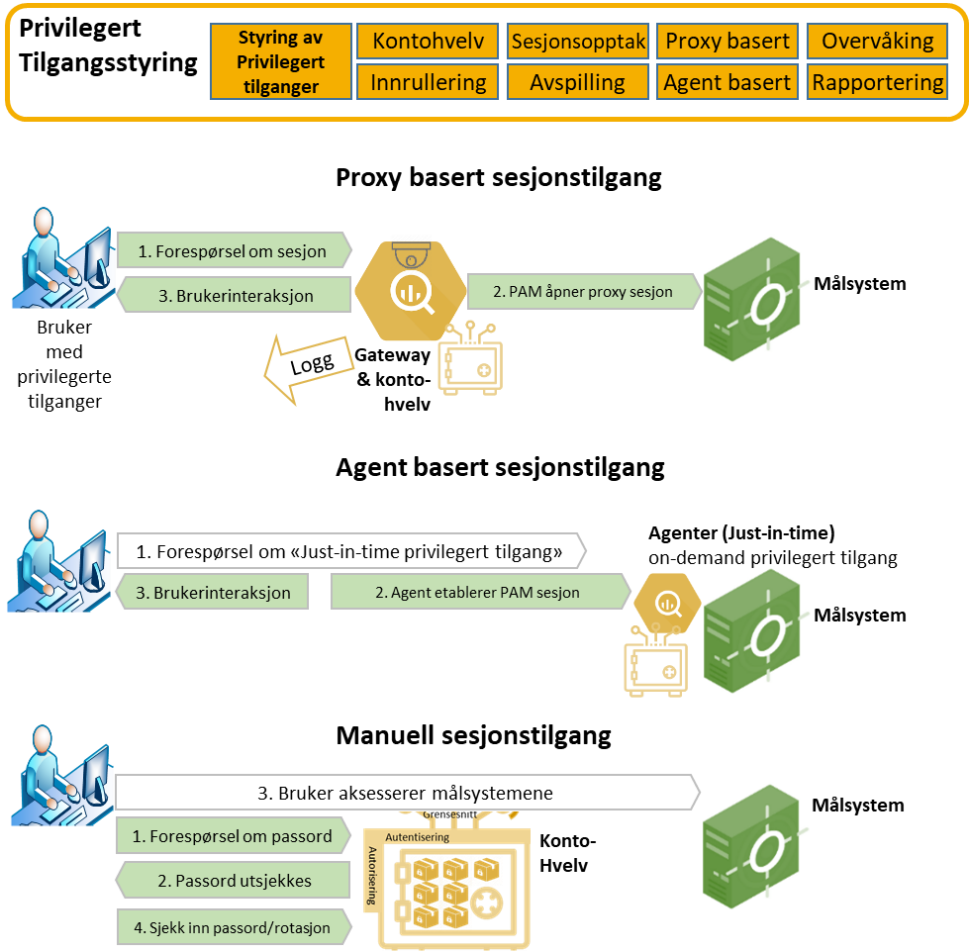
In this particular Fannie Mae incident, there are a few things that went wrong, any one of which could have prevented the breach if addressed:

- Too many people shared the UNIX root account with no individual accountability
- There was no concept of 'least privilege' access associated with the administrative account. Every administrator had access to the full power of the administrative credential, even capabilities that were far outside the scope of their responsibilities
- There was no mechanism in place to audit or watch what administrators do with their rights
- There was no concept of governance for privileged accounts
- There was no mechanism to find and remove instances of permissions that exceeded those appropriate for an individual's role

