

Sikkerhetserklæring JOINT ProsjektHotell®

JOINT erkjenner og forstår at informasjon, innhold og annen informasjon som ligger på JOINT ProsjektHotell er absolutt kritisk for din bedrift.

Vi tar ansvaret med å levere deg en pålitelig, sikker arbeidsplass meget alvorlig. Vi har lagt stor vekt på å sikre at ditt innhold alltid er tilgjengelig og sikret.

Applikasjonssikkerhet

Grunnstrukturen i JOINT ProsjektHotell er selve Documentum eRoom applikasjonen. På grunn av den sentrale bruken av applikasjonen som et felles arbeidsområde med lagring av felles informasjon, dokumenter, filer, tegninger osv må Documentum eRoom programvaren levere størst mulig sikkerhet. Documentum eRoom produktet har innebygd sikkerhet på mange områder:

- **Brukernavn og passord**
På det høyeste nivået leverer Documentum eRoom tilgangskontroll med begrenset tilgang bare til de som har gyldig brukernavn og passord. Passordet er kryptert og selvvalgt. Det er bare kjent for den som har valgt passordet. Tilleggssikkerhet er at passordet må være minst 8 tegn.
- **Tilgangskontroll på objektnivå**
Documentum eRoom applikasjonen gir også kontroll over tilgangsnivået (f eks bare lese eller også skrive tilgang) som hvert prosjektmedlem har til enkelt informasjon i prosjektet. Tilgangskontroll på objektnivå gjør det mulig å lage grupper av brukere for å raskt implementere tilgangsstrategier. Bruker du for eksempel tilgangskontroll på objektnivå og etablerer en gruppe (f.eks. Personal), kan du lage en sikkerhets strategi som gir alle medlemmer av Personal avdelingen redigeringsmulighet i en mappe, samtidig som andre medlemmer kun har lese mulighet i samme mappen.
- **Avansert identifisering**
Documentum eRoom Enterprise løsning kan bli knyttet opp mot avanserte autentiseringsløsninger som VPN, ekstranett eller "internt" nettverk. Kraftig autentisering via kodekalkulator er også en opsjon.
- **Kryptering av dataoverføringer via SSL**
For å sikre at data ikke blir fanget opp eller "sniffed" blir alle dataoverføringer mellom server og brukerens maskin kryptert ved hjelp av Secure Sockets Layer (SSL). Dette skjer før brukeren har logget seg inn på Documentum eRoom. Disse elementene arbeider sammen for å levere en god sikkerhet for all informasjon og materiale på ditt prosjektområde hos JOINT ProsjektHotell.

Driftsmiljøet

I tillegg til selve Documentum eRoom applikasjonens innebygde sikkerhet leveres det også ekstra nettverks- og serversikkerhet i driftsmiljøet med vår driftspartner Basefarm AS. Alle JOINT ProsjektHotell servere står i et sikkert datasenter med:

- 19" dataskap m/ konsollswitcher
- 3 nivåer med adgangskontroll
- Video-overvåking
- Alarmsystem
- Redundant kjøling
- Klimakontroll
- Branneteksjon m/tidlig varsling
- Gass-slukkeanlegg
- Redundant strømtilførsel
- UPS/Batteribackup og Nødstrømsgenerator

Driftsmiljøets datasentre er lokalisert i anonyme industribygg. Logoer eller andre effekter som kjennetegner vår driftspartner eksisterer ikke ved bygget. Terrenget rundt er formet slik at det er liten fare for flom. Bygningene er solide, og vi har vurdert innbruddsfaren som liten. Bygningene har montert alarmsystemer for å kunne detektere forsøk på innbrudd i god tid før de sensitive områdene av lokasjonen blir nåbare.

Lokasjonene er plassert bak flere massive ståldører som er tilkoblet et alarmsystem som overvåkes 24 timer i døgnet gjennom driftspartners driftssentral. Adgang til datasentrene gis kun til personell med spesielt behov, og da med påkrevet forhåndsgodkjenning. Adgangskort og kode er også påkrevet til enhver tid. Service teknikere og eventuelt annet personell gis kun adgang i følge med autorisert personell.

Alle ansatte hos vår driftspartner underskriver standard taushetserklæring. Dette omfatter eventuell tilgang til kundedata. Vår driftspartners ansatte har begrenset innsyn/rettigheter/tilgang til kundedata avhengig av brukere/brukergrupper, som igjen bestemmes av hvilken funksjon de har.

