(MERK: ikke endelig logo...!)

CTRL - bransjenorm for sikker online backup

INNHOLD

Om CTRL

CTRL er en teknologi- og tjenestenøytral bransjenorm etablert av IKT-Norge for sikker online backup, over det åpne internett og/eller dedikerte linjer.

CTRL stiller krav til tjenester for online backup av data fra kundens løsninger, uavhengig av om dataene finnes hos kunden eller en driftspartner, til en backupleverandørs løsning(er) og nettverk.

CTRL er ment å fungere som en veiledning for å identifisere leverandører og tjenester som tilfredsstiller et viktig sett av minimumskrav til en sikker online backuptjeneste. Målet er at kunder i hovedsak skal kunne fokusere på funksjonalitet, egenskaper og kvaliteter ved backuptjenestene og -leverandøren utover det nødvendige minimumsnivå normen stiller krav om.

CTRL stiller kun krav til backuptjenesten og -leverandøren, evt. krav til kunden/dataeieren stilles i avtalen som regulerer bruk av tjenesten.

Bakgrunn

Et selskaps verdier ligger i dataene, og sikkerhetskopier er helt nødvendig for å kunne erstatte tapte data ved feks. havarier, katastrofer, sletting eller tyveri.

i 2007 var samlet datamengede 281 exabyte, eller milliarder gigabyte (50 GB for hvert menneske på jorden). Dette er forventet å tidoble seg til 1800 exabyte til 2011, med en forventet tidobling hvert femte år[1]. Veksten av data bidrar med noen klare utfordringer for mange dataeiere som bla;

- Sikre nødvendig fortløpende backup av kritiske data.
- Håndtere den stadig voksende mengden backupdata i tillegg til orginaldataene.
- Sikker offsite oppbevaring av og tilgang til backupmedium.
- Effektiv restore fra backup.
- Dokumenetere for eiere, styre etc. at bedriftens/organisasjonens viktigste data er tilstrekkelig sikret.

Den årlige undersøkelsen i forbindelse med Nasjonal Sikkerhetsdag viser at en betydelig andel bedriftsledere anser data for å være både virksomhetskritisk og det mest verdifulle bedriften besitter. Likevel syndes det stort mot behovet for backup i norsk næringsliv. 90.8% ser på "bruk av datautstyr som en sentral del av virksomheten", mens bare 67% tar backup daglig[2].

---

[1] Tallene er hentet fra IDC, "The Diverse and Exploding Digital Universe"

[2] Nasjonal sikkerhetsdag 2010 - IT sikkerhet i Norske bedrifter

CTRL, krav til backuptjenester:

Sikring av data

Data det tas backup av skal være utilgjengelig for utenforstående og må være sikret mot innbrudd gjennom kryptering før de forlater maskinen(ene) og overføres til backup tjenesten hos tjenesteleverandøren. Kryptering på klientside skal sørge for at data ikke kan leses av noen, hverken under overføring over åpne nett, lagring i eksternt datasenter eller under tilbakekopiering over åpne nett eller tilbakelevering på flyttbart medium. Alle data skal sikres slik at de er utilgjengelige for alle andre enn eieren (kunden) i ukryptert form.

I tillegg til primærbackup sikres dataene ved backup av kundens backup, som lagres og/eller oppbevares fysisk adskilt og uavhengig av primærbackup. Metode som benyttes for backup av primærbackup og tidsintervallet for dette reguleres i avtale. Dersom data overføres mellom lokasjoner over åpne nettverk skal overføringen/dataene minst være sikret etter Datatilsynets krav/anbefaling (http://datatilsynet.no/templates/article____889.aspx) til kryptering.

Kryptering

Kryptering[3] av data er helt avgjørende for at uvedkomne ikke skal få innsyn i dataene, feks. når de sendes over internett. Data det skal tas backup av krypteres hos kunden før de sendes til backuptjenesten. Kryptering skal minst være i tråd med Datatilsynets krav til kryptering av data: http://datatilsynet.no/templates/Page____658.aspx og http://datatilsynet.no/templates/article____1024.aspx#13

Kvalitetssikring av prosesser

- Relevant databehandling skal overvåkes, status og evt. hendelser loggføres og kunde varsles etter avtale.
- Relevante ansatte hos tjenestetilbyder har underskrevet en dekkende taushetsplikterklæring.
- Det skal være en rutineansvarlig (funksjon og/eller person) som følger opp både manuelle og automatiske prosesser.
- Leverandøren skal ha prosedyre for å verifisere at tjenestens funksjonalitet, sikkerhet, etc. funger etter avtalen.
- Leverandøren skal ha etablerte rutiner for å gjennomføre regelmessig oppfølging og verifisering av at tjenesten innfrir kravene i CTRL dersom tjenesten og/eller CTRL endres.

---

[3] Les mer om kryptering hos NorSIS: http://norsis.no/leksikon/k/, Nettvett.no: http://www.nettvett.no/ikbViewer/page/nettvett/tema/artikkel?p_document_id=113371&tema=64764 og Wikipedia: http://no.wikipedia.org/wiki/Kryptering

Tilbakeføring av data

Prosedyrer, metoder (både online og evt. offline) og (respons)tid etc. for tilbakeføring av data til kunde skal være hjemlet i avtale/vilkår for tjenesten for følgende scenarier:

- gjenoppretting av data.
- opphør av avtalen.
- opphør av tjenesten.

Datasenter

Primærlokasjon, i form av tradisjonelt datasenter eller speilet skyinfrastruktur, skal være fysisk sikret i forhold til brann, vann, tyveri, og energitilgang, med nødvendige operative alternativer for umiddelbar automatisk aktivering.

Sekundærlokasjon(er) skal være tilstrekkelig sikret etter om de fungerer som et datalager eller om de leverer load balancing og/eller til redundans på tjenesten.

Overvåking skal være 24/7, og inkludere vitale datatekniske funksjoner som kommunikasjon og driftskritiske forhold i datarom.

Eierskap til data

Det skal være regulert i avtalen at kunden eier egne data.

Revisjon av CTRL

CTRL revideres av IKT-Norge hvert annet år, eller dersom det foreligger relevant markedsmessig, juridisk eller teknisk utvikling.