Sikkerhets-Utfordringer

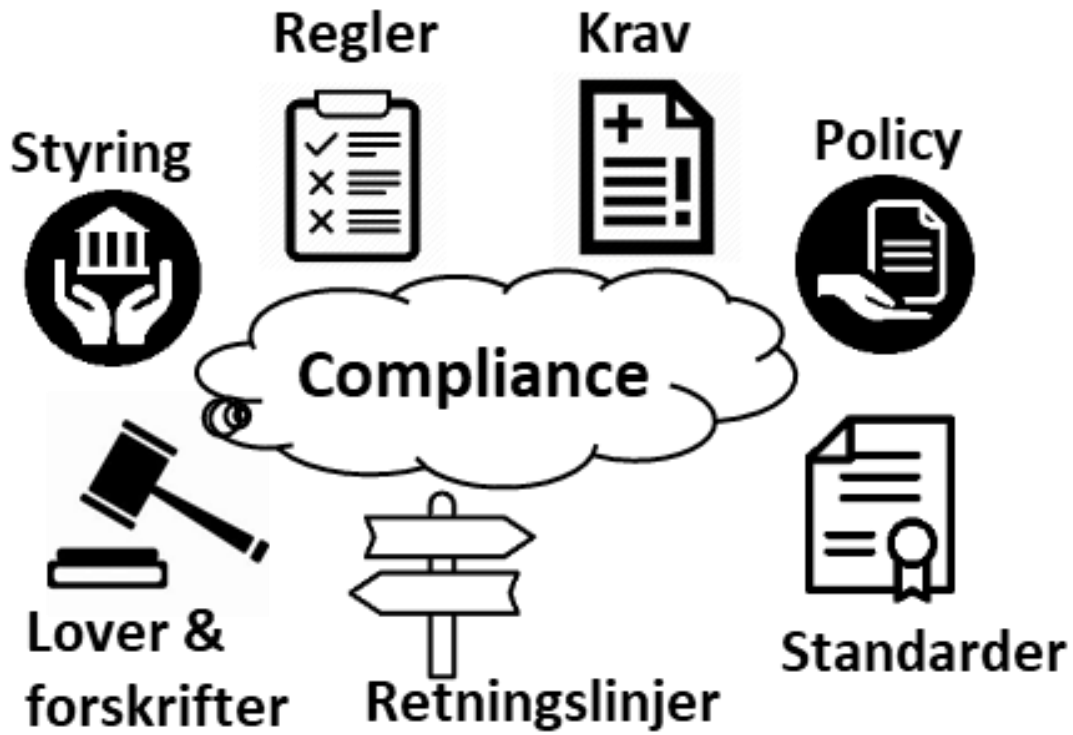
Privilegert tilgangsstyring med kontohvelv eller JIT?

- Forvaltning av privilegerte tilganger er stort fagområde, som både omfatter selve PAM-produktet med omkringliggende infrastrukturkomponenter, kombinert med prosesser/rutiner nødvendig for å tilby helhetlig sikkerhetsløsning



Styring («Governance») av privilegerte tilganger

- Opplæring i henhold til beste praksis
- God forankring og bevisstgjøring
- Policy forvaltning og håndhevelse
- Følge lover og forskrifter
- I henhold til standarder
- Oppføling av brukere med privilegier
- Sesjonsopptak og avspilling
- Revidering (audit)
- Rapportering (Hvem/hva/når)



PAM praksis/ Governance

- **Formålet** med PAM kan kun oppnås når gode prosesser og praksis blir håndhevet i organisasjonen med god støtte fra effektive PAM-produkt.
- **Oppnådd verdi**: Kun gjennom automatisering, delegering, økt pålitelighet og integrasjon med andre verktøy i virksomheten som ITSM, IdM, autorisering osv
- **Utfordring**: Fullstendig oppdagelse og forvaltning av privilegerte tilganger er en stor utfordring. Er det bedre med JIT enn kontohvelv?
- Det å administrere risiko for privilegerte tilganger er nesten umulig uten spesialisert PAM produkt, men innføring av PAM produkt medfører økt flate for potensielle angrep. PAM medfører at selve sikkerhetsrisikoen kan blir redusert!

PAM praksis/ Governance

- Ledelsen bør bygge opp en moden PAM praksis som fokuserer på organisasjon/medarbeidere og prosesser.
  - Krever mye innsats fra medarbeidere og de prosesser de følger for å adressere PAM utfordringen
  - Viktig å få etablert prosesser og prosedyrer som adresserer PAM risiko
  - Viktig å få etablert prosesser for å identifiserer alle privilegerte brukerkonti og eiere av disse i hele IKT infrastrukturen.
  - Anskaffet og installert PAM produkt skal implementeres for å **understøtte** etablerte prosesser og prosedyrer
  - **Forventningsstyring**: PAM produkt er ikke noe magisk erstatning for klar PAM visjon, praksis og prosesser!!!!

Hva betyr «Just-in-time» privileger for driftspersonalet?

- Sivilingeniør **Imran Mushtaq** har vært involvert i prosjekter med meget høy grad av teknisk kompleksitet som krever lang erfaring og dyp kompetanse
- Har gjort alt fra programmeringsoppgaver til å lede større offshore team og gi råd på mer strategisk nivå.
- Epost: imr@a-2.no / Mobil: +47 93841638