Datasenteret overvåkes 24 timer i døgnet, 365 dager i året, gjennom driftspartners vaktordning. I vaktordningen er det til enhver tid høyt kvalifiserte fagmedarbeidere med lang erfaring innen områdene nettverk, operativsystemer og applikasjoner. Tilknytning mot Internett er robust og består av eksempelvis redundant 10 Gbps forbindelse mot NIX samt redundante forbindelser mot ulike leverandører for generell internett trafikk. I tillegg har vi redundant samtrafikk mot enkelte større aktører i Norge.

For Documentum eRoom-applikasjonen benyttes Win 2003 server og IIS som plattform. Oppfølging av sikkerhetspatcher osv. skjer løpende iht. innarbeidede rutiner. Antivirusløsning støttet av Documentum eRoom er implementert.

Driftspartner har et kvalitetssystem basert på ISO 2001. Prosessene som inngår i tjenesteleveransen er i tillegg basert på ITIL.

Filserver

Lagring av filer på eRoom/Prosjekthotell skjer til en HP MSA 500 (SCSI diskhylle) som er koblet opp med full redundans. Selv om en komponent går i stykker vil fortsatt alt være tilgjengelig. Dette gir også JOINT muligheten til å legge til mer plass ved behov uten krav til nedetid.

SQL Server

Som SQL server benyttes Microsoft SQL 2005. Denne er installert på 64 bits Microsoft 2005 Server R2 for å kunne utnytte mer RAM enn man vil kunne på et 32 bits operativsystem. Hele SQL løsningen er også satt opp i cluster, noe som betyr at om databaseserveren går ned så vil en ny server automatisk ta over.

Lokalt nettverk

Alle nettverksforbindelser lokalt, herunder tilknytning til alle maskiner, har en kapasitet på 1 Gbps eller høyere. Alle kantswitcher er redundant tilkoblet kjernenettet.

Firewall

ProsjektHotell plattformen er implementert bak driftspartners brannmurtjeneste (firewall) som er basert på redundante brannmurer (firewall) levert av en anerkjent leverandør. Det er implementert unike regelsett for brannmuren og policies basert på de sikkerhetskrav ProsjektHotellet stiller. Driftspartner vil være ansvarlig for all drift, vedlikehold og overvåking av brannmuren. Brannmurtjenesten er implementert i en fullt redundant cluster løsning for å oppnå høy tilgjengelighet for ProsjektHotellets brukere.

Backup & Restore

Backuptjenesten for ProsjektHotell plattformen består av en avansert tolagsarkitektur basert på backup til disk med videre backup til bakenforliggende tape eller disklager. Denne tolagsarkitekturen gir vesentlig kortere backup- og restoretider. Backupsystemet er lokalisert på en annen adresse, hvilket betyr at så snart det er tatt backup er disse dataene lagret utenfor produksjonslokalet.

Vi har i tillegg følgende omfattende backup rutiner:

- inkrementell backup utføres to ganger daglig (kl. 12:00 og 24:00)
- slettede/endrede filer lagres i 30 dager

eRoom/ProsjektHotell har en egen versjonskontroll (track versions) av filer. Hver enkelt versjon av filen i eRoom lagres som en enkeltstående fil på serveren. Alle f.eks 15 eRoomversjoner av en fil vil dermed bli tatt backup av, uavhengig av backup systemets enkeltversjoner av hver enkelt fil.

Backup blir tatt daglig innen vår driftspartners backupvinduer, med garantert respons på restore ved eventuell hardware feil eller tap av data. Backup tjenester er online og innebærer ikke nedetid for backup. Kun autorisert personell har adgang til fysiske kopier av backup medier.

Involverte teknikere må signere taushetserklæring.

24 timers reetablering (katastrofe)

Vi har plassert flere servere i en egen serverhall i Oslo, Denne serverhallen har direkte fibertilknytning til lokasjonen hvor backup lagres. Med en slik fordeling/infrastruktur vil JOINT kunne garantere at eRoom/ProsjektHotell vil være oppe i løpet av 24 timer uansett hva som måtte hende med serverhallen som eRoom/ProsjektHotellet nå står i.

Konklusjon

Du kan stole på at vi i JOINT gjør hva vi kan for å trygge sikkerheten, ytelsen og påliteligheten på dine prosjekter. Har du spørsmål om JOINT ProsjektHotell sin sikkerhet, ytelse eller pålitelighet så send oss en melding på epost support@joint.no. Vi håper at denne informasjonen har vært til hjelp.

ss - 250308